— Daten- und Geheimnisschutz bei der Kommunikation im Unternehmenskontext

Eine Studie zur Rechtslage mit Fokus auf Messengerdienstlösungen

Version: 1.0
Veröffentlichung: Oktober 2021
Autor*innen: Dr. Manuela Wagner, Hoa Tran, Maria Pieper, Daniel Vonderau, Silvia Balaban

– Abschnitt A: Executive Summary

Die Einrichtung von Kommunikationsräumen für den betrieblichen als auch privaten Austausch der Beschäftigten im Unternehmen hat mit der mobilen Arbeitswelt an Bedeutung gewonnen. Hierfür können unterschiedlichste Kommunikations- und Kollaborationstools genutzt bzw. unternehmensseitig betrieben werden – wobei Messengerdienste immer mehr der benötigten Funktionalitäten anbieten. Daher sollten sich Unternehmen frühzeitig mit möglichen datenschutzrechtlichen Fallstricken auseinandersetzen, um keine Haftung zu riskieren. Die Sanktionsmöglichkeiten bei einem Verstoß gegen die datenschutzrechtlichen Regelungen und das damit verbundene Haftungsrisiko haben mit dem Inkrafttreten der DSGVO zugenommen. Unternehmen kommen daher nicht umhin, sich mit den datenschutzrechtlichen Pflichten auseinanderzusetzen, sofern sie u.a. keine Geldbußen bis zu 20 Millionen Euro oder 4 % ihres weltweiten Vorjahresumsatzes riskieren wollen. Sanktionen in Millionenhöhe wurden tatsächlich bereits verhängt – insgesamt waren es im Jahr 2020 ca. 160 Millionen Euro.[1] Dieser Betrag wurde nun jüngst von der Ankündigung eines Bußgeldes gegenüber WhatsApp über 225 Millionen Euro getoppt.[2]

Ergänzend liegt es aber auch im Interesse des Unternehmens, angemessene Schutzmaßnahmen im Hinblick auf den Schutz von Geschäftsgeheimnissen zu treffen, da diese nach der neuen Rechtslage durch das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) nur rechtlichen Schutz genießen, wenn die geheimen Informationen Gegenstand angemessener Schutzmaßnahmen sind. Unternehmen, die Kommunikations- und Kollaborationstools (wie bspw. Messengerdienste) sowohl für die interne als auch für die Kommunikation nach außen nutzen wollen, sollten sich daher mit den für sie einschlägigen rechtlichen Pflichten, insbesondere mit den technischen und organisatorischen Maßnahmen zur Umsetzung von Datenschutzanforderungen und zum Schutz von Geschäftsgeheimnissen auseinandersetzen. Für den Einsatz von Kommunikations- und Kollaborationsdiensten ist es insoweit ratsam, sich je nach Art der Nutzung dieser Dienste frühzeitig mit den Möglichkeiten der rechtskonformen Einbindung zu beschäftigen, um eine Haftung zu vermeiden. Am Beispiel von Messengerdiensten wird aufgezeigt, worauf beim Einsatz solcher Lösungen im Unternehmen besonders zu achten ist.

Wesentliche Aspekte:

Einsatz technischer und organisatorischer Maßnahmen zur Umsetzung von Datenschutzanforderungen und zum Schutz von Geschäftsgeheimnissen: Unternehmen sind angehalten, den Stand der Technik zu beachten und dabei auf technischer, organisatorischer und rechtlicher Ebene „angemessene“ und damit dem Risiko entsprechende, im Hinblick auf Kosten und Aufwand nicht unverhältnismäßige Maßnahmen zu ergreifen, um sowohl Kommunikationsinhalte als auch dabei anfallende Metadaten zu schützen.

Dies impliziert:

- *Schutzrichtung:* Klassische IT-Sicherheit und Know-how-Schutz richten den Blick zentral auf den Angriff

[1] Haufe, Stand 08.02.2021, abrufbar unter https://www.haufe.de/compliance/recht-politik/eu-weit-wurden-2020-dsgvo-bussgelder-fuer-160-millionen-verhaengt_230132_536480.html [letzter Abruf 31.08.2021].
[2] *Koch,* WhatsApp von irischer Datenschutzbehörde zu 225 Millionen Euro Strafe verurteilt, in: heise online, Stand 02.09.2021, https://www.heise.de/news/WhatsApp-von-irischer-Datenschutzbehoerde-zu-225-Millionen-Euro-Strafe-verurteilt-6180500.html [letzter Abruf 03.09.2021].

„von außen“ oder Innentäter, im Datenschutzrecht muss bei der Risikoidentifikation zusätzlich die Verarbeitung personenbezogener Daten selbst in die Betrachtung einbezogen werden.

- *Risikobeurteilung:* Es gilt der Grundsatz, je weniger personenbezogene Daten verarbeitet werden, desto geringer sind die Risiken. Voreinstellungen der Verschlüsselung, Anonymisierung/Pseudonymisierung, Datentrennung und ein Zugriffsmanagement nach dem Need-to-know-Prinzip sowie Transparenz können Risiken senken und damit Haftungsrisiken vermeiden.
- *Organisation:* Bei der Auswahl und Umsetzung von Kommunikations-/Kollaborationslösungen wie Messengersystemen sind (sofern vorhanden) Datenschutzbeauftragte und der Betriebsrat einzubinden.
- *Vorteile hoher Schutzmaßnahmen und eines geringen Risikos:* Ist die Datenverarbeitung im Rahmen der Umsetzung von Kommunikations-/Kollaborationslösungen nur mit einem geringen Risiko behaftet (da bereits Schutzmaßnahmen das Risiko unter die Schwelle „normal“ senken), können bestimmte Pflichten entfallen oder weniger intensiv ausfallen (bspw. die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung). Es bestehen Ausnahmen bei Melde- und Benachrichtigungspflichten nach einem Datenschutzverstoß, zudem wird die Rechtfertigung der Datenverarbeitung im Beschäftigungskontext eher gelingen.
- *Prüfkataloge:* Um bei der Auswahl eines Kommunikations-/Kollaborationssystems Lösungen mit angemessenen Schutzmaßnahmen zu finden, sollte auf Basis von Hinweisen und Leitlinien der Datenschutzaufsichtsbehörden eine anhand der konkreten Zielstellung angepasste Checkliste erstellt werden. Ein exemplarischer Prüfkatalog für Messengerdienste findet sich in Kapitel 7.

Datenschutzrechtlicher Pflichtenkatalog bei der Umsetzung von Kommunikationskanälen: Zur Ermittlung des einschlägigen Pflichtenkanons ist es entscheidend, ob Unternehmen, die ihren Beschäftigten Kommunikationskanäle bereitstellen, ausschließlich die Vorgaben der DSGVO oder zusätzlich auch des TTDSG und TKG[3] zu erfüllen haben. Die Einordnung des Unternehmens in seiner Funktion als Arbeitgeber gegenüber den Beschäftigten war bereits vor Novellierung dieser Gesetze höchst umstritten. Für die betrieblichen Kommunikationszwecke und innerbetriebliche Kommunikation (in geschlossenen Gruppen) dürften TTDSG/TKG nicht anwendbar sein. Um verbleibender Rechtsunsicherheit zu begegnen, ist zu empfehlen:

- Klare und transparente Trennung privater und betrieblicher Nutzungen sowie betriebsinterner und betriebsexterner Kommunikation (bspw. in Chat-Gruppen, Profilen, Accounts, etc.),
- Aufklärung, in welchen Kontexten Zugriffe auf personenbezogene Daten durch Unternehmen als Arbeitgeber möglich sind, unter welchen Umständen diese erfolgen und welche Daten bspw. in Umsetzung von Aufbewahrungspflichten archiviert werden,
- Ein umfassender Ausschluss privater Nutzung – wie oftmals empfohlen – erscheint hingegen nicht ratsam. Einerseits kann mangels Kontrolle und bei zurechenbarer Kenntnis einer dennoch erfolgenden privaten Nutzung eine betriebliche Übung entstehen. Damit geht die Gefahr einer unkoordinierten Umsetzung im Unternehmen einher. Andererseits können telemedien- und telekommunikationsrechtliche Datenschutzvorschriften vorsorglich adressiert werden.

[3] Begriffserläuterungen im Glossar/Abkürzungsverzeichnis, ab S. 284.

Organisation von Verantwortungssphären zwischen Unternehmen und Anbietern von Messengerlösungen: Grundsätzlich sind drei Konstellationen denkbar, wie ein Messengerdienst betrieblich eingesetzt werden kann:

(1) das Unternehmen kann diesen in eigener Verantwortung „On-Premise“ betreiben und hierfür Software-Lizenzen erwerben;
(2) das Unternehmen kann einen Dienstanbieter als Auftragsverarbeiter engagieren;
(3) verfolgt der Dienstanbieter mit der Verarbeitung personenbezogener Daten eigene Zwecke, kann das Unternehmen eine Vereinbarung zur gemeinsamen Verantwortung abschließen.

Vor- oder Nachteile hängen entscheidend von der Datenschutzkonformität des gewählten Angebots ab. Aufgrund der gesamtschuldnerischen Haftung können sich Unternehmen nicht durch Verweis auf (Mit-)Verantwortliche freizeichnen. Bei der Auftragsverarbeitung folgen Mitwirkungspflichten an der Umsetzung der Datenschutzpflichten aus dem Gesetz. Bei gemeinsamer Verantwortung muss die Aufgabenwahrnehmung im Rahmen einer Vereinbarung geregelt werden. Bieten Software-Lösungen nicht ausreichend Möglichkeiten zur Umsetzung der Datenschutzpflichten (wie bspw. Löschroutinen, Verschlüsselung, etc.), können Mängelgewährleistungsrechte nach allgemeinem Zivilrecht geltend gemacht werden. Im B2B-Bereich gelten weniger strenge Anforderungen als im Bereich des Verbraucherschutzrechts, daher sollten Unternehmen darauf achten, dass Einsatzzweck und damit die Anforderungen an die Software klar definiert sind. Unternehmen sollten bei der betrieblichen Kommunikation bedenken, dass sie einerseits das Datenschutzrecht zu wahren haben, andererseits auch gesetzlichen Aufbewahrungspflichten unterliegen können: Die Messengerlösung sollte daher sowohl den Grundsätzen der Datenminimierung und Speicherbegrenzung entsprechende Optionen bieten als auch Back-Up-Möglichkeiten zur Archivierung von geschäftlichen Nachrichten.

Liegt eine gemeinsame Verantwortung vor, da der Messenger eigene Zwecke verfolgt, bestehen allerdings durchaus datenschutzrechtliche Bedenken, wenn dessen Betreiber Daten für Werbezwecke oder zum Profiling verwenden, insbesondere wenn es sich um sog. „Verkehrsdaten“ der elektronischen Kommunikation und/oder Standortdaten handelt. Ebenso sollten Dienste gemieden werden, welche sich eine Weitergabe oder zweckändernde Weiterverwendung derartiger Daten vorbehalten.

Besondere Risiken und deren Behandlung: Datenschutzrechtlich äußerst bedenklich ist die automatische Übermittlung der Kontaktverzeichnisse von Endgeräten an die Anbieter von Messengerdiensten. Ebenfalls abraten muss man von Angeboten, welche einen Datentransfer in ein Drittland außerhalb der EU und des EWR vorsehen, für welches kein Angemessenheitsbeschluss der EU-Kommission vorliegt. Mit Wegfall des sog. „Privacy-Shield“ sind Weiterleitungen von Daten in die USA problematisch. Durch den Cloud-Act gilt dies selbst für innerhalb der EU gespeicherte Daten US-amerikanischer Unternehmen, weil auf Verlangen von US-Behörden auch außerhalb der USA gespeicherte Daten herausgegeben werden müssen. Der Einsatz von Diensten aus Drittländern ist zwar nicht per se verboten, es bestehen allerdings sehr hohe Anforderungen an die Nutzung, so sollten zusätzliche Sicherungsmaßnahmen ergriffen werden, wie bspw. Datentrennung durch gesonderte Endgeräte oder Container-Softwarelösungen, Anonymisierung/Pseudonymisierung, Schulungen etc. Für einen rein innerbetrieblichen Einsatz dürften Drittlandsysteme kaum in Frage kommen. Für Anbieter mit Sitz und Datenverarbeitung innerhalb der Schweiz gilt dagegen ein Angemessenheitsbeschluss der EU-Kommission und somit ein angemessenes Datenschutzniveau, sodass hier (derzeit) keine Unterschiede zu EU-Anbietern bestehen. Im Hinblick auf die Einbindung von Dienstleistern (sowie deren Subdienstleistern) gilt stets zu prüfen, ob mit dem Messengerdienst ein Datentransfer in ein unsicheres Drittland mit den damit verbundenen Risiken bezüglich der Gewährleistung eines angemessenen Datenschutzniveaus geplant ist bzw. nicht sicher ausgeschlossen werden kann.

Schnellcheckliste:

Die nachfolgende 11-Punkte-Checkliste zum Datenschutz sowie dem Schutz von Geschäftsgeheimnissen gibt einen komprimierten Überblick, worauf bei der Auswahl einer geeigneten Messengerdienstlösung geachtet werden sollte. Je mehr Punkte erfüllt sind, desto wahrscheinlicher ist ein rechtskonformer Einsatz des zu prüfenden Dienstes möglich. Werden aufgeführte Punkte hingegen nicht erfüllt, muss dies nicht automatisch zu einer Datenschutzwidrigkeit führen. Vielmehr ist eine Risikobewertung durchzuführen, wobei der Einsatzzweck, Betriebskontext und die Schutzbedarfe mitentscheidend sind. Insofern kann eine Abwägung zwischen einem bestmöglichen Datenschutzniveau und einer bedarfsgerechten technischen Lösung erforderlich werden. Bei der Auswahl einer Kommunikationslösung ist stets der Stand der Technik zu berücksichtigen: Bleibt der gewählte Messengerdienst hinter diesem Stand zurück, muss dies nachvollziehbar und dokumentiert begründet werden. Je geringer der technische Datenschutz im Hinblick auf das Messengerdesign ausfällt, desto eher müssen Defizite im Zweifel durch organisatorische und vertragliche Maßnahmen im Unternehmen kompensiert werden.

1. Rechtsgrundlagen	Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage, hierbei sollte beachtet werden: ☐ Angeforderte Daten sind **erforderlich** zur Umsetzung des Einsatzzwecks und ☐ Umfang Datenverarbeitung steht in angemessenem Verhältnis zum Zweck. ☐ Einwilligungen beziehen sich nur auf **optional** anzugebende Daten.
2. Transparenz	☐ **Datenschutzerklärung** vorhanden, vollständig und verständlich ☐ **Sicherheitsaudits**, Prüfungen von dritter Seite (ggf. Zertifikate) ☐ **Quellcode** öffentlich, aktuell und reproduzierbar ☐ sonstige **Dokumentation** von Sicherheitseigenschaften / Schutzmaßnahmen
3. Datensicherheit	☐ Ende-zu-Ende-Verschlüsselung ☐ Transportverschlüsselung (TLS 1.2 / TLS 1.3) ☐ Verschlüsselung **gespeicherter** Daten (inkl. Backups) ☐ Authentisierung, Authentifizierung / **Verifikation von Kontakten**
4. Datenminimierung	☐ **So wenig Daten, wie möglich**: bspw. Nutzung von IDs, Pseudonymen (sofern sinnvoll), Profilbilder optional, Blurring-Funktion, Aktivitäts- / Anwesenheitsanzeigen optional, mind. deaktivierbar ☐ **kein automatischer Adressbuchabgleich**, nur optional als Hash mit unmittelbarer Löschung (Rechtsgrundlage: Interessenabwägung) ☐ Keine Form des **Nutzertrackings**
5. Datenmanagement	☐ **Lokal** auf Endgeräten verschlüsselt / getrennt von anderen Sachverhalten; ggf. Backups auf internen Servern, verschlüsselt ☐ ggf. Mobile-Device-Management
6. Umsetzung Betroffenenrechte	☐ **Auskunft**: Datenkopie möglich ohne Rechte Dritter zu verletzen oder keine identifizierenden Daten vorhanden (Zuordnung nachweisbar tatsächlich ausgeschlossen) ☐ **Berichtigung**: Einstellungsmöglichkeiten zur Datenberichtigung ☐ **Löschung** / Sperrung: Verfahren für Umsetzung von Löschanfragen vorhanden Weitere Rechte können je nach Kontext einschlägig sein und müssen dann im Rahmen der Betroffenenrechte ebenfalls bedacht werden: ☐ Widerrufbarkeit der Einwilligung (wenn Verarbeitung auf Einwilligung beruht),

	☐ Verfahren bei Widerspruch gegen Datenverarbeitung (wenn Verarbeitung auf Interessenabwägung beruht), ☐ Umsetzung Recht auf Datenübertragbarkeit, ☐ Rechte bei automatischen Einzelfallentscheidungen.
7. Dokumentation	☐ ausreichend Information zur Durchführung einer **Risikobewertung** sowie ggf. ☐ zur Erstellung eines Verarbeitungsverzeichnis ☐ Datenschutz-Folgenabschätzung (bei hohem Risiko)
8. Datentransfers in Drittstaaten	☐ Kein Transfer in Drittstaaten außerhalb EU/EWR ohne Angemessenheitsbeschluss ☐ Anbieter und eingebundene Dienstleister unterliegen keinen Rechtsvorschriften aus **Drittstaaten zur Datenübermittlung** (z. B. Cloud Act) ☐ Falls doch: besondere technische & organisatorische Schutzmaßnahmen
9. Nutzungs-bedingungen	☐ Kein Ausschluss **geschäftlicher** Nutzung ☐ Kein Ausschluss **innerbetrieblicher** Nutzung (bei interner Kommunikation)
10. Betriebsform	☐ Messengerdienst wird **On Premise** betrieben oder ☐ Auftragsverarbeitungsvertrag beinhaltet: – ☐ Dienst verfolgt **keine eigenen** Verarbeitungszwecke / Zwecke Dritter – ☐ Dienst unterwirft sich **Weisungen** des Auftraggebers – ☐ Keine nichtabgesprochene Einbindung von **Subunternehmen** – ☐ Verschwiegenheitsvereinbarung – ☐ Dienst bietet **Garantien** für technische und organisatorische Schutzmaßnahmen
11. Unternehmens-interne Organisation	☐ Einholung **Zustimmung Betriebsrat** (sofern Datenzugriffe unternehmensseitig möglich) ☐ Ggf. interne **Richtlinie** zur Messengernutzung

Im Vorfeld der Auswahl eines geeigneten Messengerdienstes muss zunächst über wesentliche Weichenstellungen entschieden werden, welche in die vorgenannte Risikoabwägung einfließen:

Betriebsform:

On Premise (in Eigenregie)	Software-as-a-Service	Joint Controller
Unternehmen ist selbst Verantwortlicher und muss alle Datenschutzvorgaben erfüllen	Unternehmen muss Dienst mit geeigneten Garantien wählen und einen Auftragsverarbeitungsvertrag abschließen	Eine gemeinsame Verantwortlichkeit (bei der der Messengerdienst eigene Zwecke verfolgt) ist für rein innerbetriebliche Kommunikation kaum begründbar; ggf. ausnahmsweise bei externer Kommunikation: Zuweisung der Pflichten erfolgt in Vereinbarung über gemeinsame Verantwortung
Messengerdienst-Softwarehersteller treffen keine Datenschutzpflichten, jedoch können datenschutzrelevante Funktionen vertraglich geschuldet sein	Messengerdienst muss bei Erfüllung Datenschutzvorgaben unterstützen	

Einsatzzweck: Welche Datenverarbeitungen sind bezweckt? Welche natürlichen Personen sind von dieser Datenverarbeitung betroffen? Welchen Risiken werden diese Personen durch die Datenverarbeitung ausgesetzt?

Kommunikationsform	Interne Kommunikation	Externe Kommunikation
Betroffene Daten	Metadaten und Kommunikationsinhalte der Beschäftigten	Metadaten und Kommunikationsinhalte der eigenen Beschäftigten, Beschäftigten anderer Unternehmen und/oder Privatpersonen
Schutzbedarf Datenschutz:	Besondere Kategorien personenbezogener Daten Für Existenz / Ansehen (gesellschaftliche Stellung, wirtschaftliche Verhältnisse) relevante personenbezogene Daten Frei zugängliche personenbezogene Daten Pseudonymisierte Daten Anonymisierte Daten	
Schutzbedarf Geschäftsgeheimnisse:	„Kronjuwelen“: Geheimnisse, deren Offenlegung existenzbedrohend sind Strategisch wichtige Informationen Sonstige schützenswerte, sensible Daten	
Vertraulichkeitslevel und Datenzugriffsmöglichkeiten	— Auf welche Daten muss das Unternehmen zugreifen können (bspw. zur Umsetzung von Compliance-Maßnahmen)? — Bestehen Aufbewahrungspflichten (z.B. steuer-/handelsrechtliche Pflichten)? — Dient die Kommunikation nur beruflichen oder auch privaten Zwecken?	

– Inhaltsverzeichnis

Diese Studie wurde von der Threema GmbH finanziell unterstützt. Sie gibt die Sichtweise der Autor*innen wieder; eine Einflussnahme auf die Ergebnisse durch den Auftraggeber erfolgte nicht.

– Abschnitt B: Datenschutz

1 Motivation

Der Bedarf an Kommunikationsmitteln ist durch vermehrtes Home-Office und mobiles Arbeiten bedingt durch die Corona-Pandemie stark gestiegen. Aber nicht erst mit der Pandemiesituation und der damit einhergehenden Zunahme der Dezentralisierung der Arbeitsprozesse wird die Notwendigkeit digitalisierter Prozesse im Unternehmenskontext immer dringender.[4] Dabei stellt sich zentral die Frage, wie die Beschäftigten untereinander (unternehmensintern) als auch mit Kundschaft und/oder Geschäftskontakten (extern) kommunizieren. Werden bisher offline geführte Gespräche in physischen Besprechungsräumen vor Ort in den digitalen Raum verlegt, müssen zwingend die Datenschutzbelange beachtet werden. Unsicherheit besteht bei vielen Unternehmen, welche Werkzeuge verwendet werden können, da datenschutzrechtliche Bedenken durch die Datenschutzbeauftragten und Aufsichtsbehörden (Bund und Länder) kommuniziert wurden.[5] Die Zahl der Datenschutzverstöße ist mit fast 10.000 Meldungen im Jahr 2020 relativ hoch, zudem fallen die Sanktionen durchaus empfindlich aus.[6] Dies stellt die Unternehmen vor die Herausforderung, den Bedarf an digitalen Kommunikationsmitteln im Betrieb zu decken, unter der Vorgabe nur datenschutzrechtskonforme und sichere Formate einzusetzen. Viele Unternehmen, gerade auch kleinere und mittelständische Unternehmen, verfügen jedoch nicht zwangsläufig über das notwendige Know-How oder Personal, um die Frage nach der Datenschutzrechtskonformität zu beantworten. Daher ist es verständlich, wenn eine gewisse Verunsicherung herrscht, inwiefern leicht über App-Stores zugängliche Angebote für Jedermann auch im Unternehmenskontext ohne rechtliche Implikationen genutzt werden dürfen.

Neben den Möglichkeiten und Grenzen der die aktuelle Diskussion beherrschenden Videokonferenzsysteme,[7] erlangen auch andere Kommunikations- und Kollaborationssysteme immer mehr Bedeutung im Arbeitsumfeld. So ermöglichen Messengerdienste einen schnellen Austausch kleiner Textnachrichten, mittlerweile aber auch Sprachnachrichten, Audio- und Videotelefonie. Aus dem privaten Gebrauch sind diese Kommunikationsformen kaum noch wegzudenken, sodass eine Ausweitung auch auf betriebliche Kommunikationsbedürfnisse naheliegend erscheint.

Diese Studie liefert hierfür Hintergründe zu den datenschutzrechtlichen Anforderungen als auch Hinweise zum Schutz von Geschäftsgeheimnissen und bietet Empfehlungen in Form von Praxistipps und einem Handlungsleitfaden. Die Zielsetzung besteht darin, Unternehmen einen fundierten Überblick über die datenschutzrechtlichen Anforderungen sowie den Schutz von Geschäftsgeheimnissen bei der Nutzung von Kommunikations- und Kollaborationslösungen mit Schwerpunkt auf Messengerdienste zu bieten.

---

[4] Zu Chancen und Risiken: *Dietrich u. a.*, DuD 2021, 5 (5).

[5] Bspw. *Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg*, Unsere Daten: Daten nützen – Daten schützen, Tätigkeitsbericht 2020, S. 36 ff. zum datenschutzkonformen Heimarbeitsplatz sowie datenschutzfreundlicher Kommunikationsdienste und Videokonferenzen.

[6] Vgl. *BfDI*, Tätigkeitsbericht 2020, S. 103. Beispiele bei: *Lurtz*, ZD-Aktuell 2021, 05269.

[7] Zur aktuellen Diskussion siehe bspw.: ArbG Köln, Beschluss vom 24.3.2021 – 18 BVGa 11/21, zum Recht zur Durchführung einer Betriebsratssitzung als Videokonferenz; BGH, Beschluss vom 6.11.2020 – LwZR 2/20 zur Beratungsbeteiligung ehrenamtlicher Richter*innen im Wege der Telefon- oder Videokonferenz; KG Berlin, Urteil vom 12.5.2020 – 21 U 125/19 zur mündlichen Verhandlung vor Gericht per Videokonferenz.

1.1 Messengerdienste als eine Form der Kommunikations- und Kollaborationslösung

Diese Studie widmet sich der Kommunikation im Unternehmenskontext, wobei ein besonderer Blick auf die Kommunikation per Messengerdienst geworfen werden soll. Messengerdienste erlauben es regelmäßig, zwischen registrierten Nutzenden Text- und Sprachnachrichten sowie Fotos, Videos, Audiodateien und Kontaktdaten auszutauschen sowie zumeist auch via IP-Telefonie über das Internet zu telefonieren. Im Gegensatz zu der Öffentlichkeit (bzw. Teilöffentlichkeit) der Social-Media-Plattformen findet die Messengerkommunikation in geschlossenen Kanälen statt.[8] Messengerdienste sind folglich durch folgende Funktionen gekennzeichnet:

- Instant Messaging: Echtzeit-Übertragung
- Übertragung von Text, ggf. Sprache, Bild/Video und Dateien über das Internet
- Oftmals Angebot von Funktionen wie Gruppenchats, Austausch von Grafiken, Telefonie, Video- und Audiomitteilungen sowie Sticker oder Emoticons.[9]

Mittlerweile verfügen viele Messenger sowohl über Smartphone- als auch Desktopanwendungen. Dabei richten sich einige bekannte Messenger ausschließlich an der Nutzung im privaten Kontext aus. Daneben bieten Messenger Schnittstellen für Unternehmen (z. B. WhatsApp Business) oder eigene Lösungen für die innerbetriebliche Kommunikation im Unternehmen an (z. B. Ginlo Business, Threema Work, stashcat, Teamwire). Anwendungen mit Fokus auf Konferenz- und Kollaborationslösungen wie insbesondere Videokonferenzen verfügen oftmals ebenfalls über Chatfunktionen und werden zu den Messengern gezählt (z. B. Skype/Skype for Business, Microsoft Teams). Dies zeigt, dass die Welt der Messenger vielfältig ist, sodass Tabelle 1 lediglich einen exemplarischen Einblick in die verschiedensten Lösungen bieten soll.

Beispiele bekannter Messengerdienste mit Fokus auf Privatnutzung (alphabetisch sortiert)	
Discord	— Ursprünglich für Computerspieler*innen geschaffenes, kostenloses Chat-/Telefonie-Tool sowie mit Bezahlvariante „Nitro“
Facebook Messenger	— 2014 lagerte Facebook die Nachrichten-Funktion in eine eigene App aus[10] — Nach WhatsApp zweitbekannteste und -genutzte Messenger-App in Deutschland 2020[11]
iMessage	— Im Betriebssystem iOS integrierte, voreingestellte Standard-Messenger-App, nur für Apple-Geräte verfügbar[12]
Keybase	— durchgängig verschlüsseltes Chat- und Cloud-Speichersystem für Filesharing — 2020 wurde der Dienst von Zoom übernommen
Signal	— Durch gemeinnützige Stiftung finanzierter kostenloser Messenger, der auf private Nutzung ausgerichtet ist
Telegram	— Kostenloser Instant-Messaging-Dienst, der auf private Nutzung ausgerichtet ist

[8] *Mehner*, Messenger Marketing, S. 7.
[9] *Mehner*, Messenger Marketing, S. 12.
[10] *Verbraucherzentrale Nordrhein-Westfalen,* Facebook-Messenger umgehen: Nachrichten lesen ohne Zwangs-App, Stand: 21.02.2021, https://www.verbraucherzentrale.nrw/wissen/digitale-welt/soziale-netzwerke/facebookmessenger-umgehen-nachrichten-lesen-ohne-zwangsapp-13735 [letzter Abruf 06.07.2021].
[11] *statista*, Instant Messenger, S. 10.
[12] *Verbraucherzentrale,* WhatsApp-Alternativen: Messenger im Überblick, Stand 31.05.2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055 [letzter Abruf 06.07.2021].

	— Seit 2013 von den Gründern des meistgenutzten russischen sozialen Netzwerk Vk.com mit aktuellem Sitz in Dubai betrieben
viber	— kostenloser Chat Service für Smartphones und Desktop, der auf private Nutzung ausgerichtet ist
WhatsApp	— Weltweit meist verbreitete Messenger-App[13] — Im Konflikt mit Datenschutzbehörden in Europa, insbesondere wegen der Ankündigung der Weitergabe von Nutzerdaten an den Mutterkonzern Facebook[14] — WhatsApp Business API ist ein Angebot an Unternehmen, um mit Kundschaft per Messenger zu kommunizieren[15]
Beispiele für Messenger mit dualem Angebot für private und berufliche Kommunikation	
Element	— Chattool, IP-Telefonie und Videoanrufe via Matrix-Protokoll — Unabhängig von zentralem Anbieter
Microsoft Teams	— Integriert in die Microsoft 365-Suite — Bietet Telefonieren, Videokonferenzen, Kollaborationsmöglichkeiten und Chattool — Chat-Inhalte für den Betreiber lesbar, da Ende-zu-Ende-Verschlüsselung bisher nur geplant ist und nicht standardmäßig erfolgen soll[16]
ginlo	— Nachfolger der Messenger-App SIMSme der Deutschen Post.[17] — auf Datensicherheit ausgerichteter Instant-Messaging-Dienst für privaten Gebrauch (kostenlos) und Unternehmen (ginlo Business, kostenpflichtig)
Skype	— Skype für den Privatbereich (kostenlos) und Skype for Business für den Unternehmenskontext (kostenpflichtig) bieten Bildtelefonie, Videokonferenzen, IP-Telefonie, Instant-Messaging, Dateiübertragung und Screen-Sharing — Für Aufsehen sorgte ein Bericht 2013, dass Skype Textchats mitlesen kann.[18] Forschende bemängelten 2016 Sicherheitsrisiken, welche die Eignung von Skype für den Unternehmenseinsatz stark einschränken.[19]
Slack	— Plattform für kollaboratives Arbeiten, integrierbar in andere Dienste wie Microsoft Office 365 oder Google Drive. — Beinhaltet zusätzlich einen Workflow-Builder, geht somit über den reinen Messengerdienst hinaus.
Threema	— Auf Datensicherheit und Schutz der Privatsphäre ausgerichteter Messengerdienst mit

[13] *statista*, Instant Messenger, S. 7 ff.
[14] *HmbBfDI*, Anordnung des HmbBfDI: Verbot der Weiterverarbeitung von WhatsApp-Nutzerdaten durch Facebook, 11.05.2021, https://datenschutz-hamburg.de/pressemitteilungen/2021/05/2021-05-11-facebook-anordnung [letzter Abruf 07.07.2021]. Allerdings fehlt die Zuständigkeit für derartige Anordnungen, da WhatsApp seine EU-Niederlassung in Irland hat.
[15] *Mehner*, Messenger Marketing, S. 20.
[16] *Grüner,* Teams führt Ende-zu-Ende-Verschlüsselung im Juli ein, in: golem.de, Stand: 04.06.2021, abrufbar unter: https://www.golem.de/news/microsoft-teams-fuehrt-ende-zu-ende-verschluesselung-im-juli-ein-2106-157035.html [letzter Abruf 30.08.2021].
[17] *Verbraucherzentrale,* WhatsApp-Alternativen: Messenger im Überblick, Stand 31.05.2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055 [letzter Abruf 06.07.2021].
[18] *Beer,* Vorsicht beim Skypen – Microsoft liest mit, in: Heise online, 14.05.2013, abrufbar unter https://www.heise.de/security/meldung/Vorsicht-beim-Skypen-Microsoft-liest-mit-1857620.html [letzter Abruf 06.07.2021].
[19] *Wittenhorst,* Fraunhofer ESK: Skype ist Sicherheitsrisiko für Firmen, in: Heise online, 22.01.2016, abrufbar unter: https://www.heise.de/ix/meldung/Fraunhofer-ESK-Skype-ist-Sicherheitsrisiko-fuer-Firmen-3082090.html [letzter Abruf 06.07.2021].

	Sitz in der Schweiz[20] — Seit Mai 2016 bietet Threema Work eine interne Kommunikationslösung für Unternehmen und ähnliche Organisationen (z. B. Behörden[21]), so stellte bspw. 2020 das Kultusministerium Baden-Württemberg seinen Lehrkräften Threema Work zur dienstlichen Nutzung kostenlos zur Verfügung[22]
wickr	— Wickr bezeichnet sich selbst als „die sicherste, Ende-zu-Ende-verschlüsselte Kommunikationslösung der Branche“.[23] — 2021 wurde der Dienst von Amazon gekauft
Wire	— In Europa (Schweiz) ansässiger Messengerdienst — unterschiedliche Abonnementsoptionen für Unternehmen, kostenlos hingegen für den privaten Gebrauch[24]
Beispiele für Messenger für die Kommunikation innerhalb einer Organisation (keine private Nutzung)	
stashcat	— Kollaborationslösung und Business-Messenger mit Fokus auf professionelle Kommunikation und Zusammenarbeit in Unternehmen und Behörden — Funktionen wie Chats, Dateiablage, Sprach- und Videotelefonie, Videokonferenzen u. v. m. für organisationsinterne Kommunikation
Teamwire	— in Deutschland entwickelter reiner Business-Messenger, der sich primär an Unternehmen, Behörden und das Gesundheitswesen richtet[25] — So setzt bspw. seit 2017 die Polizei in Bayern auf Teamwire[26]
Beispiele Messenger für bestimmte Berufe/Berufsgruppen	
Briar	— Verschlüsselte Peer-to-Peer-Nachrichten und Foren (ohne zentrale Server) mit Fokus auf anonyme Kommunikation (mittels Anonymisierungsnetzwerk Tor) — die Zielgruppe von Briar sind (politische) Aktivist*innen, Journalist*innen etc. sowie Hilfe in Katastrophenfällen (arbeitet auch ohne Internet-Infrastruktur)[27] — aufgrund eingeschränkter Funktionalitäten von geringer Praxisrelevanz für gewöhnliche Unternehmen
Siilo	— Messaging-App für medizinische Zwecke aus den Niederlanden mit Fokus auf medizinisches Personal

[20] *Mehner*, Messenger Marketing, S. 40.
[21] *Netzpolitik.org,* Schweizer Verwaltung setzt auf Threema statt WhatsApp, 13.02.2019, https://netzpolitik.org/2019/schweizer-verwaltung-setzt-auf-threema-statt-whatsapp/ [letzter Abruf 06.07.2021].
[22] *Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, LfDI*: Gute Entscheidung für Threema – Schulen brauchen mehr Orientierung, 29.04.2020, https://www.baden-wuerttemberg.datenschutz.de/lfdi-gute-entscheidung-fuer-threema-schulen-brauchen-mehr-orientierung/ [letzter Abruf 06.07.2021].
[23] *Weidemann,* Warum Amazon diesen Team-Messenger mit Verschlüsselung gekauft hat, 28.06.2021, in: t3n, https://t3n.de/news/wickr-amazon-messenger-gekauft-1387812/ [letzter Abruf 08.08.2021].
[24] https://wire.com/de/products/personal-secure-messenger/
[25] *Weiß,* Business-Messenger Teamwire mit Statusnachrichten und Onboarding-Bot, 01.03.2021, in: heise, https://www.heise.de/news/Business-Messenger-Teamwire-mit-Statusnachrichten-und-Onboarding-Bot-5068493.html [letzter Abruf 08.08.2021].
[26] Bayern: Neuer Polizei-Messenger für Streifenbeamte, 26.05.2017 in: heise, https://www.heise.de/newsticker/meldung/Bayern-Neuer-Polizei-Messenger-fuer-Streifenbeamte-3725791.html [letzter Abruf 08.08.2021].
[27] *Kuketz,* Briar: Anonymität und Sicherheit gehen vor – Messenger Teil8, vom 10.11.2020, in: kuketz-Blog, abrufbar unter: https://www.kuketz-blog.de/briar-anonymitaet-und-sicherheit-gehen-vor-messenger-teil8/ [letzter Abruf 18.08.2021]. Nachteile liegen allerdings in einer eingeschränkten Benutzerfreundlichkeit.

	— Für Kliniken wird der kostenpflichtige Zusatzdienst Siilo connect angeboten
Beispiele für Messenger mit lokal fokussierter Verbreitung	
Kakaotalk	— koreanischer Messengerdienst, der auf private Nutzung ausgerichtet ist
Kik	— kanadischer Messengerdienst, der auf private Nutzung ausgerichtet ist
LINE	— japanischer Messenger-Service-Anbieter, der vor allem in Südostasien beliebt ist — bietet gleichzeitig eine Gaming-Plattform
WeChat	— in China mit über einer Milliarde Nutzer sehr populär, — als „One-Stop-Plattform“ integriert die App unterschiedlichste digitale Ökosysteme

Tabelle 1 Liste mit Beispielen für Messengerdienste (nicht abschließend)

Anwendungen, welche eher der Domäne der sozialen Medien zuzuordnen sind, wie bspw. Twitter, Instagram, TikTok, Facebook und Snapchat, werden in dieser Studie nicht betrachtet, auch wenn diese Möglichkeiten der Direktnachrichten anbieten. Zudem interessieren im vorliegenden Kontext primär die unter den genannten Beispielen auf geschäftliche Kommunikation ausgerichteten Messengerdienste, wobei von geschlossenen Systemen gesprochen wird, bei denen nur Nutzer*innen dieses Dienstes miteinander kommunizieren können. Daneben seien zur Vollständigkeit auch „freie“ Messenger-Apps erwähnt, die von einem Anbieter unabhängig sind und ähnlich wie E-Mail-Dienste funktionieren. Sofern diese technisch auf einem Standardprotokoll aufbauen, das Nachrichten über verschiedene Messenger-Apps interoperabel ermöglicht (bspw. XMPP oder Matrix), müssen Gesprächskontakte nicht die gleiche App installiert haben. Als Beispiele basierend auf XMPP werden für Android die Messenger: Conversations, Quicksy oder Yaxim und für iOS: ChatSecure, Monal oder Siskin genannt.[28] Für Matrix gibt es zum Beispiel den Messenger Element (früher Riot) sowohl für Android als auch für iOS.[29] XMPP und Matrix-Protokoll sind allerdings nicht für die Vermeidung bzw. den Schutz von Metadaten konzipiert.[30] Zudem erfordert die Umsetzung ein gewisses Maß an Professionalität, sodass sich diese Lösungen eher nur für Fortgeschrittene eignen.[31] Diese sind für Einsteiger folglich nicht zu empfehlen und sollen im Folgenden nicht weiter betrachtet werden.

Im Rahmen dieser Studie soll grundsätzlich die Funktionsweise klassischer Messengerdienste im Fokus stehen. Die allgemeinen rechtlichen Erwägungen können hierbei regelmäßig auf vergleichbare Kommunikations- und Kollaborationslösungen übertragen werden. Sofern eine Detailbetrachtung durchgeführt wird, kann naturgemäß nur ein kleiner Ausschnitt dieser Fülle an Lösungen exemplarisch im Einzelfall berücksichtigt werden.

[28] *Verbraucherzentrale,* WhatsApp-Alternativen: Messenger im Überblick, Stand 31.05.2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055 [letzter Abruf 06.07.2021].
[29] *Verbraucherzentrale,* WhatsApp-Alternativen: Messenger im Überblick, Stand 31.05.2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055 [letzter Abruf 06.07.2021].
[30] *Kuketz,* Conversations: Messaging über das XMPP-Protokoll – Messenger Teil6, Stand 07.09.2020, abrufbar unter: https://www.kuketz-blog.de/conversations-messaging-ueber-das-xmpp-protokoll-messenger-teil6/ [letzter Abruf 01.09.2021]; Kuketz, Element: Messaging über die Matrix – Messenger Teil7, Stand 29.10.2020 abrufbar unter: https://www.kuketz-blog.de/element-messaging-ueber-die-matrix-messenger-teil7/ [letzter Abruf 01.09.2021].
[31] Vgl. die Übersicht bei *Kuketz,* Messenger-Matrix, Stand 29.8.2021, abrufbar unter: https://www.messenger-matrix.de/messenger-matrix.html [letzter Abruf 01.09.2021].

1.2 Gesellschaftliche Bedeutung von Messengerdiensten

Nach einer Hochrechnung im Rahmen einer Studie des Bitkom e.V. ist davon auszugehen, dass im Corona-Jahr 2021 in etwa 300 Milliarden Kurznachrichten in Deutschland verschickt werden.[32] Nach einer Befragung von 1.005 Menschen erhält jede Smartphone-Nutzer*in über 16 Jahren im Schnitt 13 Kurznachrichten pro Tag. Messengerdienste haben dabei klassische SMS weitgehend abgelöst.[33] Ebenso haben die Datenschutzaufsichtsbehörden in Deutschland den Trend beobachtet, dass Messengerdienste auch vergleichbare Kommunikationsdienste wie E-Mail in den letzten Jahren zunehmend ersetzt haben und mittlerweile insbesondere im privaten Alltag zu den beliebtesten Kommunikationsformen zählen.[34] „Gründe hierfür sind neben der jederzeitigen Nutzbarkeit über Smartphone und der leichten Bedienbarkeit der Funktionsumfang, der es erlaubt, neben Textnachrichten auch Bilder, Videos oder Sprachnachrichten auszutauschen, Sprach- und Videoanrufe durchzuführen und wahlweise mit einzelnen Teilnehmern oder in der Gruppe zu kommunizieren. Hinzu kommt, dass es sich vielfach um unentgeltlich nutzbare Angebote handelt.“ [35] Insofern dürfte ein wesentlicher Grund darin liegen, dass mit der Verbreitung von Flatrate-Datentarifen im Gegensatz zum SMS-Versand keine Zusatzkosten anfallen.[36] Die Popularität gegenüber Mails dürfte zudem durch Möglichkeiten der Übermittlung von Bild- und Videodateien oder die Sprachtelefonie (Voice over IP) gesteigert worden sein.[37] Auch das klassische Telefonat musste als Kommunikationskanal erheblich Marktanteile einbüßen: Insgesamt wird das Gesprächsvolumen seit 2010 als konstant rückläufig berichtet.[38]

Mit der pandemiebedingten Zunahme des Home-Office und mobilem Arbeiten steigt neben der Bedeutung von Videokonferenzsystemen auch der Einsatz von Messengerdiensten.[39] Allerdings bemängeln Expert*innen, dass der berufliche und gewerbliche Einsatz von einigen der gängigen Messengerdienste die Datenschutzvorgaben oftmals bislang nicht oder nur bedingt erfüllt.[40] Besondere Kritik erntet dabei immer wieder der am weitesten verbreitete Dienst WhatsApp. [41]

1.3 Einzug von Messengerdiensten im Unternehmen

Der Einsatz von Messengerdiensten gewinnt auch im Business-Kontext parallel zur Verbreitung im privaten Umfeld zunehmend an Bedeutung, da mittels Kombination aus Bild- und Textelementen Emotionen via

---

[32] *Bitkom,* https://www.bitkom.org/Presse/Presseinformation/Corona-Jahr-2021-300-Milliarden-Kurznachrichten-in-Deutschland [letzter Abruf 06.07.2021].
[33] *Mehner*, Messenger Marketing, S. 12 f.
[34] *DSK - Datenschutzkonferenz*, Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, S. 1.
[35] *DSK - Datenschutzkonferenz*, Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, S. 1.
[36] *Faas*, ArbRAktuell 2018, 594 (594).
[37] *Faas*, ArbRAktuell 2018, 594 (594).
[38] *Mehner*, Messenger Marketing, S. 12.
[39] *BfDI*, Tätigkeitsbericht 2020, S. 32.
[40] *DSK - Datenschutzkonferenz*, Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, S. 1; *BfDI*, Tätigkeitsbericht 2020, S. 32.
[41] *Der Landesdatenschutzbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz,* https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/ [letzter Abruf 04.07.2021]; *DSK - Datenschutzkonferenz*, Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, S. 1.

Messenger und damit eine (audio-)visuelle bis hin zur universellen Sprache leicht transportiert werden können.[42] So kommen im Kundenkontakt verstärkt auch Emojis zum Einsatz, welche universell bestimmte Emotionen ausdrücken.[43] Somit bestehen einige Vorteile gegenüber der E-Mail als klassischem Kommunikationsformat im Unternehmen:

- Der informellere Charakter.[44]
- Beschäftigte ohne PC-Arbeitsplatz sind per Smartphone-App erreichbar.
- Je nach Sicherheitsfeatures: besserer Betrugsschutz wie z.B. CEO-Fraud,[45] wenn die Messenger-Plattform die Möglichkeit bietet, Identitäten sicher zu verifizieren.

Dazu kommt der Bequemlichkeitsfaktor: Apps nicht nur privat, sondern auch beruflich zu nutzen.[46] Verstärkend könnten hier zwei Phänomene wirken:

- **COPE – Corporate-Owned, Personally Enabled devices:** die private Nutzung unternehmensseitig bereitgestellter Smartphones, Tablets oder Laptops,
- **BYOD – Bring Your Own Device:** unternehmensseitig ermöglichten oder sogar geförderten Einsatz privater Smartphones, Tablets oder Laptops für unternehmerische Zwecke.[47]

Im Bereich der Kundenansprache werden vielfältige Vorteile benannt: Zielgruppengerechte Erreichbarkeit für Service- und Supportanfragen, Adressierung aller Altersgruppen sowie Messbarkeit von Erfolgsquoten im Hinblick auf tatsächliche Wahrnehmung der Empfänger*innen.[48] Eine YouGov-Umfrage ergab bereits im Jahr 2017: Jede*r Fünfte hält die Nutzung von Messengern in der Kommunikation mit Unternehmen für längst überfällig.[49] Haftungsrisiken können allerdings immer dann entstehen, wenn sich die Nutzung sozusagen „von unten“ ohne rechtliche Prüfung durch die Unternehmensleitung etabliert und dabei erforderliche Datenschutz- und Datensicherungsmaßnahmen nicht ausreichend bedacht werden.[50] Expert*innen sprechen bei diesem Phänomen auch von sog. Schatten-IT.[51] Aufgrund der damit verbundenen Risiken eines derartigen Wildwuchses für Datenschutz, IT-Sicherheit und Compliance wird eindringlich ein gesteuerter und kontrollierter Prozess angeraten.[52]

Einige Messenger bieten neben ihren „klassischen“ (oftmals kostenlosen) Angeboten für den Privatkundenbereich parallel für Unternehmensbedürfnisse zugeschnittene, kostenpflichtige Kommunikationslösungen, welche zum Teil auch „On-Premise“, also durch das Unternehmen selbst betrieben werden können (vgl. Tabelle 1). Im Rahmen dieser Studie sollen grundsätzlich alle Varianten betrachtet werden.

---

[42] *Mehner*, Messenger Marketing, S. 3; vgl. auch *Schrey u. a.*, MMR 2017, 656 (656).
[43] *Mehner*, Messenger Marketing, S. 3. Vgl. auch der Entwurf eigener Emojis als Marketingstrategie: Der Tagesspiegel, Hinter welchen Emojis insgeheim Unternehmen stecken, Stand 07.03.2020, abrufbar unter: https://www.tagesspiegel.de/wirtschaft/von-trucks-bis-wollsocken-hinter-welchen-emojis-insgeheim-unternehmen-stecken/25596966.html [letzter Abruf 29.09.2021].
[44] Zur Analyse des pragmatischen Charakters von Emojis als Format im „Small Talk“ via Messenger: *Beißwenger/Pappert,* Literaturwiss Linguistik 50/2020, 89 (92 ff.).
[45] Die Kontaktaufnahme erfolgt in der Regel über verfälschte E-Mail-Adressen oder verschleierte Telefonnummern. Siehe bspw. Polizei Nordrhein-Westfalen, CEO-Fraud: Hohes Betrugsrisiko für Unternehmen, abrufbar unter: https://polizei.nrw/artikel/ceo-fraud-hohes-betrugsrisiko-fuer-unternehmen [letzter Abruf 29.09.2021].
[46] *Faas*, ArbRAktuell 2018, 594 (594).
[47] *Faas*, ArbRAktuell 2018, 594 (594); *Schrey u. a.*, MMR 2017, 656 (656).
[48] *Mehner*, Messenger Marketing, S. 4.
[49] *Inhoffen*, Über WhatsApp mit Kunden kommunizieren, in: YouGov, 04.08.2017, abrufbar unter: https://yougov.de/news/2017/08/04/uber-whatsapp-mit-kunden-kommunizieren/ [letzter Abruf 27.07.2021].
[50] *Schrey u. a.*, MMR 2017, 656 (656 f.).
[51] *Rentrob/Zimmermann,* in: GI Lexikon „Schatten-IT“, Stand: 23.12.2015, abrufbar unter: https://gi.de/informatiklexikon/schatten-it [letzter Abruf 29.09.2021].
[52] *Rentrop/Zimmermann/Huber,* D•A•CH Security 2015 · syssec 2015, 291 (292 ff.) m.w.N.

1.4 Zielsetzung und juristische Methodik

Das Ziel dieser Studie liegt darin, eine fundierte Basis für die Umsetzung der digitalen Vernetzung im Unternehmenskontext zu bieten. Die Ergebnisse richten sich vor allem an Unternehmen, die ihren Beschäftigten moderne Kommunikations- und Kollaborationslösungen bereitstellen wollen. Hierbei liegt ein besonderer Fokus auf Messengerdiensten. Gerade um die datenschutzrechtliche Einordnung sowie den damit verbundenen Pflichtenkatalog ranken sich zahlreiche juristische Diskussionen, die im Folgenden analysiert werden. Erst mit einer umfassenden Aufarbeitung der rechtlichen Fallstricke können konkrete Handlungsempfehlungen für Unternehmen entwickelt werden, welche auch eine Hilfestellung für die Aufgaben von Datenschutzbeauftragten, Betriebsrat und Rechtsabteilungen bieten können.

Die Arbeit bedient sich dafür der traditionellen juristischen Methodenlehre. Dies dient der Bedeutungsermittlung von Rechtsnormen durch die Interpretation in Form der formallogischen Subsumtionstechnik im Wege der wörtlichen, historischen, systematischen, genetischen und teleologischen Auslegung von Texten.[53] Dabei gilt es zu Bedenken, dass der EU-rechtskonformen Auslegung eine besondere Bedeutung im Datenschutz-, Telekommunikations- und Telemedienrecht zukommt, da dieses überwiegend auf unionsrechtliche Verordnungen und Richtlinien zurückgeht. Während Verordnungen, wie die Datenschutz-Grundverordnung (DSGVO), gemäß Art. 288 AEUV unmittelbar anwendbar sind und Anwendungsvorrang vor mitgliedstaatlichem Recht genießen, müssen Richtlinien, wie die ePrivacy-Richtlinie, durch den deutschen Gesetzgeber in die Rechtsordnung übernommen werden und je nach Harmonisierungsgrad ausgestalten. Bei vollharmonisierenden EU-Regeln tendiert der Gestaltungsspielraum gegen Null. Hierbei stellt die DSGVO durch zahlreiche Öffnungs- und Konkretisierungsklauseln für mitgliedstaatliches Recht einen atypischen Hybrid aus Verordnung und Richtlinie dar.[54]

Bei der Identifikation des einschlägigen Rechtsrahmens stellt zudem die Gesetzeshierarchie eine wichtige Weichenstellung dar. Grundsätzlich genießt das EU-Recht Anwendungsvorrang vor nationalem Recht, d.h. dass im Konflikt stehende Normen zwar nicht ihre Gültigkeit verlieren, aber nicht mehr anzuwenden sind.[55] Im föderalen System Deutschlands haben Bundesnormen grundsätzlich Vorrang vor Landesnormen. Es gilt der Grundsatz: „Bundesrecht bricht Landesrecht“ (Art. 31 GG). Eine Ausnahme bildet wiederum das Datenschutzrecht: Hier gebietet der Subsidiaritätsgrundsatz in § 1 Abs. 1 Nr. 2 BDSG, dass landesrechtliche Datenschutzvorschriften vorrangig anzuwenden sind. Diese sind im vorliegenden Kontext der Kommunikation im Unternehmen allerdings kaum von Bedeutung, da sie primär öffentliche Stellen des jeweiligen Landes adressieren.

1.5 Eingrenzung des Untersuchungsgegenstands

Diese Studie untersucht datenschutz- und geheimnisschutzrechtliche Fragestellungen im Zusammenhang mit Kommunikationsprozessen in Unternehmen mit besonderem Fokus auf den Einsatz von Messengerdiensten. Hierbei sollen Sonderkonstellationen zunächst ausgeklammert bleiben. Denn bestimmte Berufsgruppen, wie Rechtsanwält*innen und Ärzt*innen haben als Berufsgeheimnisträger*innen besondere Pflichten zur Geheimhaltung ihnen anvertrauter Daten. Sie müssen neben dem Datenschutzrecht zusätzliche

[53] Zur juristischen Methodenlehre: *Hassemer*, ZRP 2007, 213 (215).
[54] *Kühling u. a.*, Die Datenschutz-Grundverordnung und das nationale Recht, S. 1 ff.; *Kühling/Martini*, EuZW 2016, 448 (449); *Piltz*, K&R 2016, 557 (557).
[55] *Ruffert,* in: Callies/Ruffert, EUV/AEUV Art. 1 Rn. 18.

Strafvorschriften, z. B. § 203 StGB, und Berufsrecht (z. B. BORA) beachten.[56] Diese strafrechtlich sanktionierten Verschwiegenheitspflichten können bereits die Existenz eines Kontakts erfassen.[57]

Vergleichbare Kommunikationsformen und Umsetzungsfragen auf der technischen Ebene stellen sich auch bei Behörden, Schulen und anderen öffentlichen Stellen. Allerdings sind die rechtlichen Grundlagen andere als bei privatrechtlich organisierten und tätigen Unternehmen im klassischen Sinn. Staatlich Bedienstete treffen insoweit beamtenrechtliche Grundpflichten des Beamtenstatusgesetzes (§§ 33 ff. BeamtStG) oder des Tarifvertrages für den öffentlichen Dienst der Länder (TV-L). So bestimmt bspw. im Land Berlin die Staatssekretärin für Informations- und Kommunikationstechnik im Rahmen ihrer Vorgaben zur IKT-Architektur über den Einsatz von Informationstechnik in der Berliner Verwaltung.[58] Auf eine schriftliche Anfrage antwortete die Senatsverwaltung für Inneres und Sport im Namen des Senats von Berlin, dass die Nutzung von Messengerdiensten für die dienstliche Nutzung untersagt sei.[59] Hierbei spielen neben datenschutzrechtlichen regelmäßig weitere rechtliche Erwägungen eine zentrale Rolle. Diese Kontexte sollen im Rahmen dieser Studie daher nicht weiter betrachtet werden.

Beim Einsatz von Kommunikationstechnologie an Schulen steht vor allem die Minderjährigkeit der betroffenen Personen im rechtlichen Fokus. Auch dieser Aspekt ist keine typische Fallkonstellation der hier interessierenden Problemstellungen rund um den Einsatz von Messengerdiensten im beruflichen Umfeld und ist damit nicht Gegenstand dieser Studie.

1.6 Gliederung der Studie

Die Arbeit ist wie folgt aufgebaut: Im ersten Abschnitt (Kapitel 2-5) werden die rechtlichen Anforderungen aus datenschutzrechtlicher Perspektive beleuchtet und im zweiten Teil (Kapitel 6) mit dem Schutz von Geschäftsgeheimnissen verglichen. Kapitel 2 widmet sich den Grundlagen im Hinblick auf die Einordnung und Schutzbedürftigkeit der betroffenen Daten, der Verantwortlichkeit, des anwendbaren Rechtsrahmens sowie der Umsetzung der Datenschutzgrundprinzipien, wozu auch die Reichweite relevanter Rechtsgrundlagen und die Umsetzung angemessener Schutzmaßnahmen zählen – wobei Besonderheiten der elektronischen Kommunikation zunächst ausgespart werden und sodann ein eigenes Kapitel 3 bilden. Diese Aspekte werden aus einer umfassenden Perspektive mit Bezug zur Kommunikation im Unternehmen diskutiert. In Kapitel 4 erfolgt darauf aufbauend die Analyse der konkreten Umsetzung im Bereich der Messengersysteme, besondere Risiken bei international operierenden Angeboten sowie in Kapitel 5 die Darstellung der Pflichten für Unternehmen aufgeschlüsselt danach, ob es sich um rein interne oder externe Kommunikation mit Dritten handelt. In den Anhängen finden sich Prüfkataloge zur praktischen Umsetzung des Pflichtenkanons.

Die Einführung einer Kommunikationslösung wie einem Messengerdienst kann im Unternehmen in unterschiedlichen Kontexten erfolgen und technisch unterschiedlich umgesetzt werden. Im Rahmen der Studie werden zwei Fallgruppen unterschieden:

(1) **Unternehmensinterne** Kommunikation zwischen den Beschäftigten des Unternehmens

[56] *DSK - Datenschutzkonferenz*, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, S. 2.
[57] *Faas*, ArbRAktuell 2018, 594 (596).
[58] Abgeordnetenhaus Berlin Drucksache 18/27231, S. 1.
[59] Abgeordnetenhaus Berlin Drucksache 18/27231, S. 1. Unabhängig von dieser generellen Untersagung der Messengernutzung für dienstliche Zwecke teilte die Berliner Beauftragte für Datenschutz und Informationsfreiheit mit, dass der Messengerdienst Threema nach ihrer Kenntnis datenschutzgerecht eingesetzt werden könne: Abgeordnetenhaus Berlin Drucksache 18/27231, S. 3. Da bezüglich anderer Dienste, wie bspw. Signal, Wire, Telegram, Line, Element sowie Ginlo keine umfassende datenschutzrechtliche Prüfung durchgeführt wurde, konnte hierzu keine Aussage über eine datenschutzkonforme Nutzbarkeit durch öffentliche Stellen gemacht werden.

(2) **Externe Kommunikation** im Namen des Unternehmens mit Geschäftskontakten und/oder Kundschaft des Unternehmens

Hierbei werden unterschiedliche Verantwortungslevel untersucht, je nachdem, ob das Unternehmen die Nutzung eines Dienstes anordnet, einen Dienst lediglich bereitstellt oder die Nutzung durch Beschäftigte duldet. Zudem bestehen Unterschiede, ob ein Einsatz auf privaten oder dienstlichen Endgeräten erfolgen soll. Dabei sollen bei der rechtlichen Bewertung drei verschiedene Betriebsmodelle betrachtet werden:

(1) **„On Premise“:** Unternehmen betreibt einen Messengerdienst selbst
(2) **„Software-as-a-Service“:** Unternehmen beauftragt einen Messengerdienstanbieter zur Bereitstellung eines Dienstes, wobei der Messengerdienstanbieter keine eigenen Zwecke verfolgt und den Weisungen des Unternehmens unterliegt (*Auftragsverarbeitung*)
(3) **„Joint Controller“:** Unternehmen nutzt einen Messengerdienst, dessen Anbieter eigene Zwecke bei der Datenverarbeitung verfolgt und/oder die Diensterbringung eigenverantwortlich gestaltet (*gemeinsame Verantwortung*)

2 Grundlagen datenschutzrechtlicher Anforderungen an Unternehmenskommunikation und -kollaboration

Um die datenschutzrechtlichen Anforderungen zu skizzieren, muss zunächst eine Sichtung der betroffenen Daten bei der Kommunikations- und Kollaborationsdienstnutzung erfolgen. Hierbei gilt es stets zu bedenken, welche Rechte und Freiheiten bei der Verarbeitung dieser Daten betroffen sind. Im Rahmen der Auslegung der Schutzvorschriften spielt dies immer wieder eine zentrale Rolle. Eine elementare Weichenstellung folgt ferner aus der Identifikation des Normadressaten, welcher für die Verarbeitung verantwortlich ist und an wen sich rechtliche Anforderungen richten. Danach erfolgt die Bestimmung des sachlich, persönlich und räumlich anwendbaren Rechts. Anhand der zentralen Datenschutzgrundprinzipien soll im Anschluss der gesamte Pflichtenkatalog für die Umsetzung eines angemessenen Datenschutzniveaus in seinen Grundlagen dargestellt werden. Das Kapitel schließt mit einem Verweis auf die potentiellen Rechtsfolgen bei Datenschutzverstößen.

2.1 Überblick über betroffene Daten und ihre Schutzbedürftigkeit

Um zu beurteilen, inwiefern die Kommunikation über Kommunikations- und Kollaborationsdienste im Unternehmen datenschutzrechtlichen Anforderungen unterliegt, gilt es zunächst die infrage kommenden Daten auf ihren Personenbezug hin zu untersuchen. Hierfür bedarf es zunächst eines fundierten Überblicks über potentiell betroffene Daten. Die im Rahmen der Nutzung von Kollaborationswerkzeugen wie Messengerdiensten anfallenden Daten lassen sich dabei grob in Kommunikationsinhalte und Metadaten unterteilen. Diese Differenzierung ist sinnvoll, da Schutzmechanismen wie bspw. eine Ende-zu-Ende-Verschlüsselung zwar einen Schutz vor dem Zugriff Dritter auf den Inhalt der Nachricht gewährleisten können, allerdings keine Aussage zu den Metadaten zulassen, also wer mit wem wie lange oder wie häufig kommuniziert. Der Streit um die Vorratsdatenspeicherung hat eindrücklich gezeigt, welche Bedeutung die Auswertung solcher Metadaten haben kann und welche Risiken für die Privatsphäre der betroffenen Personen daraus resultieren können.[60] Im Hinblick auf die Schutzdimension zeigen sich ebenfalls Unterschiede im Hinblick auf Inhalte der Kommunikation und die im Kontext der Kommunikation entstehenden Metadaten.

2.1.1 Kommunikationsinhalt

Die in dieser Studie im Schwerpunkt betrachteten Messengerdienste beinhalten neben der Funktion zur Übermittlung von Nachrichten in Form von Textnachrichten i.d.R. eine Reihe weiterer Funktionen.[61] Ob die dargestellten Funktionen jeweils immer alle vorliegen oder auch nur einzelne Funktionen enthalten sind, hängt vom jeweiligen Messengerdienst ab.

Nachrichtentexte

Bei Nachrichtentexten handelt es sich um die Übermittlung von Informationen in Textform. Dabei liegt der Informationsgehalt in der textuellen Beschreibung bestimmter Inhalte.

[60] Vgl. BVerfGE 125, 260 – 385; EuGH, Urteil vom 06.10.2020 – C-623/17 – Privacy International; EuGH, Urteil vom 06.10.2020 – C-511/18, C-512/18 und C-520/18 – La Quadrature du Net; EuGH, Urteil vom 21.12.2016 – C-203/15 und C-698/15 – Tele2Sverige; EuGH, Urteil vom 08.04.2014 – C-293/12 – Digital Rights Ireland.
[61] *Schneider*, ZD 2014, 231 (232).

Voice-Calls

Mit der Voice-Call-Funktion eines Messengerdienstes können Telefonate wie mit herkömmlichen Telefon- oder Mobilgeräten geführt werden, mit dem Unterschied, dass diese Telefonate über eine Datenverbindung zustande kommen. Neben dem Nachrichteninhalt werden noch zusätzliche Metadaten erzeugt.

Video-Calls

Die Video-Call-Funktion geht über die Voice-Call-Funktion hinaus, da zusätzlich zur Telefonfunktion über eine Datenverbindung noch gleichzeitig Videodaten der Telefonierenden übertragen werden. Erfasst werden neben Ton und Bild auch das Umfeld des aktuellen Aufenthaltsortes (Wohnung/Arbeitsplatz/etc.) sowie ggf. im Hintergrund befindliche Personen.[62]

Mediendateien

Eine weitere Möglichkeit Informationen mithilfe von Messengerdiensten zu übertragen, besteht im Versand von Mediendateien. Diese Mediendateien können aus Video- und/oder Tonsequenzen, Bildern, Graphiken oder sonstigen Dateianhängen bestehen. Dabei können sowohl der Inhalt dieser Dateien als auch die damit übertragenen Metadaten einen Personenbezug beinhalten.

2.1.2 Metadaten

Für den Begriff der Metadaten existiert keine allgemein gültige juristische Definition. Über die inhaltliche Reichweite des Begriffs besteht jedoch weitestgehend Konsens: [63] Unter Metadaten versteht man demnach Daten, die ihrerseits dazu dienen, ausgewählte Aspekte von (Primär) Daten zu beschreiben, wie z. B. Telefonnummern und sonstige Kontaktdetails, Zeitpunkte bzw. Dauer einer Kommunikation sowie ggf. Standort der kommunizierenden Parteien.[64] Dies bedeutet im Rahmen der Nutzung von Messengerdiensten, dass zunächst die Kommunikationsdaten, wie z. B. Nutzername und die Handynummer unter Metadaten fallen, ohne welche die Verbindung zwischen den jeweiligen Nutzenden nicht hergestellt werden kann.[65] Im beruflichen Kontext kommen Daten über berufliche Kontakte und Rückschlüsse auf Arbeitszeiten hinzu.[66]

Die datenschutzrechtliche Bedeutung von Metadaten darf dabei nicht unterschätzt werden. Bereits der EuGH hatte festgestellt, dass aus solchen Daten sehr genaue Schlüsse auf das Privatleben der Personen gezogen werden können, etwa „auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren.“[67] Im Beschäftigtenkontext kann bspw. heutzutage mithilfe sog. „People Analytics-Verfahren“ aus der Auswertung der internen Kommunikation im Unternehmen anhand der Metadaten (Empfänger*in, Absender*in, Betreff, Datum u. ä.) ermittelt werden, wie die Stimmungslage im Unternehmen ist, welche Vernetzungen zwischen Unternehmensbereichen bestehen und an welchen Stellen Expert*innen tätig sind.[68] Damit sind relevante Rückschlüsse im Rahmen der Leistungsbewertung – technisch – möglich, womit auch Gehalts- und Aufstiegsentscheidungen für Mitarbeitende verbunden sein könnten.

---

[62] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 4.
[63] *Krüger/Möllers*, MMR 2016, 728 (728).
[64] *Faas*, ArbRAktuell 2018, 594 (595); *Polst u. a.*, DuD 2021, 19 (20).
[65] *Ulbricht,* in: Messenger Marketing, S. 70.
[66] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 4.
[67] EuGH, Urteil vom 08.04.2014 – C-293/12 – Digital Rights Ireland, Rn. 27.
[68] *Dietrich u. a.*, DuD 2021, 5 (6).

2.1.3 Grundrechtliche Schutzverbürgungen

Der Umgang mit diesen Daten unterliegt je nach spezifischer Fallkonstellation unterschiedlichen Schutzbedürfnissen, welche aus den Grundrechten als objektive Werteordnung herrühren. Das einfach-rechtliche Datenschutzrecht ist im Lichte dieser grundrechtlichen Gehalte auszulegen, weshalb im Vorgriff auf die Einzeldarstellung rechtlicher Vorgaben ein kurzer Überblick über die grundrechtlichen Schutzverbürgungen erforderlich ist.

2.1.3.1 Datenschutzgrundrechte

Datenschutzgrundrechte existieren sowohl auf nationaler als auch auf internationaler Ebene und haben damit unterschiedliche Reichweite. Für Europa sind drei Grundrechtskataloge von herausragender Bedeutung: die Europäische Menschenrechtskonvention (EMRK), die EU-Grundrechtecharta (EU-GrCh) sowie die nationalen Verfassungsrechte, in Deutschland das Grundgesetz (GG).

Art. 8 EMRK

(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Die älteste Regelung zum Datenschutz als Menschenrecht gewährt die Europäische Menschenrechtskonvention (EMRK), welche durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) stetig angepasst und an aktuelle Herausforderungen fortentwickelt wird. Der Schutz des Privat- und Familienlebens wurde dabei vom EGMR weit ausgelegt, indem mehrfach betont wurde, dass eine abschließende Definition des „Privatlebens“ nicht möglich ist.[69] Dabei unterstrich das Gericht in seinen Entscheidungen sowohl die Aspekte der Selbstbestimmung[70] als auch des Datenschutzes[71]. Aus dem Grundrecht folgerte der EGMR zudem eine staatliche Handlungspflicht, wonach Vertragsstaaten ausreichende Garantien gegen Datenmissbrauch vorsehen müssen.[72]

69 EGMR, Urteil vom 19.02.2015 – 53649/09 – Ernst August von Hannover/Deutschland, Rn. 44; EGMR Urteil vom 29.04.2002 - 2346/02 - Pretty/UK, Rn. 61; EGMR, Urteil vom 2.09.2010 – 35623/05 - Uzun/Deutschland, Rn. 43; EGMR, Urteil vom 20.01.2011 – 31322/07, NJW 2011, 3773 – Haas/Schweiz, Rn. 50; EGMR, Urteil vom 23.09.2010 – 425/03– Obst/Deutschland, Rn. 39; EGMR, Urteil vom 16.02.2000 – 27798/95 – Amann/Schweiz, Rn. 65; EGMR, Urteil vom 25.09.2001, 44787/98 - P.G. u. J.H./UK, Rn. 56; EGMR, Urteil vom 28.04.2003 – 44647/98 – Peck/UK, Rn. 57; EGMR, Urteil vom 17.10.2003 – 63737/00 – Perry/UK, Rn. 36; EGMR, Urteil vom 23.09. 2010 – 1620/03 – Schuth/Deutschland, Rn. 53; EGMR, Urteil vom 12.06.2014 – 56030/07– Fernandez Martinez/Spanien, Rn. 109.

70 EGMR, Urteil vom 19.07.2012 – 497/09 - Koch/Deutschland, NJW 2013, 2953; EGMR, Urteil vom 20.01.2011 – 31322/07, NJW 2011, 3773 – Haas/Schweiz; EGMR, Urteil vom 23.09.2010 – 425/03 – Obst/Deutschland, Rn. 39; EGMR, Urteil vom 23.09. 2010 – 1620/03– Schuth/Deutschland; EGMR, Urteil vom 12.06.2014 – 56030/07 – Fernandez Martinez/Spanien, Rn. 110; EGMR, Urteil vom 29.04.2002 – 2346/02 – Pretty/UK, NJW 2002, 2851.

71 EGMR, Urteil vom 22.02.2018 – 588/13 – Libert/France, ZD 2018, 263; EGMR, Urteil vom 2.09.2010 – 35623/05 – Uzun/Deutschland, NJW 2011, 1333; EGMR, Urteil vom 29.06.2006 – 54934/00 – Weber u. Saravia/Deutschland, NJW 2007, 1433; EGMR, Urteil vom 4.12.2008 – 30562/04 – Marper/UK; EGMR, Urteil vom 16.02.2000 – 27798/95 – Amann/Schweiz; EGMR, Urteil vom 25.09.2001, 44787/98 – P.G. u. J.H./UK; EGMR, Urteil vom 28.04.2003 – 44647/98 – Peck/UK; EGMR, Urteil vom 17.10.2003 – 63737/00 – Perry/UK; EGMR, Urteil vom 26.03.1987 – 9248/81 – Leander/Schweden, Rn. 48; EGMR, Urteil vom 4.05.2000 – 28341/95 – Rotaru/Rumänien; EGMR, Urteil vom 03.04.2007 – 62617/00 – Copland/UK.

72 Meyer-Ladewig/Nettesheim, in: HK-EMRK Art. 8 Rn. 32.

In Deutschland genießt die EMRK zwar nur den Rang eines einfachen Gesetzes, wird aber bei Auslegung der nationalen Grundrechte als wichtige Rechtserkenntnisquelle herangezogen.[73] Ebenfalls hatte sie einen entscheidenden Vorbildcharakter für die Entwicklung eines eigenständigen EU-Grundrechtskatalogs.[74]

Artt. 7, 8 EU-GrCh

Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Auf Europäischer Ebene wurde mit der Etablierung eines eigenen Grundrechtskatalogs mit der Charta der Grundrechte der Europäischen Union (GrCh) europaweit ein Regelwerk geschaffen, dass Primärrechtsrang und somit dieselbe Gültigkeit wie der unionsrechtliche Vertrag von Lissabon selbst genießt. Die EU-Grundrechte kommen bei der „Durchführung des Rechts der Union“ zur Anwendung (vgl. Art. 51 EU-GrCh). Der Europäische Gerichtshof (EuGH) und das Bundesverfassungsgericht (BVerfG) befinden sich in einem kontroversen Dialog über die Reichweite des jeweiligen Grundrechtsregimes.[75] Dies hat zwar zentrale Auswirkungen auf die Zuständigkeit der Gerichte, aufgrund der weitreichenden Harmonisierung aber keine überbordenden Effekte für die Ebene der Anwendung und Auslegung des einfachen Rechts. Einige Gerichte bemühen die nationalen und europäischen Grundrechtskataloge gemeinsam.[76]

Auch das Verhältnis zwischen Art. 7 EU-GrCh und seinem „moderneren“ kleinen Bruder Art. 8 EU-GrCh ist höchst umstritten.[77] Einige sehen in „dem“ Datenschutzgrundrecht gegenüber Art. 7 GrCh, der u.a. das Recht auf Achtung des Privatlebens und der Kommunikation normiert, als lex specialis an.[78] D.h. dass Art. 8 GrCh als speziellere Vorschrift der allgemeineren Vorschrift in Art. 7 GrCh vorgehen würde. Der EuGH prüft dagegen beide Normen regelmäßig parallel und gleichrangig.[79]

73 BVerfG, Beschluss vom 26.02.2008 – 1 BvR 1602/07 – Caroline von Monaco III, Rn. 53; BVerfG, Beschluss vom 14.10.2004 – 2 BvR 1481/04 –, BVerfGE 111, 307, Rn. 30; BVerfG, Urteil vom 04.05.2011 – 2 BvR 2333/08–, BVerfGE 128, 326, Rn. 87; BVerfG, Beschluss vom 26.03.1987 – 2 BvR 589/79 –, BVerfGE 74, 358-380, Rn. 35; BVerfG, Beschluss vom 29.05.1990 – 2 BvR 254/88 –, BVerfGE 82, 106-126, Rn. 33; Kingreen/Poscher, Grundrechte, S. 20 Rn. 66/67; Kirchhof, NJW 2011, 3681 (3683).

74 Boehm/Andrees, CR 2016, 146 (148); Boehm/Cole, ZD 2014, 553 (554); Britz, EuGRZ 2009, 1 (6f.); Michl, DuD 2017, 349 (350); Marsch, Das europäische Datenschutzgrundrecht, Kap. 1.

75 EuGH, Urteil vom 26. Februar 2013, Akerberg Fransson, C-617/10, EU:C:2013:105, Rn. 29; siehe auch EuGH, Urteil vom 26. Februar 2013, Melloni, C-399/11; BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08 –, Rn. 183; BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 – Recht auf Vergessen II.

76 Sofern die materiellen verfassungsrechtlichen Wertungen sachgerecht eingestellt werden, sei den Anforderungen des Grundrechtsschutzes genügt: BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 – Recht auf Vergessen II, Rn. 124.

77 Zum Streit siehe: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 216 ff. m.w.N.

78 Statt vieler: *Bernsdorff,* in: Meyer, Charta der Grundrechte der Europäischen Union Art. 8 Rn. 13; *Kingreen,* in: Callies/Ruffert, EUV/AEUV Art. 8 Rn. 1a.

79 EuGH, Urteil vom 9.11.2010, C-92/09 und C-93/09 – Volker und Markus Schecke und Eifert, Rn. 47 ff.; EuGH, Urteil vom 13.05.2014, C-131/12 – Google Spain, Rn. 69 ff.; EuGH, Urteil vom 8.04.2014, C-293/12 und C-594/12 – Digital Rights Ireland, Rn. 29 ff.; EuGH, Urteil vom 21.12.2016, C-203/15 und C-698/15 – Tele2 Sverige Rn. 93, 129; EuGH, Urteil vom 6.10.2015, C- 362/14 – Schrems, Rn. 39 ff.

Eine wesentliche Weichenstellung ist die Tatsache, dass der EuGH jede Verarbeitung personenbezogener Daten durch Dritte als einen Eingriff in den Schutzbereich wertet.[80] Für die Rechtfertigung sind dann wiederum die in Art. 8 Abs. 2 EU-GrCh aufgeführten Grundsätzen von elementarer Bedeutung.

Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG

Recht auf informationelle Selbstbestimmung

Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme

In Deutschland hat das BVerfG in seinem wegweisenden Volkszählungsurteil aus dem Allgemeinen Persönlichkeitsrecht das Recht auf informationelle Selbstbestimmung abgeleitet.[81] Nach der Entscheidung des Gerichtes ist darunter die Befugnis des Einzelnen zu verstehen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[82] Das BVerfG hat damit einen Teilbereich des Allgemeinen Persönlichkeitsrechts im Lichte der informationstechnischen Entwicklung interpretiert.[83] Konkretisiert und fortentwickelt wurde dieses Grundrecht im Lauf der Jahre durch weiteren Entscheidungen des BVerfG.[84]

Flankiert wird dieses klassische Datenschutzgrundrecht seit 2008 durch das ebenfalls aus dem Allgemeinen Persönlichkeitsrecht entwickelten „Computergrundrecht“, dem Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme.[85] Aus verfassungsrechtlicher Perspektive erkennt das BVerfG ein erhebliches Schutzbedürfnis, welches aus der Angewiesenheit auf die Nutzung informationstechnischer Systeme folgt, für die Freiheitsverwirklichung und die allgemeine Entfaltung der Persönlichkeit an.[86] Auch juristische Personen können sich grundsätzlich nach Art. 19 Abs. 3 GG auf dieses Grundrecht berufen.[87]

2.1.3.2 Fernmeldegeheimnis

Verbürgungen vor ausforschender oder missbräuchlicher Datenerfassung finden sich neben den klassischen Datenschutzgrundrechten auch als Teilaspekte in unterschiedlichen Grundrechten.[88] In Anbetracht der Tatsache, dass Menschen auf die Nutzbarkeit informationstechnischer Infrastrukturen im Informationszeitalter angewiesen sind und ihre Alltagsgegenstände zunehmend im Internet der Dinge (IoT) vernetzt sind, geraten als besonders geregelte Garantien der Privatheit das Post- und Fernmeldegeheimnis nach Art 10 Abs. 1 GG[89]

[80] EuGH, Urteil vom 08.04.2014 – C-293/12 – Digital Rights Ireland, Rn. 36; EuGH, Urteil vom 17.10.2013 – C-291/12 – Schwarz, Rn. 25; EuGH, Urteil vom 21.12.2016 – C-203/15 und C-698/15 – Tele2 Sverige, Rn. 100; *Franzen,* in: Franzen/Gallner/Oetker, EuArbR Art. 8 GRC Rn. 7; *Jarass*, Charta der Grundrechte der Europäischen Union Art. 8 Rn. 8; *Gersdorf,* in: BeckOK InfoMedienR Art. 8 EU-GrCharta Rn. 18; *Bieker*, DuD 2018, 27 (28); *Roßnagel*, NJW 2019, 1 (2).
[81] BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, BVerfGE 65, 1 – Volkszählungsurteil.
[82] BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, BVerfGE 65, 1 (43) – Volkszählungsurteil.
[83] Zur Entwicklung des Allgemeinen Persönlichkeitsrechts: BGHZ, 13, 334 – Leserbrief; BVerfGE 34, 238; BVerfGE 34, 269 – Soraya; BVerfGE 30, 173 – Mephisto; BVerfGE 27, 1 – Mikrozensus.
[84] Vgl. etwa BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 – Recht auf Vergessen II.
[85] BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350 - Online-Durchsuchung.
[86] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 33.
[87] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 21.
[88] *Masing*, RDV 2014, 3 (3); *Geminn/Roßnagel*, JZ 2015, 703 (703); vgl. auch *Gurlit*, NJW 2010, 1035 (1036f.).
[89] BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 –, BVerfGE 130, 151-212 – Bestandsdatenspeicherung, Rn. 111 ff.; BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 66; BVerfG, Urteil vom 27. Juli 2005 – 1 BvR 668/04 – Telekommunikationsüberwachung, Rn. 80 ff.; BVerfG, Beschluss vom 03. März 2004 – 1 BvF 3/92 –, BVerfGE 110, 33-76 – Außenwirtschaftsgesetz, Rn. 100 ff.; BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94 – Telekommunikationsüberwachung, Rn. 160 ff.; BVerfG, Beschluss vom 20. Juni 1984 – 1 BvR 1494/78 –, BVerfGE 67, 157-185 - Post- und Telefonkontrolle – G10, Rn. 42 ff.

und der Schutz in der Wohnung nach Art. 13 Abs. 1 GG[90] ebenfalls in den Fokus der Betrachtung. Im Hinblick auf die Kommunikation im Unternehmenskontext ist das Fernmeldegeheimnis von besonderem Interesse.

Art. 10 Abs. 1 GG

Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

Mit dem Fernmeldegeheimnis nach Art. 10 Abs. 1 Var. 3 GG wird die körperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs geschützt.[91] Die Grundintention dieses Rechts liegt in der freien Entfaltung der Persönlichkeit und Würde des Menschen über die Abschirmung des Kommunikationsinhalts sowie Gewährleistung der Vertraulichkeit der näheren Kommunikationsumstände.[92] Dazu werden Daten über das Ob, die Zeitpunkte, die Kommunikationspartner sowie Anzahl der durchgeführten sowie versuchten Kommunikationsvorgänge gezählt.[93] Nicht unter diesem Gesichtspunkt verfassungsrechtlich geschützt ist anderseits das Vertrauen in die Integrität des Kommunikationspartners.[94] Der primäre Schutzzweck liegt in den Risiken des technischen Übermittlungsvorgangs begründet, den die Grundrechtsträger*innen anders als im Gespräch unter Anwesenden schlechter kontrollieren können und endet daher mit Abschluss des Übermittlungsvorgangs.[95]

Art. 10 Abs. 2 GG enthält eine spezifische Grundrechtsschranke:

Art. 10 Abs. 2 GG

Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

2.1.3.3 Reichweite des Grundrechtsschutzes im Privatrechtsverhältnis

Die mittelbare Drittwirkung dieser Grundrechte bedeutet, dass der Staat Private im Verhältnis gegenüber Datenschutzgefährdungen durch andere Private in ihrer informationellen Selbstbestimmung schützen muss.[96] In Bezug auf das Verhältnis von Beschäftigten zu Arbeitgeber bedeutet dies folgendes: Sofern es zu

[90] BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 116 ff.; BVerfG, Urteil vom 03. März 2004 – 1 BvR 2378/98 –, BVerfGE 109, 279-391 – großer Lauschangriff, Rn. 124; BVerfG, Beschluss vom 03. April 1979 – 1 BvR 994/76 –, BStBl II 1979, 601-604, BVerfGE 51, 97-115 – Durchsuchungsanordnung, Rn. 22 ff.; *Becker*, JZ 2017, 170 (175).

[91] BVerfGE 67, 157 (172), BVerfGE 106, 28 (35 f.).

[92] BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 64; BVerfG, Beschluss vom 03. März 2004 – 1 BvF 3/92 –, BVerfGE 110, 33-76 – Außenwirtschaftsgesetz, Rn. 101; Beschluss vom 20. Juni 1984 – 1 BvR 1494/78 –, BVerfGE 67, 157-185 - Post- und Telefonkontrolle – G10, Rn. 43.

[93] BGH, Urteil vom 13. Juli 2017 – I ZR 193/16 –, Rn. 15; BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 –, BVerfGE 130, 151-212 – Bestandsdatenspeicherung, Rn. 112; BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08 – Vorratsdatenspeicherung, Rn. 189; BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 72; BVerfG, Urteil vom 14. Juli 1999 – 1 BvR 2226/94 – Telekommunikationsüberwachung, Rn. 163; *Gurlit*, NJW 2010, 1035 (1036).

[94] *Apel*, ZD 2018, 486 (486); *Nettesheim*, VVDStRL 2011, 7 (22).

[95] BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204 – Telekommunikationsüberwachung, Rn. 77; BVerfG, Beschluss vom 09. Oktober 2002 – 1 BvR 1611/96 –, BVerfGE 106, 28-51 – Mithörvorrichtung, Rn. 22; BVerfG, Beschluss vom 25. März 1992 – 1 BvR 1430/88 –, BVerfGE 85, 386-405 – Fangschaltung, Rn. 46; *Gurlit*, NJW 2010, 1035 (1036).

[96] Vgl. BVerfG, Beschl. v. 23.10.2006 - 1 BvR 2027/02, Rn. 30, WM 2006, 2270 ff.

privatrechtlichen Streitigkeiten zwischen diesen beiden Parteien kommt, muss die Judikative den Schutzgehalt des Grundrechts beachten, wenn sie nicht das Grundrecht der Bürger*innen in seiner Funktion als Schutznorm verletzen will.[97] Folglich haben die Grundrechte eine entscheidende Bedeutung bei der Anwendung und Auslegung des einfachen Rechts.

2.1.3.4 Grundrechtskollision

Da sowohl die von einer Datenverarbeitung betroffenen Personen als auch die diese Verarbeitung durchführenden Stellen sich jeweils auf Grundrechtsschutz berufen können, muss eine Abwägung getroffen werden, welche sich oftmals bereits in der Ausgestaltung des einfachen Rechts wiederfindet. Enthalten die direkt anzuwendenden Normen Auslegungsspielräume oder Abwägungsklauseln, kommt es mittelbar zum Rückgriff auf die widerstreitenden Grundrechte.

Sämtliche Grundrechte der EU-Grundrechtecharta unterstehen der allgemeinen Schrankenregelung des Art. 52 Abs. 1 EU-GrCh. Grundrechtseingriffe müssen stets den Wesensgehalt der Rechte und Freiheiten achten.[98] Einschränkungen aufgrund des Schutzes der Rechte und Freiheiten anderer Personen bedürfen stets der Wahrung des Grundsatzes der Verhältnismäßigkeit.[99] Bewertungskriterien für eine Angemessenheitsprüfung können zunächst die Folgewirkungen auf andere Freiheitsrechte sein.[100] Den Gerichten kommt die Aufgabe zu, auf Basis des einschlägigen Fachrechts die jeweils entgegenstehenden Grundrechte der unterschiedlichen Seiten in Ausgleich zu bringen.[101]

Ähnliche Weichenstellungen gebietet das Grundgesetz: Eingriffe in das Recht auf informationelle Selbstbestimmung müssen im Rahmen der sog. „praktischen Konkordanz“ mit konfligierenden Gegenpositionen abgewogen werden und dabei einen legitimen Zweck verfolgen, zur Erreichung des Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne sein.[102] Grundrechteingriffe sind „Erforderlich“, wenn andere Maßnahmen mit geringerem Eingriffsgewicht diesen Zweck nicht vergleichbar effektiv erreichen.[103] Sie sind „Verhältnismäßig im engeren Sinne“, wenn der mit ihnen verfolgte Zweck zu dem in ihnen liegenden Eingriffsgewicht nicht außer Verhältnis steht.

2.2 Verantwortlichkeit

Die Frage nach der Verantwortlichkeit ist eine der zentralen Fragen für die Bestimmung des datenschutzrechtlichen Pflichtenkanons. Die Zuordnung der Verantwortung zu einer bestimmten Stelle entscheidet mit über die territoriale Anwendbarkeit des Datenschutzregimes in internationalen Kontexten. Sie definiert den Adressaten der datenschutzrechtlichen Pflichten. Aus Sicht der betroffenen Personen muss bekannt sein,

[97] Vgl. BVerfG, Beschl. v. 23.10.2006 - 1 BvR 2027/02, Rn. 30, WM 2006, 2270 ff.
[98] Im Rahmen der Vorratsdatenspeicherung sah der EuGH den Wesensgehalt noch nicht verletzt, da sich die erfassten Daten nicht auf den Inhalt der Kommunikation bezogen: EuGH, Urteil vom 8.04.2014, C-293/12 und C-594/12 - Digital Rights Ireland, Rn. 39.
[99] Da jede Grundrechtseinschränkung gesetzlich vorgesehen sein muss, hat dies zur Folge, dass die gesetzliche Grundlage für den Eingriff den Umfang der Einschränkung selbst festlegen muss. EuGH, Urteil vom 8.04.2014, C-293/12 und C-594/12 - Digital Rights Ireland, Rn. 38; EuGH, Gutachten vom 26.07.2017 – 1/15 –, Rn. 138; EuGH, Urteil vom 17.12.2015 – C-419/14 – WebMindLicenses, Rn. 81; *Jarass*, Charta der Grundrechte der Europäischen Union Art. 8 Rn. 13ff.
[100] *Britz*, EuGRZ 2009, 1 (10) mit Verweis auf EuGH, Urteil vom 20.05.2003, C-465/00 – ORF (Österreichischer Rundfunk), Rn. 89.
[101] BVerfG, Beschluss vom 06.11.2019 - 1 BvR 276/17 – Recht auf Vergessen II, Rn. 96.
[102] BVerfGE 150, 244 (279) – Kfz-Kennzeichenkontrollen Bayern.
[103] BVerfGE 150, 244 (280), Rn. 88 – Kfz-Kennzeichenkontrollen Bayern.

gegenüber welcher Stelle sie ihre jeweiligen Rechte geltend machen können.[104] Auch ist dieser Haftungsadressat und unterliegt bei Verstößen gegen die datenschutzrechtlichen Pflichten dem Haftungsregime insbesondere den Sanktionsmöglichkeiten der DSGVO.

2.2.1 Kriterien zur Bestimmung des Verantwortlichen nach der DSGVO

Der Adressat der datenschutzrechtlichen Vorgaben in der DSGVO ist zunächst der sog. „Verantwortliche" für die Datenverarbeitung (engl. „Controller"), welcher in Art. 4 Nr. 7 DSGVO definiert wird. Danach ergeben sich zwei Weichenstellungen für die Zuordnung der Verantwortlichkeit:

- Entscheidung über Zweck und Mittel der Verarbeitung personenbezogener Daten oder
- Zuweisung durch Unionsrecht oder Recht der Mitgliedstaaten.

Art. 4 Nr. 7 DSGVO „Verantwortlicher"

die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

Entscheidend ist dabei, wer die tatsächliche Entscheidungsbefugnis über die Datenverarbeitung hat[105] sowie über Mittel und Zwecke tatsächlich Entscheidungen treffen kann.[106] Dabei hat der EuGH mehrfach betont, dass durch eine weite Definition des Begriffs des Verantwortlichen ein wirksamer und umfassender Schutz der betroffenen Personen gewährleistet werden soll.[107]

Zweck

Unter „Zweck" wird das „erwartete Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet", verstanden.[108] D.h. der Verantwortliche ist diejenige Stelle, welche die Frage beeinflusst, *warum* personenbezogene Daten verarbeitet werden. Abgrenzend zur Auftragsverarbeitung kommt es darauf an, ob Daten zu eigenen Zwecken oder im Auftrag eines Anderen verarbeitet werden bzw. ob aus einem Eigeninteresse heraus Einfluss auf die Verarbeitung genommen wird.[109] Bei mehreren Verantwortlichen liegt eine Entscheidung über den Zweck vor, wenn ein gemeinsames Ziel zum wechselseitigen Vorteil verfolgt wird.[110]

[104] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 3; *Jung/Hansch*, ZD 2019, 143 (143).
[105] *Schild,* in: BeckOK DatenschutzR Art. 4 Rn. 87a.
[106] *Hartung,* in: Kühling/Buchner, DS-GVO Art. 4 Nr. 7 Rn. 13.
[107] EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 65; EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 66; EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 28; EuGH, Urteil vom 13.05.2014 – C-131/12 – Google Spain, Rn. 34.
[108] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 13.
[109] Vgl. EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 68; EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 68.
[110] *Schwartmann*, Ordnung der Wissenschaft 2020, 77 (78).

Mittel

Das Mittel beschreibt die Art und Weise, wie ein Ergebnis oder Ziel erreicht wird.[111] Insofern bestimmt der Verantwortliche auch das *Wie* der Verarbeitung.[112] Hier stellen sich oft schwierige Abgrenzungsfragen, welches Level an Einfluss der Verantwortliche haben muss, wenn bspw. die technische Umsetzung stark in der Hand eines Auftragsverarbeiters liegt, der aber keine eigenen Zwecke mit der Datenverarbeitung verfolgt.

Angesichts der vom EuGH präferierten weiten Auslegung kann es ausreichen, dass ein Beitrag im Sinne einer Mitwirkung zur Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten geleistet wird.[113] Wenn eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DSGVO vorliegt, muss nicht einmal ein tatsächlicher Zugang jedes Verantwortlichen zu den Daten bestehen.[114] Ebenso kann es unerheblich sein, wenn sich Stellen formal nicht als Verantwortliche oder Auftragsverarbeiter bezeichnen, da es andernfalls den Parteien eines Vertrages überlassen wäre, über die Wahl der Vertragsbedingungen und Begrifflichkeiten Verantwortung nach eigenen Interessen unabhängig von tatsächlich ausgeübten Entscheidungsfunktionen zuzuweisen.[115]

2.2.2 Die gemeinsame Verantwortung

Sofern mehrere Verantwortliche gemeinsam für die Zwecke und Mittel der Datenverarbeitung verantwortlich sind, spricht man von einer gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO. Wenn also verschiedene Stellen zusammen Verarbeitungsprozesse steuern oder darüber entscheiden, liegt eine solche gemeinsame Verantwortlichkeit vor.[116] Dabei muss nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure gegeben sein.[117] Die unterschiedlichen Stellen können vielmehr in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.[118] Gemeinsam Verantwortliche können dabei zusammen Zweck und Mittel festlegen, oder konvergierend in dem Sinne entscheiden, dass die jeweils getroffene Wahl einander ergänzt und für die Verarbeitung in einer Weise erforderlich ist, sodass sie einen spürbaren Einfluss auf die Festlegung der Zwecke und Mittel der Verarbeitung hat.[119] Ist eine Verarbeitung ohne die Mitwirkung beider Parteien nicht möglich, d.h. dass die Parteibeiträge unauflösbar miteinander verbunden sind, so kann eine konvergierende Entscheidung vorliegen. Dabei gilt jedoch zu berücksichtigen, dass bezüglich Entscheidungen über Zweck und Mittel, die in einer Verarbeitungskette vorausgehen oder nachfolgen, auch Wechsel zwischen alleiniger und gemeinsamer Verantwortlichkeit gegeben sein können.[120]

Liegt eine gemeinsame Verantwortung vor, kann eine Stelle folglich auch dann ein für die Verarbeitung Ver-

[111] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 13.
[112] *Jung/Hansch*, ZD 2019, 143 (144).
[113] EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 68; EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 31.
[114] EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 69; EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 38; EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 69.
[115] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 12.
[116] *Hartung,* in: Kühling/Buchner, DS-GVO Art. 4 Nr. 7 Rn. 12.
[117] *Forgó,* in: Autonomes Fahren, Kap. 3.5 Rn. 24.
[118] EuGH, Urteil vom 05.06.2018 – C-210/16 – Wirtschaftsakademie, Rn. 43; EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 70.
[119] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 18.
[120] EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 74.

antwortlicher sein, den alle Pflichten der einschlägigen DSGVO-Vorschriften treffen, wenn sie nicht *alle* Entscheidungen über die Zwecke und Mittel trifft.[121] Das Verhältnis gemeinsam für die Verarbeitung Verantwortlicher wird durch Art. 26 DSGVO geregelt.

2.2.3 Abgrenzung zur Auftragsverarbeitung

Gemäß Art. 4 Nr. 8 DSGVO kann eine natürliche oder juristische Person, eine Behörde, Einrichtung oder andere Stelle auch als Auftragsverarbeiter Daten im Auftrag des Verantwortlichen verarbeiten. Wesentliches Unterscheidungskriterium zu der gemeinsamen Verantwortlichkeit ist die Weisungsgebundenheit des Auftragsverarbeiters, der nur in einem vorgegebenen Rahmen des Auftragsgebers tätig werden darf.[122] Des Weiteren unterliegt der Auftragsverarbeiter nach Art. 28 Abs. 3 DSGVO einer Reihe weiterer Pflichten gegenüber dem Auftraggeber, damit dieser sicher stellen und v.a. kontrollieren kann, dass sein jeweiliger Auftragsverarbeiter die personenbezogenen Daten auch nur im Rahmen des Auftragsdatenverarbeitungsvertrages verarbeitet und sich versichern kann, dass die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters gewährleistet werden können.[123]

2.2.4 Besonderheiten im Unternehmenskontext

Im unternehmerischen Kontext ist der datenschutzrechtliche Verantwortliche zunächst das Unternehmen selbst.[124] Organisatorisch und im operativen Betrieb liegt die Aufgabe jedoch bei den Beschäftigten, da diese i.d.R. selbst diejenigen sind, die personenbezogene Daten verarbeiten.

2.2.4.1 Zurechnung des Verhaltens der Beschäftigten

Ob die Verantwortung i.S.d. Art. 4 Nr. 7 DSGVO beim Unternehmen liegt oder ausnahmsweise bei dem tatsächlich handelnden Beschäftigten, hängt davon ab, ob das Verhalten der Beschäftigten dem Unternehmen zuzurechnen ist. Hierbei ist entscheidend, ob die Datenverarbeitung zu Unternehmenszwecken oder eigenen Zwecken der Beschäftigten erfolgt. Letzterer Fall wird auch als sog. „Mitarbeiterexzess“ bezeichnet.[125] Das Unternehmen kann allerdings eine (Mit-)Verantwortung treffen. Von der Verantwortlichkeit des Arbeitgebers ist daher auszugehen, wenn die Verarbeitungstätigkeiten im Verantwortungsbereich des Unternehmens erfolgen.[126] Die Beschäftigten handeln daher in der Regel im Auftrag des Unternehmens als Arbeitgeber, sofern sie im Rahmen ihrer Tätigkeit personenbezogene Daten verarbeiten.

---

[121] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 13.
[122] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 24 f.
[123] Siehe hierzu Abschnitt 2.5.2.2.
[124] Diese haften grundsätzlich für schuldhafte Datenschutzverstöße ihrer Beschäftigten: *DSK - Datenschutzkonferenz*, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019, S. 1; *Rohrlich*, ZAP 2020, 1265 (1267); *Bertram/Falder*, ArbRAktuell 2021, 95 (95); *Dury*, ZD-Aktuell 2020, 04405.
[125] Ausführlich: *Ambrock*, ZD 2020, 492.
[126] *Jung/Hansch*, ZD 2019, 143 (145); *DSK - Datenschutzkonferenz*, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019.

2.2.4.2 Der Mitarbeiterexzess

Soweit Beschäftigte im Rahmen der tatsächlichen Möglichkeit zur Datenverarbeitung das rechtlich Erlaubte überschreiten und Daten zu eigenen Zwecken verarbeiten, handeln sie damit nicht mehr im Auftrag des Arbeitgebers und werden selbst zum Verantwortlichen.[127] Die Datenschutzkonferenz (DSK) definiert diesen Mitarbeiterexzess als „Handlung von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden kann“.[128] Es soll somit nicht primär darauf ankommen, ob die Beschäftigten subjektiv eigene Interessen verfolgen, sondern ob die Zweckbestimmung objektiv betrachtet den zugewiesenen Aufgaben entspricht.[129]

2.2.5 Folgen für die Verantwortlichkeit

Als Verantwortliche im datenschutzrechtlichen Sinne kommen im Kontext des Einsatzes von Messengerdiensten im Unternehmen grundsätzlich drei Stellen in Betracht: [130]

- das Unternehmen
- der Messengerdienstanbieter/-betreiber
- die Beschäftigten des Unternehmens (Mitarbeiterexzess).[131]

2.3 Anwendbares Recht im Beschäftigtenkontext (DSGVO, BDSG, LDSG)

Datenschutzrechtliche Anforderungen erwachsen nur, wenn das Datenschutzrecht auf den Sachverhalt anwendbar ist. Dabei gilt auch zu berücksichtigen, welches Recht räumlich einschlägig ist. Aus der deutschen Perspektive sind daher zunächst die Anwendungsvoraussetzungen folgender Regelwerke zu prüfen:

[127] *Ambrock*, ZD 2020, 492; *Jung/Hansch*, ZD 2019, 143 (145).
[128] *DSK - Datenschutzkonferenz*, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019, S. 1.
[129] *Ambrock*, ZD 2020, 492 (493).
[130] Die fallgruppenspezifische Untersuchung der Verantwortlichkeit erfolgt in Kapitel 3.
[131] Eine fallgruppenspezifische Betrachtung der Verantwortlichkeit im Einzelnen bei der Umsetzung von Messengerdiensten im Unternehmenskontext erfolgt in Abschnitten 5.2.1 und 5.3.1.

Recht der Europäischen Union:

- **Datenschutz-Grundverordnung – DSGVO:** Zentrales Instrument zum Schutz personenbezogener Daten in der EU, welche als unmittelbar anwendbare Verordnung Rechte und Pflichten statuiert, allerdings auch zahlreiche Öffnungsklauseln enthält, die weiterhin in begrenztem Umfang mitgliedstaatliche Regelungen ermöglichen.

- **ePrivacy-Richtlinie:** Bereichsspezifische Datenschutzregeln für die Telekommunikation und Telemedien, als Richtlinie allerdings nicht unmittelbar anwendbar, sondern muss durch mitgliedstaatliches Recht umgesetzt werden, welches richtlinienkonform auszulegen ist.

- **JI-Richtlinie:** Datenschutz-Richtlinie im Bereich von Justiz und Inneres

Recht der Mitgliedstaaten (hier: Deutschland):

Bundesebene

- **Bundesdatenschutzgesetz – BDSG:** füllt die Öffnungsklauseln der DSGVO konkretisierend aus und setzt die JI-Richtlinie um.

- **Telekommunikation-Telemedien-Datenschutzgesetz – TTDSG:** Umsetzung der ePrivacy-Richtlinie, wird ab 01.12.2021 in Kraft treten (vormals Telekommunikationsgesetz - TKG und Telemediengesetz - TMG)

Landesebene

- Landesdatenschutzgesetze: Baden-Württemberg **LDSG BW**, Bayern **BayDSG**, Berlin **BlnDSG**, Brandenburg **BbgDSG**, Bremen **BremDSGVOAG**, Hamburg **HmbDSG**, Hessen **HDSIG**, Mecklenburg-Vorpommern **DSG M-V**, Niedersachsen **NDSG**, Nordrhein-Westfalen **DSG NRW**, Rheinland-Pfalz **LDSG RhPfl**, Saarland **SaarlDSG**, Sachsen **SächsDSG**, Sachsen-Anhalt **DSG LSA**, Schleswig-Holstein **LDSG SH**, Thüringen **ThürDSG**

Kirchenrecht

- **Gesetz über den kirchlichen Datenschutz** (KDG) der katholischen Kirche.
- **Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland**“ (DSG-EKD)

2.3.1 Sachliche Anwendbarkeit der DSGVO

2.3.1.1 Grundsatz

Art. 2 DSGVO normiert den sachlichen Anwendungsbereich der DSGVO. Die Prüfung, ob der Anwendungsbereich der DSGVO eröffnet ist, ist stets der erste Schritt zur Ermittlung der rechtlichen Anforderungen an eine geplante Datenverarbeitung.

> **Art. 2 Abs. 1 DSGVO**
>
> Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Art. 2 Abs. 1 DSGVO nennt die grundlegenden Voraussetzungen, die erfüllt sein müssen, damit die DSGVO zur Anwendung kommt. Dies sind:

Abbildung 1 zum sachlichen Anwendungsbereich

2.3.1.2 Personenbezogene Daten

Angesichts des bezweckten Schutzes der Grundrechte natürlicher Personen bei der Verarbeitung sie betreffender Daten,[132] stehen in sachlicher Hinsicht personenbezogene Daten im Mittelpunkt, die in Art. 4 Nr. 1 DSGVO definiert sind. Danach sind unter personenbezogenen Daten alle Informationen zu verstehen, die sich auf eine *identifizierte* oder *identifizierbare* natürliche Person beziehen. Somit kann die betroffene Person

[132] Vgl. ErwGr. 1 und 2; siehe auch: *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 7.

grundsätzlich nur eine natürliche – und keine juristische Person sein.[133] Geschützt werden grundsätzlich alle Menschen unabhängig von ihrer Staatsbürgerschaft oder Unionsbürgerschaft.[134] Bei Angaben zu einer juristischen Person, reinen Unternehmensdaten und Sachinformationen, die auch nicht mittelbar zur Identifizierung einer natürlichen Person geeignet sind, ist das Datenschutzrecht nicht anwendbar.[135] Inwiefern das Gesetz zum Schutz von Geschäftsgeheimnissen an der Stelle eine Rolle spielt, wird in einem anderen Abschnitt behandelt (siehe Kapitel 6).

Art. 4 Nr. 1 DSGVO

„personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen […]

Die Definition ist weit zu verstehen.[136] Im beruflichen Kontext gilt zu bedenken, dass Daten, welche sich zunächst primär auf ein Unternehmen beziehen, gleichzeitig einen Bezug zu einer natürlichen Person aufweisen können.[137] Besonders deutlich wird das im Fall einer sog. Einmann-GmbH.[138] Ebenso bei Kaufleuten: soweit der Name der juristischen Person eine oder mehrere natürliche Personen bestimmt, können diese sich ebenfalls auf den grundrechtlich verbürgten Schutz ihrer Daten berufen.[139] Folglich bestehen vor allem in diesen Fällen typischerweise Risiken des Durchschlagens:

- Eine E-Mail-Adresse, Social-Media-Account, Messenger-ID, Telefonnummer oder ähnliches weist zwar keine Person namentlich auf, wird allerdings regelmäßig von der gleichen Mitarbeiter*in verwaltet.[140]
- Aussagen über Kleinbetriebe, Vereine oder ähnliche juristische Personen und Personengesellschaften, die sich auch auf das Verhalten der Eigentümer*innen bzw. Gesellschafter*innen, die Geschäftsführer*innen oder den Vorstand, etc. beziehen,[141]
    - Bspw. wenn der Name der juristischen Person vom Namen der natürlichen Person ableitet ist.[142]
    - Bspw. wenn sich aus dem Gesamtzusammenhang ergibt, dass eine natürliche Person alleinige Gesellschafter*in und Geschäftsführer*in ist.[143]

Als natürliche Person geschützt sind somit sowohl Privatpersonen, als auch Angestellte, Selbstständige und

[133] *Piltz*, K&R 2016, 557 (557). Zur Reichweite des Grundrechtsschutzes aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, 14 Abs. 1, 19 Abs. 3 GG sowie Art 7, Art. 8 EU-GrCh für juristische Personen siehe: *Schild,* in: BeckOK DatenschutzR Art. 4 Rn. 6 ff. m.w.N.
[134] *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 10.
[135] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 4.
[136] BGH, Urteil vom 15.06.2021 –VI ZR 576/19, Rn. 22.
[137] *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 14; *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 13.
[138] BGH, Urteil vom 17-12-1985 - VI ZR 244/84; *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 4; *Arning/Rothkegel,* in: Taeger/Gabel - DSGVO/BDSG Art. 4 Rn. 17.
[139] EuGH, Urteil vom 9. 11. 2010 - C-92, 93/09 - Volker und Markus Schecke und Eifert, Rn. 53; *Schild,* in: BeckOK DatenschutzR Art. 4 Rn. 7.
[140] *Arning/Rothkegel,* in: Taeger/Gabel - DSGVO/BDSG Art. 4 Rn. 17; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136, S. 27.
[141] *Arning/Rothkegel,* in: Taeger/Gabel - DSGVO/BDSG Art. 4 Rn. 17.
[142] EuGH, Urteil vom 9. 11. 2010 - C-92, 93/09 - Volker und Markus Schecke und Eifert, Rn. 53; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136, S. 27.
[143] BGH, Urteil vom 17-12-1985 - VI ZR 244/84.

beruflich handelnde Personen – sofern sich die Daten auf eine identifizierbare Person beziehen.[144]

2.3.1.2.1 Identifizierbarkeit

Für die Frage, ob ein Datum personenbezogen ist oder nicht, kommt es darauf an, ob eine natürliche Person anhand der Daten bereits identifiziert ist oder identifiziert werden kann. Als Möglichkeit zur Identifizierung nennt Art. 4 Nr. 1 DSGVO insbesondere die Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Hierbei macht die verwendete Begrifflichkeit des „insbesondere“ deutlich, dass es sich um sog. Regelbeispiele handelt und die Aufzählung folglich nicht abschließend ist.[145]

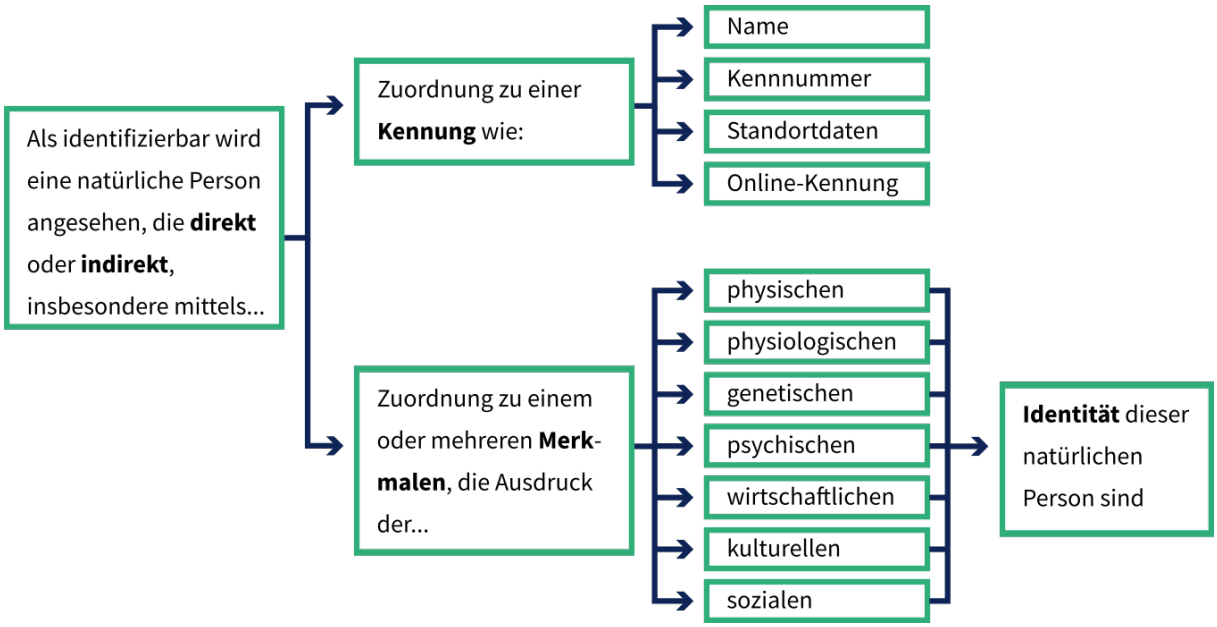


Abbildung 2 Regelbeispiele für die direkte und indirekte Identifizierbarkeit in Art. 4 Nr. 1 DSGVO

Ob eine Person identifizierbar ist, hängt entscheidend von den Informationen ab, zu denen der Verantwortliche Zugang hat. Ein wegweisendes Urteil hat an dieser Stelle der EuGH in der Sache Breyer zur Frage des Personenbezugs dynamischer IP-Adressen gefällt:

[144] EuGH, Urteil vom 30. 5. 2013 – C-342/12 – Equipamentos para o Lar S/Autoridade para as Condições de Trabalho [ACT]; *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 4.
[145] *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 15.

EuGH, Urteil vom 19.10.2016 - C-582/14 – Breyer

- Ein personenbezogenes Datum muss nicht für sich genommen die Identifizierung der betreffenden Person ermöglichen.
- Selbst wenn sich die Identität der natürlichen Person nicht unmittelbar aus den vorliegenden Daten ergibt, kann diese identifizierbar sein, wenn entsprechende **Zusatzinformationen** einholbar sind.
- Dies ist nicht der Fall, wenn die Identifizierung der betreffenden Person **gesetzlich verboten** oder **praktisch nicht durchführbar** wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung *de facto* vernachlässigbar erschiene.
- Rechtliche Möglichkeiten sind auch dann gegeben, wenn diese die Mitwirkung eines Dritten, bspw. einer zuständigen Behörde erfordern.

Folglich ist es für die Annahme der Identifizierbarkeit ausreichend, dass grundsätzlich eine Möglichkeit besteht, identifizierende Informationen bei einem Dritten einzuholen, selbst wenn hierfür zunächst die Mitwirkung einer Behörde angefragt werden muss.[146] Dieses noch zur Datenschutzrichtlinie ergangene Grundsatzurteil lässt sich auf die DSGVO übertragen.[147] Dies zeigt sich insbesondere in den Erwägungsgründen, die inhaltlich weitgehend auf den bereits zuvor entwickelten Weichenstellungen der Datenschutzrichtlinie beruhen:[148]

Erwägungsgrund 26, S. 3 DSGVO

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.

Erwägungsgrund 26, S. 4 DSGVO

Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Eine Person kann somit bereits dann identifiziert werden, wenn sie sich von allen anderen Personen einer

[146] EuGH, Urteil vom 19.10.2016 - C-582/14 – Breyer, Rn. 48.
[147] *Klar/Kühling,* in: Kühling/Buchner, DS-GVO Art. 4 Nr. 1 Rn. 20; *Piltz*, K&R 2016, 557 (561).
[148] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 67 f.

Gruppe eindeutig unterscheiden lässt (Aussondern).[149] Die *Möglichkeit* einer Identifizierung unter verhältnismäßigem Aufwand ist somit ausreichend.[150]

Sofern Zweifel bestehen, ob personenbezogene Daten vorliegen, können die von der Art-29-Datenschutzgruppe (Vorgänger des Europäischen Datenschutzausschusses EDSA – *European Data Protection Board*) noch zur Datenschutzrichtlinie entwickelten Abgrenzungskriterien herangezogen werden:[151]

Artikel-29-Datenschutzgruppe WP 136, 2007

- **Inhaltselement:** Angaben sind eindeutig „über" eine bestimmte Person
- **Zweckelement:** Daten werden unter Berücksichtigung aller Begleitumstände mit dem Zweck verwendet, eine Person zu beeinflussen, zu beurteilen oder in einer bestimmten Weise zu behandeln
- **Ergebniselement:** die Verwendung könnte sich unter Berücksichtigung aller jeweiligen-Begleitumstände auf die Rechte und Interessen einer bestimmten Person auswirken.

Die genannten Elemente sind alternativ, nicht kumulativ zu verstehen.[152] Dabei können auch Bezüge zu mehreren Personen bestehen. Bspw. kann eine Nachricht inhaltlich auf eine Person bezogen sein und aus den Metadaten Rückschlüsse auf die absendende oder empfangende Person zulassen. Die Erfassung dieser Daten kann dem Zweck dienen, diese Personen nachzuverfolgen und/oder kann bestimmte Folgen für diese Personen haben. Beim Ergebniselement werden nicht nur negative oder nachhaltige Folgen erfasst – ausreichend ist, dass „die Person aufgrund der Verarbeitung solcher Daten anders als andere Personen behandelt werden könnte."[153]

Damit fallen sowohl persönliche als auch sachliche Angaben unter den Begriff personenbezogene Daten.

- **Persönliche Angaben** sind z.B. Name, Alter, Anschrift, Geschlecht, Geburtsdatum, Telefonnummer, Fingerabdrücke, Fotos oder Videos.[154]
- **Sachliche Angaben** sind etwa die Beziehung des Betroffenen zur Umwelt, Sachen oder Dritten, wie Angaben zum Umfeld, seiner finanziellen Situation, Vertragsbeziehung, Kommunikationsverhalten, etc.[155] Auch die Erfassung von Arbeitszeiten fallen regelmäßig unter die personenbezogene Daten.[156]

Bei Messengerdiensten spielen die Kommunikationsdaten eine zentrale Rolle, die regelmäßig als personenbezogene Daten zu sehen sind. Dies gilt sowohl für Metadaten (z.B.: Name, Telefon-Nr. oder Anschrift aus

[149] *Hornung/Herfurth*, in: König/Schröder/Wiegand, Big Data, S. 149 (153); *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136, S. 14; *Roßnagel*, ZD 2013, 562 (563); *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 58 f.

[150] BGH Urteil vom 16. Mai 2017 – VI ZR 135/13; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136, S. 14; *Bergt*, ZD 2015, 365 (369); *Kring/Marosi*, K&R 2016, 773; *Jensen/Knoke*, ZD-Aktuell 2016, 05416; *Weinhold*, ZD-Aktuell 2016, 05366; *Kühling/Klar*, ZD 2017, 27; *Ernst,* in: Paal/Pauly, DS-GVO Art. 4 Rn. 11.

[151] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136, S. 7 ff.; bestätigt in der Rechtsprechung des EuGHs zur RL 95/46/EG: EuGH, Urteil vom 20.12.2017 – C-434/16 – Nowak, Rn. 35.

[152] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136, S. 13.

[153] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136, S. 13.

[154] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 4 Rn. 14.

[155] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 4 Rn. 14.

[156] EuGH, Urteil vom 30. 5. 2013 – C-342/12 – Equipamentos para o Lar S/Autoridade para as Condições de Trabalho [ACT].

dem Kontaktverzeichnis des Smartphones des Messengerdienst-Nutzenden) als auch für Inhaltsdaten (z. B.: Chat-Inhalt oder Anrufe).[157]

Beispiele für personenbezogene Daten:

- (dynamische und statische) IP-Adressen,
- Telefonnummern,[158]
- Werbe-ID,
- International Mobile Station Equipment Identity (IMEI),[159]
- International Mobile Subscriber Identity (IMSI)[160]

2.3.1.2.2 Besondere Kategorien personenbezogener Daten

Im Rahmen der personenbezogenen Daten genießen besondere Kategorien personenbezogener Daten nach Art. 9 Abs.1 DSGVO höhere Schutzanforderung (sog. sensible Daten). Die Einordnung ist zwar für die Anwendbarkeit der DSGVO nicht von Bedeutung, soll nichtsdestotrotz an dieser Stelle bereits angerissen werden. Zu diesen Daten gehören Angaben über:

- Rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- die Gewerkschaftszugehörigkeit
- genetische Daten,[161] biometrischen Daten[162] zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten[163]
- und Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Diese Datenkategorien kommen in den Metadaten bzw. im Kontaktverzeichnis eines Messengerdienstnutzenden in der Regel nicht vor (siehe Abschnitt 2.1). Allerdings wäre zu beachten, dass sich diese sensiblen Daten aus dem Inhalt des Chats oder aus den ausgetauschten Dokumenten/Fotos/Videos ergeben könnten.

Liegen besondere Kategorien personenbezogener Daten vor, bestehen besonders hohe Anforderungen an die Legitimierung einer Verarbeitung dieser Daten. Ob im Einzelfall besondere Kategorien personenbezogener Daten gegeben sind und welche Konsequenzen dies für die Kommunikation im Unternehmenskontext

---

[157] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 4 Rn. 14; *Broy,* in: Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. B. XI. 1. Rn. 13; vgl. auch *Jandt/Karg,* in: *Jandt/Steidle*, Datenschutz im Internet, Kap. A. II. Rechtliche Grundlagen Rn. 98 ff.

[158] Auch bei Nebenstellenapparaten, wenn eine Zuordnung zu einzelnen Beschäftigten möglich ist: BAG, Beschluss vom 27.05.1986 - 1 ABR 48/84.

[159] Die *International Mobile Station Equipment Identity* ist eine weltweit eindeutig identifizierende 15-stellige Seriennummer für GSM- oder UMTS-Endgeräte.

[160] Die *International Mobile Subscriber Identity* wird in GSM-, UMTS- und LTE-Mobilfunknetzen zur eindeutigen Identifizierung der Netzteilnehmenden genutzt.

[161] Definiert in Art. 4 Nr. 13 DSGVO als: „genetische Daten" personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

[162] Definiert in Art. 4 Nr. 14 DSGVO als: „biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

[163] Definiert in Art. 4 Nr. 15 DSGVO als: „Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

hat, soll an anderer Stelle erläutert werden (siehe Abschnitt 2.4.1.4).

2.3.1.2.3 Anonymisierung

Die DSGVO selbst definiert die Anonymisierung nicht. Sie stellt allerdings klar, dass die DSGVO nicht für anonyme bzw. anonymisierte Daten anwendbar sein soll.

Erwägungsgrund 26, S. 5, 6 DSGVO

Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymen Daten, auch für statistische oder für Forschungszwecke.

Die Abgrenzung personenbezogener und anonymer Daten stellt eine der wesentlichsten Herausforderungen des Datenschutzrechts dar. Insbesondere kann ein Datensatz durch ein identifizierendes Merkmal „infiziert" werden, sodass – auch wenn unbeabsichtigt – ein „Hineinwachsen" in den Personenbezug möglich ist.[164] Die Schwierigkeit bei der Bestimmung der Re-Identifizierungsrisiken liegt darin, dass bspw. durch fortschreitende Verknüpfung mit weiteren Datenbeständen (Stichwort Big Data) oder verbesserte Identifizierungstechniken, die Gefahr eines dynamischen „Hineinwachsens" in den Personenbezug droht.[165] Gerade die stetige Verbesserung der Rechenkapazität kann dazu führen, dass anonyme Datenbestände erneut bestimmten Personen zugeordnet werden können.[166] Die Übergänge zwischen anonymen und personenbezogenen Daten können folglich fließend und zeitvariabel sein, sodass Re-Identifizierungsrisiken stets bedacht werden sollten. Absehbare oder zu erwartende zukünftige Entwicklungen in Bezug auf Kontextwissen, Technik oder dem Wert der Informationen sollten daher antizipiert werden.[167] Empfohlen wird daher eine regelmäßige (Neu-)Bewertung der Verhältnismäßigkeit des Aufwands der De-Anonymisierung.[168]

In unterschiedlichsten Kontexten werden Daten in gehashter Form übermittelt. Das VG Bayreuth entschied hierzu, dass durch den Vorgang des „Hashens" die Daten nicht i.S.d. (damals noch einschlägigen) § 3 Abs. 6 BDSG a.F. anonymisiert würden, da es weiterhin mit nicht nur unverhältnismäßigem Aufwand möglich ist, sie einer bestimmten oder bestimmbaren Person zuzuordnen: „zumal andernfalls auch ein sich an die Übermittlung anschließender Datenabgleich seitens [des Anbieters] nicht möglich wäre."[169]

In praktischer Hinsicht besteht die Möglichkeit, vorsorglich im Zweifel von einem Personenbezug auszugehen und die datenschutzrechtlichen Vorschriften zu beachten.[170] Auch wenn im Rahmen elektronischer Kom-

[164] *Weichert*, DuD 2007, 113 (117); *Marnau*, DuD 2016, 428; *Hornung/Herfurth*, in: König/Schröder/Wiegand, Big Data, S. 149 (165); *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" - WP 136; *Kühling/Klar*, ZD 2017, 27 (28).
[165] *Marnau*, DuD 2016, 428 (429); *Roßnagel*, ZD 2013, 562 (566); *Sarunski*, DuD 2016, 424 (427); *Boehme-Neßler*, DuD 2016, 419 (422); *Hornung/Herfurth*, in: König/Schröder/Wiegand, Big Data, S. 149 (165); *Raabe/Wagner*, DuD 2016, 434 (435); *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 35.
[166] *Karg*, DuD 2015, 520 (526).
[167] *Hammer/Knopp*, DuD 2015, 503 (507); vgl. auch *Piltz*, K&R 2016, 557 (561).
[168] *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 35; *Roßnagel*, ZD 2018, 243 (247); *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 13; *Klar/Kühling,* in: Kühling/Buchner, DS-GVO Art. 4 Nr. 1 Rn. 22.
[169] VG Bayreuth, Beschluss vom 08.05.2018 – B 1 S 18.105 –, Rn. 47; bestätigt durch: Bayerischer Verwaltungsgerichtshof, Beschluss vom 26.09.2018 – 5 CS 18.1157 –, Rn. 11 ff.
[170] *Hornung/Herfurth*, in: König/Schröder/Wiegand, Big Data, S. 149 (166 f.). Andere fordern wiederum die Steuerung von (Re-)Identifizierungsrisiken durch datenschutzrechtliche Vorsorgeregelungen: *Roßnagel/Scholz*, MMR 2000, 721 (728 ff.).

munikation oftmals von anonymer Kommunikation die Rede ist, sollte angesichts der Fülle anfallender Daten sowie der notwendigen Zuordenbarkeit der Teilnehmenden eher von Pseudonymität im Rechtssinne gesprochen werden. Zu unterstreichen ist insoweit, dass es für die Einordnung als personenbezogen und damit die Anwendbarkeit der DSGVO nicht darauf ankommt, dass die betroffenen Personen namentlich bekannt sind. Der Einsatz von Anonymisierungstechniken kann allerdings im Rahmen der Rechtmäßigkeit einer Datenverarbeitung eine entscheidende Rolle spielen, da hiermit Risiken für die Rechte und Freiheiten betroffener Personen minimiert werden.

2.3.1.2.4 Pseudonymisierung

Anders als die Anonymisierung führt die Pseudonymisierung regelmäßig nicht zum Ausschluss des Personenbezugs und damit verbleibt es bei der Anwendbarkeit des Datenschutzrechts.[171] Definiert wird die Pseudonymisierung als:

> **Art. 4 Nr. 5 DSGVO „Pseudonymisierung“**
>
> die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

Zur Anwendbarkeit des Datenschutzrechts hebt Erwägungsgrund 26 S. 2 DSGVO hervor:

> Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.

Die Pseudonymisierung ermöglicht gegenüber der Anonymisierung, dass Personen wiedererkennbar bleiben, ohne dass jedoch eine vollständige Identifikation möglich ist.[172] Ist eine Zuordnungsregel zwischen Pseudonym und Person bekannt, ist die Pseudonymisierung rücknehmbar, sodass wieder ein Personenbezug hergestellt werden kann.[173] Zudem gilt zu bedenken, dass häufig verwendete Pseudonyme auch einen Wiedererkennungseffekt ggü. Dritten auslösen können. [174] Sie können – je nach konkreten Umständen – daher eine ähnlich identifizierende Wirkung haben, wie der Name. Folglich gilt die Pseudonymisierung zwar als eine Schutzmaßnahme, führt aber regelmäßig nicht zur Unanwendbarkeit des Datenschutzrechts.[175]

[171] *Köllmann*, NZA 2020, 831 (832). *Ernst,* in: Paal/Pauly, DS-GVO Art. 4 Rn. 40; *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 32; *Schmitz*, ZD 2018, 5 (6); a.A. *Roßnagel*, ZD 2018, 243 (244); *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 91.
[172] *Probst*, in: Bäumler/von Mutius, Anonymität im Internet, S. 179 (185).
[173] *Köllmann*, NZA 2020, 831 (832).
[174] vgl. ErwGr. 30 DS-GVO; zu indirekt identifizierenden Kennnummern siehe beispielsweise: EuGH, Urteil vom 20. Dezember 2017 – C-434/16 – Nowak, Rn. 29; zu statischen IP-Adressen: EuGH, Urteil vom 19. Oktober 2016 – C-582/14 – Breyer, Rn. 36; *Golembiewski*, in: Bäumler/von Mutius, Anonymität im Internet, S. 107 (109); *Roßnagel/Scholz*, MMR 2000, 721 (727); *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 102. Zur Verkettbarkeit: *Hansen*, in: Bäumler/von Mutius, Anonymität im Internet, S. 198 (201).
[175] *Ernst,* in: Paal/Pauly, DS-GVO Art. 4 Rn. 40; *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 32; *Schmitz*, ZD 2018, 5 (6); a.A. *Roßnagel*, ZD 2018, 243 (244); *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 91.

2.3.1.2.5 Zwischenfazit zum Personenbezug

Mit der Formulierung „alle Informationen“ wird deutlich, dass der Anwendungsbereich sehr weit gefasst ist und die personenbezogenen Daten vielfältig sein können.[176] Irrelevant sind Fragen dazu, in welcher Form Informationen vorliegen, wie sie gespeichert sind, ob sie neu sind oder wie sensibel diese Daten sind.[177] Geschützt sind natürliche Personen, wobei Unternehmens- und Sachdaten je nach Kontext auch Rückschlüsse auf die dahinter stehende Person zulassen können. Zur genauen Abgrenzung hilft die Prüfung, ob sich Inhalt, Zweck oder Ergebnis der Datenverarbeitung auf eine bestimmte Person beziehen. Zur Feststellung, ob sich die Daten auf eine identifizierbare Person beziehen, müssen alle legal und mit verhältnismäßigem Aufwand zugänglichen Zusatzinformationen berücksichtigt werden – wobei sowohl aktuelle Technologien als auch technologische Entwicklungen berücksichtigt werden müssen. Daher sollten De-Anonymisierungsrisiken regelmäßig evaluiert werden, sofern eine Datenverarbeitung außerhalb des Anwendungsbereichs des Datenschutzrechts stattfinden soll. Sobald eine Identifizierung möglich ist, liegen personenbezogene Daten vor und das Datenschutzrecht wird anwendbar.

2.3.1.3 Ganz oder teilweise automatisierte Verarbeitung

Weiterhin müssen personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden, damit der Anwendungsbereich der DSGVO eröffnet ist. Der Begriff der „Verarbeitung“ wird definiert als:

> **Art. 4 Nr. 2 DSGVO**
>
> jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

Aus dieser Definition ist zu erkennen, dass der Begriff sehr weit auszulegen ist und letztlich jede Form von Datenverarbeitungstätigkeiten umfasst.[178] Dies gilt auch für flüchtige Verarbeitungen.[179] Ebenso gilt zu bedenken, dass auch eine Anonymisierung unter den Verarbeitungsbegriff subsumiert wird.[180] Folglich sind die Grundsätze der DSGVO zunächst auch dann zu beachten, wenn beabsichtigt wird, Daten anonym zu verarbeiten, sofern dies erst über eine Durchzuführende Anonymisierung möglich wird.

Die Differenzierung zwischen einer ganz oder teilweise automatisierten Verarbeitung erfolgt über mögliche händische Zwischenschritte. Eine Teilautomatisierung liegt etwa vor, wenn personenbezogene Daten manuell in eine digitale Datenbank eingegeben werden.[181]

---

[176] EuGH, Urteil vom 20.12.2017 – C-434/16 – Nowak, Rn. 33 ff. m.w.N.
[177] statt vieler: *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 8.
[178] *Kühling/Raab,* in: Kühling/Buchner, DS-GVO Art. 2 Rn. 15; *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 2 Rn. 5; *Roßnagel,* in: NK Datenschutzrecht Art. 2 Rn. 14.
[179] Vgl. insoweit die geänderte Sichtweise des BVerfG zur Rechtfertigungsbedürftigkeit: BVerfGE 150, 309 (330), Rn. 54 – Kfz-Kennzeichenkontrollen BW-HE; BVerfGE 150, 244-309, Rn. 39 – Kfz-Kennzeichenkontrollen Bayern.
[180] *BfDI*, Positionspapierzur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, S. 5; *Roßnagel,* in: NK Datenschutzrecht Art. 4 Nr. 2 Rn. 12; *Klabunde,* in: Ehmann/Selmayr - DSGVO Art. 4 Rn. 23.
[181] *Bäcker,* in: BeckOK DatenschutzR Art. 2 Rn. 3.

2.3.1.4 Nicht automatisierte Verarbeitung

Auch die nichtautomatisierte Verarbeitung personenbezogener Daten unterfällt dem sachlichen Anwendungsbereich der DSGVO, wenn diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der Schutz natürlicher Personen soll technologieneutral sein und daher neben der automatisierten gleichermaßen auch die manuelle Verarbeitung von personenbezogenen Daten umfassen (vgl. Erwägungsgrund 15).[182]

Art. 4 Nr. 6 DSGVO

„Dateisystem" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird

Somit werden grundsätzlich auch alle geordneten manuellen Datenverarbeitungen erfasst, sodass selbst handschriftliche Notizen unter den Anwendungsbereich fallen, sofern diese nach gewissen strukturierenden Kriterien geordnet werden.[183]

2.3.1.5 Unterschiede zwischen privater und dienstlicher Kommunikation

Werden Kommunikations- bzw. Kooperationstools eingesetzt, kann es rechtlich einen Unterschied machen, ob dies zum privaten Austausch im Familien- und Freundeskreis oder zur beruflichen Kommunikation erfolgt. Denn die DSGVO nimmt reine Privatkontexte vom Anwendungsbereich aus.

Art. 2 Abs. 2 Buchst. c) DSGVO

Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,

Art. 2 Abs. 2 DSGVO nennt Ausnahmen vom Anwendungsbereich, bei deren Vorliegen die DSGVO trotz Erfüllung der in Art. 2 Abs. 1 DSGVO genannten Voraussetzungen dennoch keine Anwendung findet. Eine der wichtigen Ausnahmen im Kontext der Kommunikation via Messengerdienst oder sozialen Netzwerken ist in Buchstabe c geregelt. Danach werden Datenverarbeitungen im persönlichen oder familiären Bereich vom Anwendungsbereich der Verordnung ausgenommen. Dies ist dann der Fall, wenn die Datenverarbeitung durch eine natürliche Person „ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird" (EG 18 S. 1 DSGVO). Diese sog. Haushaltsausnahme beruht auf dem Gedanken, dass eine übermäßige Regulierung die freie Entfaltung der Persönlichkeit gefährden könnte und dient somit dem Schutz der Privatsphäre.[184] Dies führt zu unterschiedlichen Konsequenzen bei der Verwendung von Kommunkationslösungen im privaten und im dienstlichen Kontext.[185]

[182] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 2 Rn. 5.
[183] EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 57.
[184] *Bäcker,* in: BeckOK DatenschutzR Art. 2 Rn. 12; *Kühling/Raab,* in: Kühling/Buchner - DS-GVO/BDSG Art. 2 Rn. 10; *Gola/Lepperhoff*, ZD 2016, 9 (11).
[185] Eine Datenverarbeitung, die auch – aber nicht nur – persönlichen Zwecken dient, dürfte dabei nicht privilegiert sein: *Piltz*, K&R 2016, 557 (558).

2.3.2 Räumliche Anwendbarkeit der DSGVO

Art. 3 DSGVO bestimmt die räumliche Anwendbarkeit der DSGVO und ist in drei Absätze aufgeteilt. Dabei sind zwei wesentliche Prinzipien zu unterscheiden: Sitzlandprinzip (Abs. 1) und das Marktortprinzip (Abs. 2).[186]

2.3.2.1 Sitzlandprinzip

Art. 3 Abs. 1 betrifft Sachverhalte, in denen sich die Niederlassung in der Union befindet, die an der Datenverarbeitung beteiligt ist. Das Sitzlandprinzip schreibt die Regelung aus der Datenschutzrichtlinie in Art. 4 Abs. 1 Buchst. a RL 95/46/EG fort.[187] Demzufolge findet die DSGVO auf die Verarbeitung personenbezogener Daten Anwendung, soweit diese seitens eines Verantwortlichen oder Auftragsverarbeiters im Rahmen der Tätigkeit einer Niederlassung in der EU erfolgt. Dabei muss sich die datenverarbeitende Hardware nicht in der Union befinden.[188] Diese Entkopplung zwischen Sitz der Niederlassung und tatsächlichem Ort der Datenverarbeitung ist der zunehmend globalen und vernetzten Verarbeitung der Daten, bspw. in der Cloud, geschuldet. [189] Folglich ist es unerheblich, ob die Verarbeitung selbst in der EU stattfindet. Erfolgt die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit einer in der EU verorteten Niederlassung, ist die DSGVO bereits anwendbar.[190] Sofern das Unternehmen, in dessen (Mit-)Verantwortung die Datenverarbeitung liegt, seinen Sitz innerhalb der EU hat, ist die DSGVO aufgrund des Sitzlandprinzips anwendbar.

2.3.2.2 Marktortprinzip

Die DSGVO erweitert ihren räumlichen Anwendungsbereich auf nicht in der EU niedergelassene Stellen, wenn diese Waren oder Dienstleistungen unentgeltlich oder entgeltlich an betroffene Personen anbieten oder das Verhalten betroffener Person beobachten, auch wenn der Verantwortliche oder Auftragsverarbeiter keine (relevante) Niederlassung in der Union hat (Marktortprinzip).[191] Die betroffenen Personen, deren Daten verarbeitet werden, müssen sich (zumindest vorübergehend) im Unionsgebiet aufhalten, wobei ein (fester) Wohnsitz oder die Unionsbürgerschaft dagegen keine Voraussetzung sind.[192] Mit dem Marktortprinzip wird sichergestellt, dass auch die verantwortlichen Unternehmen, die sich zwar nicht in der Union niedergelassen haben, aber dennoch aktiv in datenschutzrechtlich relevanter Weise am europäischen Binnenmarkt teilnehmen, an die Anforderungen der DSGVO gebunden sind.[193]

Art. 3 Abs. 2 DSGVO

Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der

[186] *Piltz,* in: Gola DS-GVO, Art. 3 Rn. 5.
[187] *Piltz*, K&R 2016, 557 (558).
[188] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG Art. 3 Rn. 7. Eine Niederlassung kann bspw. bereits bei Vorhandensein einer Vertretung und eines Bankkontos in einem Mitgliedstaat gegeben sein: *Piltz*, K&R 2016, 557 (558); *Mausbach*, ZD 2019, 450 (451).
[189] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG Art. 3 Rn. 7.
[190] EuGH, Urt. v. 28.7.2016 – C-191/15 – Verein für Konsumenteninformation, Rn. 74; *Piltz,* in: Gola DS-GVO, Art. 3 Rn. 8.
[191] Zu Auslegungsschwierigkeiten bei Anwendung des Marktotprinzips, wenn eine Niederlassung in der Union existiert, das Sitzlandprinzip aber nicht greift: *Piltz*, K&R 2016, 557 (559). Zur Auslegung des „Beobachtens“: *Mausbach*, ZD 2019, 450 (451).
[192] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 3 Rn. 8; *Zerdick,* in: Ehmann/Selmayr - DSGVO Art. 3 Rn. 17.
[193] *Ennöckel,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 3 Rn. 12; *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG Art. 3 Rn. 16; *Piltz*, K&R 2016, 557 (558).

> Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht
>
> a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
>
> b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

Absatz 3 erstreckt den Anwendungsbereich der DSGVO zudem auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt. Dies bezieht sich insbesondere auf die diplomatischen oder konsularischen Vertretungen eines Mitgliedstaates im Ausland außerhalb der EU.[194]

2.3.3 Sachliche und räumliche Anwendbarkeit des BDSG

Neben bzw. ergänzend zu den Vorgaben der DSGVO können im hier betrachteten Kontext auch relevante Vorgaben aus dem mitgliedstaatlichen Recht – hier dem deutschen Recht – erwachsen. Insofern kommt es auch auf die sachliche und räumliche Anwendbarkeit des BDSG an. Die Rolle des BDSG hat sich mit der Einführung der DSGVO gewandelt, da die DSGVO als EU-Verordnung Anwendungsvorrang genießt und damit das bisherige BDSG a.F. weitgehend verdrängt hätte. Die Aufgabe des novellierten BDSG liegt nun zum einen in der Ausfüllung von Öffnungs- und Konkretisierungsklauseln der DSGVO und zum anderen der Umsetzung der JI-Richtlinie.

2.3.3.1 Sachlicher und persönlicher Anwendungsbereich

Das BDSG gilt gemäß §1 Abs. 1 S. 1 Nr. 1, 2 und S. 2 BDSG für die Verarbeitung personenbezogener Daten durch:

- öffentliche Stellen des Bundes,
- öffentliche Stellen der Länder, in bestimmten Fällen sofern nicht ein Landesgesetz den Datenschutz bereits regelt,
- sonstige Adressaten (nichtöffentliche Stellen), unter denselben Voraussetzungen, die der sachlichen Anwendbarkeit der DSGVO entsprechen.

Öffentlich Stellen sind Stellen, die öffentlich-rechtliche Aufgaben wahrnehmen.[195] Hier gilt das BDSG für sämtliche Formen der Verarbeitung personenbezogener Daten und ist somit weiter als die DSGVO.[196] Für die sonstigen nichtöffentlichen Stellen entspricht die Formulierung des sachlichen Anwendungsbereichs hingegen bewusst der des Art. 2 Abs. 1 Buchst. c DSGVO (inkl. Haushaltsausnahme in Art. 2 Abs. 2 DSGVO), um die sachliche Anwendung des BDSG im Rahmen der Öffnungsklauseln inhaltsgleich zur Anwendung der DSGVO zu gestalten.[197]

[194] *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 3 Rn. 21.
[195] *Gusy/Eichenhofer,* in: BeckOK DatenschutzR, § 1 Rn. 73; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 4.
[196] *Ernst,* in: Paal/Pauly, DS-GVO, § 1 Rn. 2; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 5.
[197] BT-Drs. 18/11325, S. 79; *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 12.

Darüber hinaus gilt das BDSG nach § 26 Abs. 7 BDSG in Beschäftigungsverhältnissen auch für die nicht dateimäßige Verarbeitung personenbezogener Daten (siehe Abschnitt 2.4.1.3.3.2).[198]

2.3.3.2 Räumlicher Anwendungsbereich

Bezüglich der Anwendbarkeit auf öffentliche Stellen bedarf es keiner spezifischen Regelungen zum territorialen Anwendungsbereich (vgl. § 1 Abs. 4 S. 1 BDSG). Für die nichtöffentlichen Stellen gibt § 1 Abs. 4 S. 2 Nr. 1-3 BDSG Auskunft über die Reichweite der räumlichen Anwendbarkeit:

- der Verantwortliche oder Auftragsverarbeiter verarbeitet personenbezogene Daten im Inland,
- die Datenverarbeitung erfolgt im Rahmen der Tätigkeiten einer inländischen Niederlassung des Verantwortlichen oder Auftragsverarbeiters oder
- die Verarbeitung erfolgt im Anwendungsbereich der DSGVO.

Die erste Alternative knüpft an die Belegenheit der IT-Infrastruktur an.[199] Diese steht in gewissem Widerspruch zur DSGVO, welche an die Niederlassung anknüpft und den Ort der Datenverarbeitung selbst bewusst unberücksichtigt lässt.[200] Das BDSG könnte folglich auch in Fällen zur Anwendung kommen, in denen die DSGVO nicht anwendbar ist.[201] Die zweite Alternative entspricht dem Sitzlandprinzip der DSGVO.[202] Die letzte Alternative ist als Verweis auf das Marktortprinzip zu verstehen, d.h. das BDSG kommt auch in Fällen zur Anwendung, in denen zwar keine Niederlassung im Inland besteht, die DSGVO nichtsdestotrotz über Art. 3 Abs. 2 DSGVO anwendbar ist.[203] Im Wege der einschränkenden Auslegung wird angeraten, das BDSG entgegen des als zu weit geraten kritisierten Wortlauts nicht in Fällen anzuwenden, in denen lediglich Bezug zu einem anderen EU-Staat besteht.[204]

Sind die genannten Alternativen nicht einschlägig, so gelten nach § 1 Abs. 4 S. 3 BDSG nichtsdestotrotz die Regelungen zu den Aufsichtsbehörden, Sanktionen und Rechtsbehelfen in den §§ 8-21, 39 und 44 BDSG.[205]

2.3.3.3 Grundsatz der Subsidiarität

Gemäß § 1 Abs. 2 S. 1 BDSG gehen andere Rechtsvorschriften des Bundes über den Datenschutz den Vorschriften des BDSG vor. Das BDSG findet nur insoweit Anwendung, wie die vorrangige Spezialregelung einen Sachverhalt nicht oder nicht abschließend regelt (§ 1 Abs. 2 S. 2 BDSG). In Fällen der Tatbestandskongruenz gehen somit speziellere Regelungen dem BDSG vor, sofern der Regelungsgegenstand deckungsgleich ist.[206] Das BDSG hat folglich den Charakter eines Auffanggesetzes.[207] Es kommt nur zur Anwendung, wenn keine spezifischere Regelung besteht oder diese nicht abschließend ist. Im vorliegenden Unternehmenskontext

---

[198] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 13.
[199] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 29; *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 22 ff.
[200] *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 23; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 18.
[201] *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 24. Da diese Frage außerhalb des Anwendungsbereichs der DSGVO liegt, besteht kein Grund für die Annahme der Europarechtswidrigkeit (str. vgl. *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 30.).
[202] *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 17.
[203] *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 29; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 19; *Ernst,* in: Paal/Pauly - DS-GVO BDSG, § 1 Rn. 12; *Gusy/Eichenhofer,* in: BeckOK DatenschutzR, § 1 Rn. 101c.
[204] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 34; *Ernst,* in: Paal/Pauly - DS-GVO BDSG, § 1 Rn. 12.
[205] *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 19; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 17.
[206] *Schmidt,* in: Taeger/Gabel - DSGVO/BDSG, § 1 Rn. 16; *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 15.
[207] *Ernst,* in: Paal/Pauly - DS-GVO BDSG, § 1 Rn. 6 ff.; *Gola/Reif,* in: Gola/Heckmann - BDSG, § 1 Rn. 11; *Klar,* in: Kühling/Buchner - DS-GVO/BDSG, § 1 Rn. 14.

relevante Spezialregelungen finden sich bspw. in der Abgabenordnung (AO), im Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) oder Kreditwesengesetz (KWG).

§ 1 Abs. 5 BDSG weist auf den aus Art. 288 Abs. 2 AEUV folgenden Anwendungsvorrang des EU-Rechts hin. Dieser Absatz hat lediglich klarstellende Funktion.[208]

2.3.4 Sachliche Anwendbarkeit des Landesdatenschutzrechts

Die Landesdatenschutzgesetze gelten regelmäßig nur für die Verarbeitung personenbezogener Daten durch öffentliche Stellen des jeweiligen Landes.[209] Hierbei handelt es sich zumeist um Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (vgl. § 2 Abs. 1 S. 1 LDSG BW). § 2 Abs. 2 LDSG BW weitetet den Anwendungsbereich in Baden-Württemberg auch auf juristische Personen und sonstige Vereinigungen des privaten Rechts aus, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in § 2 Abs. 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen beteiligt sind.

Für die im Rahmen dieser Studie betrachteten Sachverhalte der Kommunikation im und mit Unternehmen ist das Landesdatenschutzrecht folglich nicht relevant.

2.3.5 Zwischenergebnis zum anwendbaren Recht und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Die Grundlegenden Weichenstellungen zur Anwendbarkeit des Datenschutzrechts setzt die DSGVO. Hierbei ist im Wesentlichen zu klären:

- Werden **personenbezogene Daten** verarbeitet?
  - Im Hinblick auf Messengerdienste sind sowohl Kommunikationsinhaltsdaten als auch Metadaten in den Blick zu nehmen.
  - Bei Anonymisierung ist zu klären, ob Daten hinreichend anonym sind und wie (Re-) Identifizierungsrisiken zu bewerten sind.
- Wer ist der für die Verarbeitung **Verantwortliche:** hat dieser seinen Sitz in der EU (Sitzlandprinzip) oder greift das Marktortprinzip?
  - Die räumliche Anwendbarkeit der DSGVO für den Einsatz von Messengerdiensten gegenüber betroffenen Personen, die sich in der EU aufhalten, dürfte regelmäßig jedenfalls über das Marktortprinzip gegeben sein.

Dem BDSG kommt insbesondere bei der Verarbeitung personenbezogener Daten im Beschäftigtenverhältnis Bedeutung zu, da die DSGVO insoweit in Art. 88 DSGVO eine Öffnungsklausel für Konkretisierungen im mitgliedstaatlichen Recht bereit hält. Im vorliegend betrachteten Kontext der Kommunikation im Unternehmenskontext ist die Datenverarbeitung nach Landes- und Kirchenrecht nicht relevant und soll daher nicht weiter beleuchtet werden.

[208] BT-Drs. 18/11325, S. 80.
[209] Siehe bspw. § 2 Abs. 1 LDSG Baden-Württemberg.

Neuerungen werden sich ab Geltung des TTDSG und TKG (neu) in Deutschland ergeben, da insoweit OTT-Dienste explizit in den Geltungsbereich einbezogen werden sollen. Die Regelungen könnten allerdings ein kurzes Intermezzo darstellen, sofern die EU-ePrivacy-VO verabschiedet wird. Dieser Aspekt wird daher in einem eigenen Kapitel in Kapitel 3 beleuchtet.

2.4 Umsetzung der Datenschutzgrundprinzipien in der Unternehmenskommunikation

Dem Datenschutzrecht liegen wesentliche Grundprinzipien zu Grunde. Diese grundlegenden Datenschutzprinzipien werden in Art. 5 DSGVO festgehalten. Sie gelten für jede Datenverarbeitung unmittelbar, unabhängig davon, ob es sich beim jeweiligen Verantwortlichen oder Auftragsverarbeiter um eine private Stelle oder Träger hoheitlicher Gewalt handelt.[210] Verstöße gegen die Datenschutzgrundprinzipien des Art. 5 DSGVO können Sanktionen gemäß Art. 83 DSGVO nach sich ziehen (siehe Abschnitt 2.6).[211] Zudem werden die Prinzipien durch die Vorgaben der DSGVO sowie – im Rahmen der Öffnungsklauseln – durch das BDSG konkretisiert. Anhand der einzelnen Datenschutzprinzipien sollen im Folgenden der datenschutzrechtliche Pflichtenkanon erläutert werden, welcher für eine datenschutzgerechte Kommunikation im unternehmerischen Kontext erheblich ist.

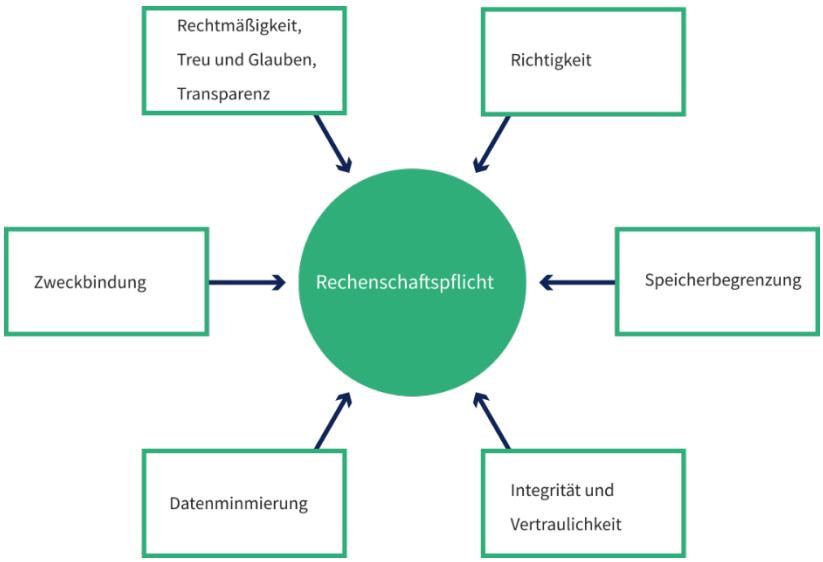


Abbildung 3 Die Datenschutzgrundprinzipien in Art. 5 DSGVO

[210] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 5 Rn. 1.
[211] Zur Verbindlichkeit der Grundprinzipien: *Albrecht*, CR 2016, 88 (91); *Schantz,* in: BeckOK DatenschutzR Art. 5 Rn. 2 m.w.N.

2.4.1 Rechtmäßigkeit, Treu und Glauben

> **Art. 5 Abs. 1 Buchst. a DSGVO**
>
> Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden

Das in Art. 5 Abs. 1 Buchst. a DSGVO kodifizierte Datenschutzprinzip besteht aus drei Teilbereichen: der *Rechtmäßigkeit*, der Verarbeitung nach *Treu und Glauben* und der Nachvollziehbarkeit bzw. *Transparenz*.[212] Die Rechtmäßigkeit der Verarbeitung wird in Art. 6 DSGVO konkretisierend geregelt (bzw. in Art. 9 DSGVO für besondere Kategorien personenbezogener Daten).

Der Grundsatz der Verarbeitung nach Treu und Glauben lässt sich besser mit Grundsatz der „Fairness" umschreiben.[213] Abgestellt werden kann auf die absehbare, vernünftige Erwartungshaltung der betroffenen Person, womit die Gewährleistung einer fairen Verarbeitung verbunden wäre.[214] Diesem Grundsatz kommt insbesondere bei Interessenabwägungen und im Rahmen von Verhältnismäßigkeitserwägungen eine Bedeutung zu.[215] Andere wiederum nennen den Grundsatz zuvörderst im Zusammenhang mit der Transparenz.[216] Erst die Möglichkeit eine Datenverarbeitung nachvollziehen und verstehen zu können, bildet einen Vertrauensanker für eine „faire" Verarbeitung.[217] Gerade die heimliche Datenverarbeitung wird als typischer Verstoß gegen den Fairnessgrundsatz genannt. [218] Der Grundsatz der Transparenz stellt daher Schnittmengen zum Grundsatz von Treu und Glauben dar und wird an vielen Stellen der DSGVO präzisiert. Dieser Grundsatz wird in einem separaten Abschnitt näher erläutert (siehe Abschnitt 2.4.2).

2.4.1.1 Verbot mit Erlaubnisvorbehalt

Grundlage jeder Datenverarbeitung muss, folgt man der engeren Auslegung des Begriffs Rechtmäßigkeit,[219] eine der in Art. 6 Abs. 1 DSGVO genannten Legitimationsgrundlagen sein. Dies entspricht dem Prinzip des Verbots mit Erlaubnisvorbehalt, welches die Datenverarbeitung, die im sachlichen und räumlichen Anwendungsbereich gemäß Art. 2, 3 DSGVO liegt, grundsätzlich verbietet, es sein denn, einer der in Art. 6 Abs. 1 DSGVO geregelten Erlaubnistatbestände liegt vor. Dies folgt auch aus der Tatsache, dass der EuGH bereits jegliche Form der Verarbeitung personenbezogener Daten als Eingriff in den Schutzbereich des Art. 8 Abs. 1 EU-GrCh wertet.[220]

---

[212] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 5 Rn. 3.
[213] *Schantz*, in: BeckOK DatenschutzR Art. 5 Rn. 7; *Herbst*, in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 14; *Frenzel*, in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 18; vgl. *Albrecht*, CR 2016, 88 (91).
[214] *Spindler/Dalby*, in: Recht der elektronischen Medien Art. 5 Rn. 5; *Schantz*, in: BeckOK DatenschutzR Art. 5 Rn. 8.
[215] *Spindler/Dalby*, in: Recht der elektronischen Medien Art. 5 Rn. 5.
[216] Im Hinblick auf den gleichlautenden Grundsatz im Rahmen der grundrechtlichen Verbürgung des Art. 8 EU-GrCh: *Purtova*, Property rights in personal data, S. 152; *Marsch*, Das europäische Datenschutzgrundrecht, S. 170 ff. vgl. zur Ableitung der Informationspflichten aus dem sekundärrechtlich verankerten Grundsatz von Treu und Glauben: EuGH, Urteil vom 01. Oktober 2015 – C-201/14 – Bara, Rn. 34.
[217] *Wagner,* Datenökonomie und Selbstdatenschutz, S. 234.
[218] *Schantz,* in: BeckOK DatenschutzR Art. 5 Rn. 8; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 15; *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 18; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 45; *Reimer*, in: Sydow, Europäische Datenschutzgrundverordnung Art. 5 Rn. 14.
[219] Zum wissenschaftlichen Streit: *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 5 Rn. 4 m.w.N.
[220] EuGH, Urteil vom 08. April 2014 – C-293/12 – Digital Rights Ireland, Rn. 36; EuGH, Urteil vom 17. Oktober 2013 – C-291/12 – Schwarz, Rn. 25; EuGH, Urteil vom 21. Dezember 2016 – C-203/15 und C-698/15 – Tele2 Sverige, Rn. 100; *Franzen,* in: Franzen/Gallner/Oetker,

2.4.1.2 Legitimationsgrundlagen der DSGVO

Die Notwendigkeit für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage heranziehen zu müssen, geht zurück auf die Datenschutzgrundrechte und wird im Rahmen der DSGVO durch den Grundsatz der Rechtsmäßigkeit in Art. 5 Abs. 1 Buchst. a sowie die Regelungen in Art. 6 Abs. 1 und Art. 9 Abs. 1, 2 DSGVO unterstrichen. Je nach Verarbeitungskontext kommen unterschiedliche Legitimationstatbestände in Betracht. Ob und unter welchen Bedingungen diese beim Einsatz von Kommunikationstools im Unternehmenskontext tatsächlich erfüllt sind, soll im Kapitel 5 weiter beleuchtet werden.

2.4.1.2.1 Einwilligung

Art. 6 Abs. 1 Buchst. a DSGVO

Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

Art. 4 Nr. 11 DSGVO

„Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Die Einwilligung ist in Art. 6 Abs.1 DSGVO an erster Stelle der Erlaubnistatbestände als Ausdruck datenschutzrechtlicher Selbstbestimmung normiert.[221] Damit sollte die betroffene Person in die Lage versetzt werden, privatautonom über das „Ob" und „Wie" der Verarbeitung ihrer personenbezogenen Daten zu bestimmen. Der Grundgedanke besteht darin, dass demjenigen kein Unrecht geschieht, der „sich mit klarem Kopf, hinreichend informiert und ohne Zwang" eine bestimmte Datenverarbeitung ausgesucht hat.[222] Entsprechend müssen aber auch die Anforderungen an eine wirksame Einwilligung erfüllt sein, um legitimierend zu wirken.

Die DSGVO schreibt dabei keine bestimmte Form für das Erteilen einer Einwilligung vor.[223] Erwägungsgrund 32 S. 1 stellt sogar die elektronische und mündliche Erklärung der Schriftform gleich. Der Verantwortliche hat also grundsätzlich eine freie Auswahl, welches Formverfahren er anwenden möchte, trägt aber die Nachweispflicht dafür, dass eine wirksame Einwilligung der betroffenen Person vorliegt, Art. 7 Abs. 1 DSGVO.[224] Daher wird zu Dokumentationszwecken von konkludenten oder mündlichen Einwilligungen zumeist eher abgeraten – auch wenn diese grundsätzlich wirksam wären.[225]

2.4.1.2.1.1 Wirksamkeitsvoraussetzungen

Die Wirksamkeitsvoraussetzungen einer Einwilligung sind in Art. 4 Nr. 11, Art. 6 Abs. 1 Buchst. a und Art. 7

EuArbR Art. 8 GRC Rn. 7; *Jarass*, Charta der Grundrechte der Europäischen Union Art. 8 Rn. 8; *Gersdorf,* in: BeckOK InfoMedienR Art. 8 EU-GrCharta Rn. 18; *Bieker*, DuD 2018, 27 (28); *Roßnagel*, NJW 2019, 1 (2).

[221] *Schulz,* in: Gola DS-GVO, Art. 6 Rn. 21. Aus dieser Stellung folgt allerdings keine Vorrangwirkung, a.A. *Sattler*, JZ 2017, 1036 (1040).

[222] *Samardzic/Becker*, EuZW 2020, 646 (649).

[223] EuGH, Urteil vom 1. Oktober 2019, Az. C-673/17 – Planet49; *Ziebarth/Elsaß*, ZUM 2018, 578 (579).

[224] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 22.

[225] *Steege*, MMR 2019, 509 (511).

Abs. 1-4 DSGVO geregelt. Danach müsste eine wirksame Einwilligung folgende Kriterien erfüllen:

2.4.1.2.1.1.1 Bestimmt

Die betroffene Person muss ihre Einwilligung „für einen oder mehrere Zwecke“ geben. Diese Zwecke müssen so präzise wie möglich beschrieben werden. Eine pauschale Einwilligung ist stets unwirksam.[226] Die betroffene Person muss nach Ansicht des EDSA in Bezug auf jeden dieser Zwecke eine Wahlmöglichkeit haben.[227] Dies erfordert:

- Spezifizierung des Zwecks als Schutz vor schleichender Funktionserweiterung,
- Granularität bei Einwilligungsanfragen und
- Klare Trennung von Informationen, die sich auf die Einwilligung beziehen, von Informationen über andere Angelegenheiten.[228]

2.4.1.2.1.1.2 Informiert

Die Einwilligung muss auch „in informierter Weise“ abgegeben werden. D. h. vor der Datenverarbeitung muss die betroffene Person wissen und verstehen, auf welche personenbezogene Daten sich die Einwilligung bezieht, was mit den Daten geschehen soll und wer für die Datenverarbeitung verantwortlich ist (Erwägungsgrund 42 S. 4 DSGVO).[229] Dafür muss die Datenschutzerklärung in verständlicher und leicht zugänglicher Form und in klarer, einfacher Sprache erfolgen. Betrifft die Datenschutzerklärung mehrere Sachverhalte, sind die jeweilige Sachverhalte eindeutig voneinander zu unterscheiden, Art. 7 Abs. 2 DSGVO. In der Praxis gilt allerdings zu bemängeln, dass dies gerade bei umfangreicher Datenverarbeitungspraxis zu großer Informationsflut führt.[230] Insofern werden auch Zweifel geäußert, ob das Anliegen der Informiertheit so erreicht wird.[231] Der EDSA nennt die folgenden Angaben als Mindestset an Informationen:[232]

- Identität des Verantwortlichen
- Zweck der Datenverarbeitung
- Welche (Art von) Daten erfasst sind
- Bestehen des Widerrufsrechts

---

[226] *Buchner/Kühling,* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 62; *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 8; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 39; *Stemmer,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 7 Rn. 76.; *Ernst,* in: Paal/Pauly - DS-GVO BDSG Art. 4 Rn. 78. Zu Ausnahmen in der Forschung vgl. Erwägungsgrund 33.

[227] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 13.

[228] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 14.

[229] *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 34.

[230] *Samardzic/Becker*, EuZW 2020, 646 (651). Zu Optionen gestufter Informationskonzepte: *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 40. Negativbeispiel bei: LG Frankfurt, Urteil vom 10.06.2016 – 2-3 O 364/15.

[231] *Hermstrüwer*, Informationelle Selbstgefährdung, S. 282 ff.; *Wagner*, Datenökonomie und Selbstdatenschutz, S. 354; vgl. auch zur Kosten-Zeitaufwand-Relation: *McDonald/Cranor*, ISJLP 2008, 543; *Acquisti/Grossklags*, IEEE Security and Privacy Magazine 2005, 26.

[232] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 15.

- Sofern einschlägig: Informationen über automatisierte Entscheidungsfindung
- zu den möglichen Risiken von Datenübermittlungen (auch aufgrund des Fehlens eines Angemessenheitsbeschlusses oder geeigneter Garantien)

2.4.1.2.1.1.3 Durch eine aktive Handlung

Für eine wirksame Einwilligung ist stets eine Erklärung oder eine sonstige eindeutig bestätigende Handlung erforderlich.[233] Erwägungsgrund 32 S. 3 erläutert diese Voraussetzung dahingehend, dass Stillschweigen oder vorangekreuzte Kästchen nicht genügen. Auch der EuGH stellte klar, dass nur ein Opt-In eine wirksame Einwilligung darstellt – ein Opt-Out hingegen nicht.[234]

2.4.1.2.1.1.4 Freiwillig

Eine wirksame Einwilligung muss freiwillig erfolgen, d. h. ohne jeden Zwang oder Druck.[235] Dies ist dann nicht der Fall, wenn die betroffene Person faktisch keine andere Wahl hat, als der Datenverarbeitung zuzustimmen (vgl. EG 42 S. 5). Um in den Genuss einer Dienstleistung oder einer anderen vertraglichen Leistung zu kommen, könnte oftmals keine realistische Möglichkeit bestehen, die Einwilligung zu verweigern oder zurückzuziehen.[236] Ebenso übermäßige Anreize können die Freiwilligkeit gefährden.[237] Eine wirksame Einwilligung ist auch zu verneinen, wenn die Beziehung zwischen der betroffenen Person und dem Verantwortlichen von einem klaren Ungleichgewicht geprägt ist und deshalb die Einwilligung mutmaßlich unfreiwillig erfolgte.[238] Eine Unfreiwilligkeit kann laut EG 43 insbesondere in folgenden Fällen vorliegen:

Machtasymmetrien	Pauschaleinwilligung	Kopplungsverbot
Es besteht ein klares Ungleichgewicht zwischen Verantwortlichem und betroffener Person. Es handelt sich bei dem Verantwortlichen um eine Behörde.	Es ist nicht möglich eine gesonderte Einwilligung in verschiedene Verarbeitungsvorgänge zu geben, obwohl dies im Einzelfall angebracht wäre.	Die Einwilligung ist Bedingung für einen Vertrag (einschließlich einer Dienstleistung), für deren/dessen Erfüllung die Datenverarbeitung nicht erforderlich ist

Abbildung 4 Beispiele für Unfreiwilligkeit der DSGVO

[233] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 18.
[234] EuGH, Urteil vom 1. Oktober 2019, Az. C-673/17 – Planet49.
[235] *Stemmer,* in: BeckOK DatenschutzR Art. 7 Rn. 39; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 26 f. *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 21.
[236] *Stemmer,* in: BeckOK DatenschutzR Art. 7 Rn. 40; *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 7 Rn. 14.
[237] LG Stuttgart, Urteil vom 13. August 1998 – 17 O 329/98 –, Rn. 30; offen gelassen OLG Stuttgart, Urteil vom 27. November 1998 – 2 U 111/98 –, Rn. 34; *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 15, 82 ff. Siehe auch zur sittenwidrigen Kopplung von Gewinnspielen mit dem Warenabsatz aufgrund psychischen Kaufzwangs: BGH, Urteil vom 05. Februar 1998 – I ZR 151/95 – Rubbelaktion, Rn. 15; BGH, Urteil vom 16. März 1989 – I ZR 241/86 – Gewinnspiel, Rn. 44; BGH, Urteil vom 19. Dezember 1975 – I ZR 120/74 – Versandhandels-Preisausschreiben, Rn. 31.
[238] Statt vieler: *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 7 Rn. 17.

Machtasymmetrien: Explizit genannt werden Behörden, da im Bürger-Staat-Verhältnis zu vermuten ist, dass Bürger*innen bei behördlichen Maßnahmen kaum ausreichende Entscheidungsspielräume verbleiben.[239] Die Einwilligung ist zwar nicht generell ausgeschlossen, es besteht aber ein erhöhter Prüfungs- und Begründungsaufwand.[240] Typische Konstellationen sind Monopolstellungen.[241] Besondere Abhängigkeiten bestehen zudem bei wichtigen Leistungen, wie im Bereich der Daseinsvorsorge.[242] Eine weitere Unsicherheit besteht im Hinblick auf die Freiwilligkeit im Arbeitsverhältnis.[243] Zwar hatte die EU-Kommission die Einwilligungsmöglichkeit im Arbeitsverhältnis in ihrem DSGVO-Entwurf noch ausgeschlossen.[244] Diese Einschränkung wurde allerdings für die finale Fassung gestrichen. Nichtsdestotrotz werden vom Arbeitgeber gewünschte Datenverarbeitungen als typische die Entschließungsfreiheit hemmende Konstellationen eines Machtungleichgewichts genannt.[245] Der deutsche Gesetzgeber hat diese Frage im Rahmen der Öffnungsklausel des Art. 88 DSGVO für den Bereich des Beschäftigungsverhältnisses spezifisch in § 26 Abs. 2, 3 BDSG adressiert (siehe hierzu ausführlich in Abschnitt 2.4.1.2.1.2). Aber auch sozialer Druck (bspw. zur Mithilfe bei der Eindämmung einer Pandemie) kann zu faktischen Zwängen führen.[246] Ebenso sollten Netzwerkeffekte und Lock-In-Effekte gerade im Bereich sozialer und/oder beruflicher Interaktion nicht unterschätzt werden.[247] Auch solche Zwangslagen angemessen zu berücksichtigen, erscheint aus verfassungsrechtlicher Sicht geboten.[248]

Pauschaleinwilligungen: Der Grundsatz der „differenzierten Einwilligung" gebietet es, dass mehrere voneinander getrennte Datenverarbeitungsvorgänge nicht lediglich unter eine pauschale Einwilligungsoption gestellt werden dürfen.[249] Ist die getrennte Einwilligungsmöglichkeit in verschiedenen Datenverarbeitungsvorgängen nicht möglich, obwohl es im konkreten Kontext angebracht wäre, wird das Fehlen der Freiwilligkeit vermutet.[250]

Kopplungsverbot: Besonders umstritten ist im Zusammenhang mit der Auslegung des Merkmals der Freiwilligkeit das in Art. 7 Abs. 4 DSGVO normierte sog. „Kopplungsverbot".[251] Dieses besagt, dass bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung getragen werden muss, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Folglich handelt es sich bereits dem Wortlaut nach nicht

---

[239] Differenzierend zwischen Eingriffsverwaltung und schlicht-hoheitlichem Handeln: *Samardzic/Becker*, EuZW 2020, 646 (652).
[240] Statt vieler: *Samardzic/Becker*, EuZW 2020, 646 (652).
[241] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 7 Rn. 17.
[242] Vgl. zur Forderung einer eDaseinsvorsorge: *Luch/Schulz*, MMR 2009, 19. Für eine Art „soziale Grundversorgung": *Kamp/Rost,* DuD 2013, 80 (82).
[243] *Samardzic/Becker*, EuZW 2020, 646 (652); für Einwilligungsmöglichkeiten: *Brink/Schwab*, ArbRAktuell 2018, 111 (113).
[244] Erwägungsgrund 34 in: EU-Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Brüssel, den 25.1.2012, KOM (2012) 11 final.
[245] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 7; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 27.
[246] *Samardzic/Becker*, EuZW 2020, 646 (652).
[247] Zu Netzwerkeffekten: *Monopolkommission*, Wettbewerb 2018, S. 243; *Monopolkommission*, Sondergutachten 68: Wettbewerbspolitik: Herausforderung digitale Märkte, S. 33; zu den Nutzungszahlen siehe: *Engels*, Datenschutzpräferenzen von Jugendlichen in Deutschland, S. 10.
[248] *Samardzic/Becker*, EuZW 2020, 646 (652).
[249] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 12; *Krohm*, ZD 2016, 368 (373).
[250] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 12; *Krohm*, ZD 2016, 368 (373).
[251] Zum Streit siehe: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 312 ff.

um ein Verbot im engeren Sinne.[252] Nichtsdestotrotz plädiert u.a. der EDSA für die Annahme einer vergleichbaren Wirkung.[253] In der Gesamtschau mit den Erwägungsgründen 42, 43 sei praktisch ein Verbot beabsichtigt. [254] Gefordert wird, dass jede Art von Nachteil berücksichtigungsfähig sein sollte, unerheblich, ob es sich um einen materiellen oder immateriellen Nachteil handelt.[255] Daraus sei ein *Regel-Ausnahme-Verhältnis* dergestalt zu entnehmen, dass eine Vermutung der Unfreiwilligkeit im Fall einer Kopplung als Regel gleichwohl die Möglichkeit der Einwilligung in vertragsfremde Zwecke als Ausnahme nicht vollständig ausschließt.[256]

Erwägungsgrund 42 S. 5

Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

Der Gegenansicht nach handelt es sich lediglich um eine Auslegungshilfe, da sich ein striktes Kopplungsverbot in den Verhandlungen zur DSGVO eben nicht durchgesetzt hätte.[257] Dabei wird u. a. vertreten, dass die Erwägungsgründe restriktiv auszulegen seien, denn ein Nachteil bei Verweigerung oder Widerruf der Einwilligung könne nur bei schwerwiegenden Folgen, aber nicht bei bloßen Unannehmlichkeiten wie der Nichtgewährung von Preisnachlässen oder privatautonomer Ablehnung eines Vertragsschlusses angenommen werden – jedenfalls sofern keine monopolartigen Strukturen oder ein Fall der Daseinsvorsorge gegeben sei.[258] Somit müssten bei wertender Betrachtung entsprechende Drucksituation in die Beurteilung mit einbezogen werden.[259] Der Schutzzweck der Regelung greife erst bei Nachteilen „von gewissem Gewicht“,[260] dem Ausnutzen einer „starken Position“,[261] der Vorenthaltung einer informatorisch-kommunikativen Grundversorgung[262]

[252] *Brockmeyer*, ZD 2018, 258 (262); *Dammann*, ZD 2016, 307 (311); *Engeler*, ZD 2018, 55 (58); *Franzen,* in: Franzen/Gallner/Oetker, EuArbR Art. 7 DS-GVO Rn. 9; *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 18; *Heckmann/Paschke,* in: Ehmann/Selmayr - DSGVO Art. 7 Rn. 95; *Kugelmann*, DuD 2016, 566 (567); *Schantz*, NJW 2016, 1841 (1845); *Schätzle*, PinG 2017, 203 (205); *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 22; *Spindler*, JZ 2016, 805 (807); *Wybitul u. a.*, ZD 2017, 503 (507); *Schneider*, Datenschutz, S. 162.

[253] *Albrecht*, CR 2016, 88 (91); *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 71 Rn. 44; *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 8f.; *Dammann*, ZD 2016, 307 (311); *Härting*, CR 2016, 735 (739); *Härting*, Datenschutz-Grundverordnung, S. 96 Rn. 392; *Krauß u. a.*, DuD 2017, 217 (219); *Krönke*, Der Staat 2016, 319 (327); *Krohm*, ZD 2016, 368 (373).

[254] *Dammann*, ZD 2016, 307 (311); so wohl im Ergebnis auch: *Gierschmann*, ZD 2016, 51 (54); *Wybitul*, ZD 2016, 203 (205); *Wybitul*, BB 2016, 1077 (1081).

[255] *Härting*, Datenschutz-Grundverordnung, S. 97 Rn. 398; *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 10.

[256] ÖOGH, Urteil vom 31.8.2018 – 6 Ob 140/18h, Rn. 46, ZD 2019, 72 (73); *Albrecht*, CR 2016, 88 (91); *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 9; *Ernst*, ZD 2017, 110 (112); *Härting*, CR 2016, 735 (739); *Härting*, Datenschutz-Grundverordnung, S. 96 Rn. 394; *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, S. 88 Rn. 20; *Schätzle*, PinG 2017, 203 (205); *Schantz*, NJW 2016, 1841 (1845).

[257] *Kugelmann*, DuD 2016, 566 (567); *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 18; *Engeler*, ZD 2018, 55 (58f.); *Schneider*, Datenschutz, S. 164 ff.; *Gola*, K&R 2017, 145 (147); *Selk*, DANA 2016, 59 (61); *Klement,* in: NK Datenschutzrecht Art. 7 Rn. 58.

[258] *Schulz* in: Gola DS-GVO Art. 7 Rn. 26; *Gola*, K&R 2017, 145 (147); *Klement,* in: NK Datenschutzrecht Art. 7 Rn. 62; ähnlich *Plath,* in: Plath, DSGVO/BDSG Art. 7 Rn. 19 f.

[259] *Kugelmann*, DuD 2016, 566 (567); *Schulz,* in: Gola DS-GVO, Art. 7 Rn. 22; *Stemmer,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 7 Rn. 42; *Plath,* in: Plath, DSGVO/BDSG Art. 7 Rn. 19. *Engeler* nimmt hingegen eine Prüfpflicht an. Der Regulierungsintention entgegensetzend argumentiert er, dass aus der Regelung zunächst die grundsätzliche Anerkennung der Überschreitbarkeit der Erforderlichkeitsgrenze durch eine Einwilligung folge: *Engeler*, ZD 2018, 55 (59).

[260] *Stemmer,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 7 Rn. 38.

[261] Eine starke Position sei anzunehmen, wenn der Verantwortliche die Vertragserfüllung von der Einwilligungserteilung abhängig machen kann und es dem Betroffenen nicht freisteht, die gewünschte Leistung anderweitig zu erhalten: *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 20.

[262] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 165 Die Grundversorgung sei bei Telefon- und Internetzugang erfüllt. Dagegen zählt *Gola* den Personenverkehr, die Versorgungswirtschaft, das Versicherungswesen und soziale Netzwerke zu Formen von relevanten, monopolartigen Angeboten, die das Kopplungsverbot eröffnen sollten: *Gola*, K&R 2017, 145 (147).

oder „sachfremde“ Kopplungen.[263] Eine freie Wahl könne aber auch bei Verzicht auf einen Dienst ausgeübt werden.[264] Eine Kommerzialisierung der Einwilligung in Form der Gegenleistung für eine vermeintlich kostenlose Leistung solle weiterhin möglich bleiben, soweit die Wahl dieses Vertragsmodells freiwillig erfolge.[265]

2.4.1.2.1.1.5 Widerrufbar

Gemäß Art. 7 Abs. 3 S. 1 DSGVO haben betroffene Personen das Recht, jederzeit ihre Einwilligung zu widerrufen. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein. Ferner ist die betroffene Person vor Abgabe der Einwilligung über ihr Widerrufsrecht zu belehren, Art. 7 Abs. 3 S. 3 DSGVO.

Umstritten ist, ob eine auf der Einwilligung beruhende Datenverarbeitung nach Widerruf auf eine andere Legitimationsgrundlage gestützt werden kann.[266] Da dem Grenzen gesetzt sind, sollten von Beginn an Datenverarbeitungen nur dann auf die Einwilligung gestützt werden, wenn eine Verarbeitung nach Widerruf unterbleiben kann. Erfordert die Erfüllung einer vertraglichen Pflicht oder Erbringung einer Dienstleistung eine fortgeführte Verarbeitung dieser Daten, war die Einwilligung offensichtlich nicht die richtige Wahl. Liegt eine andere Rechtsgrundlage vor, sollten zudem keine zusätzlichen Einwilligungen „zur Absicherung“ eingeholt werden, um das Instrument der Einwilligung nicht zum rein formalisierten Akt verkommen zu lassen.[267] Werden personenbezogene Daten im Rahmen einer vertraglich geschuldeten Diensterbringung auf Grundlage der Einwilligung erhoben, muss es sich um optionale Daten handeln.

2.4.1.2.1.2 Sonderfall: Einwilligung im Arbeitsverhältnis

Das Erteilen einer Einwilligung im Arbeitsverhältnis weist einige Besonderheiten auf. Erwägungsgrund 155 DSGVO räumt den Mitgliedstaaten insofern die Möglichkeit ein, Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen zu erlassen.[268]

2.4.1.2.1.2.1 Materielle Voraussetzungen

§ 26 Abs. 2 BDSG ergänzt und konkretisiert die DSGVO-Vorschriften zur Einwilligung in Artt. 4 Nr. 11, 6 Abs. 1 Buchst. a und Art. 7 sowie Art. 8 und Art. 9 Abs. 2 Buchst. a DSGVO.

---

[263] *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 18; *Schulz,* in: Gola DS-GVO Art. 7 Rn. 25; *Gola*, K&R 2017, 145 (147).
[264] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 165.
[265] *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 33; *Schulz,* in: *Gola*, Gola DS-GVO Art. 7 Rn. 23; *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (91); *Frenzel,* in: Paal/Pauly, DS-GVO Art. 7 Rn. 21; *Malgieri*, International Review of Law, Computers & Technology 2018, 118 (129); *Plath,* in: Plath, DSGVO/BDSG Art. 7 Rn. 21; *Heckmann/Paschke,* in: Ehmann/Selmayr - DSGVO Art. 7 Rn. 96; *Buchner/Kühling,* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 51.
[266] Siehe Abschnitt 2.4.6.1.1.
[267] Zur Beobachtung einer Art „Klickermüdung“: *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 17; vgl. auch die Befürchtung eines „Choice Overload“: *Hermstrüwer*, Informationelle Selbstgefährdung, S. 369; *Richter*, PinG 2018, 6 (7). Zu Problemen der Einwilligung: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 310 m.w.N.
[268] Vgl. BT-Drs. 18/11325, S. 97.

§ 26 Abs. 2 S. 1, 2 BDSG

Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Aufgrund der abhängigen Stellung der Beschäftigten ist die Möglichkeit einer Einwilligung im Beschäftigtenkontext rechtspolitisch höchst umstritten.[269] § 26 Abs. 2 BDSG versucht diesen Bedenken Rechnung zu tragen, da besondere Beurteilungskriterien für die Freiwilligkeit genannt werden:

- Grad der Abhängigkeit,
- Umstände des Einzelfalls,
- rechtliche oder wirtschaftliche Vorteile,
- gleichgelagerte Interessen.
- Bei den Umständen des Einzelfalls sollten neben der Art der betroffenen Daten und der Eingriffstiefe auch der Zeitpunkt der Einwilligungserteilung bedacht werden.[270] So nennt die Gesetzesbegründung als Beispiel größerer Drucksituationen die Zeit vor Abschluss eines Arbeitsvertrags.[271]
- Als Fälle eines rechtlichen oder wirtschaftlichen Vorteils zählt der Gesetzgeber ein betriebliches Gesundheitsmanagement zur Gesundheitsförderung oder der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen auf.[272] Gleichgelagerte Interessen lägen bei einer Geburtstagliste oder Nutzung von Fotos im Intranet zur Umsetzung eines „betrieblichen Miteinanders“ vor.[273]

2.4.1.2.1.2.2 Formelle Voraussetzungen

Die Einwilligung wurde zunächst unter den Grundsatz des Schriftformerfordernisses gestellt (Abweichungen möglich). Umstritten war, ob hierin ein Verstoß gegen die DSGVO liegt, da zusätzliche Kriterien gegenüber der Einwilligung nach EU-Recht aufgestellt wurden.[274] Zudem wurde kritisiert, dass damit digitale Einwilligungsmanagementlösungen verhindert werden.[275] Entsprechend der Zielsetzung alle Gesetze auf Digitaltauglichkeit zu überprüfen, wurde mit dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz die elektronische Form hinzugefügt.[276]

§ 26 Abs. 2 S. 3, 4 BDSG

Die Einwilligung hat **schriftlich** oder **elektronisch** zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form

[269] *Artikel-29-Datenschutzgruppe*, Opinion 2/2017 on data processing at work - WP 249, S. 23.; dagegen grundsätzlich anerkannt: BAG, Urteil vom 11. 12. 2014 – 8 AZR 1010/13, NJW 2015, 2140.
[270] BT-Drs. 18/11325, S. 97.
[271] BT-Drs. 18/11325, S. 97.
[272] BT-Drs. 18/11325, S. 97.
[273] BT-Drs. 18/11325, S. 97.
[274] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 73.
[275] *Brecht u. a.*, PinG 2018, 10 (13).
[276] BT-Drs, 19/11181, S. 19.

angemessen ist.

Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht […] **in Textform** aufzuklären.

2.4.1.2.1.3 Zwischenergebnis zur Einwilligung und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Der Ausspruch „Mit der „Einwilligung“ geht eben alles – oder jedenfalls fast alles.“[277] gilt nach wie vor für wirksame Einverständniserklärungen der betroffenen Person. Wie weit die Schutzwirkung der Einwilligung reicht, hängt maßgeblich von der Auslegung der Wirksamkeitsvoraussetzungen, vornehmlich dem Merkmal der Freiwilligkeit, ab. Sowohl für Messengerdienstanbieter als auch Unternehmen bestehen insofern bis zu einer abschließenden höchstrichterlichen Entscheidung gewisse Rechtsunsicherheiten, wenn sie die von ihnen verantwortete Datenverarbeitung auf eine Einwilligung stützen wollen.

Die Einwilligung in die Verarbeitung von personenbezogenen Daten im Rahmen der Nutzung eines Messengerdienstes, welche für die Erbringung des Dienstes selbst nicht erforderlich ist, dürfte jedenfalls – auch bei enger Auslegung – in folgenden Fällen als unfreiwillig gewertet werden:

- dem Messengerdienst kommt eine Monopolstellung zu, es bestehen keine/kaum vergleichbare Wechselalternativen,
- Netzwerkeffekte führen zu einem Lock-In-Effekt, sodass ein Wechsel auf einen anderen Messengerdienst bzw. ein anderes Kommunikationsmedium zwar theoretisch möglich, aber faktisch ausgeschlossen ist,[278]
- Fälle der Daseinsvorsorge. Insofern wird diskutiert, ob eine „soziale Grundversorgung“ bei Messengerdiensten oder sozialen Medien anzunehmen ist, ohne deren Zugang eine kommunikative Ausgrenzung zu befürchten wäre.[279]

Gerade bei solchen Messengerdiensten, welche keine interoperablen Schnittstellen zu Konkurrenzprodukten bereitstellen und deren Beliebtheit mit der Anzahl der Nutzenden steigt, kann die Befürchtung einer Einschränkung der sozialen, auf digitaler Kommunikation basierenden Anbindung an das lebensnotwendige soziale Umfeld dazu führen, dass die Einwilligungserklärung kaum noch Ausdruck der Selbstbestimmung ist, sondern vielmehr zur bloßen Zustimmungsfiktion verkommt.[280] Art. 7 Abs. 4 DS-GVO steht einer Einwilligung hingegen dann nicht entgegen, wenn zumutbare, alternative Zugangsmöglichkeiten ohne Einwilligungserfordernis zur Verfügung stehen.[281] Dies wäre der Fall, wenn ein gleiches Angebot desselben Anbieters auch ohne Einwilligung bereitgestellt wird – sofern dieses nicht unangemessen teurer ausfällt.[282] Andere wollen auch ein vergleichbares

[277] *Samardzic/Becker*, EuZW 2020, 646 (648).
[278] Vgl. hierzu: *Schantz*, NJW 2016, 1841 (1845). *Schwartmann/Hentsch*, RDV 2015, 221 (228); *Kamp/Rost*, DuD 2013, 80 (82); a.A. *Buchner*, DuD 2010, 39 (41).
[279] *Kamp/Rost*, DuD 2013, 80 (82).
[280] *Kamp/Rost*, DuD 2013, 80 (82); *Roßnagel u. a.*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, S. 91; *Seidel*, ZG 2014, 153 (155).
[281] *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 33; *Metzger*, AcP 2016, 817 (824); *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 101; *Krohm/Müller-Peltzer*, ZD 2017, 551 (553); *Heckmann/Paschke,* in: Ehmann/Selmayr - DSGVO Art. 7 Rn. 96; *Schafft/Ruoff*, CR 2006, 499 (504).
[282] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 9; *Gierschmann*, ZD 2016, 51 (54). *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 71 Rn. 44. *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 101.

Angebot von Drittanbietern als ausreichend gelten lassen.[283] Hinzu kommt, wenn in einem monopolistisch oder oligopolistisch geprägten Markt mit geringen Ausweichmöglichkeiten der berufliche oder soziale Status tangiert ist.[284] Insofern treffen bei der Nutzung von Messengerdiensten im Unternehmen mehrere wesentlich die Freiwilligkeit hemmende Faktoren aufeinander: die durch Gruppendynamik entstehende Abhängigkeit von einer Leistung (Netzwerkeffekte, Lock-In), die Bedeutung für die Teilhabe an digitalen Kommunikationsprozessen sowie das Abhängigkeitsverhältnis und die Weisungsgebundenheit im Beschäftigungsverhältnis.

Intensiv wurde die Frage eines mittelbar wirkenden Zwangs in Dreieckskonstellationen Arbeitgeber – betroffene Person – Verantwortlicher/Dienstanbieter im Rahmen der Corona-Warn-Apps diskutiert.[285] Insofern ist hierbei zu klären, ob externe Effekte dem Verantwortlichen zurechenbar sind.[286] Die Frage ist nicht leicht zu beantworten, ob selbst bei erheblichem externem Druck die gesetzlichen Minimalanforderungen der DSGVO erfüllt sind, oder ob hier eine Einwilligung schlechthin ausscheidet.[287] Insofern könnte zwischen einer dienstlichen Anordnung und einer Empfehlung durch den Arbeitgeber differenziert werden – wobei auch letztere sozialen Druck ausüben kann.[288]

Als Zwischenergebnis lässt sich folgendes festhalten: Möchte ein Unternehmen die Nutzung eines Messengerdienstes eröffnen, anregen oder gar anordnen, und dieser Dienst auf einer Einwilligung zur Legitimation der Datenverarbeitung basiert, bestehen erhebliche Zweifel an der Wirksamkeit einer solchen Einwilligung. Daher ist es zu empfehlen, Angebote zu nutzen, für die keine Erteilung einer Einwilligung erforderlich ist. Unschädlich könnte hingegen die Einräumung der Möglichkeit zur Einwilligung bei reinen Zusatzfunktionalitäten sein, die aber für die Messengernutzung selbst nicht erforderlich sind.

Insgesamt dürften bloß optional bereitzustellende Daten unter eine Einwilligung fallen. Sofern die Umsetzung von Messengerdienstfunktionen von der Verarbeitung personenbezogener Daten abhängig ist, könnte eher Art. 6 Abs. 1 Buchst. b DSGVO (Erfüllung eines Vertrags) einschlägig sein.

Praxistipp:

(1) Keine für die Umsetzung eines Messengerdienstes erforderlichen Funktionen sollten von der Erteilung einer wirksamen Einwilligung der Beschäftigten abhängig sein
   a. Es bestehen Zweifel an der Wirksamkeit aufgrund von Freiwilligkeitsdefiziten
   b. Die Einwilligung muss ohne Nachteile jederzeit widerrufbar sein

(2) Einwilligungen kommen aber dort in Frage, wo eine zusätzliche Datenbereitstellung optional gestaltet ist, weil sie für die Diensterbringung selbst nicht erforderlich ist
   a. Es muss sichergestellt sein, dass Beschäftigte solche optionalen Daten freiwillig (selbst) bereitstellen
   b. Die Option muss jederzeit mit Wirkung für die Zukunft deaktivierbar sein

[283] *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 7 Rn. 33; *Brockmeyer*, ZD 2018, 258 (262); *Plath,* in: Plath, DSGVO/BDSG Art. 7 Rn. 19 f. *Buchner/Kühling,* in: Kühling/Buchner, DS-GVO Art. 7 Rn. 52.
[284] *Metzger*, AcP 2016, 817 (823f.) bezogen auf die privat oder beruflich motivierte Mitgliedschaft in sozialen Netzwerken.
[285] *Samardzic/Becker*, EuZW 2020, 646 (652); *Köllmann*, NZA 2020, 831 (832).
[286] Ablehnend: *Samardzic/Becker*, EuZW 2020, 646 (652).
[287] Vgl. Bedenken bei: *Köllmann*, NZA 2020, 831 (832).
[288] *Köllmann*, NZA 2020, 831 (835).

2.4.1.2.2 Vertrag

Eine Datenverarbeitung ist auch dann rechtmäßig, wenn die Erfüllung eines Vertrags dies erfordert. Wichtig dabei ist, dass die betroffene Person selbst die Vertragspartei sein muss. Die Verarbeitung selbst kann hingegen auch von einem Dritten durchgeführt werden, sofern dies für die Erfüllung des Vertrags mit der betroffenen Person erforderlich ist.[289] Dies gilt auch unabhängig von der Vertragsart.[290] Entscheidend sind somit:

- Das Merkmal der Erforderlichkeit
- Die Qualifikation der betroffenen Person als Vertragspartei

Art. 6 Abs. 1 Buchst. b DSGVO

die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

Im Unternehmenskontext hat das Unternehmen ein Vertragsverhältnis mit der Kundschaft und den Beschäftigten. Im Hinblick auf die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis auf Grundlage des Arbeitsvertrags ist § 26 BDSG lex specialis (zu den Anforderungen siehe Abschnitt 2.4.1.3.3).[291] Es sind unterschiedliche Vertragsmodelle denkbar.

2.4.1.2.2.1 Erforderlichkeit

Eine Datenverarbeitung kann nur über einen Vertrag legitimiert werden, wenn diese zur Vertragserfüllung tatsächlich erforderlich ist. Hier kann eine strenge oder weniger strenge Auslegung vorgenommen werden:

Extensive Auslegung: nach einer Ansicht definiere der jeweilige Dienstanbieter die Leistung in den konkret vorliegenden Vertragsklauseln, sodass sich die Erforderlichkeit stark von den Nutzungsbestimmungen ableite.[292] Kritisiert wird, dass der Vertragspartner dann sein angebotenes Leistungsspektrum beliebig weit formulieren könne und so weitreichende Datenverarbeitungen legitimieren könnte.[293] Anbieter könnten mit dem Angebot zahlreicher Zusatzleistungen ein beliebig weites Gesamtpaket schnüren, unabhängig davon, ob die Nutzenden dieses tatsächlich auch abrufen wollen.

[289] *Albers/Veit,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 6 Rn. 30; *Schantz,* in: NK Datenschutzrecht Art. 6 Rn. 22; *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, § 2 Rn. 26.
[290] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 290 f.
[291] *Wolff/Kosmider*, ZD 2021, 13 (14); *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 20; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 7.
[292] *Żdanowiecki*, DSRITB 2018, 559 (566); *Malgieri*, International Review of Law, Computers & Technology 2018, 118 (129); *Engeler*, ZD 2018, 55 (57). *Schantz* stellt entscheidend auf die Erkennbarkeit ab, da nur dann die Vereinbarung vom Willen der Parteien getragen wird: *Schantz,* in: NK Datenschutzrecht Art. 6 Rn. 25 ff.
[293] *Graf von Westphalen/Wendehorst*, BB 2016, 2179 (2179). *Radlanski* bezeichnet dies als „konstruierte Erforderlichkeit". Eine weitere Möglichkeit, die Erforderlichkeit auszudehnen, liegt in der tatsächlichen Erweiterung des Funktionsumfangs: *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 119.

Restriktive Auslegung: Nach einer restriktiven Auslegung des Erforderlichkeitsbegriffs ist dieses Tatbestandsmerkmal nur gegeben, wenn der Leistungserfolg einer Primär- oder Sekundärpflicht ohne die Datenverarbeitung nicht herbeigeführt werden kann, d.h. Unmöglichkeit i.S.d. § 275 Abs. 1 BGB ohne Durchführung der Datenverarbeitung gegeben wäre.[294] Demnach wäre eine objektiv-abstrakte Bestimmung des funktionalen Vertragsgegenstands zu Grunde zu legen.[295] Diese könnte sich am für den jeweiligen Vertragstypus aufgrund hergebrachter wirtschaftlicher Erfahrungen allgemein anzunehmenden Wesenskern bzw. eigentlichen Sinn der vertraglichen Austauschbeziehung orientieren.[296]

Beanstandet wird an dieser abstrakt-wertenden Herangehensweise wiederum die Gefahr der Unbestimmtheit, insbesondere bei komplexeren Vertragskonstellationen, sowie mögliche Übertragungsschwierigkeiten der hergebrachten Erfahrungssätze auf moderne, unkonventionelle Vertragsgestaltungen.[297] Befürchtet wird außerdem eine Hemmungswirkung für Vertragsgestaltungsentwicklungen.[298] Sofern mit der extensiven Auslegung dagegen das Kriterium der Erforderlichkeit durch die bewusste Ausformung des konkreten Vertragsinhalts grundsätzlich frei und privatautonom gesteuert werden kann, verschiebt sich die Prüfung der Wirksamkeit von einer datenschutzrechtlichen Kontrolle auf die Wirksamkeitskontrolle nach §§ 134, 138, 242 BGB bzw. § 305 ff. BGB, wenn es sich um allgemeine Geschäftsbedingungen handelt.[299] In letzterem Fall umfasst die AGB-Kontrolle jedoch nicht die Leistungsbestimmung selbst.[300] Weitere Argumente streiten für die restriktive Auslegung:

- **Einheitliche Auslegung:** Im Rahmen des Art. 6 Abs. 1 DSGVO findet sich die Anforderung der Erforderlichkeit mehrfach. Im Zusammenhang mit primär öffentlich-rechtlich motivierter Datenverarbeitung wird die „Erforderlichkeit“ im Sinne einer zwingenden Voraussetzung verstanden, d.h. dass das jeweils angestrebte Ziel ohne Datenverarbeitung anders nicht erreicht werden kann.[301] Dagegen befürworten Einzelstimmen unterschiedliche Maßstäbe für Datenverarbeitung durch staatliche Stellen gegenüber denen durch den Privatrechtsverkehr.[302] Zwar sind private Stellen anders als staatliche nicht direkt Grundrechtsverpflichtete.[303] Den Staat treffen jedoch im Rahmen der mittelbaren Drittwirkung der Grundrechte Handlungspflichten ein angemessenes Schutzniveau sicherzustellen.[304]
- **Abgrenzung zur Einwilligung:** Während sich im Zivilrecht der auf der Privatautonomie basierende Gestaltungswille der Parteien im Vertrag manifestiert, ist die Einwilligung das Steuerungsinstrument

---

[294] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 8; *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG - WP 217, S. 21; *Albers/Veit,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 6 Rn. 32; *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 6 Rn. 20; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 6 Rn. 11; *Golland*, MMR 2018, 130 (130); *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (220).

[295] vgl. *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 3 Rn. 43 f.; *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG - WP 217, S. 22.

[296] *Buchner/Petri,* in: Kühling/Buchner, DS-GVO Art. 6 Rn. 39 ff.

[297] *Engeler*, ZD 2018, 55 (57); a.A. *Härting*, CR 2016, 735 (740) weist darauf hin, dass sich auch im Bereich der digitalen Inhalte Geschäftsmodelle etabliert haben, die Nutzererwartungen prägen.

[298] *Engeler*, ZD 2018, 55 (57).

[299] Die Prüfung der Treuwidrigkeit und der guten Sitten würde dem „ansonsten der Beliebigkeit anheimfallenden Erforderlichkeitsbegriff die nötige Bestimmtheit verleihen“: *Engeler*, ZD 2018, 55 (57, 60).

[300] BGH, Urteil vom 05. Oktober 2017 – III ZR 56/17 –, Rn. 15; BGH, Urteil vom 22. September 2016 – III ZR 264/15 –, Rn. 12; BGH, Urteil vom 09. Oktober 2014 – III ZR 32/14 –, Rn. 37; BGH, Urteil vom 13. Januar 2011 – III ZR 78/10 –, Rn. 15; BGH, Versäumnisurteil vom 06. Juli 2011 – VIII ZR 293/10 –, Rn. 10; BGH, Urteil vom 12. Juni 2001 – XI ZR 274/00 –, BGHZ 148, 74-84, Rn. 12; BGH, Urteil vom 12. Dezember 2000 – XI ZR 138/00 –, BGHZ 146, 138-144, Rn. 12; BGH, Urteil vom 24. März 1999 – IV ZR 90/98 –, BGHZ 141, 137-152, Rn. 25; kritisch *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749).

[301] *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 6 Rn. 28 ff. *Buchner/Petri,* in: Kühling/Buchner, DS-GVO Art. 6 Rn. 15.

[302] *Frenzel,* in: Paal/Pauly, DS-GVO Art. 6 Rn. 14.

[303] *Frenzel,* in: Paal/Pauly, DS-GVO Art. 6 Rn. 14.

[304] Siehe Abschnitt 2.1.3.3.

für autonome Entscheidungen im Datenschutzrecht.[305] Insofern bestehen auch besondere Aufklärungs- und Transparenzpflichten sowie Widerrufsrechte (vgl. Art. 7 DSGVO), welche durch eine extensive Auslegung des Art. 6 Abs. 1 Buchst. b DSGVO nicht umgangen werden sollten.[306]

— **Orientierung am Grundsatz der Datenminimierung**: Bereits im Rahmen der Datenschutzrichtlinie bestand Streit darüber, ob Erforderlichkeit eng mit „Unerlässlichkeit" oder weiter mit der „vernünftigerweise" zur Sicherung der ordnungsgemäßen Vertrags- bzw. Nutzungsdurchführung gleichzusetzen war.[307] Soweit die Erforderlichkeit beliebig steuerbar ist, drohen allerdings Ziele wie die Datenminimierung sowie deren Konkretisierung im Rahmen des *Privacy by Design* und *Privacy by Default* gemäß Art. 25 DS-GVO unterlaufen zu werden.[308]

Erste Gerichtsurteile scheinen eine vermittelnde Position einzunehmen, wonach zwar kein strenger Maßstab anzulegen sei, d.h. nicht erst bei Unmöglichkeit von der Erforderlichkeit auszugehen sei, die Kriterien nichtsdestotrotz *objektiv* zu bestimmen sind.[309] Die Verarbeitung muss nach vernünftiger Würdigung objektiv sinnvoll im Kontext des Vertragszwecks sein.[310] Erforderlichkeit ist bei den essentialia negotii (lateinisch für wesentliche Geschäftseigenschaften)[311] des Vertrags gegeben.[312]

2.4.1.2.2.2 Mögliche Vertragsparteien im Kontext des Messengereinsatzes im Unternehmen

Kundensicht: Sofern Kundschaft oder Wirtschaftskontakte eigenverantwortlich Messengerdienste installieren, um in Kontakt mit dem Unternehmen zu treten, sind sie selbst Vertragspartner im Hinblick auf die Kommunikationsdurchführung durch den Messengerdienst. In der Vergangenheit war zwar noch umstritten, ob ein Vertrag insofern mit dem Applikationsanbieter oder Marktplatzanbieter (Appstore, Playstore, etc.) zustande kommt, allerdings kommt es hier auf die eindeutige vertragsrechtliche Einordnung im Hinblick auf den Verantwortlichen nicht an.[313] Ausreichend ist, dass der Verantwortliche, welcher nicht selbst an dem Vertrag beteiligt ist, durch den Vertragspartner in die Vertragsanbahnung und/oder -durchführung im Sinne einer Funktionsübertragung eingeschaltet ist.[314] Im Verhältnis App-Store und App-Anbieter wäre dies unzweifelhaft der Fall (entweder über eine Vertretung, als Erfüllungsgehilfe oder Zulieferer).[315] Unsicherer ist dies, wenn Daten durch das Unternehmen verarbeitet werden: eine solche Verarbeitung dürfte regelmäßig den auf die Übermittlung von Kommunikationsinhalten betreffenden Vertrag überschreiten. Vielmehr wäre zu

[305] vgl. *Albers/Veit,* in: BeckOK DatenschutzR Art. 6 Rn. 29; *Stemmer,* in: BeckOK DatenschutzR Art. 7 Rn. 41; *Nebel*, K&R 2019, 148 (150); *Buchner/Petri,* in: Kühling/Buchner - DS-GVO/BDSG Art. 6 Rn. 26; *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 6 Rn. 18.

[306] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 299; *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3747); *Buchner/Petri,* in: Kühling/Buchner - DS-GVO/BDSG Art. 6 Rn. 26.

[307] BT-Drs 13 / 7385, S. 24; *Müller-Broich*, TMG, § 14 Rn. 3; *Spindler/Schuster*, Recht der elektronischen Medien, § 14 TMG Rn. 4. *Plath*, BDSG, § 14 TMG Rn. 13.; vgl. auch BGH, Urteil vom 16. Mai 2017 – VI ZR 135/13 –, BGHZ 215, 55-69, Rn. 30 ff.

[308] *Engeler*, ZD 2018, 55 (57).

[309] VG Mainz, Urteil vom 20.2.2020 – 1 K 467/19.MZ, Rn. 30.

[310] OLG München, Urteil vom 16.1.2019 – 7 U 342/18, Rn. 30

[311] Essentialia negotii bezeichnen die wesentlichen Vertragsbestandteile, ohne die kein sinnvoller Vertrag zustande käme.

[312] VG Mainz, Urteil vom 20.2.2020 – 1 K 467/19.MZ, Rn. 30; kritisch: *Blasek*, ZD 2020, 376 (379).

[313] Bezüglich der früheren Gestaltung der App-Stores: *Datta/Klein*, CR 2017, 174 (175); *Ewald,* in: Apps und Recht, S. 14 f.; *Feldmann*, DSRITB 2011, 47 (49); *Lachenmann,* in: *Solmecke u. a.*, Solmecke/Taeger/Feldmann, Mobile Apps, S. 123 ff.; *Klein/Datta*, CR 2016, 587 (587); *Kremer*, CR 2011, 769 (769). Zum Streit: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 291 f.

[314] *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 6 Rn. 18. *Schantz* plädiert für die Einräumung eines Widerspruchsrechts analog Art. 21 DS-GVO, wenn die Verantwortlichkeit bei einem Dritten liegt: *Schantz,* in: NK Datenschutzrecht Art. 6 Rn. 22.

[315] Siehe zu den bei Apps auf intelligenten Endgeräten an der Datenverarbeitung beteiligten Parteien: *Artikel-29-Datenschutzgruppe*, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten - WP 202, S. 11ff.

prüfen, ob parallel die Kommunikation mit dem Unternehmen im Rahmen und auf Grundlage eines gesonderten Vertragsverhältnisses beruht.[316] Auch eine Vertragsanbahnung wäre eine möglich Legitimationsgrundlage zur Verarbeitung personenbezogener Daten, sofern diese auf Anfrage der betroffenen Person erfolgt.[317]

Unternehmenssicht: Für das Unternehmen können sich zwei unterschiedliche Konstellationen stellen: Verantwortlichkeit für die Verarbeitung personenbezogener Daten der Beschäftigten und Verantwortlichkeit für die Verarbeitung personenbezogener Daten von Kundschaft/Geschäftskontakten. Ist die Nutzung eines Messengerdienstes oder vergleichbaren Kommunikationstools erforderlich zur Erfüllung des Arbeitsvertrags, enthalten Art. 88 DSGVO i.V.m. § 26 Abs. 1 BDSG Spezialregelungen für die Verarbeitung der Beschäftigtendaten (vgl. Abschnitt 2.4.1.3.3). Bezüglich der Verarbeitung von personenbezogenen Kundendaten oder Daten von Geschäftskontakten, kommt es wiederum darauf an, ob diese Kommunikation im Rahmen dessen stattfindet, was zur Erfüllung des Vertrages bzw. zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (sofern diese auf Anfrage der betroffenen Person erfolgen).

Dienstanbietersicht: Wählt das Unternehmen einen Messengerdienst, um interne oder externe Unternehmenskommunikation zu organisieren, könnte ein direktes Vertragsverhältnis zum Messengerdienst vorliegen oder die Beschäftigten schließen einen eigenständigen Vertrag ab. Im Ersteren Fall wären die Beschäftigten als betroffene Personen nicht Vertragspartei, sodass eine Rechtfertigung der Datenverarbeitung durch den Messengerdienst nicht über Art. 6 Abs. 1 Buchst. b DSGVO möglich wäre. Für die Verarbeitung der Unternehmensdaten bedarf es mangels datenschutzrechtlicher Betroffenheit keiner spezifischen Rechtsgrundlage.[318]

Aus dem Blickwinkel des Messengerdienstes ist es hingegen regelmäßig nicht ersichtlich, ob die Nutzenden den Dienst (kostenpflichtig/kostenlos) herunterladen, um privat oder beruflich zu kommunizieren. Einige Messengerdienste schließen in ihren AGB die berufliche Nutzung aus. Insofern stellt sich aus der zivilrechtlichen Perspektive die Frage, ob mit der Installation der Messenger-App ein Vertrag mit den datenschutzrechtlich betroffenen Beschäftigten zustande kommt, der dann wiederum als Rechtsgrundlage für eine Datenverarbeitung dienen kann. Der Grundsatz des Venire Contra Factum Proprium[319] könnte es der betroffenen Person verwehren, sich auf Mängel beim Vertragsschluss zu berufen.

Liegt hingegen eindeutig ein Vertragsverhältnis zwischen Unternehmen und Messengerdienst vor, wäre an eine Auftragsverarbeitung zu denken (siehe Abschnitt 2.5.2.2). Der Messengerdienst-Anbieter wäre dann als der „verlängerte Arm“ des Unternehmens dazu berechtigt, die Daten von Kundschaft/Beschäftigten im Interesse des Unternehmens zu verarbeiten, sofern dieses über eine Rechtsgrundlage verfügt.

Kontakte: Personen, die sich im Kontaktbuch des Nutzenden befinden und selbst den Messengerdienst nicht nutzen, sind in keinem Fall Vertragspartei. Sofern ihre Daten ausgelesen und/oder weitergeleitet werden, ist ein Rückgriff auf Art. 6 Abs. 1 Buchst. b DSGVO ausgeschlossen.

---

[316] vgl. *Rohrlich*, ZAP 2020, 1265 (1267).

[317] Insgesamt besteht kein strenges vertragsrechtliches Verständnis, da der Begriff nach Unionsrecht auszulegen ist: *Schulz,* in: Gola DS-GVO, Art. 6 Rn. 27 ff. *Albers/Veit,* in: BeckOK DatenschutzR Art. 6 Rn. 30.

[318] Unternehmen könnten allenfalls Interesse daran haben gesonderte Vereinbarungen zur Einhaltung von Geheimhaltungsmaßnahmen zum Schutz von Geschäftsgeheimnissen haben, siehe hierzu Kapitel 6. Zudem kann das TTDSG im Hinblick auf den Schutz des Fernmeldegeheimnisses bei juristischen Personen einschlägig sein, siehe Kapitel 3.

[319] Dieser Grundsatz steht für widersprüchliches Verhalten und schützt die Gegenseite nach dem Grundsatz von Treu und Glauben nach § 242 BGB, siehe hierzu: BGH, Urteil vom 16.03.2017 - I ZR 39/15, Rn. 96.

2.4.1.2.2.3 Zwischenergebnis zum Vertrag und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Die Legitimation einer Datenverarbeitung zur Erfüllung eines Vertrags erscheint aus der Perspektive des Angebots eines Messengerdienstes eine relevante Rechtfertigungsgrundlage, da die Umsetzung von Kommunikationsfunktionen gänzlich ohne Datenverarbeitung zumeist kaum auskommen wird. Aus Unternehmenssicht ist Obacht geboten, zu prüfen, welche Vertragsbeziehungen im Einzelfall bestehen, ob alle betroffenen Personen selbst Vertragspartei geworden sind und ob die anvisierte Datenverarbeitung tatsächlich zur Erfüllung dieses Vertrags oder vorvertraglicher Maßnahmen erforderlich ist (siehe zu fallgruppenspezifischen Analyse Kapitel 5).

Bei strenger Auslegung des Kriteriums der Erforderlichkeit, kann diese Rechtsgrundlage nur die zur Umsetzung der Messengerfunktionalitäten *notwendigen*, personenbezogenen Daten erfassen. Für Daten, welche lediglich *nützlich* sind, bspw. um die User-Experience zu steigern, wäre fraglich, ob dies den Vertragserfolg tangiert. Wird diese Datenbereitstellung optional gestaltet, wäre wiederum eine Einwilligung denkbar. Diese darf allerdings nicht an die Vertragserfüllung gekoppelt werden (insbesondere, wenn weitere die Freiwilligkeit ausschließende Merkmale hinzukommen), sondern es sollte dann auch möglich sein, den Messengerdienst ohne die entsprechende Datenbereitstellung zu nutzen.

2.4.1.2.3 Lebenswichtige Interessen

Art. 6 Abs. 1 Buchst. d DSGVO

die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen

Im Rahmen der Unternehmenskommunikation wird diese Legitimationsgrundlage regelmäßig ausscheiden und wird daher im Folgenden nicht näher erläutert. Nichtsdestotrotz geben bspw. die Messengerdienste WhatsApp und Facebook-Messenger an, personenbezogene Daten zum Schutz lebenswichtiger Interessen zu verarbeiten.[320] Welche Daten hierfür erforderlich sind und in welchem Zusammenhang der Betrieb eines Messengerdienstes zum Schutz des Lebens, der körperlichen Unversehrtheit oder der Sicherheit besteht, lässt sich aus den Erklärungen leider nicht eindeutig entnehmen. Zu den verwendeten Datenkategorien verweist die Datenschutzrichtlinie lediglich auf die allgemeinen Abschnitte.[321]

2.4.1.2.4 Interessenabwägung

Art. 6 Abs. 1 Buchst. f DSGVO

die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht

[320] Siehe hierzu: https://www.whatsapp.com/legal/privacy-policy-eea?eea=1#privacy-policy-vital-interests (Stand und https://de-de.facebook.com/policy.php (Stand 21.08.2020) [letzter Zugriff 28.07.2021].
[321] Siehe hierzu: https://www.whatsapp.com/legal/privacy-policy-eea?eea=1#privacy-policy-vital-interests (Stand und https://de-de.facebook.com/policy.php (Stand 21.08.2020) [letzter Zugriff 28.07.2021].

> die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Im Rahmen des Art. 6 Abs. 1 Buchst. f DSGVO ist das berechtigte Interesse des Verantwortlichen (oder eines Dritten) an der Verarbeitung der personenbezogenen Daten mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Peron(en) in Relation zu setzen.[322] Insofern sind drei wesentliche tatbestandsmerkmale zu prüfen:

- Berechtigtes Interesse
- Erforderlichkeit
- Überwiegen der Interessen

Berechtigtes Interesse: jedes rechtmäßige rechtliche, tatsächliche, wirtschaftliche oder immaterielle Interesse.[323]Anhaltspunkte für berechtigte Interessen finden sich in den Erwägungsgründen 47, 48 und 49.

Beispiele in den Erwägungsgründen 47, 48, 49 DSGVO:

- IT-Sicherheit
- Betrugsprävention
- Konzerndaten (Übermittlung innerhalb von Unternehmensgruppen)
- Direktwerbung

Erforderlichkeit: ist nicht gegeben, wenn ein milderes, gleich effizientes Mittel vorhanden ist.[324] Existieren datenschutzfreundliche Lösungen, deren Einsatz technisch möglich und wirtschaftlich zumutbar ist, ohne die Verarbeitungsziele zu beeinträchtigen, lässt sich eine Verarbeitung ohne Einsatz dieser Lösungen nur schwer begründen.[325] Eine Datenverarbeitung kann Erforderlich sein, wenn Alternativen technisch und organisatorisch nicht oder nur mit einem unzumutbaren wirtschaftlichen Aufwand umsetzbar sind, bspw. wenn datenschutzfreundliche Technik nicht am Markt verfügbar ist.[326]

Überwiegen der Interessen: Bei der Abwägung können die unterschiedlichen Grundrechte, wie bspw. Informations-, Presse- und Meinungsfreiheit oder die Berufsausübung eine Rolle spielen.[327] EG 47 DSGVO benennt zudem die potentiellen Folgen und vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zum Verantwortlichen beruhen. Dabei soll nach Ansicht des EDSA nicht ausschließlich auf die subjektiven Erwartungen der konkret betroffenen Personen, sondern vielmehr an den Erwartungen eines objektiven Dritten in der konkreten Situation abgestellt werden.[328] Weitere Abwägungskriterien sind: Intensität, u. a. durch die Art der gesammelten Informationen (Informationsgehalt), Umfang (Informationsdichte), Anzahl der betroffenen Personen, tatsächlichen Interessen der Gruppe der betroffenen Personen, Verfügbarkeit

[322] *Spindler/Dalby,* in: Recht der elektronischen Medien Art. 6 Rn. 14; *Wolff/Kosmider*, ZD 2021, 13 (16).
[323] *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG - WP 217, S. 30 ff.; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 6 Rn. 22.
[324] *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG - WP 217, S. 37.
[325] Vgl. BGH, Urteil vom 15. Mai 2018, VI ZR 233/17, Rn. 25 (noch zur alten Rechtslage im Hinblick auf das Merkmal der Erforderlichkeit).
[326] Vgl. OVG Lüneburg, Urt. v. 7.9.2017 – 11 LC 59/16, CR 2017, 805 (807).
[327] *Albers/veit,* in: BeckOK DatenschutzR Art. 6 Rn. 49.
[328] *European Data Protection Board*, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, Angenommen am 29. Januar 2020, S. 13.

alternativer Mittel sowie Art und Umfang der Datenbewertung.[329]

2.4.1.2.4.1 Unternehmenssicht

Bezüglich der Verarbeitung personenbezogener Daten der Beschäftigten wird die Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO von § 26 BDSG verdrängt (siehe Abschnitt 2.4.1.3.3).[330] Im Hinblick auf die Verarbeitung von Kundendaten sowie Daten von Geschäftskontakten muss für den Einzelfall geprüft werden, inwiefern überwiegende Unternehmensinteressen eine Datenverarbeitung rechtfertigen. Eine durchgeführte Abwägung sollte stets gut dokumentiert werden, um die Erwägungen bei Bedarf einer Aufsichtsbehörde gegenüber belegen zu können.[331]

2.4.1.2.4.2 Dienstanbietersicht

Im Fall der Nutzung von Messengerdiensten ist es durchaus zweifelhaft, in welchen Fällen überhaupt ein berechtigtes Interesse des Messengerdienstanbieters besteht. Zählt man die Sicherstellung der IT-Sicherheit nicht bereits zur Erforderlichkeit der Vertragserfüllung, wäre die Interessenabwägung einschlägig. Die Ermöglichung sicherer Kommunikation, Ausfallsicherheit sowie eine technisch reibungslose Dienstbereitstellung, wie auch Information zu Updates und Sicherheitswarnungen und technischer Support dürften regelmäßig bereits zur Vertragserfüllung zählen. Interessen zur Betrugsprävention könnten bei kostenpflichtigen Diensten bzw. zahlungsrelevanten Informationen bestehen. Insofern wäre eine Einzelfallprüfung durchzuführen. Die Nennung der Direktwerbung in EG 47 zeigt zwar, dass es sich um ein berechtigtes Interesse handeln kann, allerdings besagt diese Erwähnung nichts zur Erforderlichkeit und Überwiegen der Betroffeneninteressen im Einzelfall.[332]

Im Hinblick auf die Ausforschung von Nutzenden oder Übermittlung von Kontaktdaten zu Marketing- oder Werbezwecken dürfte diese Legitimationsgrundlage spätestens bei der Abwägung mit schutzwürdigen Belangen der betroffenen Personen regelmäßig ausscheiden.[333] In Fällen, in welchen die Telefonnummern und der Klarnamen in Klartext (d.h. ungehasht) an Messengerdienste übermittelt und/oder längerfristig gespeichert werden, wäre fraglich, ob das Interesse des Messengerdienstes eine Kontaktliste zu erstellen, hinter den Interessen der betroffenen Person nicht regelmäßig zurückbleibt. Eine Übermittlung des gesamten Kontaktverzeichnisses kann ebenfalls nicht auf die Interessenabwägung gestützt werden.[334]

2.4.1.3 Öffnungsklauseln

Gem. Art. 6 Abs. 2 DSGVO können die Mitgliedstaaten *spezifische Bestimmungen* zur Anpassung der Anwendung der Vorschriften der DSGVO in Bezug auf die Verarbeitung zur Erfüllung von Abs. 1 S. 1 Buchst. c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präzise bestimmen, um eine rechtmäßige und nach Treu und Glaube erfolgende Verarbeitung zu gewährleisten.

---

[329] *European Data Protection Board*, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, Angenommen am 29. Januar 2020, S. 12.
[330] Vgl. *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 10.
[331] *Rohrlich*, ZAP 2020, 1265 (1267).
[332] *Felber*, ZD 2018, 382 (387).
[333] Vgl. VGH München, Beschluss vom 26.09.2018 – 5 CS 18.1157, Rn. 27 ff.; VG Bayreuth, Beschluss vom 8.5.2018 – B 1 S 18.105, Rn. 59 ff.
[334] Vgl. noch zur alten Rechtslage: *Schrey u. a.*, MMR 2017, 736 (737).

2.4.1.3.1 Erfüllung einer rechtlichen Verpflichtung

Art. 6 Abs. 1 Buchst. c DSGVO

die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt

Nach Buchstabe c kann mit einer rechtlichen Verpflichtung auch eine Legitimationsgrundlage zur Datenverarbeitung einhergehen. Diese rechtliche Verpflichtung kann sich aus EU-Recht oder aus dem Recht des Mitgliedstaates, dem der Verantwortliche unterliegt, ergeben (Art. 6 Abs. 3 S. 1 DSGVO). Nach dem deutschen Recht könnten für die betriebliche Kommunikation folgende rechtliche Verpflichtungen in Betracht kommen:

- Aufzeichnungspflichten (z. B. § 57a StVZO) und Dokumentationspflichten (z. B. § 17 Abs. 1 MiLoG),
- Aufbewahrungs- und Speicherpflichten (z. B. § 257 HGB; § 147 AO),
- Pflichten zur Verarbeitung von Kundendaten (z. B. § 312e Abs. 1 S. 1 Nr. 3 BGB);
- Risikominimierungspflichten (§ 10 Abs. 2 KWG),
- Meldepflichten (§ 28a SGB IV),
- Abgleichpflichten (VO (EG) Nr. 881/2002, VO (EG) Nr. 2580/2001, sog. Anti-Terror-Listen),
- Übermittlungspflichten (§ 63a Abs. 3 StVG) etc.[335]

Zunächst verpflichten unterschiedliche handels- oder gesellschaftsrechtliche Vorgaben (bspw. § 35a Abs. 1 S. 1 GmbHG, § 80 Abs. 1 AktG, § 37a HGB oder § 125a HGB) im Rahmen der Geschäftskorrespondenz zur Angabe bestimmter Informationen wie Firma, Rechtsform, Sitz des Unternehmens, Post-/Lieferanschrift, Name der Ansprechperson und ggf. deren Funktion und / oder Abteilungszugehörigkeit.[336] Zu den Geschäftsbriefen zählen jede nach außen gerichtete Mitteilung der Gesellschaft, die inhaltlich deren geschäftliche Betätigung betrifft (wie z.B. Vertragsangebote und Vertragsabschlüsse) oder die Übermittlung von Informationen.[337] Entscheidend ist die geschäftliche Kommunikation und nicht die Form der Mitteilung: daher fallen sowohl Telefaxe, E-Mail, SMS, Twitter-Mitteilungen, Blogbeiträge als auch Messengernachrichten unter die Geschäftsbriefe. [338]

Im Rahmen der Unternehmenskommunikation könnten daneben insbesondere die gesetzliche Aufbewahrungspflicht nach § 257 HGB und die steuerliche Aufbewahrungspflicht nach § 147 AO für das Unternehmen relevant werden. Jeder Kaufmann ist gemäß § 257 Abs. 1 HGB verpflichtet, bestimmte in seinem Geschäftsbetrieb anfallende Unterlagen für 6 Jahre oder im Falle von Buchungsbelegen für 10 Jahre geordnet aufzubewahren. Dass bei Geschäftsbriefen teilweise die Mindestangaben wie Rechtsform, Sitz, Registergericht etc. nach § 35a Abs. 1 S.1 GmbHG bzw. § 80 Abs. 1 AktG sowie § 37a HGB oder § 125a HGB nicht eingehalten werden können, ist dann unschädlich, wenn den Gesprächskontakten die Angaben bereits bekannt sind.[339] Sodann können auch Messengernachrichten unter die gesetzlichen Aufbewahrungspflichten fallen, wenn sie empfangende oder abgesandte Handelsbriefe oder Buchungsbelege enthalten. „Handelsbriefe“ betreffen ein Handelsgeschäft i.S.d. §§ 343, 344 HGB – wozu alle Schriftstücke zählen, die der Vorbereitung, dem Ab-

[335] *Schulz,* in: Gola DS-GVO, Art. 6 Rn. 44.
[336] *Helfrich,* in: Forgó/Helfrich/Schneider - Betrieblicher Datenschutz, Kap. 3 B. II. Rn. 14.
[337] *Schrey u. a.*, MMR 2017, 656 (658).
[338] *Schrey u. a.*, MMR 2017, 656 (658); vgl. auch *Wolf, de*, NZA 2010, 1206 (1208).
[339] *Schrey u. a.*, MMR 2017, 656 (659).

schluss, der Durchführung oder Rückabwicklung von Handelsgeschäften dienen (z.B. Angebote, Bestellungen und Rechnungen). [340]

Allerdings ist zu beachten, dass diese Pflicht lediglich den Kaufmann bzw. das Unternehmen trifft, das den Messengerdienst nutzt, nicht aber den Messengerdienstanbieter selbst. Daher kann der Messengerdienstanbieter sich nicht auf diese rechtliche Verpflichtung berufen und die Messengernachrichten auf seinen Servern für 6 bis 10 Jahren trotz Löschungsverlangens der betroffenen Personen speichern. Unternehmen haben aber dann die Möglichkeit, um dieser Pflicht nachzukommen, die Chatverläufe bzw. die Messengernachrichten zu exportieren und zentral bei sich separat abzulegen.[341] Das Gleiche gilt auch für die steuerliche Aufbewahrungspflicht.

2.4.1.3.2 Erfüllung einer Aufgabe im öffentlichen Interesse

Art. 6 Abs. 1 Buchst. e DSGVO

die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

Art. 6 Abs. 1 Buchst. e DSGVO betrifft die Datenverarbeitung im öffentlichen Interesse. Adressat sind daher lediglich Stellen, die öffentliche Aufgaben oder im öffentlichen Interesse liegende Aufgaben wahrnehmen, welches im Kontext der Nutzung von Messengerdiensten regelmäßig nicht der Fall ist. Aus diesem Grund wird diese Legitimationsgrundlage nicht näher erläutert.

2.4.1.3.3 Spezielle Rechtsgrundlagen für die Datenverarbeitung im Beschäftigtenkontext

Für die Verarbeitung personenbezogener Daten der Beschäftigten durch ihren Arbeitgeber enthält die DSGVO eine Öffnungsklausel für mitgliedstaatliches Recht. In der Literatur wird diskutiert, wie weit die Kompetenz der nationalen Gesetzgeber reicht, also insbesondere welchen Gestaltungsspielraum diese Öffnungsklausel bietet.[342]

2.4.1.3.3.1 Reichweite der Öffnungsklausel

Art. 88 Abs. 1 DSGVO

Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, [...] vorsehen.

Dies betrifft insbesondere folgende Aspekte:

[340] *Schrey u. a.*, MMR 2017, 656 (659).
[341] Vgl. *Schrey u. a.*, MMR 2017, 656 (659).
[342] Zur Diskussion siehe *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG Art. 88 Rn. 30 ff. m.w.N.

- Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten,
- des Managements, der Planung und der Organisation der Arbeit,
- der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz,
- des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie
- für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses

Mitgliedstaatliche Normen, die von dieser Regelungsoption Gebrauch gemacht haben, gehen in diesem Bereich den Vorschriften der DSGVO vor – auch wenn sich dies nicht aus der Regelung selbst ergibt, so doch aus dem Sinn und Zweck.[343] Weitere Impulse gibt die DSGVO den Mitgliedstaaten für die Umsetzung der Öffnungsklausel im 2. Absatz mit:

Art. 88 Abs. 2 DSGVO

Diese Vorschriften umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.

Parallel bleiben aber die übrigen, allgemeinen Bestimmungen der DSGVO weiter anwendbar.[344] Zudem sind die mitliedstaatlichen Regelungen im Lichte der DSGVO EU-rechtskonform auszulegen.[345] Insofern können die Anforderungen der DSGVO im Bereich des Beschäftigtendatenschutzes als „Mindeststandard“ bezeichnet werden.[346]

2.4.1.3.3.2 Umsetzung im BDSG in Deutschland

Der deutsche Gesetzgeber hat von der Öffnungsklausel Gebrauch gemacht und den Beschäftigtendatenschutz in § 26 BDSG geregelt. Diese Generalklausel führt die bisherige Regelung vor der DSGVO fort.[347]

§ 26 Abs. 1 S. 1 BDSG

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies

[343] *Riesenhuber,* in: BeckOK DatenschutzR Art. 88 Rn. 16.
[344] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 20.
[345] *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 4.
[346] *Dietrich u. a.*, DuD 2021, 5 (7).
[347] *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 9; *Dietrich u. a.*, DuD 2021, 5 (8).

für die

- Entscheidung über die **Begründung** eines Beschäftigungsverhältnisses oder
- nach Begründung des Beschäftigungsverhältnisses für dessen **Durchführung** oder
- Beendigung oder
- zur Ausübung oder Erfüllung der sich aus einem **Gesetz** oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der **Interessenvertretung** der Beschäftigten erforderlich ist.

Der Gesetzgeber hat sich zunächst gegen eine konkretisierende Detailregelung entschieden, aber „behält sich vor“ spezifische Fragen des Datenschutzes im Beschäftigungsverhältnisses entweder im Rahmen dieser Regelung oder eines gesonderten Gesetzes konkretisierend zu regulieren und sich hierbei an der bereits zur Vorgängerregelung ergangenen Rechtsprechung zu orientieren.[348] Dies gilt für Problemfelder wie „insbesondere für das Fragerecht bei der Begründung eines Beschäftigungsverhältnisses, den expliziten Ausschluss von heimlichen Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten sowie den Ausschluss von umfassenden Bewegungsprofilen, den Ausschluss von Dauerüberwachungen und die Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken.“[349]

Zudem gewährt § 26 Abs. 1 S. 2 BDSG spezifische Orientierung für Arbeitgeber im Hinblick auf den Umgang mit potentiell straffällig gewordenen Beschäftigten:

§ 26 Abs. 1 S. 2 BDSG

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Die Verarbeitung von besonderen Kategorien personenbezogener Daten ist in § 26 Abs. 3 BDSG geregelt. Daraus ergeben sich insgesamt 3 Erlaubnistatbestände:

- Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses (Generalklausel), § 26 Abs. 1 S. 1 BDSG
- Datenverarbeitung zum Zweck der Aufdeckung von Straftaten, § 26 Abs. 1 S. 2 BDSG
- Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigtenverhältnis, § 26 Abs. 3 BDSG

Für die Nutzung von Kommunikations- und Kollaborationswerkzeugen im Unternehmen ist der erste Erlaubnistatbestand der relevanteste Ausgangspunkt. Für die aktuelle Regelung sind besonders die folgenden Prüfpunkte maßgeblich, welche im Anschluss besprochen werden sollen:

- Personenbezogene Daten von Beschäftigten (Definition des/der Beschäftigten)
- Zwecke des Beschäftigungsverhältnisses

[348] BT-Drs. 18/11325, S. 97.
[349] BT-Drs. 18/11325, S. 97.

- Erforderlichkeit

Flankiert werden diese grundlegenden Weichenstellungen mit einem Hinweis auf die Datenschutzgrundprinzipien: § 26 Abs. 5 BDSG enthält einen deklaratorischen Verweis auf die Grundsätze des Art. 5 DSGVO.[350]

Eine Besonderheit der Norm liegt im sachlichen Anwendungsbereich, welcher weiter gefasst ist: § 26 Abs. 7 BDSG legt fest, dass die Regelungen dieses Paragraphen im Beschäftigungsverhältnis auch dann gelten sollen, wenn personenbezogene Daten von Beschäftigten nicht-automatisiert verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.[351] § 26 BDSG weicht damit in seinem sachlichen Anwendungsbereich von dem der DSGVO in Art. 2 Abs. 1 DS-GVO (auch bei privaten Stellen) ab, indem die Regelungen für *jegliche* Art der Verarbeitung von Beschäftigtendaten für Gültig erklärt werden.[352] Wie weit diese Ausdehnung reicht, ist wiederum nicht unumstritten. So sollten persönliche und dem „gesellschaftlichen Smalltalk zuzurechnende, nicht protokollierte Gespräche“ zwischen Beschäftigten und/oder Vorgesetzen nicht unter die datenschutzrechtliche Reglementierung fallen.[353] Bei der Nutzung von Messengerdiensten und ähnlichen Kommunikationstools liegt allerdings ohnehin eine automatisierte Datenverarbeitung vor.

2.4.1.3.3.2.1 Definition der Beschäftigten

Der persönliche Anwendungsbereich wird durch die Definition des Beschäftigten in § 26 Abs. 8 BDSG determiniert. Diese Aufzählung ist abschließend.[354]

§ 26 Abs. 8 BDSG

Beschäftigte im Sinne dieses Gesetzes sind:

1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
2. zu ihrer Berufsbildung Beschäftigte,
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu

[350] *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 10.
[351] BT-Drs. 18/11325, S. 99.
[352] *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 11; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 29.
[353] *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 13.
[354] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 7; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 28.

diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,

7. Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

Arbeitnehmer*in i.S.d. § 26 Abs. 8 BDSG ist, wer sich vertraglich zu weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit gegen Vergütung verpflichtet hat.[355] Dieser Begriff folgt aus § 611a Abs. 1 BGB zum Arbeitsvertrag.[356]

§ 611a Abs. 1 BGB

Durch den Arbeitsvertrag wird der Arbeitnehmer im Dienste eines anderen zur Leistung weisungsgebundener, fremdbestimmter Arbeit in persönlicher Abhängigkeit verpflichtet. Das Weisungsrecht kann Inhalt, Durchführung, Zeit und Ort der Tätigkeit betreffen. Weisungsgebunden ist, wer nicht im Wesentlichen frei seine Tätigkeit gestalten und seine Arbeitszeit bestimmen kann. Der Grad der persönlichen Abhängigkeit hängt dabei auch von der Eigenart der jeweiligen Tätigkeit ab. Für die Feststellung, ob ein Arbeitsvertrag vorliegt, ist eine Gesamtbetrachtung aller Umstände vorzunehmen. Zeigt die tatsächliche Durchführung des Vertragsverhältnisses, dass es sich um ein Arbeitsverhältnis handelt, kommt es auf die Bezeichnung im Vertrag nicht an.

Die Reichweite ist bewusst weit gewählt, sodass alle in Abhängigkeit stehende Beschäftigten von arbeitnehmerähnlich Beschäftigten, über Auszubildende bzw. zur Arbeitserprobung am Berufsleben Teilnehmende, Leiharbeiter*innen bis hin zu leitenden Angestellten erfasst werden.[357] Zudem erfolgte eine Ausdehnung auf das Vorfeld einer Beschäftigung, d.h. das Stadium der Bewerbung, sowie die Zeit nach der Beendigung des Beschäftigungsverhältnisses. Diese weite Definition ist nicht ohne Kritik geblieben, da Bedenken aufgeworfen wurden, ob hiermit die Reichweite der Öffnungsklausel des Art. 88 DSGVO überschritten wird.[358] Andererseits präferiert auch der EuGH eine weiten Arbeitnehmerbegriff.[359] Ausschlaggebend ist danach die das Rechtsverhältnis prägende Rechte- und Pflichtenstruktur, insbesondere *„dass jemand während einer bestimmten Zeit für einen anderen nach dessen Weisungen Leistungen erbringt, für die er als Gegenleistung eine Vergütung erhält“.*[360]

Weiterhin umstritten ist, ob auch Organmitglieder, wie Geschäftsführer*innen einer GmbH oder Vorstandmitglieder einer AG, als Beschäftigte gelten sollten.[361] Hier wird argumentiert, dass diese auf Grundlage freier Dienstverträge i.S.d. § 611 BGB und nicht im Rahmen eines Arbeitsvertrags tätig werden.[362] Sie werden eher der Arbeitgeberseite als der Arbeitnehmerseite zugeordnet.[363] Andererseits können auch freie Dienstverträge

[355] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 22.
[356] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 7.
[357] *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 14; *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 22.
[358] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 6.
[359] EuGH, Urteil vom 11.11.2015 – C-422/14– Pujante Rivera, Rn. 29; EuGH, Urteil vom 9.7.2015 – C-229/14 – Balkaya, Rn. 34; EuGH, Urteil vom 13.02.2014 – C-596/12 – Kommission/Italien, Rn. 17.
[360] EuGH, Urteil vom 11.11.2015 – C-422/14 – Pujante Rivera, Rn. 29.
[361] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 22.
[362] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 7.
[363] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 104.

unter die weite Definition des EuGH subsumiert werden.[364] Sollten diese Personen nicht unter die Regelungen des § 26 BDSG fallen, verbliebe der Rückgriff auf Art. 6 Abs. 1 Buchst. b und f DSGVO. Im Rahmen der Interessenabwägung wäre es in diesem Fall sicherlich nicht abwegig, auch das Interesse einer einheitlichen Rechtsanwendung im Betrieb als berechtigtes Interesse anzuerkennen.

2.4.1.3.3.2.2 Zwecke des Beschäftigungsverhältnisses

Hierunter fallen jegliche Zwecke des Beschäftigungsverhältnisses. Diese können sich aus dem Arbeitsvertrag, gesetzlichen Vorschriften (wie z.B. dem Steuerrecht, Sozialversicherungsrecht, etc.) oder Kollektivverträgen ergeben.[365] Unter Kollektivvereinbarungen sind Tarifverträge, Betriebsvereinbarungen und Dienstvereinbarungen zu verstehen (vgl. Erwägungsgrund 155 DSGVO).[366] Der Zweck sollte zudem von der Rechtsprechung gebilligt sein. [367]

2.4.1.3.3.2.3 Erforderlichkeit

Zentraler Maßstab der rechtfertigenden Wirkung des § 26 BDSG ist die Frage der *Erforderlichkeit* zur Zweckerreichung.[368] Insbesondere an dieser Stelle gebietet sich ein Rückgriff auf die Grundrechte – denn in Ausfüllung dieser Frage sind die widerstreitenden Grundrechtspositionen in Form der praktischen Konkordanz abzuwägen.[369] „Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.“[370] Da das Kriterium gegenüber der alten Rechtslage vor der DSGVO bewusst beigehalten wurde, kann auf die bisher bereits ergangene Rechtsprechung rekurriert werden.[371]

Das allgemeine Persönlichkeitsrecht schützt die Beschäftigten u.a. vor einer lückenlosen technischen Überwachung am Arbeitsplatz durch heimliche Videoaufnahmen (Totalüberwachung).[372] Eingriffe liegen vor bei Maßnahmen, die einen ständigen Überwachungsdruck erzeugen, dem sich die Beschäftigten während ihrer Tätigkeit nicht entziehen können.[373]

---

[364] Vgl. EuGH, Urteil vom 11.11.2010 – C-232/09 – Danosa, Rn. 29; EuGH, Urteil vom 9.7.2015 – C-229/14, NJW 2015, 2481 Rn. 32 f. – Balkaya; EuGH, Urteil vom 13.02.2014 – C-596/12 – Kommission/Italien, Rn. 17.
[365] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 24.
[366] BT-Drs. 18/11325, S. 97.
[367] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25.; vgl. auch LAG Berlin-Brandenburg, Urteil vom 30.08.2018 – 26 Sa 1151/17, Rn. 79 f.
[368] *Gräber/Nolden,* in: Paal/Pauly - DS-GVO BDSG, § 26 Rn. 13.
[369] BT-Drs. 18/11325, S. 97; *Pötters,* in: Gola DS-GVO, Art. 88 Rn. 5.
[370] BT-Drs. 18/11325, S. 97.
[371] *Gräber/Nolden,* in: Paal/Pauly - DS-GVO BDSG, § 26 Rn. 14; *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 57; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 23; *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 19; *Dietrich u. a.*, DuD 2021, 5 (8).
[372] BAG, Urteil vom 27.03.2003 – 2 AZR 51/02 – BAGE 105, 356-365, Rn. 25; *Dietrich u. a.*, DuD 2021, 5 (8).
[373] BAG, Urteil vom 27.03.2003 – 2 AZR 51/02 – BAGE 105, 356-365, Rn. 25; BAG, Urteil vom 07. Oktober 1987 – 5 AZR 116/86 –, Rn. 15

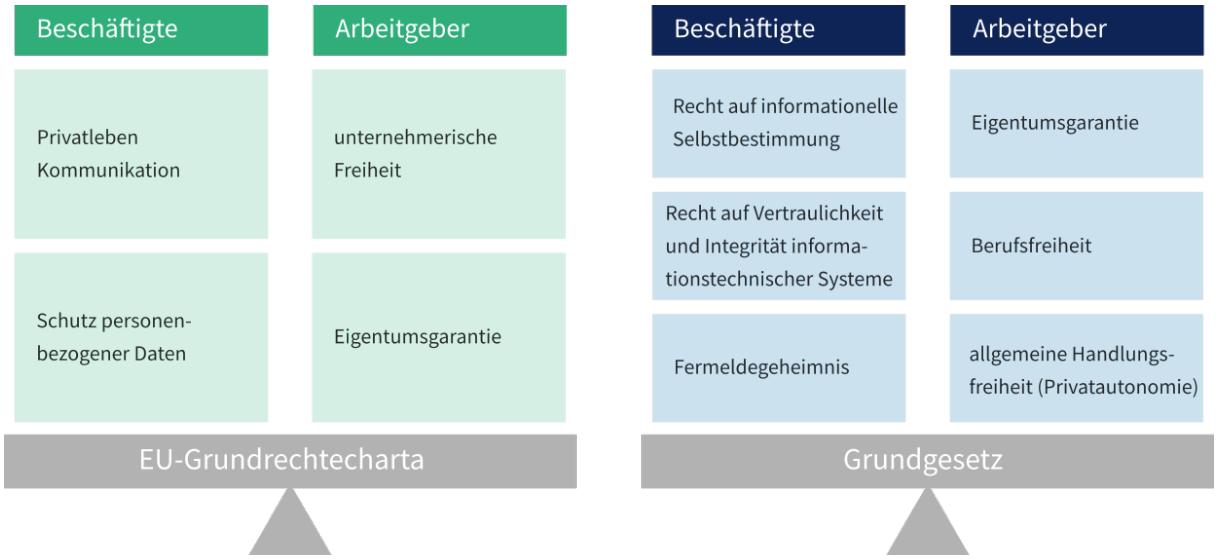


Abbildung 5 Klassische Grundrechtsabwägung im Beschäftigungskontext

Ferner ist Art. 88 Abs. 2 DSGVO als Maßstab heranzuziehen.[374] Zunächst darf also in die Privatsphäre und Persönlichkeitsrechte der Beschäftigten nicht tiefer eingegriffen werden, als dies zur Erfüllung der Zwecke des Beschäftigungsverhältnisses notwendig ist. In Fortführung des bisherigen Systems ist diese Erforderlichkeitsprüfung wie eine Verhältnismäßigkeitsprüfung wie folgt durchzuführen:[375]

Geeignetheit

Im ersten Schritt ist zu prüfen, ob die Maßnahme überhaupt geeignet ist, das verfolgte Ziel zu erreichen oder zumindest zu fördern.[376]

Erforderlichkeit

Im zweiten Schritt ist zu erwägen, ob andere weniger eingriffsintensive Mittel zur Zielerreichung zur Verfügung stehen. [377] Dieses Mittel ist bevorzugt zu nutzen, wenn dieses in gleicher Weise ohne Abstriche bei der

[374] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 18; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 23.
[375] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 18; *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 16; *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 63; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 37.
[376] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 16.
[377] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 19; *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 16.

Qualität zur Zweckerreichung geeignet ist.[378] Dabei wird den Arbeitgeber im Rahmen ihrer Unternehmerfreiheit ein Entscheidungsspielraum über die Organisation betrieblicher Abläufe zugesprochen.[379] Eine existierende grundrechtsschonendere Verarbeitungsmethode muss dann nicht gewählt werden, wenn diese wirtschaftlich nicht zweckmäßig oder technisch gar nicht umsetzbar ist.[380]

Angemessenheit

Im letzten Schritt der Angemessenheitsprüfung erfolgt die Abwägung zwischen den Interessen der Arbeitgeber mit denen der Beschäftigten. Die Schwere des Eingriffs in Arbeitnehmerrechte darf nicht außer Verhältnis zum Gewicht der rechtfertigenden Gründe stehen.[381] Hierbei muss ein „unantastbarer Bereich privater Lebensgestaltung in jedem Fall gewahrt bleiben".[382] Zum Teil kann man sich hier an der sog. Sphärentheorie orientieren:[383]

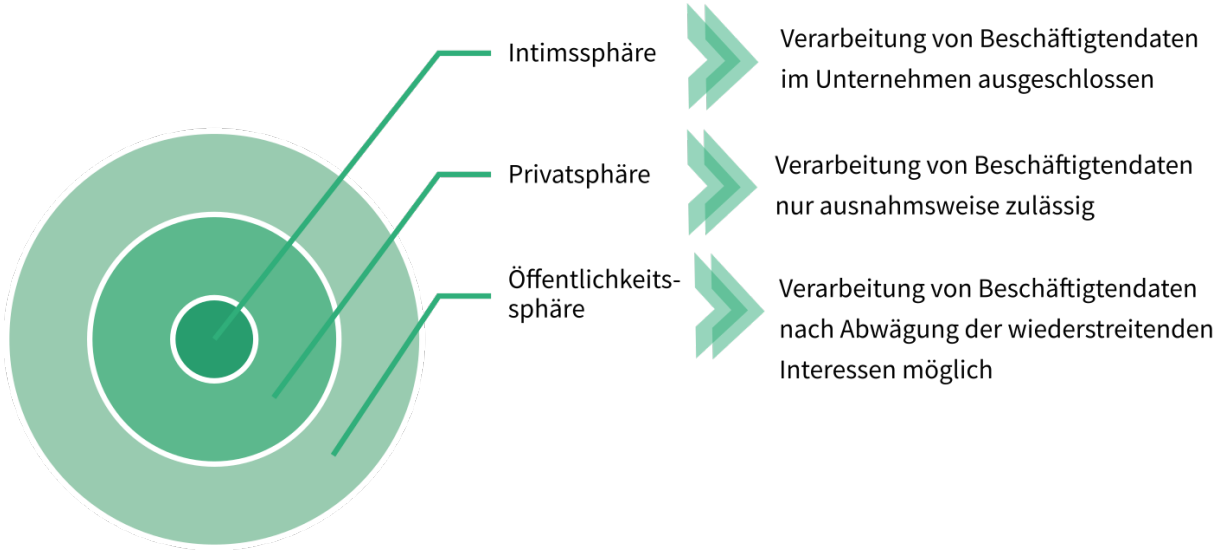


Abbildung 6 Die Sphärentheorie im Beschäftigungskontext

Insgesamt gilt: Je tiefer der Eingriff in die Persönlichkeitssphäre der Beschäftigten ausfällt, desto gewichtiger müssen die Interessen der Arbeitgeber ausfallen. Eine „totale, unbegrenzte Überwachung und Erfassung der Daten der Beschäftigten" gilt als unzulässig.[384] Denn dies würde zu einem unzulässigen Überwachungsdruck führen.

---

[378] Vgl. BAG, Beschluss vom 15.04.2014 – 1 ABR 2/13 (B) –, BAGE 148, 26-41, Rn. 41; BAG, Urteil vom 27.03.2003 – 2 AZR 51/02 –, BAGE 105, 356-365, Rn. 32; BAG, Urteil vom 21.6.2012 – 2 AZR 153/11, Rn. 38; BAG, Urteil vom 22.09.2016 – 2 AZR 848/15 –, BAGE 156, 370-383, Rn. 28; BAG, Urteil vom 20.10.2016 – 2 AZR 395/15 –, BAGE 157, 69-83, Rn. 22; LAG Berlin-Brandenburg, Urteil vom 30.08.2018 - 26 Sa 1151/17, Rn. 80.

[379] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 16; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 38.

[380] *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 38.

[381] *Maschmann,* in: Kühling/Buchner - DS-GVO/BDSG, § 26 Rn. 19; *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 37.; BAG, Urteil vom 17.11.2016 – 2 AZR 730/15 –, Rn. 30; BAG, Beschluss vom 15.04.2014 – 1 ABR 2/13 (B) –, BAGE 148, 26-41, Rn. 41; BAG, Urteil vom 20.06.2013 – 2 AZR 546/12 –, BAGE 145, 278-295, Rn. 23 ff.; BAG, Urteil vom 22.09.2016 – 2 AZR 848/15 –, BAGE 156, 370-383, Rn. 28.

[382] BAG, Urteil vom 7.9.1995 – 8 AZR 828/93, NZA 1996, 637 (638): „Ein unantastbarer Bereich privater Lebensgestaltung muss in jedem Fall gewahrt bleiben"; BAG, Urteil vom 06.06.1984 – 5 AZR 286/81, Rn. 23.

[383] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25.

[384] BAG, Beschluss vom 29.06.2004 – 1 ABR 21/03 –, BAGE 111, 173-190, Rn. 44 ff.; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 25; *Dietrich u. a.*, DuD 2021, 5 (7).

Diese Verhältnismäßigkeitsprüfung steht in enger Wechselwirkung zum Grundsatz der Datenminimierung.[385] Denn der Einsatz von Technologien, welche am Ziel ausgereichtet sind so wenig personenbezogene Daten wie möglich zu verarbeiten oder auf Anonymisierung oder Pseudonymisierung setzen, können sich positiv auf die Interessenabwägung auswirken.

Als weiteres Kriterium die Verhältnismäßigkeitsprüfung positiv zu beeinflussen, wird der Grundsatz der Direkterhebung genannt. [386] Hier wird es als weniger Eingriffsintensiv gewertet, wenn Daten bei der betroffenen Person erhoben werden – als wenn diese aus Drittquellen bezogen werden. Auch wenn die DSGVO diesen Grundsatz anders als das BDSG a.F. nicht kennt, dürfte die verbesserte Nachvollziehbarkeit unter dem Aspekt von Treu und Glauben (bzw. Fairness) und Transparenz durchaus auch unter der interpretationsleitenden Maxime der DSGVO weiter beachtet werden können. [387] Denn die betroffene Person erfährt auf diese Weise von der Datenverarbeitung und kann entsprechend ihre Rechte geltend machen.

Ferner können die in Erwägungsgründen 47 und 48 DSGVO genannten Kriterien, welche im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO eine Rolle spielen, mit herangezogen werden.[388] Hier sind bspw. die berechtigten Erwartungen der betroffenen Person zu nennen.[389] Insofern bestehen durchaus sich überschneidende Impulse für die Abwägung der Grundrechtskonflikte auf DSGVO- und BDSG-Ebene.

2.4.1.3.4 Zwischenergebnis zum Beschäftigtendatenschutz und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Im Rahmen des Beschäftigungskontextes sowie der Erfüllung rechtlicher Verpflichtungen durch die Arbeitgeber richtet sich die Rechtmäßigkeit der Verarbeitung aufgrund des partiellen Richtliniencharakters der DSGVO nicht nach dieser, sondern nach nationalem Recht. Die wichtigste Rechtsgrundlage bietet hier § 26 BDSG, dessen sachlicher und persönlicher Anwendungsbereich weit gezogen wurden. Die Norm ist beim Einsatz von Messengerdiensten im Unternehmenskontext relevant, wenn folgende Fragen zutreffen:

- Handelt es sich bei den betroffenen Personen um **Beschäftigte**?
- Erfolgt die Datenverarbeitung für **Zwecke des Beschäftigungsverhältnisses**?
- Ist die Datenverarbeitung erforderlich, d.h. **geeignet, erforderlich und angemessen**?

2.4.1.4 Sonderfall: Verarbeitung besonderer Kategorien personenbezogener Daten

Die oben geschilderten Legitimationsgrundlagen betreffen die Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 1 DSGVO. Allerdings differenziert die DSGVO zwischen „normalen“ personenbezogenen Daten nach Art. 4 Nr. 1 DSGVO und besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO, für deren Verarbeitung andere Legitimationsgrundlagen gelten (siehe auch Abschnitt 2.3.1.2.2).

[385] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 67.
[386] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 68.
[387] Vgl. *Riesenhuber,* in: BeckOK DatenschutzR, § 26 Rn. 68.
[388] *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 41.
[389] Siehe Abschnitt 2.4.1.2.4.

2.4.1.4.1 Vorliegen besonderer Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten in Bilddaten: Grundsätzlich wird bei Bild- und Videodaten der Umstand diskutiert, dass das Äußere teilweise auch Rückschlüsse auf Herkunft (durch Hautfarbe, Augenform, etc.) sowie Gesundheitszustand (bspw. durch körperliche Beeinträchtigungen) ermöglichen kann und das Tragen religiöser Symbole die religiöse oder weltanschauliche Überzeugung anzeigt.[390] Grundsätzlich sollen auch Daten erfasst werden, aus denen die genannten Kategorien mittelbar hervorgehen (bspw. aus dem Gesamtzusammenhang).[391] Dies führte bereits zur Annahme, bei jeglicher Form der Videoüberwachung im öffentlichen Raum seien besondere Kategorien personenbezogener Daten betroffen.[392] Im Rahmen von Messengerdiensten werden zumeist Profilbilder genutzt, sodass sich eine ähnliche Problematik stellen würde. Allerdings wurde dieser Einschätzung zu Recht entgegengehalten, dass diskriminierende[393] oder freiheitseinschränkende Wirkungen der Datenverarbeitung erst zu befürchten sind, wenn tatsächlich entsprechende Rückschlüsse gezogen werden, sodass der Schutzzweck der Norm eher die zielgerichtete Erfassung dieser Daten adressiert.[394] Würden bspw. zur Erstellung personalisierter Werbung derartige Informationen abgeleitet, müsste sich diese Tätigkeit nach Art. 9 Abs. 2 DSGVO messen lassen. Das Verbot in Art. 9 Abs. 1 DSGVO ist hingegen nicht eröffnet, wenn diese Daten nur beiläufig erhoben werden, nach dem Verwendungskontext keine Auswertungsabsicht besteht und eine solche Auswertung auch nicht im Nachhinein erfolgt.[395] Gegen eine verobjektivierende, den Verarbeitungskontext und Auswertungsabsicht nicht berücksichtigende Sichtweise[396] spricht, dass andernfalls der Anwendungsbereich erheblich ausgedehnt würde und damit dem Schutzziel besonders sensible und kritische Datenverarbeitungen zu steuern nicht Rechnung getragen würde.[397]

Besondere Kategorien personenbezogener Daten in den Metadaten: Sind in den Metadaten Klarnamen und/oder Daten zum Geburts- oder Wohnort enthalten, können diese ebenfalls Angaben zur rassischer und ethnischer Herkunft ermöglichen.[398] Dienstanbieter, die auf das Adressbuch zugreifen, erhalten zusätzlich Zugang zu den Namen der Kontakte, ohne dass die Kontakte hierfür einwilligt haben. Fraglich ist auch hier, ob der Name allein als rassische und ethnische Angabe zu sehen und somit als besondere Kategorie personenbezogener Daten zu betrachten ist. Zwar lässt sich möglicherweise schon allein aus dem Namen einer Person eine rassische oder ethnische Herkunft ableiten bzw. vermuten; dies sollte aber nur im Ausnahmefall bei Hinzutreten besonderer Umstände zur Anwendbarkeit des Art. 9 DSGVO führen.[399] Das Merkmal der „rassischen Herkunft“ bezieht sich vor allem auf die biologische Abstammung und vererbbare Eigenschaften, während bei der „ethnischen Herkunft“ eher der kulturelle Aspekt gemeint wird, der eine Menschengruppe

---

[390] Vgl. hierzu *Schneider/Schindler*, ZD 2018, 463 (456 f.).
[391] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 13; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 11.
[392] Schleswig-Holsteinischer Landtag Drucksache 19/429, S. 144.
[393] Hintergrund der Aufnahme der rassischen und ethnischen Herkunft ist u.a. das Diskriminierungsverbot in Art. 21 EU-GrCh, *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 29; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 25; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 15.
[394] Unabhängiges Landeszentrum für Datenschutz (ULD), Schriftliche Anhörung des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtages zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Gesetzentwurf der Landesregierung Drucksache 19/429, S. 8; *Schneider/Schindler*, ZD 2018, 463 (467).; vgl. auch BVerfGE 120, 378.
[395] *European Data Protection Board*, Guidelines 3/2019 on processing of personal data through video devices, S. 14; *Schneider/Schindler*, ZD 2018, 463 (467).; vgl. auch BAG, Urteil vom 25.09.2013 - 10 AZR 270/12, Rn. 49 (zur alten Rechtslage).
[396] befürwortend: *Petri,* in: NK Datenschutzrecht Art. 9 Abs. 12.
[397] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 13; ähnlich *Mester,* in: Taeger/Gabel - DSGVO/BDSG Art. 9 Rn. 7.
[398] *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 29; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 29.
[399] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 26; *Mester,* in: Taeger/Gabel - DSGVO/BDSG Art. 9 Rn. 7.

kennzeichnet.[400] Dazu zählen besonders Sprache, Geschichte, Tradition, gemeinsame Werte, ein Zusammengehörigkeitsgefühl als Gruppe und die „sprachlichen und kulturellen Beziehung eines Menschen zu seinen Vorfahren".[401] Insgesamt wäre auch hier die Argumentation entsprechend der Bilddaten einschlägig: es kommt für die Sensibilität der Daten auf den Kontext der Datenverarbeitung an, also ob diese Angaben auch für eine Herkunftsanalyse bzw. -prognose genutzt werden. Schlussfolgend gehören Namen der Messengernutzenden sowie aus dem Adressbuch der Nutzenden nicht zu den besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO, es sei denn sie werden in diese Richtung verarbeitet.

Besondere Kategorien personenbezogener Daten in den Gesprächsinhalten: Möglicherweise ergeben sich entsprechende Daten auch aus den Gesprächs- und Chat-Inhalten. Diese Gesprächs- und Chat-Inhalte werden laut Auskunft von den meisten Messengerdienst-Anbietern Ende-zu-Ende-verschlüsselt. Das heißt, niemand außer dem vorgesehenen Empfänger soll reguläre Chat-Nachricht lesen oder Gespräche mithören können, auch nicht der Dienstanbieter. Außerdem werden Nachrichten nach der Zustellung von Messengern wie Threema und Signal umgehend unwiderruflich vom Server gelöscht und sodann nur auf den Geräten der beteiligten Kommunikationspartner gespeichert.[402] Aus diesem Grund ist der Austausch von Gesprächs- und Chat-Inhalte bei bestimmten Messengerdienst-Anbietern datenschutzrechtlich unbedenklich.

Aus Sicht des Unternehmens, in dessen Verantwortung entsprechende Daten gespeichert werden, dürfte es regelmäßig zweckdienlich sein sicherzustellen, dass keine als besondere Kategorien personenbezogener Daten einzustufender Informationen verarbeitet werden, da andernfalls die Rechtfertigungshürden aufgrund des erhöhten Schutzniveaus steigen.

2.4.1.4.2 Ausdrückliche Einwilligung

Bei der Verarbeitung besonderer Kategorien personenbezogener Daten, in der ein besonderes Risiko für die Rechte der betroffenen Personen bestehen kann, reicht eine einfache Einwilligung nicht aus, vielmehr muss diese durch eine ausdrückliche Einverständniserklärung ausdrücken, dass sich die betroffene Person dieser Risiken bewusst ist.[403] Somit ist bei der Verarbeitung sensibler Daten ein gesteigertes Maß an Bestimmtheit erforderlich, wozu sowohl ein Hinweis auf die Sensitivität oder besonderen Charakter der Daten als auch die Genauigkeit in Bezug auf die Nennung der konkret betroffenen Daten und des Verwendungszwecks gezählt wird.[404] Das Erfordernis der Ausdrücklichkeit ändert zwar grundsätzlich nichts an der generellen Formlosigkeit der Einwilligung.[405] Eine Einwilligung durch schlüssiges oder konkludentes Verhalten wird in der Literatur allerdings ausgeschlossen.[406] Folglich steigern sich die Anforderungen an die Einwilligung sowohl in inhaltlicher Sicht im Hinblick auf Aufklärung und Verständlichkeit als auch in praktischer Sicht bezüglich des Aktivitätslevels bei Erteilung der Einwilligungserklärung.

In § 26 Abs. 3 S. 2 BDSG wird ebenfalls ausgedrückt, dass auch bei der Verarbeitung besonderer Kategorien personenbezogener Daten eine Einwilligung nach den genannten Maßstäben grundsätzlich möglich ist, sich die Einwilligungserklärung allerdings ausdrücklich auf diese Daten beziehen muss.

---

[400] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 16. *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 26.
[401] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 16; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 26; Beispiele auch bei: *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 16.
[402] Siehe bspw. die Angaben von Threema unter: https://threema.ch/de/messenger-vergleich [letzter Abruf 17.08.2021].
[403] *European Data Protection Supervisor (EDPS)*, A Preliminary Opinion on data protection and scientific research, S. 19; *Roßnagel*, ZD 2019, 157 (161).
[404] *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 51; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 47.
[405] *Samardzic/Becker*, EuZW 2020, 646 (651).
[406] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 47; *Molnár-Gábor*, DSRITB 2018, 159 (163).

2.4.1.4.3 Sonstige Ausnahmen vom Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten

Bereits erwähnt wurde die Möglichkeit der ausdrücklichen Einwilligung. Daneben sieht Art. 9 Abs. 2 DSGVO weitere Möglichkeiten der Ausnahme vom Verarbeitungsverbot vor. Im Folgenden werden die im Rahmen der Messengernutzung durch Unternehmen relevantesten vorgestellt:

Arbeitsrecht: Art. 9 Abs. 2 Buchst. b DSGVO trägt dem Umstand Rechnung, dass Arbeitgeber im Rahmen des Beschäftigungsverhältnisses eine Vielzahl auch unter den Katalog des Art. 9 Abs. 1 DSGVO fallende Daten verarbeiten müssen. Hierbei handelt es sich nicht um einen Legitimationstatbestand selbst, sondern es wird auf das Recht der Union, der Mitgliedstaaten, Betriebsvereinbarungen und Tarifverträge verwiesen.[407] Da diese Kontexte regelmäßig außerhalb der Nutzung von Messengerdiensten liegen, soll dieser Fall nur kurz im Hinblick auf die Besonderheiten dieser Kommunikationsform angerissen werden. Erfasst wären – sofern spezialgesetzlich verankert – Verarbeitungsbefugnisse bspw. zu Zwecken der Renten- und Sozialversicherung, Krankenversicherung, Krankheitstage, Sozialhilfe, Wohnungs-, Familien- oder Ausbildungsförderung.[408] Entscheidende Hürden sind zum einen das Kriterium der Erforderlichkeit und zum anderen „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ eingerichtet werden.[409] Die Garantien werden nicht definiert, in der Literatur erörtert werden sowohl die Verstärkung der Betroffenenrechte (auf Auskunft, Berichtigung, Löschung etc.) als auch technische und organisatorische Maßnahmen (bspw. Pseudonymisierung und Verschlüsselung).[410] Dies bedeutet aber auch, dass Daten bspw. zum gesundheitlichen Zustand bei Krankmeldungen besonders geschützt in Personalakten verwahrt werden müssen, sodass eine zufällige Kenntnisnahme ausgeschlossen ist. [411]

Im Rahmen der Sonderregelung zum Beschäftigtendatenschutz im BDSG widmet sich § 26 Abs. 3 BDSG der Verarbeitung besonderer Kategorien personenbezogener Daten. Diese ist zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Insofern ist auch hier eine Erforderlichkeitsprüfung durchzuführen.[412] Flankierend sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (vgl. § 22 Abs. 2 BDSG). Je wirkungsvoller die gewählten Schutzmaßnahmen sind, desto eher fällt eine Interessenabwägung zugunsten der Zulässigkeit einer Datenverarbeitung aus.[413]

---

[407] *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 52; *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 20; *Mester,* in: Taeger/Gabel - DSGVO/BDSG Art. 9 Rn. 21; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 37.
[408] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 20; *Mester,* in: Taeger/Gabel - DSGVO/BDSG Art. 9 Rn. 21.
[409] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 39; für eine enge Auslegung: *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 54; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 41.
[410] *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 28.
[411] BAG, Urteil vom 12.9.2006 – 9 AZR 271/06, Rn. 22 ff.; *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 40.
[412] *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 51.
[413] *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 53.

Rechtsprechung der Arbeitsgerichte

- Personalakten dürfen nicht allgemein zugänglich sein und müssen sorgfältig verwahrt werden (BAG, Urteil vom 12.9.2006 – 9 AZR 271/06):
  - „Das Geheimhaltungserfordernis im Hinblick auf Teile der Personalakte kann durchaus unterschiedlich sein. […] Zu den besonders sensiblen Daten gehören insbesondere solche über den körperlichen, geistigen und gesundheitlichen Zustand und allgemeine Aussagen über die Persönlichkeit des Arbeitnehmers. Sie bedürfen deshalb des verstärkten Schutzes."
  - „Grundsätzlich hat der Arbeitnehmer keinen Anspruch auf eine bestimmte Art und Weise der Geheimniswahrung sensibler Daten. […] Dabei obliegt es grundsätzlich dem Arbeitgeber im Rahmen seiner Personal- und Organisationsfreiheit zu bestimmen, wie das besondere Geheimhaltungsbedürfnis des Arbeitnehmers an sensiblen Daten umgesetzt wird."

Öffentlich gemachte Daten: Art. 9 Abs. 2 Buchst. e DSGVO erlaubt die Verarbeitung besonderer Kategorien personenbezogener Daten, wenn es sich um Daten handelt, „die die betroffene Person offensichtlich öffentlich gemacht hat". In diesem Fall besteht keine besondere Schutzbedürftigkeit.[414] Der Verantwortliche muss in diesem Fall die Rechtmäßigkeit der Verarbeitung aber weiterhin an Art. 6 Abs. 1 DSGVO messen.[415] Voraussetzungen sind:

- Öffentlichkeit der Daten: ist gegeben, sofern die Daten dem Zugriff einer unbestimmten Anzahl von Personen ohne wesentliche Zulassungsschranke offen stehen.[416] Bei sozialen Netzwerken ist dies der Fall, wenn die Daten der Allgemeinheit zugänglich sind und nicht nur innerhalb geschlossener/privater Gruppen geteilt wurden.[417] Abgrenzungsschwierigkeiten bestehen bei Gruppen, die aus einer nicht mehr eindeutig bestimmbaren Personengruppe bestehen bzw. bei denen alle Interessierten Mitglied werden können.[418]
- Offensichtliche Veröffentlichung durch betroffene Person selbst: die Veranlassung muss sichtbar von der betroffenen Person selbst erfolgt sein, selbst wenn diese (bspw. im Rahmen der Presseberichterstattung) von Dritten durchgeführt wird. [419] Es muss aus Sicht eines objektiven Dritten ein unzweideutiger, bewusster Willensakt, der final auf die Entäußerung der Information gerichtet ist, gegeben sein.[420]

[414] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 25.
[415] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 77; *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 64; *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 25; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 57.
[416] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 26; *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 45; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 78; *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 65.
[417] *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 26.
[418] vgl. auch *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 58.
[419] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 79; *Schulz,* in: Gola DS-GVO, Art. 9 Rn. 26.
[420] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 45; *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 66; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 80; *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 9 Rn. 36; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 59.

Bei Zweifeln befürworten zahlreiche Kommentierungen den Ausschluss des Legitimationstatbestands.[421] Dies entspricht auch dem Grundsatz, dass der Verantwortliche nachweispflichtig ist, und dementsprechend den Ausnahmetatbestand nachweisen können muss.

2.4.1.5 Zwischenergebnis zum Grundsatz der Rechtmäßigkeit und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Für jede Verarbeitung personenbezogener Daten muss der Verantwortliche in der Lage sein, eine Rechtsgrundlage vorzuweisen. Dabei können auch mehrere Rechtsgrundlagen parallel eingreifen. Inwiefern die hier beschriebenen Rechtsgrundlagen im Kontext der Kommunikation im Unternehmen tatsächlich eingreifen, wird näher in Kapitel 5 beleuchtet.

2.4.2 Transparenz

Die Art. 12 bis 15 der DSGVO konkretisieren die Pflichten der Verantwortlichen hinsichtlich der Informationen, die vor oder bei der Verarbeitung der betroffenen Person zur Verfügung gestellt werden müssen. Diese datenschutzrechtlichen Informationspflichten basieren auf dem Prinzip der Transparenz, das über Art. 8 Abs. 2 EU-GrCh auch grundrechtlich verankert ist. Während Art. 13 f. DSGVO Informationspflichten *vor* der Datenverarbeitung adressieren, sind in Art. 15 DSGVO die Auskunftsrechte der Betroffenen normiert.[422]

2.4.2.1 Grundsatz

Im EG 39 werden die Grundsätze der Datenverarbeitung näher erläutert. Bestimmte Informationspflichten stellen danach die Basis für eine „faire und transparente Verarbeitung“ dar.[423]

Erwägungsgrund 39 S. 2 – 5 DSGVO

Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden,

[421] *Schiff,* in: Ehmann/Selmayr - DSGVO Art. 9 Rn. 45; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 9 Rn. 80; *Albers/Veit,* in: BeckOK DatenschutzR Art. 9 Rn. 67; *Petri,* in: NK Datenschutzrecht Art. 9 Rn. 62.

[422] Umstritten ist, ob die Informationen zwingend vor oder spätestens gleichzeitig mit der Datenerhebung bereitzustellen sind: *Schmidt-Wudy,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 13 Rn. 79; *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 13 Rn. 56; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 13 Rn. 12; *Knyrim,* in: Ehmann/Selmayr - DSGVO Art. 13 Rn. 10; *Franck,* in: Gola DS-GVO, Art. 13 Rn. 36.

[423] Weitere Grundsätze, die in EG 39 erläutert werden betreffen die Beschränkung und Festlegung der Speicher- bzw. Löschfristen sowie die Berichtigungspflicht und die Sicherheit bzw. Vertraulichkeit der personenbezogenen Daten.

wie sie ihre diesbezüglichen Rechte geltend machen können.

Regelungen genereller Art sind in Art. 12 DSGVO enthalten, der u.a. verschiedene Modalitäten zur Bereitstellung der Informationen sowie Umsetzung der Rechte der betroffenen Personen normiert:

- Verantwortliche treffen „geeignete Maßnahmen“ zur Umsetzung der Informations-, Auskunfts- und sonstigen Betroffenenrechte.
- Informationen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.
- Auskünfte sind auf Antrag „unverzüglich“ bereitzustellen, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags (Verlängerungen um zwei Monate möglich, bei Komplexität / Anzahl der Anträge). Eine Reaktion muss in jedem Fall innerhalb eines Monats erfolgen.
- Antworten sollten elektronisch erfolgen, wenn die betroffene Person diesen Kommunikationsweg wählt.
- Auskünfte sind unentgeltlich bereitzustellen. Ausnahmen sind offenkundig unbegründete oder exzessive Anträge (hier darf ein angemessenes Entgelt berechnet oder Auskunft verweigert werden).
- Bei Zweifeln über die Identität des Antragstellenden dürfen weitere Informationen zur Identitätsbestätigung angefordert werden.
- Informationen dürfen in Kombination mit standardisierten Bildsymbolen bereitgestellt werden – sofern elektronisch, sollten diese maschinenlesbar sein.

2.4.2.2 Informationspflichten

Konkrete Angaben der zu übermittelnden Informationen, dem Informationszeitpunkt und möglichen Ausnahmen sind in Art. 13 und 14 geregelt. Art. 13 DSGVO adressiert hierbei die Datenerhebung *bei der* betroffenen Person. Art. 14 DSGVO enthält hingegen Besonderheiten, wenn die Daten *nicht bei der* betroffenen Person selbst erhoben werden.

2.4.2.2.1 Datenerhebung bei der betroffenen Person

Adressat der Informationspflichten des Art. 13 DSGVO ist der Verantwortliche. Abs. 1 und 2 DSGVO legen diejenigen Informationen fest, die bereitgestellt werden müssen: diese werden in Tabelle 2 aufgelistet. Wenn eine Weiterverarbeitung zu einem anderen Zweck als den, für den die personenbezogenen Daten ursprünglich erhoben wurden, erfolgen soll, so hat der Verantwortliche nach Art. 13 Abs. 3 DSGVO der betroffenen Person vor dieser Weiterverarbeitung zusätzlich Informationen über diesen neuen Zweck und alle anderen maßgeblichen Informationen gemäß Abs. 2 zur Verfügung zu stellen.

2.4.2.2.2 Datenerhebung nicht bei der betroffenen Person

Art. 14 DSGVO regelt die Art und den Umfang der Informationspflicht des Verantwortlichen gegenüber der betroffenen Person, wenn und soweit die Daten nicht bei der betroffenen Person selbst erhoben werden. Die Abs. 1 und 2 entsprechen hierbei den Regelungen des Art. 13 Abs. 1 und 2 DSGVO (vgl. Tabelle 2 mit Hervorhebungen bei Abweichungen). Abs. 3 regelt, den spätesten Mitteilungszeitpunkt:

- Innerhalb einer „angemessenen Frist“ nach Erlangung der Daten, spätestens innerhalb eines Monats,

- Spätestens zum Zeitpunkt der ersten Kommunikationsaufnahme zur betroffenen Person,
- Bei Offenlegung an andere Empfänger: spätestens bei erster Offenlegung.

Art. 13 Abs. 1, 2 DSGVO	Art. 14 Abs. 1, 2 DSGVO
(1) a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;	(1) a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;	b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;	c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;	d) die Kategorien personenbezogener Daten, die verarbeitet werden
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten	e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.	f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.
(2) a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer	(2) a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
	b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;	c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird	d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde	e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte	f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;

f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.	g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Tabelle 2 Vergleich der nach Art. 13 und Art. 14 DSGVO bereitzustellenden Informationen (Unterschiede grün hervorgehoben)

Wenn der Verantwortliche beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten ursprünglich erhoben wurden, so stellt er der betroffenen Person auch hier nach Art. 14 Abs. 4 DSGVO vor einer Weiterverarbeitung erweiterte Informationen zur Verfügung. Art. 14 Abs. 5 DSGVO enthält Ausnahmeregelungen und bestimmt dementsprechend diejenigen Fälle, in denen Absatz 1, 2, 3 und 4 keine Anwendung finden. Weitere Ausnahmen finden sich in den §§ 29 Abs. 1 S. 1 und 33 BDSG.

2.4.2.2.3 Formvorschriften

Nach Art. 12 Abs. 1 S. 2 DSGVO erfolgt die Übermittlung der Informationen schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Dies führt dazu, dass der Verantwortliche eine freie Wahl der Form hat, es besteht auch kein Vorrang der schriftlichen vor der elektronischen Form (technikneutral).[424] Weniger relevant im Rahmen der Nutzung elektronischer Kommunikationswerkzeuge ist die in Art. 12 Abs. 1 S. 3 DSGVO normierte Möglichkeit einer mündlichen Informationsbereitstellung. Grundsätzlich wird für eine gewisse Fixierung der Mitteilung plädiert.[425] Empfohlen werden zudem insbesondere bei sehr langen Datenschutzerklärungen sog. multi-layered notices, also der Darstellung in mehrschichtiger Form, sodass sich betroffene Personen einen schnellen Überblick verschaffen können.[426]

Einen innovativen Ansatz enthalten Art. 12 Abs. 7 und 8 DSGVO mit Regelungen zur möglichen Verwendung von standardisierten Bildsymbolen – allerdings ohne diese näher zu konkretisieren. Des Weiteren sind Regelungen zur Umsetzung durch die EU-Kommission in Form von delegierten Rechtsakten aktuell noch nicht vorhanden. Will ein Verantwortlicher Piktogramme oder andere grafische Elemente einsetzen, sind diese stets neben der textuellen Informationsbereitstellung zu sehen. Eine Pflicht zusätzlich Bildsymbole zu verwenden besteht nicht.[427]

2.4.2.2.4 Ausnahmen

Verfügt die betroffene Person bereits über alle relevanten Informationen, so finden die Absätze 1, 2 und 3 des Art. 13 DSGVO (bzw. 1-4 des Art. 14 DSGVO) hingegen keine Anwendung (Art. 13 Abs. 4 und Art. 14 Abs. 5

[424] *Quaas,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 12 Rn. 27; *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 12 Rn. 16; *Greve,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 12 Rn. 18.
[425] *Paal/Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 12 Rn. 38; *Quaas,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 12 Rn. 27.
[426] *Paal/Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 12 Rn. 39.
[427] *Grewe,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 12 Rn. 32 m.w.N.

Buchs. a) DSGVO). Der Verantwortliche hat zu beweisen, dass die Informationen bereits bekannt sind.[428] Gestritten wird darüber, ob Informationspflichten nur *insgesamt* oder auch *teilweise* entfallen können.[429] Im Rahmen der elektronischen Kommunikation dürfte dieser Ausnahme keine besondere Bedeutung zukommen, da sich die Informationstexte leicht verlinken lassen.[430]

Bezüglich der in Art. 14 Abs. 5 DSGVO geregelten weiteren Ausnahmen von der Informationspflicht ist umstritten, ob diese analog auch für Art. 13 DSGVO herangezogen werden könnten. [431] Diese beziehen auch die Unmöglichkeit, einen unverhältnismäßig hohen Aufwand, die ausdrückliche Regelungen durch Rechtsvorschriften sowie berufliche Geheimhaltungspflichten mit ein. Mit Verweis auf EG 62, welcher nicht nach Erhebung bei der betroffenen Person oder bei Dritten differenziert, wird es zumindest als diskutabel aufgeworfen, ob eine Analogie möglich wäre.[432] Dagegen wird eingewandt, dass es bereits an einer planwidrigen Regelungslücke fehle und die Interessenlagen andere seien. [433] Bei einer Erhebung bei der betroffenen Person sind kaum Fälle denkbar, in welchen Unmöglichkeit anzunehmen wäre.[434]

2.4.2.2.5 Zwischenergebnis zu den Informationspflichten und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Für die Verwendung von Messengerdiensten im Unternehmenskontext ist zunächst relevant, wer Adressat der jeweiligen Informationspflichten und wem gegenüber zu informieren ist, also wer zu den betroffenen Personen zählt. Informationspflichten werden in der Praxis häufig über die Datenschutzerklärungen erfüllt. Hier zeigt sich jedoch, dass je ausführlicher der für die Verarbeitung Verantwortliche über die Datenverarbeitungsvorgänge, deren Zwecke, die Betroffenenrechte usw. informiert, desto unübersichtlicher kann die Informationsvermittlung für die betroffene Person werden. Zumeist besteht die Schwierigkeit die Balance zwischen der Verständlichkeit und der Nachvollziehbarkeit auf der einen Seite und der Informationsüberflutung auf der anderen Seite zu halten. Insbesondere bei der Verwendung von Messengerdiensten auf dem Smartphone kann dies aufgrund der geringeren Bildschirmgröße eine Herausforderung darstellen.

2.4.2.3 Auskunftsrechte

Das Auskunftsrecht des Art. 15 DSGVO steht den betroffenen Personen zu und umfasst zum einen das Recht eine Bestätigung zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden, und sofern dies der Fall ist, das Recht auf Auskunft über diese personenbezogenen Daten sowie die Mitteilung der:

- Verarbeitungszwecke,
- Kategorien personenbezogener Daten, die verarbeitet werden,
- Empfänger(-Kategorien), denen Daten offengelegt werden/wurden,

---

[428] *Wudy,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 13 Rn. 94.
[429] *Knyrim,* in: Ehmann/Selmayr - DSGVO Art. 13 Rn. 68; vgl. auch *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 13 Rn. 10.
[430] Siehe kritisch für den Offline-Bereich: *Knyrim,* in: Ehmann/Selmayr - DSGVO Art. 13 Rn. 68.
[431] *Wudy,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 13 Rn. 95.
[432] *Paal/Hennemann,* in: Paal/Pauly - DS-GVO BDSG Art. 13 Rn. 35.
[433] *Wudy,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 13 Rn. 95; *Ingold,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 13 Rn. 11; *Dix,* in: NK Datenschutzrecht Art. 13 Rn. 22.
[434] Franck beschreibt hingegen die Fallkonstellation einer unaufgeforderten Kontaktaufnahme durch die betroffene Person mit Unmöglichkeit einer Rückantwort aufgrund von Zugangshindernissen bei der betroffenen Person: *Franck,* in: Gola DS-GVO, Art. 13 Rn. 45. In solchen Ausnahmefällen dürfe es nicht dem Verantwortlichen Nachteile bereiten.

- Speicherdauer oder Kriterien für deren Festlegung,
- Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie Widerspruchsrecht,
- Beschwerderechte bei Aufsichtsbehörde,
- Herkunft der Daten, sofern nicht bei der betroffenen Person selbst erhoben, und
- bei Bestehen einer automatisierten Entscheidungsfindung gemäß Art. 22 DSGVO: aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Der Auskunftsanspruch besteht auch für die Verarbeitung personenbezogener Daten im Arbeitsverhältnis.[435] Die Reichweite über welche Daten Auskunft zu erteilen ist, hängt auch von der Bestimmung des Personenbezugs ab, denn nur über die konkret verarbeiteten personenbezogenen Daten ist Auskunft zu erteilen (vgl. Abschnitt 2.3.1.2 zum Personenbezug und Abschnitt 2.3.1.3 zum Begriff der Verarbeitung).[436] Der BGH positionierte sich jüngst gegen eine teleologische Reduktion, welche die erfassten Informationen nach Signifikanz einschränken würde.[437] Auch ist es unerheblich, ob die Information dem Auskunftsersuchenden bereits bekannt ist.[438] Bei Kommunikationsprozessen im Beschäftigungskontext, wie bspw. E-Mail-Korrespondenz, dürften aus der Perspektive des Arbeitgebers regelmäßig personenbezogene Daten vorliegen.[439] Auch gespeicherte elektronische Kommunikation über Messenger fällt hierunter.[440] Daneben steht der Anspruch auf die aufgelisteten Kontextinformationen (Metainformationen), die selbst keinen Personenbezug aufweisen müssen. Diese korrespondieren teilweise mit den Informationspflichten aus Art. 13, 14 DSGVO.[441]

Auskunftsberechtigte sind nach EG 63 S. 7 DSGVO berechtigt, ihr Auskunftsersuchen auf bestimmte Informationen oder Verarbeitungsvorgänge zu beziehen.[442] Eine Beschäftigte kann bspw. ihren zunächst umfassend bestehenden Auskunftsanspruch auf personenbezogene Leistungs- und Verhaltensdaten einschränken. Ferner sollen Betroffene ihr Recht „problemlos“ und in „angemessenen“ Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können (EG 63 S. 1 DSGVO). Artt. 12 und 15 DSGVO regeln zudem das Verfahren, wie und von wem ein Auskunftsersuchen zu stellen ist und wie und in welcher Form der Verantwortliche hiermit umzugehen hat. Das Auskunftsrecht steht der betroffenen Person zu und kann durch einen Antrag an den Verantwortlichen wahrgenommen werden, d.h. die betroffene Person muss ihr Recht aktiv wahrnehmen.[443]

Die DSGVO schreibt für das Auskunftsrecht – abgesehen von der Frage der Antwort auf elektronische Auskunftsersuchen – keine spezifische Umsetzung vor, was dem Grundsatz der Technikneutralität der DSGVO entspricht.[444] Nichtsdestotrotz bietet EG 63 S. 4 DSGVO einen Impuls, wie Verantwortliche das Recht auf Auskunft umsetzen könnten:

---

[435] LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, Rn. 172; *Düwell/Brink*, NZA 2016, 665 (667).
[436] BGH, Urteil vom 15.06.2021 –VI ZR 576/19, Rn. 22; *Engeler/Quiel*, NJW 2019, 2201 (2202). Zur Abgrenzung vgl. auch LG Köln, Teilurteil vom 18.03.2019 - 26 O 25/18, Rn. 15; KG, Beschluss vom 23.10.2018 – 6 U 45/1.
[437] BGH, Urteil vom 15.06.2021 –VI ZR 576/19, Rn. 22.
[438] BGH, Urteil vom 15.06.2021 –VI ZR 576/19, Rn. 25.
[439] Vgl. LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, Rn. 175. Schreiben der betroffenen Personen an Verantwortliche sowie Korrespondenz mit Dritten über den Betroffenen sind ebenfalls regelmäßig vom Auskunftsanspruch erfasst: BGH, Urteil vom 15.06.2021 –VI ZR 576/19, Rn. 25 f.
[440] LG Bonn, Urteil vom 01.07.2021 – 15 O 372/20, Rn. 22.
[441] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 10.
[442] LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, Rn. 176.
[443] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 13 Rn. 1; ausführlich zum Auskunftsrecht: *Engeler/Quiel*, NJW 2019, 2201.
[444] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 44a.

Erwägungsgrund 63 S. 4 DSGVO

Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde.

2.4.2.3.1 Recht auf Kopie der verarbeiteten personenbezogenen Daten

Art. 15 Abs. 3 DSGVO schreibt ferner vor, dass und in welcher Form eine Kopie über die Daten der betroffenen Person zur Verfügung zu stellen sind. Dieses Recht auf Kopie kann als ein mit der Geltung der DSGVO neu eingeführtes Recht bezeichnet werden.[445] Wurde der Antrag elektronisch gestellt wird, sind die Informationen on einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sich nichts anderes ergibt. Erst für „weitere Kopien", welche die betroffene Person beantragt, darf ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangt werden. Um eine exzessive Nutzung dieses Rechts zu verhindern sind die Kosten für weitere Kopien von der betroffenen Person zu tragen. Der Unterschied zwischen Auskunft nach Art. 15 Abs. 1 DSGVO und dem Recht eine Kopie zu erhalten liegt in der Art der Darstellung der bereitzustellenden Informationen, denn ersteres enthält zunächst keine Vorgaben hinsichtlich der Präsentation der Daten.[446] Letztere kommt einer wahrheitsgetreuen Abbildung der tatsächlichen Verarbeitungsprozesse nahe.[447]

2.4.2.3.2 Ausnahmen

Es bestehen unterschiedlichste Szenarien, in denen eine Auskunft nicht erteilt werden kann:

Mangelnde Identifizierbarkeit: In Art. 11 DSGVO wird der Sonderfall geregelt, dass der Verantwortliche die betreffende Person nicht (mehr) identifizieren kann. Der Verantwortliche soll nicht verpflichtet werden, mehr Daten als unbedingt erforderlich zu erheben und/oder zu speichern, um die Betroffenenrechte umzusetzen. Dies entspricht den Grundsätzen der Datenminimierung und Speicherbegrenzung.[448] Macht die betroffene Person ihr Auskunftsrecht geltend, ist sie hierüber zu informieren, da die weiteren Betroffenenrechte in Artt. 15 bis 20 DSGVO keine Anwendung mehr finden und nicht mehr wahrgenommen werden können, sofern eine Zuordnung beispielsweise eines Auskunftsersuchens zu den vorhandenen Daten aufgrund der fehlenden Zuordenbarkeit nicht mehr möglich ist. Gemäß Art. 12 Abs. 2 S. 2 DSGVO darf sich in diesen Fällen des Art. 11 Abs. 2 DSGVO der Verantwortliche allerdings nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte nach den Artt. 15 bis 22 DSGVO tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren. Die betroffene Person kann allerdings zusätzliche Informationen bereitstellen, die ihre Identifizierung ermöglichen.[449]

Diese Ausnahme entfaltet besonders bei der Möglichkeit „anonymer" oder pseudonymer Nutzung von Kommunikationswerkzeugen praktische Bedeutung und ist der weiten Definition personenbezogener Daten geschuldet. Hier können rechtlich gesehen grundsätzlich Identifizierungsmöglichkeiten anzunehmen sein, sodass es sich um personenbezogene Daten handelt, der Verantwortliche diese Mittel zur Identifizierung aber

[445] *Engeler/Quiel*, NJW 2019, 2201 (2201).
[446] *Engeler/Quiel*, NJW 2019, 2201 (2202).
[447] Beispiele bei: *Engeler/Quiel*, NJW 2019, 2201 (2203). Eine Aufbereitung oder Modifikation der personenbezogenen Daten kann nicht verlangt werden: *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 40.
[448] *Wolff,* in: BeckOK DatenschutzR Art. 11 Rn. 4, 8; *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 11 Rn. 1.
[449] In diesem Fall leben die Pflichten der Artt. 15 ff. DSGVO wieder auf: *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 11 Rn. 10.

nicht nutzt.[450] Die Befreiung von den Pflichten der Artt. 15 ff. DSGVO greift allerdings nur, wenn es dem Verantwortlichen nicht mit eigenen, intern verfügbaren Mitteln gelingt, eine Zuordnung des Antragstellenden vorzunehmen.[451] Zudem gilt natürlich zu bedenken, dass eine eindeutige Identifizierung nicht Klarnamen, Adresse, Geburtsdatum etc. bedeutet, sondern auf verschiedenen Wegen der Authentisierung sichergestellt werden kann, dass keine Auskunftsdaten an nicht berechtigte Personen herausgegeben werden (bspw. Missbrauch eines Pseudonyms nach Identitätsdiebstahl).[452]

Rechte und Freiheiten anderer Personen: Das Recht auf Erhalt einer Kopie gemäß Art. 15 Abs. 3 DSGVO darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen (Art. 15 Abs. 4 DSGVO). Hierzu werden auch die Rechte juristischer Personen gezählt.[453] Zu den „anderen Personen" zählt auch der Verantwortliche selbst.[454] Anders als der Auskunftsanspruch, steht das Recht auf Kopie unter einem Abwägungsvorbehalt. [455] Es wird zwar vertreten, dass sich diese Einschränkung auch auf den Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO beziehe.[456] Dies entspricht allerdings nicht dem Wortlaut.[457] Unklar ist, ob es sich bloß um ein Redaktionsversehen handelt. [458]

Das Recht auf Kopie kann folglich ausgeschlossen oder eingeschränkt sein,

- wenn in der Kopie personenbezogene Daten enthalten sind, die sich auf Dritte beziehen, sodass in einer Weitergabe eine Verletzung ihrer Datenschutz- und Persönlichkeitsrechte läge,
- wenn die Herausgabe Urheberrechte oder Geschäftsgeheimnisse berührt, wenn deren Schutz die Rechte der auskunftsstellenden betroffenen Person überwiegen (vgl. EG 63 S. 5 DSGVO),
- bei unverhältnismäßigem Aufwand sollte der Verantwortliche verlangen können, dass die betroffene Person ihr Auskunftsersuchen präzisiert (vgl. EG 63 S. 7 DSGVO), offensichtlich unbegründete oder exzessive Anfragen können abgelehnt werden (vgl. Art. 12 Abs. 5 S. 2 DSGVO).[459]
- Den Verantwortlichen trifft insoweit die Beweislast einer konkreten Kollisionslage (die bloße Besorgnis der Gefährdung dieser Rechte reicht nicht) und darf nach herrschender Meinung nicht jegliche Auskunft verweigern, sondern die Mitteilung entsprechend kürzen (z.B. Teilkopie, Schwärzungen, etc.).[460] Auch dieser Ausschluss dürfte für elektronische Kommunikationsdienste von erheblicher Bedeutung sein, da zumeist die Kommunikationspartner natürliche Personen sind und damit Datenschutzrechte geltend machen können. Ein weiteres Beispiel könnten übermittelte Medien sein. Hier könnten die Urheberrechte anderer Personen betroffen sein.

Entgegenstehende Interessen (BDSG): Beschränkungen des Auskunftsrechts durch mitgliedstaatliches Recht sind nach der Maßgabe des Art. 23 DSGVO möglich.[461] Bestimmte Beschränkungen können durchaus zur Umsetzung eines grundrechtlichen Schutzauftrags geboten sein, wie bspw. die Erfüllung der Pflichten

[450] *Wolff,* in: BeckOK DatenschutzR Art. 11 Rn. 12.
[451] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 11 Rn. 13 ff. *Wolff,* in: BeckOK DatenschutzR Art. 11 Rn. 15 ff.
[452] *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG Art. 11 Rn. 15 f.
[453] *Engeler/Quiel*, NJW 2019, 2201 (2203).
[454] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 42.
[455] *Engeler/Quiel*, NJW 2019, 2201 (2203).
[456] So *Paal* in: Paal/Pauly - DS-GVO BDSG Art. 15 Rn. 41; *Specht,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 15 Rn. 22.
[457] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 33.
[458] So *Specht,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 15 Rn. 22.
[459] *Engeler/Quiel*, NJW 2019, 2201 (2203); *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 42b.
[460] *Specht,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 15 Rn. 24; *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 42a.
[461] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 33.

von Berufsgeheimnisträgern, oder zum Schutz behördlicher Informanten.[462] Nach § 34 Abs. 1 i.V.m. § 29 Abs. 1 S. 2 BDSG besteht das Recht auf Auskunft nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.[463] Diese Regelungen in § 34 Abs. 1 i.V.m. § 29 Abs. 1 und 2 BDSG beruhen nach Einschätzung des LAG Baden-Württemberg auf der Öffnungsklausel des Art. 23 Abs. 1 Buchst. i DSGVO, wonach zum Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen Informations- und Benachrichtigungspflichten des Verantwortlichen bzw. das Auskunftsrecht betroffener Personen beschränkt werden können.[464]

2.4.2.3.3 Zwischenergebnis zum Auskunftsrecht und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Auskunftsersuchen können betroffene Personen an den Verantwortlichen stellen – dies könnten die Arbeitgeber/das Unternehmen und/oder der Messengerdienstanbieter sein. Der Verantwortliche kann zur Erfüllung seiner korrespondierenden Auskunftspflichten einen Auftragsverarbeiter, der in die Verarbeitung involviert ist, einbeziehen. Bei einer gemeinsamen Verantwortlichkeit müssen die jeweiligen Verantwortlichen Stellen dafür Sorge tragen, dass die notwendigen Informationen an die betroffene Person übermittelt werden. In Kommunikationskontexten ist im Hinblick auf den Schutz der Rechte Dritter zu beachten, dass Inhalte, die weitere Personen betreffen, von der Bereitstellung einer Kopie ggf. ausgenommen werden müssen. Festzuhalten bleiben als wesentliche Parameter zur Möglichkeit eines Auskunftsersuchens:

Antrag: keine Formerfordernisse oder Begründung erforderlich

Frist: Beantwortung eines Auskunftsersuchens innerhalb eines Monats

Kosten: Auskunftserteilung unentgeltlich (Ausnahme Missbrauchsfälle)

Form: grundsätzlich formfrei; in elektronischer Form, sofern Antrag elektronisch erfolgte (und kein anderes Format gewünscht)

2.4.3 Zweckbindung

Bereits in Art. 8 Abs. 2 EU-GRCh („festgelegte Zwecke“) findet sich der Grundsatz der Zweckbindung.[465] Aufgrund der unmittelbaren Wechselwirkung zu den weiteren Datenschutzgrundsätzen, ist der Grundsatz der Zweckbindung eines der zentralen Prinzipien des europäischen und deutschen Datenschutzrechts und ist zudem unmittelbarer Ausfluss des grundrechtlich geschützten Rechts auf informationelle Selbstbestimmung.[466] Er wird als Ausdruck des Grundsatzes der Verhältnismäßigkeit verstanden.[467]

---

[462] *Bäcker,* in: Kühling/Buchner - DS-GVO/BDSG Art. 15 Rn. 33; vgl. *Franck,* in: Gola DS-GVO, Art. 15 Rn. 36.
[463] LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, Rn. 179.
[464] LAG Baden-Württemberg, Urt. v. 20.12.2018 – 17 Sa 11/18, Rn. 179.
[465] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 57.
[466] *Culik/Döpke*, ZD 2017, 226 (227). Vgl. zur Bedeutung des Verarbeitungszwecks: *Raabe/Wagner*, Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data, S. 16 f.; BVerfGE 65, 1 – Volkszählungsurteil.
[467] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 57 ff.

Art. 5 Abs. 1 Buchst. b DSGVO

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Dem Grundsatz der Zweckbindung folgend sind Zwecke im Vorfeld der Verarbeitung so zu formulieren, dass sie eindeutig sind. Hiermit soll sichergestellt werden, dass sich Verantwortliche *vor* der Verarbeitung bewusstwerden, welches Ziel mit der Verarbeitung verfolgt wird und dies den betroffenen Personen im Rahmen der Informationspflichten kommunizieren können. Des Weiteren dürfen personenbezogene Daten nicht auf eine Art und Weise weiterverarbeitet werden, die mit dem ursprünglich festgelegten Zweck nicht vereinbar ist.[468]

2.4.3.1 Zweckfestlegung

Um prüfen zu können, ob sich eine Datenverarbeitung (noch) im festgelegten Zweck bewegt, oder bereits eine Zweckänderung vorliegt, ist es entscheidend, wie konkret Verarbeitungszwecke festgelegt werden müssen. Entsprechend des risikobasierten Ansatzes[469] der DSGVO wird vertreten, dass sich auch der Konkretisierungsgrad der Zweckfestlegung am Risiko orientieren sollte, d.h. bei geringen Risiken könnten Zwecke weiter gefasst werden als bei risikobehafteten Verarbeitungsarten oder -kontexten.[470] Es ist durchaus möglich, mehrere Zwecke zu benennen, zu pauschal gehaltene Zweckangaben sollen hingegen nicht genügen.[471]
Art. 5 Abs. 1 Buchst. b DSGVO benennt die folgenden Kriterien für die Zweckfestlegung:

- **Festgelegt:** beschreibt die Erforderlichkeit einer hinreichenden Konkretisierung der verfolgten Zwecke. Diese ist relevant, um Ziel und Umfang einer Datenverarbeitung klar und präzise genug einzugrenzen, dass bspw. im Rahmen der Informationspflichten ausreichend Transparenz erreicht wird, die Erforderlichkeit einer Datenverarbeitung zur Zielerreichung prüfbar ist, im Rahmen der Einwilligung die Tragweite der Einwilligungserklärung durch die betroffene Person abgeschätzt werden kann oder im Rahmen der Interessenabwägung die in Verhältnis zu setzenden Interessenlagen hinreichend klar definiert sind.[472]
- **Eindeutig:** steht auch für das „Merkmal des Erklärens“ (dies wird mit dem englischen Begriff des „explicit“ deutlicher).[473] Die Angabe eines Zwecks soll unmissverständlich und unzweideutig zum Ausdruck kommen.[474]
- **Legitim:** der gewählte Zweck darf nicht im Konflikt mit der Rechtsordnung stehen.[475]

Die Angabe eines Zwecks hat folglich weitreichende Folgen, da die Zielsetzung entscheidenden Einfluss auf die Art und Dauer der Verarbeitung personenbezogener Daten hat.[476] Die Verarbeitung personenbezogener Daten ist grundsätzlich nur insoweit zulässig, wie sie vom gewählten Zweck getragen wird.

[468] Siehe hierzu: *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on Purpose Limitation - WP 203.
[469] Zum risikobasierten Ansatz: *Bieker u. a.*, DuD 2018, 492 (492 f.); *Veil*, ZD 2015, 347 (347 ff.); *Schröder*, ZD 2019, 503; *Voigt,* in: Konzerndatenschutz Teil 3, Kapitel 2 Grundsätze der Verarbeitung nach der DSGVO, Rn. 14; *Martin u. a.*, DuD 2020, 149 (150 f.).
[470] *Grafenstein, von*, DuD 2015, 789; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 5 Rn. 14.
[471] *Culik/Döpke*, ZD 2017, 226 (227).
[472] *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on Purpose Limitation - WP 203, S. 12 ff.
[473] *Monreal*, ZD 2016, 507 (509).
[474] *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on Purpose Limitation - WP 203, S. 17.
[475] *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on Purpose Limitation - WP 203, S. 19 f.; *Monreal*, ZD 2016, 507 (509).
[476] Vgl. *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 5 Rn. 34.

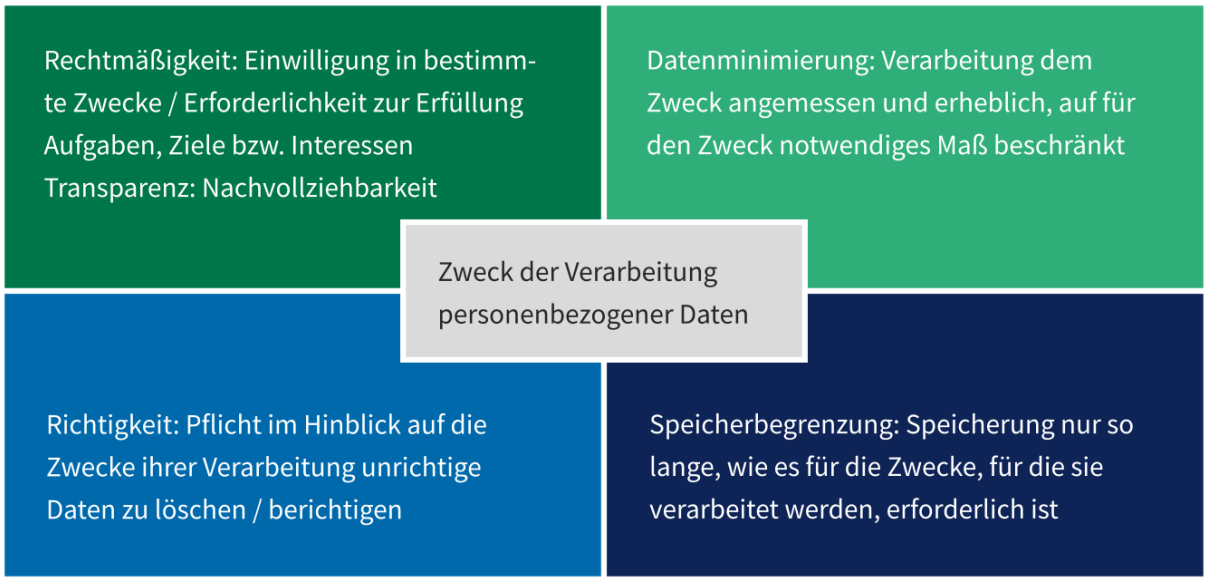


Abbildung 7 Wechselbeziehung des Zweckbindungsgrundsatzes zu anderen Datenschutzgrundprinzipien

Die betroffene Person muss anhand der Zweckangabe wissen können, wofür ihre personenbezogenen Daten verwendet werden sollen. Nicht ausreichend sind Angaben wie beispielsweise „für Marketingzwecke“, da die betroffene Person sich hierbei kein Bild davon machen kann, welche Verarbeitungen hier stattfinden können.[477]

Praxistipp:

Verantwortliche Stellen sollten davon ausgehen, dass zu unklar formulierte Zwecke, die für die betroffene Person nicht nachvollziehbar sind, im Zweifelsfall zu ihren Lasten gehen und zu einer unzulässigen Verarbeitung führen könnten.[478]

2.4.3.2 Vereinbarkeit der Zwecke / Kompatibilitätstest

Die „Zweckbindung“ gilt nicht umfassend. Gleichwohl ist auch eine Zweckänderung grundsätzlich möglich, sofern eine Vereinbarkeit der Zwecke vorliegt. Art. 6 Abs. 4 DSGVO regelt die Möglichkeiten, Grenzen und Rahmenbedingungen einer Verarbeitung personenbezogener Daten zu Zwecken, die von denjenigen abweichen, zu denen die Daten ursprünglich erhoben wurden.

[479]

- Eine Rechtsvorschrift der Union oder der Mitgliedstaaten erlaubt die Zweckänderung, wobei diese Vorschrift eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum

[477] *Wolff,* in: BeckOK DatenschutzR, Kap. Syst. A. Prinzipien, Rn. 19.
[478] Vgl. *Helfrich* in: Handbuch Multimedia-Recht, Teil 16.1 Rn. 92; *Simitis,* in: Simitis, BDSG, § 28 Rn. 42.
[479] Kritisch im Kontext umfangreicher Datenverarbeitung: *Culik/Döpke*, ZD 2017, 226 (228).

Schutz bestimmter Ziele darstellen muss (vgl. Art. 23 Abs. 1 DSGVO).[480]

- Es liegt eine Vereinbarkeit der Zwecke vor. Eine solche wird bspw. im Rahmen der Forschung angenommen, wobei die Reichweite dieser Forschungsprivilegierung durchaus umstritten ist.[481]
- Die Vereinbarkeit der Zwecke wird durch den sog. Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO nachgewiesen.[482]

Ergeben sich bspw. nach Vertragsbeendigung und/oder nach Erfüllung der ursprünglichen Zwecke der Verarbeitung berechtigte Interessen zur weiteren Verarbeitung (insbesondere Speicherung zur späteren Weiterverarbeitung), so ist zu prüfen, ob ein Fall einer zulässigen Zweckänderung nach Art. 6 Abs. 4 DSGVO vorliegt. Umstritten ist bei einer Zweckänderung auf Basis des Kompatibilitätstests, ob nur dieser durchzuführen ist, oder zusätzlich auch eine neue Rechtsgrundlage gegeben sein muss.[483] So lautet EG 50 S. 2 DS-GVO „In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten." Hierbei soll es sich allerdings um ein redaktionelles Versehen handeln.[484] Mit Verweis auf die Entstehungsgeschichte der DSGVO und die grundrechtliche Verbürgung des Zweckbindungsprinzips wird trotz des Erwägungsgrunds gefordert, dass eine Weiterverarbeitung zu neuen Zwecken wie nach der bisherigen Rechtslage nur nach einer Zwei-Stufen-Prüfung aus Kompatibilitätstest und zusätzlicher Rechtsgrundlage zulässig sein soll.[485] Andere Autoren fordern hingegen kompensatorisch gesteigerte Anforderungen an Transparenz und Datenrichtigkeit.[486]

Vielfach dürfte der Streit in der Praxis dahinstehen. Denn neben der Möglichkeit der Einwilligung dürften die neuen Zwecke zumeist auf der Wahrnehmung berechtigter Interessen beruhen. Die Anforderungen des Kompatibilitätstests zwischen (altem) Primär- und (neuem) Sekundärzweck überschneiden sich in einigen wesentlichen Punkten mit den Anforderungen an die Interessenabwägung.[487] Gemäß Art. 6 Abs. 4 DSGVO müssen bei einer Zweckänderung, die nicht durch Einwilligung oder eine Rechtsvorschrift bereits legitimiert ist, mindestens folgende Kriterien „berücksichtigt", d.h. geprüft werden:

- jede Verbindung zwischen den Erhebungs- und Weiterverarbeitungszwecken,
- Zusammenhang und Kontext der Erhebung, insbesondere Beziehung zwischen Verantwortlichem und betroffener Person,
- Art und Sensibilität der personenbezogenen Daten, insbesondere ob es sich um besondere Kategorien personenbezogener Daten oder strafrechtlich relevante Daten handelt,
- Mögliche Folgen der beabsichtigten Weiterverarbeitung für die betroffene Person
- Einsatz geeigneter Schutzmaßnahmen wie Pseudonymisierung oder Verschlüsselung.

Die genannten Kriterien sind nicht abschließend und nicht obligatorisch, da es sich nur um eine Pflicht zur

[480] Für eine restriktive Auslegung: *Culik/Döpke*, ZD 2017, 226 (229).
[481] *Weichert*, ZD 2020, 18 (21); *Johannes/Richter*, DuD 2017, 300 (301).; für eine einschränkende Auslegung: *Roßnagel*, ZD 2019, 157 (162); *Roßnagel,* in: NK-DatenschutzR NK Datenschutzrecht Art. 5 Rn. 103 ff.
[482] Zur Entstehungsgeschichte: *Albrecht*, CR 2016, 88 (92).
[483] Zum Streit: *Schantz*, NJW 2016, 1841 (1844); *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 76; *Piltz*, K&R 2016, 557 (566); *Culik/Döpke*, ZD 2017, 226 (230); *Richter*, DuD 2016, 581 (584); *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3746); *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 31.
[484] *Richter*, DuD 2016, 581 (584).
[485] *Schantz*, NJW 2016, 1841 (1844); *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 76; a.A. *Piltz*, K&R 2016, 557 (566).
[486] *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 31.
[487] Vgl. auch *Culik/Döpke*, ZD 2017, 226 (229).

„Berücksichtigung“ handelt.[488]

Nach der Terminierung eines Vertrages wertet es der European Data Protection Board als grundsätzlich entgegen der Erwartungen der betroffenen Personen und der Grundsätze der Fairness und Zweckbindung, wenn Daten mittels eines Auswechselns der Rechtsgrundlage einfach weiterverarbeitet werden.[489] Es bestehen allerdings auch Möglichkeiten, die eine Weiterverarbeitung legitimieren. Die Löschpflichten gelten nicht, wenn die Verarbeitung für bestimmte Zwecke weiterhin erforderlich ist, einschließlich der Erfüllung einer Rechtspflicht nach Art. 17 Abs. 3 Buchst. b DSGVO oder der Begründung, Ausübung oder Abwehr von Rechtsansprüchen nach Art. 17 Abs. 3 Buchst. e DSGVO. Rechtliche Aufbewahrungsfristen sollten allerdings von Beginn an kommuniziert werden, sodass kein Fall der Zweckänderung vorliegt.

2.4.3.3 Zwischenergebnis zur Zweckbindung und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Das Prinzip der Zweckbindung bedeutet für den für die Verarbeitung Verantwortlichen, dass sie sich vorab vor einer Datenverarbeitung Gedanken über den Zweck der Verarbeitung der personenbezogenen Daten machen muss. Diese Zwecke sind der betroffenen Person in einer Art und Weise zu nennen, die für diese nachvollziehbar bzw. verständlich ist.

Mit der Verfolgung eigener oder fremder Zwecke, entscheidet sich zudem die Frage nach der (ggf. gemeinsamen) Verantwortlichkeit in Abgrenzung zur Auftragsverarbeitung. Sofern in der Unternehmenskommunikation das einen Kommunikationsdienst verwendende Unternehmen als verantwortliche Stelle anzusehen ist, so müsste dieses die Zwecke festlegen und die Beschäftigten bzw. weitre betroffene Personen entsprechend informieren.

2.4.4 Datenminimierung

Der Grundsatz der Datenminimierung basiert auf dem Gedanken, dass die Datenverarbeitung in Umfang und Eingriffsintensität auf das Maß begrenzt werden soll, welches für die Zweckerreichung wirklich erforderlich ist. Insgesamt sollten so wenig personenbezogene Daten wie möglich verarbeitet werden.

[488] *Culik/Döpke*, ZD 2017, 226 (229).
[489] *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, S. 12.

Art. 5 Abs. 1 Buchst. c DSGVO

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein

2.4.4.1 Grundsatz

Besondere Erwähnung findet der Grundsatz der Datenminimierung im Rahmen der Regelungen zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in Art. 25 DSGVO.[490] Die Zielsetzung des Konzepts „Privacy by Default & Design“ beschränkt sich allerdings nicht auf die Datenminimierung, sondern die Einhaltung aller in Art. 5 DSGVO niedergelegten Datenschutzprinzipien sowie dem Schutz der in Art. 1 Abs. 2 DSGVO genannten Grundrechte und Grundfreiheiten natürlicher Personen, d.h. insbesondere das in Art. 8 EU-GrCh niedergelegte Recht auf Schutz personenbezogener Daten aber auch die über Art. 7 EU-GrCh garantierte Achtung des Privat- und Familienlebens.[491]

2.4.4.2 Datenminimierung und Datenschutz durch Technikgestaltung

In Art. 25 DSGVO sind die Prinzipien „Privacy by Default & Design“ normiert. Das Prinzip der Datenminimierung kann schon dadurch umgesetzt werden, dass so wenig wie möglich personenbezogene Daten verarbeitet werden. Dies kann durch entsprechende Voreinstellungen in den Anwendungen erreicht werden. Des Weiteren kann das Prinzip der Datenminimierung durch Privacy by Design umgesetzt werden, indem schon im Entwicklungsprozess analysiert wird, welche Datenverarbeitung für einen Dienst notwendig und erforderlich sind und sich dementsprechend im Rahmen einer Anforderungsanalyse einer Dienst- oder Systementwicklung die notwendigen Daten und Datenverarbeitungsvorgänge identifizieren lassen. Da Art. 25 DSGVO sanktionsbewerte Vorgaben macht, soll im Folgenden analysiert werden, welche konkreten Anforderungen sich aus der Vorschrift unter besonderer Berücksichtigung der Kommunikation im Unternehmenskontext ableiten lassen.

Adressat der Verpflichtung zum Privacy by Design/Default i.S.d. Art. 25 Abs. 1 und 2 DSGVO ist nur der Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO. Im Umkehrschluss bedeutet dies jedoch, dass die Hersteller von Produkten und Dienstleistungen nicht den Pflichten der Verordnung unterworfen sind. Die Vorstellung des Verordnungsgebers war, dass der Mechanismus des Privacy by Design „übers Dreieck“ wirken soll.[492] Dies wird weiterhin deutlich in Erwägungsgrund 78:

Erwägungsrund 78 S. 4 DSGVO

In Bezug auf die Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten oder Produkten die entweder auf der Verarbeitung personenbezogener Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller […] ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte,

[490] Vgl. *Grages/Plath*, CR 2017, 791 (796).
[491] *Baumgartner/Gausling*, ZD 2017, 308 (309).
[492] Vgl. *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 25 Rn. 25.

> Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.

2.4.4.2.1 Risikobasierter Ansatz und Bestimmung des Risikos

Art. 25 Abs. 1 DSGVO statuiert keine Pflicht besondere Technologien einzusetzen, sondern folgt dem technologieneutralen Ansatz der DSGVO.[493] Vielmehr sind unter Berücksichtigung der folgenden Aspekte „geeignete technische und organisatorische Maßnahmen“ als auch „die notwendigen Garantien“ umzusetzen, um den Anforderungen der DSGVO zu genügen:

- Stand der Technik,
- Implementierungskosten,
- Art, Umfang, Umstände und Zwecke der Verarbeitung sowie
- Unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.

Je höher der Schutzbedarf und die Eingriffsintensität ausfällt, desto höhere Anstrengungen werden im Hinblick auf die zu ergreifenden Maßnahmen gestellt.[494] Art. 26 Abs. 1 DSGVO adressiert hierbei zwei Zeitpunkte:

- zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch
- zum Zeitpunkt der eigentlichen Verarbeitung.

In dieser Norm manifestiert sich der Vorfeldschutzcharakter des Datenschutzrechts.[495] Einen der zentralen Abwägungsfaktoren stellt dabei der Begriff des Risikos dar: Diese Formulierung entspricht dem risikobasierten Ansatz der DSGVO, welcher sich auch ganz maßgeblich in Art. 24, 32 und 35 DSGVO wiederspiegelt.[496] Entsprechend muss der verantwortliche eine Risikoanalyse in Form einer systematischen und gründlichen Bewertung der Verarbeitungstätigkeit durchführen, um Gegenmaßnahmen dem entsprechenden Risiko anzupassen.[497] Dabei fordert der EDSA, dass Verantwortliche ihre Verarbeitungsvorgänge durch regelmäßige Überprüfungen der Wirksamkeit der von ihnen gewählten Maßnahmen und Sicherheitsvorkehrungen stets aktualisieren und neu bewerten.[498]

2.4.4.2.2 Ermittlung des Stands der Technik

Art. 25 Abs. 1 DSGVO verpflichtet zum Einsatz angemessener und „geeigneter“ technischer und organisatorischer Maßnahmen (TOM) sowie „notwendiger“ Schutzmaßnahmen („Garantien“).[499] TOMs können in einem weiten Sinne als alle Methoden oder Mittel verstanden werden, die ein für die Verarbeitung Verantwortlicher einsetzen kann, um die Rechte und Freiheiten betroffener Personen zu schützen und die Grundsätze der

[493] Siehe EG 15 S. 1 DSGVO; vgl. auch VG Gelsenkirchen, Urt. v. 27.4.2020 – 20 K 6392/18 NVwZ-RR 2020, 1070 Rn. 64.
[494] *Bieker*, DuD 2018, 27 (27).
[495] Siehe zum Vorfeldschutz: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 89 ff.; vgl. auch *Bieker u. a.*, DuD 2018, 492 (492).
[496] *Baumgartner/Gausling*, ZD 2017, 308 (310). Zum risikobasierten Ansatz: *Bieker u. a.*, DuD 2018, 492 (492 f.); *Veil*, ZD 2015, 347 (347 ff.); *Schröder*, ZD 2019, 503; *Voigt,* in: Konzerndatenschutz Teil 3, Kapitel 2 Grundsätze der Verarbeitung nach der DSGVO, Rn. 14; *Martin u. a.*, DuD 2020, 149 (150 f.).
[497] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9.
[498] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 11.
[499] Die DSGVO verwendet zwar in der deutschen Sprachfassung den Begriff „Garantien“. Der Begriff „safeguards“ der englischen Version, lässt sich inhaltlich allerdings besser mit Schutzvorkehrung oder Sicherungsmaßnahme übersetzen.

DSGVO einzuhalten.[500] Die DSGVO verweist zwar vielfach auf den „Stand der Technik", enthält allerdings keine eigenständige Definition, sodass auf die in anderen Rechtskontexten entwickelten Grundsätze zurückgegriffen werden muss. [501]

2.4.4.2.2.1 Abgrenzung „allgemein anerkannte Regeln der Technik", „Stand der Technik" und „Stand der Wissenschaft und Technik"

Im Rahmen des deutschen Verfassungsrechts hat das BVerfG aufgezeigt, welcher Nuancierungen sich der Gesetzgeber bedienen kann, wenn rechtliche Anforderungen an aktuelle Entwicklungen aus der technischen Domäne geknüpft werden sollen: [502]

„Allgemein anerkannte Regeln der Technik": Dieser Maßstab beschreibt die herrschende Auffassung unter den Praktiker*innen sowie bereits praktisch Bewährtes. Diese Regeln werden aber regelmäßig hinter weiterstrebenden, neueren technischen Entwicklungen hinterherhinken.[503]

„Stand der Wissenschaft und Technik": Bei der Nutzung dieser Terminologie werden die vom Normadressaten zu berücksichtigenden Anforderungen „an die Front der technischen Entwicklung verlagert".[504]

„Stand der Technik": ist angesiedelt zwischen den beiden zuvor genannten Technologieniveaus.[505] Auch der BGH verortet den Stand der Technik nicht in der Branchenüblichkeit, sofern der in der Branche praktizierte Standard hinter technisch Möglichem und rechtlich Gebotenen Standards zurückbleibt.[506] Normen und Standards, d.h. Regelungswerke von Standardisierungsgremien und internationalen Organisationen für Normung können als Indizien herangezogen werden.[507] Ist die technische Entwicklung über den Stand einer Norm hinausgegangen, reicht die Erfüllung der Norm hingegen nicht aus.[508]

2.4.4.2.2.2 Stand der Technik im Zivil- und Strafrecht

Auch wenn der Begriff grundsätzlich nach Unionsrecht zu bestimmen ist, lohnt ein vergleichender Blick auf die Verwendung der Begrifflichkeit in anderen Rechtsgebieten.

„Stand der Technik" im Produkthaftungsrecht: § 1 Abs. 2 Nr. 5 ProdHaftG befreit den Hersteller eines Produkts i.S.d. § 2 ProdHaftG, wenn ein der Fehler i.S.d. § 3 Abs. 1 ProdHaftG nach dem „*Stand der Wissenschaft und Technik*" in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte. Ob ein Fehler vorliegt, hängt von den berechtigten Sicherheitserwartungen der in einem bestimmten Bereich vorherrschenden Verkehrsauffassung im Zeitpunkt des Inverkehrbringens ab, welche wiederum daran anknüpfen, was objektiv wissenschaftlich-technisch möglich ist.[509] Der Stand der Wissenschaft und Technik bezeichnet den „Inbegriff der Sachkunde […], die im wissenschaftlichen und techni-

---

[500] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 6.
[501] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 8.
[502] BVerfGE 49, 89 (135 ff.) – Kalkar I.
[503] BVerfGE 49, 89 (135 ff.) – Kalkar I.
[504] BVerfGE 49, 89 (135 ff.) – Kalkar I.
[505] *Bundesverband IT-Sicherheit e.V. (TeleTrusT),* Handreichung zum „Stand der Technik", S. 11.
[506] BGHZ 181, 253 = NJW 2009, 2952 (2953); *Bräutigam/Klindt*, NJW 2015, 1137 (1141); *Schrader*, DAR 2016, 242 (243).
[507] BGH, Urteil vom 27.09.1994 - VI ZR 150/93, NJW 1994, 3349 (3350).
[508] BGH, Urteil vom 27.09.1994 - VI ZR 150/93, NJW 1994, 3349 (3350).
[509] BGH, Urteil vom 16.06.2009 - VI ZR 107/08, BGHZ 181, 253, NJW 2009, 2952 (2953); *Gomille*, JZ 2016, 76 (77); *Wagner,* in: MüKoBGB, § 1 ProdHaftG Rn. 50; *Seibl,* in: BeckOGK Zivilrecht, § 1 ProdHaftG Rn. 1222.

schen Bereich vorhanden ist, also die Summe an Wissen und Technik, die allgemein anerkannt ist und allgemein zur Verfügung steht."[510] Um den aktuellen Stand festzustellen, kann oftmals auf Regelungswerke von Standardisierungsgremien und internationalen Organisationen für Normung (DIN, IEC, ISO) zurückgegriffen werden.[511] Da aber in den meisten Kontexten eine völlige Gefahrlosigkeit nicht erwartbar ist, orientiert sich der Maßstab grundsätzlich auch an der Bedeutung der gefährdeten Rechtsgüter und der Schadenseintrittswahrscheinlichkeit.[512] Je größer die Gefahren sind, desto höher fallen die Sicherheitserwartungen aus.[513] Im Hinblick auf den Haftungsausschluss kommt es nicht auf die individuellen Kenntnisse des Herstellers, sondern wieder wesentlich auf den Stand der Wissenschaft und Technik an.[514] Der Nachweis stellt recht hohe Anforderungen an das Qualitätsmanagement des Herstellers um zu beweisen, dass alle zum maßgeblichen Zeitpunkt verfügbaren Erkenntnisse ausgeschöpft wurden und die Gefährlichkeit des Produkts folglich von niemandem hätte erkannt werden können.[515]

„Stand der Technik" im Wettbewerbsrecht: Der österreichische Oberste Gerichtshof (ÖOGH) stellte zum Stand der Technik fest, dass dieser sich einer einheitlichen Auslegung entzieht: so wird im Wettbewerbsrecht als „Stand der Technik" einerseits das Fachwissen bezeichnet, über das der/die „Durchschnittsfachmann/fachfrau" auf dem betreffenden Gebiet verfügt (allgemein bekannt in Fachkreisen), – andererseits werden auch bestimmte Produkteigenschaften oder Herstellungsmethoden als zum „Stand der Technik" gehörend bezeichnet. „Das schließt aber nicht aus, dass die dafür notwendigen Informationen im Sinn von Anleitungen oder Plänen geheim sein können, wenn sie der Fachmann nur mit erheblichem Aufwand entwickeln kann."[516]

2.4.4.2.2.3 Definition des Europäischen Datenschutzausschusses (EDSA)

Der Europäische Datenschutzausschuss verortet in seinen Guidelines den "Stand der Technik" zwischen dem innovativeren Stand der "vorhandenen wissenschaftlichen Erkenntnisse und Forschung" und den etablierteren "allgemein anerkannten Regeln der Technik". Der "Stand der Technik" kann somit als das Technologieniveau einer Dienstleistung, Technologie oder eines Produkts identifiziert werden, das auf dem Markt existiert und am effektivsten ist, um die identifizierten Ziele zu erreichen. [517]

Abbildung 8 Abgrenzung der Technologiestände[518]

[510] *Seibl,* in: BeckOGK Zivilrecht, § 1 ProdHaftG Rn. 123; *Gomille*, JZ 2016, 76 (78).
[511] BGH, Urteil vom 27.09.1994 - VI ZR 150/93, NJW 1994, 3349 (3350).
[512] *Schrader*, DAR 2016, 242 (242 f.); *Gomille*, JZ 2016, 76 (77); *Bodungen, von/Hoffmann*, NZV 2018, 97 (98).
[513] BGH, Urteil vom 16.06.2009 - VI ZR 107/08, NJW 2009, 2952 (2953 f.), Rn. 18; *Horner/Kaulartz*, CR 2016, 7 (11).
[514] BT-Drs. 11/2447, S.15; *Schrader*, DAR 2016, 242 (243); *Wagner,* in: MüKoBGB, § 1 ProdHaftG Rn. 54.
[515] *Gomille*, JZ 2016, 76 (79); *Wagner/Goeble*, ZD 2017, 263 (266).
[516] ÖOGH, Entscheidung vom 26.01.2021 – 4Ob188/20f, Rn. 35; vgl. auch BGH, Urteil vom 22.3.2018 – I ZR 118/16, Rn. 35 ff.
[517] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 8.
[518] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik", S. 11.

Technische Entwicklungen im Stadium des "Stands der Wissenschaft und Forschung" sind zumeist sehr dynamisch und gehen mit der Erreichung der Marktreife bzw. ihrer Markteinführung in das Stadium "Stand der Technik" über.[519]

2.4.4.2.2.4 Stand der Technik bei Messengerdiensten

Der Stand der Technik orientiert sich folglich auch bei Messengerdiensten an der am Markt verfügbaren Bestleistung. Mit verfügbaren Diensten, welche einen datensparsamen Ansatz sowohl im Privatkunden- als auch im Business-Bereich verfolgen, bedarf es eines erheblich größeren Begründungsaufwands, wenn eine eingriffsintensivere Variante gewählt wird.

Die Einhaltung (bzw. Berücksichtigungspflicht) des Standes der Technik muss alle relevanten Komponenten der Datenverarbeitung, einschließlich aller Datenübertragungs- und Datenspeicherungsmöglichkeiten umfassen.[520] Typische TOMs im Hinblick auf Datenminimierung, aber auch Datensicherheit,[521] die dem Stand der Technik entsprechen, sind u.a.:

- Möglichkeit pseudonymer Nutzung;
- lokale Datenverarbeitung auf Endgeräten, Minimierung der Datenübermittlung an Backend-Systeme (insbesondere in Drittländern);
- Zwei-Faktor-Authentifizierung oder Multi-Faktor-Authentifizierung; gegenseitige Authentisierung der Kommunikationspartner;
- Ende-zu-Ende-Verschlüsselung, Verschlüsselung während des Transports, Verschlüsselung der gespeicherten Daten;
- Sicherung privater Schlüssel vor unberechtigtem Zugriff;
- Ganzheitliche Sicherheitsarchitektur: Bereitstellung sicherer Software-Administration, Patch-Management; Umsetzung des Need-to-Know-Prinzips;
- Aufklärung der Nutzer*innen über unterschiedlich (sichere) Konfigurationsmöglichkeiten.

Im Hinblick auf die Messenger-Angebote am Markt hat die Verbraucherzentrale NRW Funktionen der Messenger verglichen (Stand 19.04.2021).[522] Der Vergleich bezieht sich zwar auf die Privatkunden-Apps, soll aber nichtsdestotrotz zur Dokumentation des Stands der Technik hier herangezogen werden. Die Auswahl der dargestellten Messenger ist beschränkt auf solche, welche als besonders datenschutzfreundlich bekannt sind (und eine gewisse Verbreitung erreicht haben).[523]

---

[519] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 12.
[520] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 16.
[521] Zur Datensicherheit siehe Abschnitt 2.4.7.
[522] Verbraucherzentrale NRW, Datenschutz bei Messengern im Überblick, Stand 19.04.2021, abrufbar unter: https://www.verbraucherzentrale.de/sites/default/files/2021-04/Messenger-Vergleiche_Tabelle_2021_VZNRW.pdf [letzter Zugriff 30.07.2021].
[523] Der Vergleich der Verbraucherschutzzentrale NRW umfasst zudem die Messenger: Facebook-Messenger, Skype, Telegram und WhatsApp. Mit dem Faktor der Verbreitung wird strenggenommen bereits die Grenze zu den allgemein anerkannten Regeln der Technik erreicht.

		ginlo	Signal	Threema	Wire
Datenschutzerklärung (Deutsch)		Ja	Nur in Englisch	Ja	Ja
Angaben für Registrierung	Klarname	Nein	Nein	Nein	Nein
	Telefonnummer	Ja	Ja	Nein	Nein
	E-Mail-Adresse	Nein	Nein	Nein	Ja
Angaben für Nutzung	Profilbild	Optional	Optional	Optional	Optional
	Aktiv-Status	Abschaltbar	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden
	Tipp-Status	Nicht vorhanden	Abschaltbar	Abschaltbar	Nicht abschaltbar
	Lesebestätigung	Abschaltbar	Abschaltbar	Abschaltbar	Abschaltbar
Zugriff auf Kontakte erforderlich		Nein	Nein	Nein	Nein
Ende-zu-Ende-Verschlüsselung		Ja	Ja	Ja	Ja
Einverständnis für Gruppenchat		Nicht aktivierbar	Nicht aktivierbar	Nicht aktivierbar	Nicht aktivierbar
Selbstlösch-Funktion für Nachrichten		Für Text und Medien vor Absenden separat aktivierbar	In Chats aktivierbar	Nicht verfügbar	Für Text und Medien vor Absenden separat aktivierbar
Serverstandort		Deutschland	USA	Schweiz	EU und Schweiz
Geschäftsmodell		Kostenpflichtige Business-Dienste	Spenden	Kostenpflichtige App	Kostenpflichtige Business-Dienste
Back-Up möglich		Ja, auf genutztem Gerät	Ja, auf genutztem Gerät	Ja, Speicherort wählbar	Ja, Speicherort wählbar
Account innerhalb der App löschbar		Ja	Ja	Ja	Ja

Tabelle 3 Ausschnitt aus dem Messengervergleich der Verbraucherzentrale NRW (Stand 19.04.2021)

2.4.4.2.3 Implementierungskosten

Unter den Implementierungskosten dürfen sowohl Anschaffungs- und Allgemeinkosten, Zeitressourcen sowie Personalkosten berücksichtigt werden.[524] Der Verantwortliche kann dabei das Verhältnis zwischen wirtschaftlichem Aufwand und praktischem Mehrwert für den Schutz der Daten miteinbeziehen.[525] Die Klärung, ob eine Maßnahme wirtschaftlich ist, erfordert eine individuelle Betrachtung des festgestellten Schutzbedarfs sowie der Realisierungskosten der erforderlichen Maßnahme.[526] Allerdings kann nach Einschätzung des Europäischen Datenschutzausschusses ein Verweis auf zu hohe Kosten nicht von der Gewährleistung der Pflichten der DSGVO entbinden.[527]

[524] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9.
[525] *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 25 Rn. 22.
[526] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 10.
[527] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9; vgl. auch *Baumgartner/Gausling*, ZD 2017, 308 (310).

2.4.4.2.4 Art, Umfang, Umstände und Zwecke der Verarbeitung

Unter diesem Prüfungspunkt sind die Begleitumstände, Eigenschaften und Charakteristika einer geplanten Datenverarbeitung zu berücksichtigen, bspw.: [528]

- Werden besondere Kategorien personenbezogener Daten verarbeitet?
- Sind automatische Entscheidungsfindungen geplant?
- Besteht ein Machtungleichgewicht zwischen Verantwortlichem und betroffener Person?
- Sind Hürden für betroffene Personen bei der Rechtewahrnehmung zu befürchten?

Der Umfang stellt auf die Größenordnung und Reichweite der Verarbeitung ab, die Umstände betreffen sowohl den Verarbeitungskontext als auch die Erwartungen der betroffenen Personen, während sich der Zweck auf die Ziele der Verarbeitung bezieht. [529]

2.4.4.2.5 Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken

Methoden zur Ermittlung und Klassifizierung des in der DSGVO zentralen Begriffs des Risikos sind nicht unmittelbar in der DSGVO vorhanden. Entsprechend der in Art. 1 Abs. 2 DSGVO niedergelegten Ziele der DSGVO, stellt der Risikobegriff der DSGVO auf die Rechte und Freiheiten natürlicher Personen ab, welche insbesondere im Schutz der Grundrechte und Grundfreiheiten verankert sind.[530] Besonders relevant ist in diesem Zusammenhang das Recht auf Schutz personenbezogener Daten in Art. 8 EU-GrCh, aber auch der Schutz des Privatlebens in Art. 7 EU-GrCh, die Meinungsfreiheit in Art. 11 EU-GrCh, die Versammlungsfreiheit in Art. 12 EU-GrCh sowie das Diskriminierungsverbot in Art. 21 EU-GrCh können typischerweise durch die Verarbeitung personenbezogener Daten und die daraus resultierenden Folgen tangiert werden.[531] Welche Grundrechtspositionen im Einzelfall betroffen sind, hängt von der konkreten Verarbeitungssituation und ihrem Kontext ab. Erwägungsgrund 75 DSGVO gibt weitere Hinweise, wie die Risikobeurteilung nach der DSGVO zu erfolgen hat:

> Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte […]

Beispiele: die Verarbeitung führt zu …

- einer Diskriminierung,
- einem Identitätsdiebstahl oder -betrug,
- einem finanziellen Verlust,
- einer Rufschädigung,
- einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- der unbefugten Aufhebung der Pseudonymisierung,
- anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann,

[528] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9.
[529] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 9.
[530] *Bieker u. a.*, DuD 2018, 492 (492); *Bieker*, DuD 2018, 27 (27 f.); vgl. auch *Martin u. a.*, DuD 2020, 149 (150).
[531] *Bieker u. a.*, DuD 2018, 492 (492).

- wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht [bspw. Verzicht auf Ausübung ihrer Grundrechte[532]] oder
- daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren,
- wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden,
- wenn persönliche Aspekte bewertet werden, insbesondere
  - wenn Aspekte, welche die Arbeitsleistung,
  - wirtschaftliche Lage,
  - Gesundheit,
  - persönliche Vorlieben oder Interessen,
  - die Zuverlässigkeit oder das Verhalten
  - den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen,
- wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder
- wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

Zusammenfassend ist nach der DSGVO ein Risiko stets dann anzunehmen, wenn die Möglichkeit besteht, dass ein Ereignis unmittelbar oder mittelbar zu einem Schaden für eine oder mehrere natürliche Personen führt.[533] Bereits ein *ungerechtfertigter* Eingriff in das Grundrecht einer natürlichen Person kann insofern als (immaterieller) Schaden gewertet werden – ungeachtet davon, ob daraus weitere materielle oder physische Schäden resultieren.[534]

DSK, Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen

- „Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.
- Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.“

[532] *Bieker u. a.*, DuD 2018, 492 (493).
[533] *DSK - Datenschutzkonferenz*, Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen, S. 1; *Martin u. a.*, DuD 2020, 149 (150 f).
[534] *Bieker u. a.*, DuD 2018, 492 (493); *Martin u. a.*, DuD 2020, 149 (151). Wichtig zu bedenken ist hierbei, dass nicht bereits mit jedem Eingriff in Art. 8 Abs. 1 EU-GrCh, d.h. jeder rechtfertigungsbedürftigen Verarbeitung personenbezogener Daten ein Risiko i.S.d. Art. 25 Abs. 1 DSGVO vorliegen kann: *Veil*, NVwZ 2018, 686 (694); *Bieker*, DuD 2018, 27 (29); *Magiera*, DÖV 2000, 1017 (1022); *Wagner*, Datenökonomie und Selbstdatenschutz, S. 233.

Schwierigkeiten bereitet die Risikobeurteilung, wenn konstatiert wird, dass die vom Verantwortlichen anzustellende Bewertung „in Worte gefasst“ werden kann, aber „nicht in sinnvoller Weise zahlenmäßig quantifiziert werden kann.“[535] Insofern gilt auch zu bedenken, dass das klassische Risikomanagement zumeist Risiken aus Perspektive der Organisation (und nicht der betroffenen Person) betrachtet und zudem oftmals eher von „greifbaren“ materiellen oder physischen Schäden ausgeht.[536] Vorgeschlagen wird zur Herstellung einer Vergleich- und Überprüfbarkeit die Einteilung in Kategorien, d.h. die stufenweise Kategorisierung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden bspw. in die Risikokategorien gering – normal – hoch. [537] Jede durchschnittliche Datenverarbeitung wäre als „normal“ einzustufen, sodass das Prädikat „gering“ den Einsatz geeigneter TOMs impliziere. [538] Für den Verantwortlichen wäre der in Abbildung 9 dargestellte Prozess zu durchlaufen.

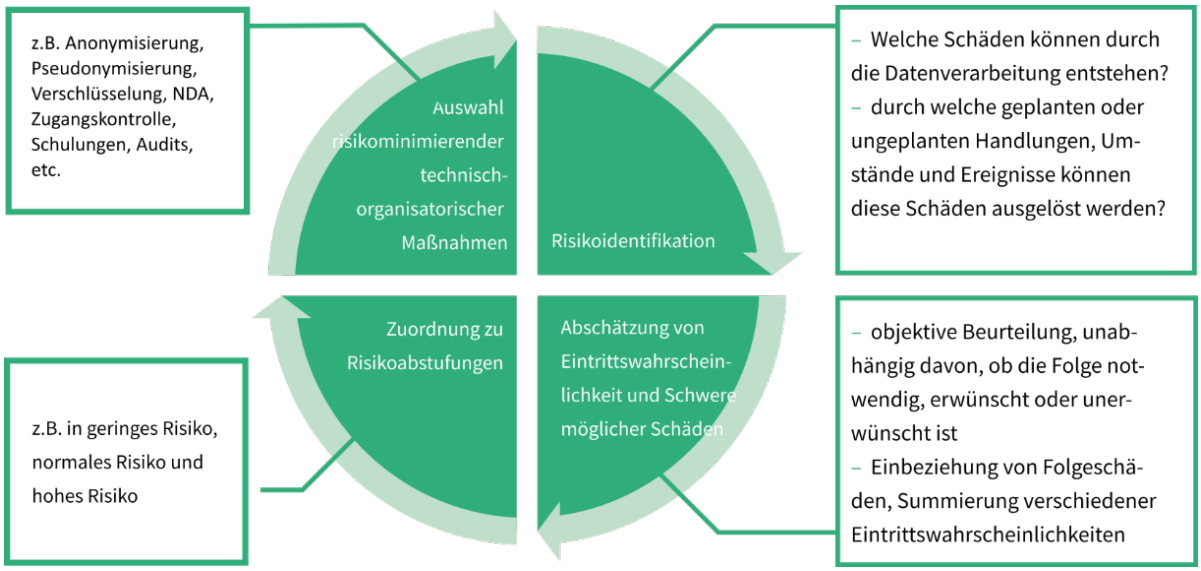


Abbildung 9 Risikobeurteilung

Bei der Feststellung eines hohen Risikos ist eine Datenschutz-Folgenabschätzung durchzuführen (siehe Abschnitt 2.4.4.2.1). Bezüglich der potentiell schadensauslösenden Ereignisse wird darauf hingewiesen, dass neben den geplanten Verarbeitungsfolgen auch unbeabsichtigte Negativfolgen, die durch Abweichungen vom „Best-Case-Szenario“ entstehen könnten, berücksichtigt werden sollten. [539] Bei der Identifikation der Risikoquellen sollten anders als in der IT-Sicherheit bei der Angreifermodellierung nicht nur aus Sicht des Verantwortlichen potentielle Angriffe „von außen“ antizipiert werden, sondern aus Sicht der betroffenen Person ausgehend jegliche Risikoquelle zu bedenken, welche anhand von Schutzzielen klassifiziert werden könnten.[540]

[535] *Bieker u. a.*, DuD 2018, 492 (493).
[536] *Martin u. a.*, DuD 2020, 149 (151); *Schiering u. a.*, DuD 2020, 161 (162). In diesem Sinne sollte nicht von „Angreifern“ als Risiko-Quelle gesprochen werden, da Risikoauslöser auch interner Natur, wie die eigenen Beschäftigten sein können. „Beteiligte“ oder „beteiligte Akteure“ werden als neutrale Begriffe vorgeschlagen, in: *Schiering u. a.*, DuD 2020, 161 (162).
[537] *Bieker u. a.*, DuD 2018, 492 (493).
[538] *Bieker u. a.*, DuD 2018, 492 (493).
[539] *Bieker u. a.*, DuD 2018, 492 (493).
[540] *Bieker u. a.*, DuD 2018, 492 (494).

2.4.4.2.5.1 Modelle zur Operationalisierung der Anforderungen der DSGVO

Mit dem Standard-Datenschutzmodell (SDM)[541] sollen Anforderungen der DSGVO für den Verantwortlichen leichter handhabbar werden und so eine rechtskonforme und überprüfbare Umsetzung erreichbar sein, u.a. durch eine objektive und überprüfbare Beurteilung eines Verfahrens.[542] Das SDM besteht aus mehreren Bausteinen, u.a. zum Aufbewahren, Dokumentieren, Löschen und Vernichten und Berichtigen. Diese sollen rechtliche Anforderungen in konkrete technische und organisatorische Maßnahmen „übersetzen".[543] Die aktuellen Bausteine sind auf Seiten der Landesbehörden abrufbar.[544]

Das Modell orientiert sich dabei an den Gewährleistungszielen der Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit.[545] Diese Ziele sollen die Modellierung von funktionalen Anforderungen in praktischen Anwendungsfällen vereinfachen und die einfache Visualisierung von Konflikten unterstützen. Sie werden auch als „Optimierungsgebote" gefasst.[546] Die technische Gestaltung von Verarbeitungstätigkeiten sollte sich an diesen Zielen orientieren und auf diese Weise die rechtlichen Anforderungen der DSGVO in technische und organisatorische Maßnahmen transferieren.[547] Für die unterschiedlichen technischen Komponenten (Daten, Systeme, Dienste, Prozesse) beschreibt das SDM mit seinen Bausteinen Referenzmaßnahmen, die sich systematisch an den Gewährleistungszielen orientieren und so eine strukturierte Umsetzung in der Praxis befördern sollen. Dabei muss stets bedacht werden, dass ein Datenschutzmanagementprozess ein zyklischer Prozess ist.[548] Dies bedeutet, es sind regelmäßige Überprüfungen der Wirksamkeit der Maßnahmen erforderlich.

2.4.4.2.5.2 Schutzstufenkonzept

Um neben der Eintrittswahrscheinlichkeit die Schwere eines möglichen Schadens zu bemessen, können personenbezogene Daten in unterschiedliche Schutzstufen eingeordnet werden. Eine solche Klassifizierung erleichtert die Einschätzung der Sensitivät bestimmter Daten, muss im Rahmen der Gefahren- und Risikoanalyse zur Auswahl geeigneter TOMs gemeinsam mit den entsprechenden Eintrittswahrscheinlichkeiten betrachtet werden.

Stufe	Personenbezogene Daten	Beispiele	Schwere eines möglichen Schadens
A	Daten wurden von betroffenen Personen frei zugänglich gemacht	Telefonverzeichnis, eigene frei zugänglich gemachte Webseite	geringfügig

[541] Zum Standard-Datenschutzmodell: https://www.datenschutzzentrum.de/sdm/ [letzter Abruf 20.07.2021].
[542] *Bieker*, DuD 2018, 27 (27).
[543] Vgl. BfDI, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/SDM.html [letzter Abruf 18.08.2021].
[544] Siehe: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ [letzter Abruf 18.08.2021].
[545] Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und-prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, S. 10, abrufbar unter: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b.pdf [letzter Abruf 18.08.2021].
[546] Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und-prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, S. 9.
[547] Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und-prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, S. 25 ff.
[548] Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und-prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, S. 31.

B	Daten wurden nicht frei zugänglich gemacht, aber eine besondere Beeinträchtigung ist bei unsachgemäßer Handhabung nicht zu erwarten	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien	
C	Unsachgemäße Handhabung dieser Daten können betroffene Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigen („Ansehen“)	Einkommen, Grundsteuer, Ordnungswidrigkeiten	überschaubar
D	Unsachgemäße Handhabung dieser Daten können betroffene Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen *erheblich* beeinträchtigen („Existenz“)	Arbeitszeugnisse, dienstliche Beurteilungen, Gesundheitsdaten, Schulden, Pfändungen, Sozialdaten, Anstaltsunterbringung, Straffälligkeit, sonstige Daten besonderer Kategorien nach Art. 9 DS-GVO	substantiell
E	Unsachgemäße Handhabung dieser Daten können Gesundheit, Leben oder Freiheit der betroffenen Person beeinträchtigen	Daten über mögliche Opfer einer Straftat, Zeugenschutzprogramm	groß

Tabelle 4 Niedersächsisches Schutzstufenkonzept der LfD Niedersachsen[549]

2.4.4.3 Datenminimierung und datenschutzfreundliche Voreinstellungen

Diese Vorgabe des Art. 25 Abs. 2 DSGVO trägt dem Umstand Rechnung, dass Nutzende datenverarbeitender Systeme oftmals die voreingestellten Werkseinstellungen nicht maßgeblich verändern.[550] Um die Ziele der Datenminimierung auch effektiv umzusetzen, sind Verantwortliche angehalten, Voreinstellungen so wählen, dass nur für den jeweils bestimmten Verarbeitungszweck erforderliche Daten erhoben werden, d.h. im Hinblick auf Menge der personenbezogenen Daten, den Umfang der Verarbeitung dieser Daten, der Speicherdauer sowie der Zugänglichkeit nur das entsprechend der einschlägigen Legitimationsgrundlage nach Art. 6 Abs. 1 DSGVO zwingend erforderliche Minimum vorgesehen werden soll.[551]

2.4.4.4 Datenminimierung im Rahmen des Beschäftigungsverhältnisses

§ 26 Abs. 3 S. 3 i.V.m. § 22 Abs. 2 S. 2 BDSG zählen beispielhaft Schutzmaßnahmen auf, die bei der Verarbeitung *besonderer Kategorien* personenbezogener Daten zu berücksichtigen sind.

[549] Die Landesbeauftragte für den Datenschutz Niedersachsen, Schutzstufenkonzept der LfD Niedersachsen, Stand: Oktober 2018, abrufbar unter: https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/schutzstufen/schutzstufen-56140.html [letzter Abruf 13.08.2021].
[550] *Baumgartner/Gausling*, ZD 2017, 308 (312).
[551] *European Data Protection Board*, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, S. 11.

1. **technisch organisatorische Maßnahmen (TOMs)**,
2. **Kontrolle & Revisionsfähigkeit:** Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. **Lehrgänge/Schulungen:** Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Benennung einer oder eines **Datenschutzbeauftragten**,
5. **Zugangsbeschränkungen:** Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. **Pseudonymisierung**,
7. **Verschlüsselung**,
8. **Anforderungen an Datenverarbeitungssysteme:** Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9. **Interne/externe Audits:** Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs
10. **spezifische Verfahrensregelungen** bei Weiterverarbeitung für andere Zwecke

Diese Maßnahmen zeigen starke Überschneidungen mit Art. 25, 32 DSGVO.[552]

2.4.4.5 Die Datenschutz-Folgenabschätzung als Ausfluss des risikobasierten Ansatzes

Wird im Rahmen der Risikobeurteilung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen festgestellt, muss eine Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO durchgeführt werden. Insofern sind Verarbeitungskonzepte nicht per se verboten, sondern es wird eine Struktur forciert, die eine umfassenden, vollständige und kontinuierliche Identifikation, Bewertung sowie Eindämmung und Überwachung der Risiken gewährleisten soll.[553] Erst wenn im Rahmen der DSFA keine risikominimierenden Maßnahmen umsetzbar erscheinen und das Risiko weiterhin hoch bleibt, muss die zuständige Aufsichtsbehörde nach Art. 36 DSGVO konsultiert werden.

Notwendigkeit der DSFA: eine gesetzliche Pflicht zur Durchführung einer DSFA besteht, wenn die geplante Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Insofern sollte es für einen umfassenden Schutz ausreichen, wenn ein Teilbereich besonders risikobehaftet ist – selbst wenn dies nicht für den gesamten Verarbeitungsvorgang gelten mag.[554] Bezüglich der geschützten „Rechte und Freiheiten" gelten die gleichen Erwägungen wie bei Art. 25 DSGVO (Privacy by Design, Abschnitt 2.4.4.2.5). Zudem nennt Art. 35 Abs. 3 DSGVO Beispiele, in denen stets von der Erforderlichkeit einer DSFA auszugehen ist. Art. 35 Abs. 4 und 5 DSGVO ermöglichen es ferner den Aufsichtsbehörden Positiv- und Negativlisten aufzustellen und somit Fälle zu benennen, in denen die DSFA stets notwendig ist oder nicht notwendig ist. Die DSK hat eine solche nicht-abschließende Liste erstellt.[555] In allen übrigen Fällen ist

[552] Zur Auslegung siehe: *Rose,* in: Taeger/Gabel - DSGVO/BDSG, § 22 Rn. 51 ff.; *Frenzel,* in: Paal/Pauly - DS-GVO BDSG, § 22 Rn. 12 ff.; *Weichert,* in: Kühling/Buchner - DS-GVO/BDSG, § 22 Rn. 33 ff.
[553] *Bieker u. a.*, DuD 2018, 492 (494 f.); *Martin u. a.*, DuD 2020, 149 (153); *Schiering u. a.*, DuD 2020, 161 (162).
[554] *Martin u. a.*, DuD 2020, 149 (150).
[555] DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, abrufbar unter: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf [letzter Abruf 21.07.2021].

mithilfe einer Risikoabschätzung eine Schwellwertanalyse durchzuführen.[556] Die Artikel-29-Datenschutzgruppe hat auf Grundlage von Art. 35 und EG 71, 75 sowie 91 DSGVO neun Kriterien entwickelt, anhand derer sich beurteilen lässt, ob voraussichtlich ein hohes Risiko besteht:[557]

- Verarbeitungen, die Verhalten bewerten oder einstufen, u.a. Erstellen von Profilen und Prognosen
- automatisierte Entscheidungen mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
- systematischer Überwachung
- vertrauliche oder höchstpersönliche Daten
- Verarbeitung von Daten in großem Umfang, zu messen anhand:
  - Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe;
  - verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente;
  - Dauer oder Dauerhaftigkeit der Datenverarbeitung;
  - geografisches Ausmaß der Datenverarbeitung
- Abgleichen oder Zusammenführen von Datensätzen aus verschiedenen Quellen, die zu unterschiedlichen Zwecken erhoben wurden oder von unterschiedlichen Verantwortlichen stammen, in einer Weise, die über die vernünftigen Erwartungen der betroffenen Personen hinausgehen
- Daten zu schutzbedürftigen Betroffenen und bei Machtungleichgewichten, wie bspw. bei Kindern, Beschäftigten, Teilen der Bevölkerung mit besonderem Schutzbedarf (psychisch Kranke, Asylbewerber*innen, Senior*innen, Patient*innen usw.) und Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der des für die Verarbeitung Verantwortlichen vorliegt
- innovative Nutzungen oder die Anwendung neuer technologischer oder organisatorischer Lösungen (z.B. Fingerabdruck- und Gesichtserkennung für die Zugangskontrolle)
- Fälle, in denen die Verarbeitung die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages hindert (z.B. Auskunfteien)
- Ein hohes Risiko ist stets dann zu erwarten, wenn zwei oder mehr Kriterien gegeben sind. Hohe Risiken können aber auch vorliegen, wenn nur eines oder keines der Kriterien erfüllt sind – insofern kommt es immer auf eine Betrachtung des Einzelfalls an.[558]

Durchführung der DSFA: Art. 35 Abs. 7 DSGVO umschreibt die Umsetzung der DSFA. In organisatorischer Hinsicht nimmt die Rolle des/r Datenschutzbeauftragten eine bedeutende Position ein: sie hat gemäß Art. 35 Abs. 2 und Art. 39 Abs. 1 Buchst. c DSGVO die Durchführung der DSFA zu überwachen und den Verantwortlichen zu beraten. Der EDSA betont dabei, dass es Aufgabe des Verantwortlichen ist die DSFA durchzuführen.[559] Datenschutzbeauftragte können ihrer Überwachungsfunktion nicht gerecht werden, wenn die Aufgabe der DSFA an sie delegiert wird.[560] Sowohl der Rat des Datenschutzbeauftragten als auch Begründungen

[556] *Bieker u. a.*, DuD 2018, 492 (495).
[557] *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" - WP248 Rev.01, S. 10 ff.
[558] *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" - WP248 Rev.01, S. 12.
[559] *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" - WP248 Rev.01, S. 17; *Martin u. a.*, DuD 2020, 149 (151).
[560] *Martin u. a.*, DuD 2020, 149 (151).

für Abweichungen von diesem Rat, sollten schriftlich dokumentiert werden.[561] Erfolgt die Datenverarbeitung durch einen Auftragsverarbeiter, muss dieser bei der DSFA-Durchführung unterstützen (Art. 28 Abs. 3 Buchst. f DSGVO). Bei gemeinsam für die Verarbeitung Verantwortlichen müssen deren jeweilige Aufgaben genau festgelegt werden und in ihrer DSFA hinterlegt sein, welcher Verantwortliche für die verschiedenen Maßnahmen zuständig ist, mit denen die Risiken mitigiert werden. [562]

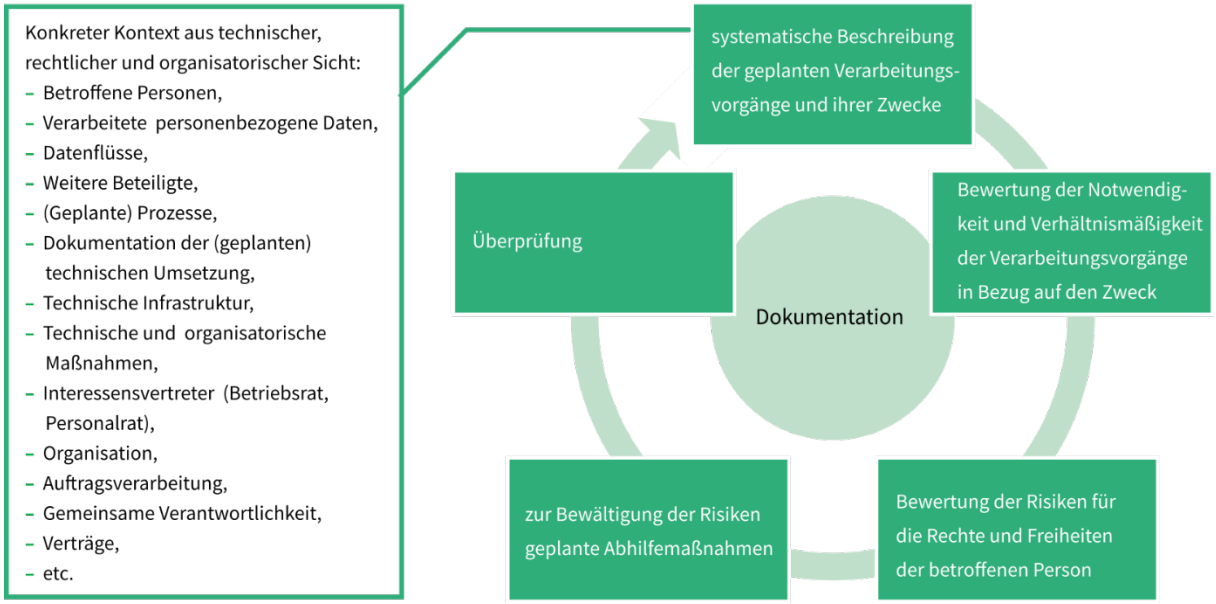


Abbildung 10 Durchführung einer DSFA gemäß Art. 35 Abs. 7, 11 DSGVO

Hersteller von Systemen oder Komponenten sind hingegen nicht verpflichtet, eine DSFA durchzuführen, da sie keine Verantwortlichen sind, sofern sie nicht in Datenverarbeitungsvorgänge eingebunden sind. Sie könnten allerdings eine generische DSFA für ihre Produkte erstellen und ihren Kundschaft bereitstellen.[563] Von Vorteil wäre, dass sie sich am besten mit der Technologie auskennen – gleichzeitig bestehen Nachteile, wenn der spätere Anwendungskontext nicht ausreichend überblickt wird, und somit eine sinnvolle Risikoanalyse kaum möglich ist.[564] Da eine DSFA zum Ziel hat systematisch neue Situationen zu untersuchen, kann eine DSFA für bereits untersuchte Fälle (d.h. für in einem bestimmten Zusammenhang und zu einem bestimmten Zweck durchgeführte Verarbeitungsvorgänge) nicht mehr notwendig sein.[565] Dies wäre der Fall bei:

- Erfassung derselben Art von Daten
- Verarbeitung zum gleichen Zweck
- Einsatz einer ähnlichen Technologie

[561] *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" - WP248 Rev.01, S. 18.
[562] *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" - WP248 Rev.01, S. 8.
[563] *Martin u. a.*, DuD 2020, 149 (151).
[564] *Martin u. a.*, DuD 2020, 149 (151).
[565] *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" - WP248 Rev.01, S. 8.

Daraus folgt, dass eine Referenz-DSFA zur Nutzung durch mehrere Verantwortliche durchaus möglich ist. Für den Verantwortlichen verbleibt zwar die Pflicht eine DSFA vorweisen zu können, es dürfen hierfür aber Referenz-DSFAs und Angaben aus einer vom Produktlieferanten erstellten DSFA verwendet werden. [566]

Konsultation Aufsichtsbehörde: Können Abhilfemaßnahmen das Risiko nicht ausreichend senken (hohes Restrisiko) und will der Verantwortliche an der geplanten Datenverarbeitung festhalten, ist eine vorherige Konsultation bei der Aufsichtsbehörde durchzuführen. Die Behörde ist gemäß Art. 36 Abs. 2 DSGVO verpflichtet, innerhalb von 8 Wochen eine schriftliche Empfehlung zu unterbreiten, und kann ihre in Artikel 58 DSGVO genannten Befugnisse ausüben.

Art. 35 Abs. 11 DSGVO zeigt, dass es sich bei der DSFA nicht um einen einmaligen, linearen Prozess handelt, sondern regelmäßige Überprüfungen der Restrisiken sowie der Umsetzung der DSFA während des gesamten Lebenszyklus der Verarbeitungsvorgänge als auch eine erneute Durchführung der DSFA erforderlich sind, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Selbst wenn der Verantwortliche eine DSFA nicht für erforderlich hält, sollte diese Entscheidung schriftlich begründet und dokumentiert werden. [567] Dies reiht sich in die sonstigen Dokumentationspflichten ein: so ist das Führen eines Verzeichnisses von Verarbeitungsvorgängen gemäß Art. 30 Abs. 1 DSGVO (abgesehen von den Ausnahmenfällen des Art. 30 Abs. 5 DSGVO) ohnehin stets erforderlich.

Praxistipp:

(1) Dokumentation der Risikobeurteilung sowie
   a. Dokumentation der Entscheidung für/gegen Durchführung einer Datenschutz-Folgenabschätzung (inkl. Begründung).
   b. Kam es zu einer Fehleinschätzung, kann es Einfluss auf potentielle Sanktionen haben, ob diese auf einer nachprüfbaren Begründung basiert.

(2) Unternehmen, welche neuartige Kommunikationswerkzeuge einsetzen wollen, sollten eine Datenschutz-Folgenabschätzung durchführen.

(3) Anbieter dieser Werkzeuge müssen als gemeinsam Verantwortliche oder Auftragsverarbeiter bei der Durchführung unterstützen, wenn sie an der Verarbeitung personenbezogener Daten beteiligt sind (bspw. bei Cloud-Anbindung, Software-as-a-Service-Diensten).

(4) Anbieter von Kommunikationslösungen, die an der Datenverarbeitung nicht beteiligt sind, können ihr Angebot nichtsdestotrotz um eine Muster-DSFA erweitern, in denen eine systematische Beschreibung der Verarbeitungsvorgänge und technischen Parameter bereits erarbeitet ist, sodass anwendende Unternehmen lediglich die konkrete Umsetzung berücksichtigen müssen.

[566] *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" - WP248 Rev.01, S. 8.
[567] *Bieker u. a.*, DuD 2018, 492 (495).

2.4.4.6 Zwischenergebnis zur Datenminimierung und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Eine der zentralen Weichenstellungen innerhalb des modernen Datenschutzrechts ist die Ermittlung des konkreten Risikos einer geplanten Datenverarbeitung für die betroffenen Personen und die Minimierung dieses Risikos durch die Auswahl geeigneter Schutzmaßnahmen technischer oder organisatorischer Natur (TOMs). Insofern kommt bei der Auswahl einer im Unternehmenskontext geeigneten Messengerdienstlösung – unabhängig davon, ob eigenverantwortlich „On-Premise" betrieben oder als Software-as-a-Service – dem nach der konkreten technischen Umsetzung erforderlichen Umfang sowie Art und Weise der Datenverarbeitung eine ganz entscheidende Rolle zu: Je weniger personenbezogene Daten für die Umsetzung des Messengerdienstes verarbeitet werden müssen, desto geringer fallen die Risiken aus. Dies hat auch zur Folge: je geringer die Risiken durch das technische Systemdesign bereits sind, desto weniger Pflichten treffen die für den Einsatz verantwortliche Stelle, weitere Maßnahmen zu ergreifen. So entfällt bspw. die Pflicht eine DSFA durchzuführen, wenn mit der Datenverarbeitung kein hohes Risiko verbunden ist.

Den Verantwortlichen treffen folgende Pflichten:

- Beurteilung des für die betroffenen Personen mit der Datenverarbeitung verbundenen Risikos: Analyse der Datenschutzfreundlichkeit der Technikgestaltung und Voreinstellungen
- Bei hohem Risiko: Durchführung einer DSFA, ggf. Konsultation der Aufsichtsbehörde
- Ergreifen von geeigneten Schutzmaßnahmen (TOMs)
- Dokumentation des ermittelten Risikos sowie der Implementierung von Schutzmaßnahmen
- Regelmäßige Re-Evaluation des Risikos

2.4.5 Richtigkeit

Mit dem Grundsatz der Richtigkeit wird dem Verantwortlichen die Pflicht auferlegt, die Richtigkeit der verarbeiteten personenbezogenen Daten aus eigener Initiative aktiv zu überprüfen.[568] Nach EG 39 S. 11 DSGVO sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

Art. 5 Abs. 1 Buchst. d DSGVO

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden

Aus dem Grundsatz der Richtigkeit der Daten ergibt sich somit bereits eine Löschpflicht auf Seiten des Verantwortlichen.[569] Auch der Anspruch auf Berichtigung ist hier verankert. „Sachlich richtig" ist ein objektives

[568] *Pötters,* in: Gola DS-GVO, Art. 5 Rn. 24; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 5 Rn. 24; *Schantz,* in: BeckOK DatenschutzR Art. 5 Rn. 28.
[569] vgl. *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 41. Zu den Löschpflichten siehe Abschnitt 2.4.6.1.

Kriterium bei Tatsachenangaben und dann erfüllt, wenn die über die betroffene Person gespeicherten Informationen mit der Realität übereinstimmen.[570] Bei Werturteilen kann hingegen weder von „richtig“ noch „unrichtig“ gesprochen werden, da diese subjektiver Natur sind. [571] Mit dem Zusatz „erforderlichenfalls“ wird deutlich, dass die Daten nicht in jedem Fall auf dem neuesten Stand sein müssen – oftmals dürften sich Angaben auch auf bestimmte Zeitpunkte beziehen. [572] Kommt es auf den jeweiligen historischen Kontext an, machen nachträgliche Veränderungen der Wirklichkeit, wie bspw. die Änderung von Vor-/Nachnamen oder der Geschlechtszugehörigkeit, die gespeicherten personenbezogenen Daten nicht falsch – insbesondere wenn es um die Dokumentation eines historischen Geschehensablaufs geht.[573] Insofern besteht hier auch ein enger Bezug zum Verarbeitungszweck (vgl. Abschnitt 2.4.3).

Im Rahmen des Profilings weist EG 71 DSGVO darauf hin, dass der Verantwortliche technische und organisatorische Maßnahmen treffen muss, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird.

2.4.5.1 Recht auf Berichtigung

Art. 16 S. 1 DSGVO gewährt der betroffenen Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Der Anspruch ergänzt den Grundsatz der Datenrichtigkeit.[574]

Ausübung des Rechts: Ein Berichtigungsantrag kann formlos (schriftlich, mündlich, elektronisch, etc.) gestellt werden und ist kostenfrei.[575] Es muss lediglich substantiiert dargelegt werden, dass die personenbezogenen Daten der betroffenen Person unrichtig sind.[576]

Unverzügliche Berichtigung: Nach dem üblichen juristischen Sprachgebrauch meint „unverzüglich“ regelmäßig „ohne schuldhaftes Zögern“ (vgl. § 121 Abs. 1 S. 1 BGB).[577] Ergänzend setzt Art. 12 Abs. 3 S. 1 eine absolute Frist von einem Monat für die Entscheidung über den Berichtigungsantrag. Diese Frist kann gemäß Art. 12 Abs. 3 S. 2 DSGVO um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Verzögert sich die Berichtigung kann die betroffene Person gemäß Art. 18 Abs. 1 Buchst. a DSGVO die Einschränkung der Verarbeitung verlangen (ob ein Antrag auf Berichtigung gleichzeitig eine Einschränkung der Verarbeitung impliziert, ist im Wege der Auslegung zu ermitteln).[578]

Berichtigung: Die Korrektur der Daten kann durch eine Veränderung, vollständige oder teilweise Löschung, Vervollständigung oder ergänzende Klarstellung erfolgen.[579] Der Verantwortliche ist ferner nach Art. 19 S. 1

---

[570] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 60; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 139.
[571] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 60; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 140; a.A. *Schantz,* in: BeckOK DatenschutzR Art. 5 Rn. 27. Auch Werturteile insbesondere Prognosen und Korrelationen könnten falsch sein, wenn sie auf fehlerhafter Tatsachengrundlage beruhen, von falschen Prämissen ausgehen oder das Ergebnis unrichtiger Schlussfolgerungen sind.
[572] OVG Hamburg, Urteil vom 27.5.2019, Az. 5 Bf 225/18.Z, Rn. 22; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 5 Rn. 61; vgl. auch *Frenzel,* in: Paal/Pauly - DS-GVO BDSG Art. 5 Rn. 40; *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 5 Rn. 24; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 141.
[573] OVG Hamburg, Urteil vom 27.5.2019, Az. 5 Bf 225/18.Z, Rn. 22.
[574] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 2.
[575] *Reif,* in: Gola DS-GVO, Art. 16 Rn. 17.
[576] *Kammann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 22; *Reif,* in: Gola DS-GVO, Art. 16 Rn. 17.
[577] *Reif,* in: Gola DS-GVO, Art. 16 Rn. 18; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 23.
[578] *Reif,* in: Gola DS-GVO, Art. 16 Rn. 18.
[579] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 18 ff.

DSGVO verpflichtet, etwaige Empfänger, denen die berichtigten Daten offengelegt wurden, über die Berichtigung zu informieren. Diese Informationspflicht entfällt, wenn sie sich als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist. Verlangt die betroffene Person eine Unterrichtung über die Empfänger, trifft den Verantwortlichen nach Art. 19 S. 2 DSGVO die Pflicht diese umzusetzen.

Unrichtige Daten: Es gelten die Erwägungen zu Art. 5 Abs. 1 Buchst. d DSGVO. Unstreitig sind Tatsachen, die einem empirischen Beweis zugänglich sind und nicht mit der Realität übereinstimmen (bzw. zum maßgeblichen Zeitpunkt nicht übereinstimmten), als unrichtig zu berichtigen – unabhängig davon auf welcher Ursache die Unrichtigkeit beruht.[580] Problematischer ist die Frage bei Werturteilen.[581] Einige wollen diese von vorneherein herausnehmen, da sie weder „richtig“ noch „falsch“ sein können, sondern eine Meinung repräsentieren.[582] Andere präferieren ein differenziertes Vorgehen: Werturteile von Privaten fallen unter die Meinungsfreiheit und unterfallen – sofern keine Tatsachenbestandteile enthalten sind – nicht dem Anwendungsbereich der Berichtigungspflicht. Ein solcher Schutz gelte hingegen nicht für öffentliche Stellen.[583] Andere wiederum präferieren stets eine Grundrechtsabwägung, insbesondere vor dem Hintergrund, dass sich Werturteil und Tatsachengrundlagen oftmals nicht klar trennen lassen. [584] Insofern lässt sich aktuell nicht abschließend sagen, welche personenbezogene Daten vom Berichtigungsanspruch erfasst werden.

2.4.5.2 Recht auf Vollständigkeit

Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person nach Art. 16 S. 2 DSGVO das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

Dies lässt sich als Spezialfall der in Satz 1 genannten Berichtigung sehen.[585] Wann Daten unvollständig sind, lässt sich nur *relativ* anhand des konkret verfolgten Verarbeitungszecks feststellen. [586] Eine der Unrichtigkeit gleichstehende Bedeutung besteht, wenn die Daten zwar für sich genommen richtig sind, aber in der Gesamtheit eine objektiv falsche Aussage treffen oder durch die Lückenhaftigkeit objektiv missverständlich sind. [587] Folglich kommt es auf den Gesamtkontext an.[588] Eine Berichtigungspflicht soll zudem nur bestehen, wenn die Vervollständigung im Hinblick auf die Zwecke relevant ist. [589]

Als Unterfall des Berichtigungsanspruchs soll die Vervollständigung ebenfalls „unverzüglich“ erfolgen und die Mitteilungspflichten nach Art. 19 DSGVO auslösen.[590]

---

[580] *Worms,* in: BeckOK DatenschutzR Art. 16 Rn. 52; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 8 ff.
[581] Siehe zur Behandlung von Werturteilen in der Rechtsprechung: *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 19 m.w.N.
[582] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 8; *Roßnagel,* in: NK Datenschutzrecht Art. 5 Rn. 140; *Reif,* in: Gola DS-GVO, Art. 16 Rn. 10.
[583] *Worms,* in: BeckOK DatenschutzR Art. 16 Rn. 55.
[584] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 21.
[585] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 4.
[586] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 26; *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 36; *Worms,* in: BeckOK DatenschutzR Art. 16 Rn. 58; *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 16 Rn. 18.
[587] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 36; *Meents/Hinzpeter,* in: Taeger/Gabel - DSGVO/BDSG Art. 16 Rn. 21.
[588] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 36.
[589] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 16 Rn. 37; *Dix,* in: NK Datenschutzrecht Art. 16 Rn. 18; *Meents/Hinzpeter,* in: Taeger/Gabel - DSGVO/BDSG Art. 16 Rn. 21.
[590] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 16 Rn. 30, 31; *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 16 Rn. 20; *Worms,* in: BeckOK DatenschutzR Art. 16 Rn. 62; *Dix,* in: NK Datenschutzrecht Art. 16 Rn. 18.

2.4.5.3 Zwischenergebnis zum Grundsatz der Richtigkeit und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Den Verantwortlichen treffen die folgenden Pflichten und Organisationsobliegenheiten:

- Angemessene Maßnahmen zur regelmäßigen Prüfung auf Unrichtigkeit und aktive Berichtigung bzw. Löschung unrichtiger Daten sowie ggf. Aktualisierung veralteter Daten.
- Etablierung organisatorischer Maßnahmen zur Umsetzung bzw. Beantwortung von Berichtigungsanfragen innerhalb der gesetzlichen Fristen sowie ggf. Mitteilung an etwaige Empfänger der Daten über die Berichtigung.
- Vorsehen von Möglichkeiten einer Einschränkung der Verarbeitung für die Dauer, die der Verantwortliche benötigt, um die Richtigkeit der personenbezogenen Daten zu überprüfen.

2.4.6 Speicherbegrenzung

Der Grundsatz der Speicherbegrenzung als Ergänzung zum Zweckbindungsgrundsatz legt eine zeitliche Begrenzung für die Verarbeitung personenbezogener Daten fest. Laut Art. 5 Abs. 1 Buchst. e DSGVO dürfen die gespeicherten Daten die betreffende Person nur so lange identifizieren oder zu ihrer Identifizierung beitragen, wie es für den Zweck der Verarbeitung erforderlich ist. Löschpflichten sind in Art. 17 DSGVO normiert. Konkretisierend schlägt EG 39 S. 9 und S.10 die Verwendung von Löschfristen vor.

> **Art. 5 Abs. 1 Buchst. e DSGVO**
>
> Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; [...]

2.4.6.1 Löschpflichten

Mit dem Recht auf Löschung gewährt die DSGVO der betroffenen Person einen Anspruch, vom Verantwortlichen die unverzügliche Löschung ihrer personenbezogenen Daten zu fordern, sofern einer der nachfolgenden in Art. 17 Abs. 1 DSGVO dargelegten Fälle vorliegt.

2.4.6.1.1 Löschgründe

Ein Grund zur Löschung soll demnach in folgenden Fällen bestehen:

Zweck der Verarbeitung entfallen (Buchst. a) Wenn und soweit die personenbezogenen Daten der betroffenen Person für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind, hat eine Löschung zu erfolgen. Die Pflicht zur Löschung entfällt jedoch, soweit eine zulässige Zweckänderung (vgl. Art. 6 Abs. 4 DSGVO) vorliegt und die Daten für diesen neuen Zweck noch erforderlich

sind.[591] Im Falle nichtautomatisierter Datenverarbeitung kann nach § 35 Abs. 1 BDSG ebenfalls von einer Löschung abgesehen werden, wenn die Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Interesse der betroffenen Person als gering anzusehen ist. Durch die Einschränkung auf nichtautomatisierte Datenverarbeitung findet diese Vorschrift auf die untersuchte Anwendung keine Anwendung.

Widerruf der Einwilligung (Buchst. b) Hat die betroffene Person ihre Einwilligung gemäß Art. 6 Abs. 1 Buchst. a oder Art. 9 Abs. 2 Buchst. a DSGVO gegeben und ist die Datenverarbeitung hierauf gestützt, so hat bei Widerruf dieser Einwilligung eine Löschung zu erfolgen, sofern eine weitere Rechtsgrundlage für die Verarbeitung nicht vorhanden ist. Umstritten ist, ob hiermit trotz Widerruf der Einwilligung ein Wechsel der Rechtsgrundlage möglich ist.[592] Dies würde der betroffenen Person allerdings nur eine Autonomie suggerieren, wenn sie mit Ausübung ihres Widerrufsrechts praktisch „ins Leere laufen“ würde.[593] Mit dem Verweis auf die fortdauernde Rechtfertigung auf Basis anderweitiger Rechtsgrundlagen zeigt diese Norm richtigerweise vielmehr auf, dass die ursprüngliche Verarbeitung gleichzeitig auf mehrere Erlaubnistatbestände, also eine Einwilligung und gleichzeitig eine andere Rechtsgrundlagen gestützt werden kann.[594] Ist die Datenverarbeitung zur Zweckerreichung dieser weiteren Rechtsgrundlage weiterhin erforderlich, muss keine Löschung erfolgen.[595] Ein Teilwiderruf (d.h. entweder auf Teile der Einwilligung oder Teile der Verarbeitung) soll hingegen keinen wirksamen Löschungsgrund für die nicht erfassten Teile begründen. Konsequenterweise soll bei Untrennbarkeit dieser Teile auch kein Löschungsgrund i.S.v. Buchst. b vorliegen.[596]

Widerspruch (Buchst. c) Legt die betroffene Person Widerspruch gemäß Art. 21 Abs. 1 DSGVO gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, so hat eine Löschung zu erfolgen. Liegt ein Widerspruch nach Art. 21 Abs. 2 DSGVO (Widerspruchsrecht im Rahmen von Direktwerbung) vor, hat eine Löschung ohne weitere Bedingung zu erfolgen.

Unrechtmäßige Verarbeitung (Buchst. d) Wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden, hat eine Löschung zu erfolgen. Entgegen der missverständlichen Formulierung (”verarbeitet wurden”), soll die *gegenwärtige* Recht- bzw. Unrechtmäßigkeit der Verarbeitung maßgeblich sein.[597] Die Unrechtmäßigkeit soll nicht nur vorliegen, wenn ein Rechtmäßigkeitsgrund i.S.v. Art. 6 bzw. Art. 9 DSGVO fehlt, sondern nach EG 65 auch, wenn die Verarbeitung “aus anderen Gründen” gegen die DSGVO verstößt.[598]

Erfüllung einer rechtlichen Verpflichtung (Buchst. e) Eine Löschung hat ebenfalls zu erfolgen, wenn und soweit die Löschung zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten, dem der Verantwortliche unterliegt, erforderlich ist. Ob Mitgliedsstaaten aufgrund dieser Regelung ermächtigt sind, Löschpflichten zu erlassen, ist jedoch umstritten.[599] Der Begriff der rechtlichen Verpflichtung soll dabei aber weit verstanden werden und sich nach Art. 6 Abs. 1 Buchst. c DSGVO richten: Demnach muss es ich um eine Rechtspflicht nach objektivem und hinreichend klarem sowie vorhersehbaren Recht handeln und muss nicht zwingend die Form eines Gesetzes haben. Rechtskräftige Entscheidungen von Behörden und Gerichten sollen daher ebenfalls ausreichend sein.[600]

---

[591] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 23.
[592] *Plath,* in: *Plath*, Plath, DSGVO/BDSG Art. 7 Rn. 15.; *Stemmer,* in: Wolff/Brink, BeckOK Datenschutzrecht Art. 7 Rn. 91.1.
[593] *Artikel-29-Datenschutzgruppe*, Guidelines on consent under Regulation 2016/679 - WP 259, S. 23.
[594] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 23 ff.
[595] *European Data Protection Board*, Guidelines 05/2020 on consent under Regulation 2016/679, S. 24.
[596] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 25.
[597] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 26.
[598] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 27.
[599] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 27; *Worms,* in: BeckOK DatenschutzR Art. 17 Rn. 45; *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 16; *Nolte/Werkmeister,* in: Gola DS-GVO, Art. 17 Rn. 26.
[600] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 28; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 30; *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 16.

2.4.6.1.2 Unverzügliche Löschung

Beim Vorliegen einer der vorgenannten Fälle, sind die Daten mit Personenbezug unverzüglich zu löschen. „Unverzüglich“ bedeutet in diesem Zusammenhang, dass einzelfallabhängig anhand der konkreten Verarbeitung und dem damit verbundenen Löschungsaufwand bestimmt werden muss, wann eine Löschung zu erfolgen hat.[601] Bei der Prüfung der Zeitspanne ist v.a. zu berücksichtigen, dass dem Verantwortlichen ausreichend Zeit für die rechtliche Prüfung der Ausschlusstatbestände in Art. 17 Abs. 3 DSGVO eingeräumt werden muss.[602] Fraglich ist, ob sich daher eine pauschale Gleichsetzung mit dem Begriff der Unverzüglichkeit aus Art. 16 S. 1 DSGVO verbietet.[603] Anhaltspunkte können hier zwar Art. 12 Abs. 3, 4 DSGVO liefern, der ein Tätigwerden ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags fordert.[604] Zu beachten ist jedoch, dass die Frist von einem Monat bereits die Ausnahme und damit die zeitliche Obergrenze darstellt.[605] Im Einzelfall soll folglich eher ein kürzerer aber ausnahmsweise auch längerer Zeitraum in Betracht kommen.[606]

2.4.6.1.3 Umsetzung der Löschung

Eine Definition von Löschen existiert in der DSGVO nicht und schreibt auch keine spezifische Löschmethode vor.[607] Durch die alternative Erwähnung des Begriffs des Löschens neben dem Begriff der Vernichtung in Art. 4 Nr. 2 DSGVO lässt sich aber ableiten, dass beide Begriffe nicht synonym zu gebrauchen sind und ein Unterschied besteht. [608] Das BDSG a.F. definierte das Löschen in § 3 Abs. 4 Nr. 5 als „Unkenntlichmachen gespeicherter personenbezogener Daten”. „Vernichten“ bezeichnet die physische Zerstörung des Datenträgers. Da Datenträger allerdings regelmäßig nur überschrieben werden, meint Löschung im technischen Sinn einen Vorgang, nach dessen Ende auf die Daten bzw. deren Inhalt nicht mehr mit den üblichen Verfahren zugegriffen werden kann – es also unmöglich ist, die in den Daten verkörperte Information wahrzunehmen.[609] Entscheidend ist, dass die Daten nicht mehr verarbeitet und zu diesem Zweck auch nicht mehr ohne übermäßigen Aufwand wiederhergestellt werden können.[610] Daten können demnach

- durch ordnungsgemäße Vernichtung des betreffenden Datenträgers oder
- durch (mehrfaches) Überschreiben gelöscht werden (physikalische Löschung).

Die bloße Löschung einer Verknüpfung, eines Verweises im Dateisystem oder einer Zugriffsmöglichkeit auf einen Datensatz (auch logische Löschung genannt) führt dagegen regelmäßig nicht zu einer tatsächlichen Löschung, sondern macht den Datensatz höchstens schwerer auffindbar.[611] Im Hinblick auf die technische Umsetzung gilt zu beachten, dass der Erfolg der Löschungshandlung bei auf einem wiederbeschreibbaren Datenträger zu löschenden Daten, nicht schon dann eintritt, wenn die betreffenden Speicherplätze zum

---

[601] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31.
[602] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31; *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 8; *Peuker,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 17 Rn. 38.
[603] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31.
[604] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 46; *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31; *Peuker,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 17 Rn. 38.
[605] *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 40.
[606] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 31; *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 17 Rn. 40; a.A. *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 8 (wonach die Monatsfrist nicht überschritten werden dürfe).
[607] *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 5; *Peuker,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 17 Rn. 31.
[608] *Peuker,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 17 Rn. 32.
[609] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 29; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 37.
[610] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 17 Rn. 30.
[611] *Dix,* in: NK Datenschutzrecht Art. 17 Rn. 5; a.A. wohl *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 39.

neuen Beschreiben freigegeben sind, sondern erst beim tatsächlichen Überschreiben.[612] Dies bedeutet, dass die in den Betriebssystemen zur Verfügung stehenden einfachen Löschbefehle nicht ausreichen: In diesen Fällen kann der Einsatz von Löschsoftware notwendig werden.[613]

Praxistipp:

Im IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) befasst sich ein Baustein mit Löschen und Vernichten und gibt einen Überblick über Methoden zur Löschung und Vernichtung von Daten.[614] Im Bereich der technischen Normungen kann zudem – je nach Fallgestaltung – auf die DIN 66398 (Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten) sowie die DIN 66399 (Büro- und Datentechnik - Vernichtung von Datenträgern) zurückgegriffen werden.[615] Im Rahmen des Standard-Datenschutzmodells bietet Baustein 60 „Löschen und Vernichten“ Hinweise zur Umsetzung der DSGVO.[616]

2.4.6.1.4 Ausnahmen von der Löschpflicht

Art. 17 Abs. 1 und 2 DSGVO gelten jedoch nicht, soweit die Verarbeitung erforderlich und einer der nachfolgenden und in Art. 17 Abs. 3 DSGVO dargelegten Fälle vorliegt. Ein Recht zur Löschung soll demnach in folgenden Fällen nicht bestehen:

Freie Meinungsäußerung (Buchst. a) Eine Löschung hat nicht zu erfolgen, soweit die Verarbeitung zur Ausübung des Rechtes auf freie Meinungsäußerung und Information (Art. 11 Abs. 1 GRCh) erforderlich ist.

Rechtliche Verpflichtung (Buchst. b) Der Verantwortliche hat dem Löschgesuch nicht zu entsprechen, soweit die Verarbeitung für die Erfüllung bestimmter rechtlicher Verpflichtungen bzw. für bestimmte Aufgabenwahrnehmungen erforderlich ist. Zu den rechtlichen Verpflichtungen wird auf die Ausführungen zu Art. 6 DSGVO unter 2.4.1.3.1 verwiesen.

Öffentliches Interesse (Buchst. c) Ein Löschrecht ist ebenfalls nicht gegeben, soweit die Verarbeitung erforderlich ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Abs. 2 Buchst. h und i sowie Artikel 9 Abs. 3 DSGVO.

Archiv, Forschung und Statistik (Buchst. d) Eine gewisse Aufweichung des Grundsatzes der Speicherbegrenzung besteht bei im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder für statistische Zwecke gemäß Artikel 89 Abs.1 DSGVO, soweit das Lösch-

[612] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 38.
[613] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 17 Rn. 38.
[614] BSI, IT-Grundschutz-Kompendium, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6 [letzter Abruf 18.08.2021].
[615] Siehe hierzu https://www.din.de/de/wdc-beuth:din21:249218525 [letzter Abruf 18.08.2021].
[616] SDM - Baustein 60 “Löschen und Vernichten”, Version V1.0a, abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell [letzter Abruf 18.08.2021].

recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt.[617]

Rechtsansprüche (Buchst. e) Wenn der Zweck der Verarbeitung wegfällt, die betroffene Person die Daten aber zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt. Aus der Formulierung „benötigt" ergibt sich, dass zumindest eine hinreichende Wahrscheinlichkeit für eine rechtliche Auseinandersetzung bestehen muss.[618]

2.4.6.2 „Recht auf Vergessenwerden"

Das Recht auf Vergessenwerden hatte bereits der EuGH mit dem Urteil *Google v. Spain* im Jahr 2014 auf Grundlage des Rechts auf Löschung aus der Datenschutz-Richtlinie abgeleitet.[619] Mit der DSGVO wurde in Art. 17 Abs. 2 DSGVO nun Klarheit darüber geschaffen, dass betroffene Personen gegenüber dem für die Verarbeitung Verantwortlichen verlangen können, nach einer Veröffentlichung ihrer personenbezogenen Daten ein Löschungsverlangen an andere Stellen weiterzuleiten.[620]

Art. 17 Abs. 2 DSGVO

Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

2.4.6.3 Zwischenergebnis zum Grundsatz der Speicherbegrenzung und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Da sich die Löschpflichten nach der Zweckerreichung und damit der verfolgten Zielsetzung und zu Grunde liegenden Rechtsgrundlage richten, kann es im Hinblick auf den Betrieb und im Hinblick auf die Kommunikation im und mit dem Unternehmen zu unterschiedlichen Löschfristen kommen. Daher ist ein Löschmanagement essentiell, um vorab ggf. für unterschiedliche Datenkategorien unterschiedliche Löschfristen vorzusehen. Im Rahmen der Transparenzpflichten muss die Speicherdauer oder zumindest die Kriterien für die Festlegung dieser Speicherdauer den betroffenen Personen mitgeteilt werden. Vorbedingung hierfür ist es, dass sich der/die Verantwortliche/n zunächst selbst einen Überblick über die betroffenen Daten, die Verarbeitungsschritte, die Verarbeitungszwecke und die dafür jeweils einschlägigen Rechtsgrundlagen macht.

[617] Zu Privilegien der Forschung siehe: *European Data Protection Supervisor (EDPS)*, A Preliminary Opinion on data protection and scientific research, S. 23; *Johannes/Richter,* DuD 2017, 300 (301); *Molnár-Gábor,* DSRITB 2018, 159 (164); *Wirth,* ZUM 2020, 585 (591 ff.).
[618] *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 18 Rn. 22 f.
[619] EuGH, Urteil vom 13.05.2014 – C-131/12 – Google/Spain.
[620] *Albrecht*, CR 2016, 88 (93).

2.4.7 Datensicherheit

Art. 5 Abs. 1 Buchst. f DSGVO enthält den Grundsatz der „Integrität und Vertraulichkeit".

> **Art. 5 Abs. 1 Buchst. f DSGVO**
>
> Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen

Dieses Datenschutzprinzip wird in Art. 32 DSGVO konkretisiert und erlegt dem Verantwortlichen sowie dem Auftragsverarbeiter (teilweise gemeinsam) die Pflicht zur Sicherung der Daten auf.

2.4.7.1 Bedeutung des risikobasierten Ansatzes

Im Hinblick auf ein angemessenes Schutzniveau gelten die bereits durch den risikobasierten Ansatz[621] nach Art. 25 Abs. 1 DSGVO bekannten Kriterien:

- Stand der Technik,
- Implementierungskosten,
- Art, Umfang, Umstände und Zwecke der Verarbeitung sowie
- unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Art. 32 Abs. 2 DSGVO weist zudem darauf hin, dass bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen sind, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

2.4.7.2 Umsetzungsmöglichkeiten

Art. 32 Abs. 1 DSGVO bietet neben den Abwägungskriterien zur Bestimmung risikoadäquater „geeigneter technischer und organisatorischer Maßnahmen" (TOMs) zur Erreichung eines angemessenen Schutzniveaus auch Beispiele solcher Maßnahmen. Mit den Worten „gegebenenfalls unter anderem" wird deutlich, dass es sich nur um eine Aufzählung nicht abschließender Beispiele handelt:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

[621] Dieser gilt auch im Rahmen des Art. 32 DSGVO: *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik", S. 9.

- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- Hierbei gilt zu bedenken, dass die Auswahl geeigneter TOMs, insbesondere unter Berücksichtigung des (jeweils aktuellen) Stands der Technik, nicht eine einmalige Maßnahme bleiben darf, sondern mittels einer transparenten Methode zum Vergleich der am Markt verfügbaren Alternativen regelmäßig wiederholt werden sollte.[622]

Pseudonymisierung: Soweit einer Pseudonymisierung unterzogene Daten durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können, werden diese weiterhin als personenbezogene Daten zu betrachten sein (vgl. EG 26 S. 2 DSGVO).[623] Entsprechend der Definition der Pseudonymisierung kann diese nicht bei jeglichem Ersetzen des bürgerlichen Namens durch eine Kennziffer vorliegen, wenn diese Daten ohne Weiteres einer identifizierbaren Person zugeordnet werden können.[624] Zwar werden als Beispiele für Pseudonyme auch Künstlernamen, Telefonnummern, E-Mail-Adressen, Benutzernamen und Personalnummern genannt.[625] Sog. „offene Pseudonyme“[626] wie Telefonnummern, deren Zuordnung zu einer konkreten Person über öffentlich zugängliche Telefonverzeichnisse oder ähnliches leicht umsetzbar ist, und „Personenpseudonyme“,[627] die einer Person fest zugewiesen sind, erfüllen allerdings kaum die Anforderungen der Definition. Zu unterscheiden ist somit zwischen dem Pseudonym nach allgemeinem Sprachgebrauch, das bereits bei der Ersetzung des Namens durch einen erfundenen „Decknamen“ oder eine Kennziffer gegeben ist, und der Pseudonymisierung i.S.d. Art. 4 Nr. 5 DS-GVO.[628] Insofern wird vorgeschlagen, zwischen formaler, faktischer und absoluter Pseudonymität zu differenzieren.[629] Entsprechend erhöht oder senkt die Pseudonymisierung das Schutzlevel.

Verschlüsselung: Im Hinblick auf E-Mail stellte die DSK fest, dass sowohl Ende-zu-Ende-Verschlüsselung als auch Transportverschlüsselung von Verantwortlichen mindestens im Rahmen der Abwägung notwendiger Maßnahmen berücksichtigt werden müssen, da beide Verfahren für ihren jeweiligen Anwendungszweck Risiken für die Vertraulichkeit der übertragenen Nachrichten mindern.[630] Da die meisten Messengerdienste mittlerweile über Ende-zu-Ende-Verschlüsselung verfügen, kann dies bereits als branchenspezifisch bewährte allgemeine Regel der Technik gewertet werden – welche noch über den Stand der Technik hinausgeht.[631] Andernfalls wäre ein „mitlesen“ der Kommunikationsinhalte, welche zwischen den Kommunikationspartnern ausgetauscht werden, durch den Messengerdienstbetreiber möglich.[632]

---

[622] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 12.
[623] Siehe hierzu: *Roßnagel/Scholz*, MMR 2000, 721 (725).
[624] *Ernst,* in: Paal/Pauly, DS-GVO Art. 4 Rn. 42.
[625] *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 94.
[626] Zum Begriff siehe: *Roßnagel/Scholz*, MMR 2000, 721 (727); ähnlich *Probst*, in: Bäumler/von Mutius, Anonymität im Internet, S. 179 (185).
[627] Zum Begriff siehe: *Hansen*, in: Bäumler/von Mutius, Anonymität im Internet, S. 198 (205).
[628] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 506 ff.
[629] *Ziebarth,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 4 Rn. 98.
[630] *DSK - Datenschutzkonferenz*, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, S. 3.
[631] Vgl. zur Abgrenzung: Abschnitt 2.4.4.2.2 (im Rahmen des „Stands der Technik“ im Hinblick auf datenschutzfreundliche Technikgestaltung).
[632] *Schrey u. a.*, MMR 2017, 736 (737).

Schutzziele: In der IT-Sicherheit werden klassischerweise die Schutzziele Vertraulichkeit (**C**onfidentiality), Integrität (**I**ntegrity) und Verfügbarkeit (**A**vailability) fokussiert sowie um die Ziele Authentizität, Verbindlichkeit, Resilienz, und Anonymität erweitert.[633] Cybersicherheit“ bezeichnet „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.“[634]

Schutzziele		Beschreibung	Typische Angriffe
Confidentiality	Vertraulichkeit	Schutz vor dem Abhören / Mitlesen von Daten; Zugriff auf Informationen und Systeme nur durch Berechtigte möglich	Man-in-the-Middle
Integrity	Integrität	Schutz vor der Manipulation von Daten; Informationen sind inhaltlich korrekt, unversehrt und vollständig	
Availability	Verfügbarkeit	Schutz vor Systemausfällen; Informationen sind für Berechtigte zugänglich und nutzbar	Denial-of-Service
Authenticity	Authentizität	Garantie für Echtheit einer Nachricht / Vertrauenswürdigkeit von Daten	Spoofing
Non-Repudiation	Verbindlichkeit	Eine Partei kann eine durchgeführte Handlung nicht abstreiten; eindeutige Zuordnung zu einer Quelle	
Resilience	Resilienz	Widerstandsfähigkeit gegenüber Sabotage	
Anonymity	Anonymität	Schutz der Identität	

Tabelle 5 Schutzziele der Informationssicherheit

In Anlehnung an das Standard-Datenschutzmodell[635] können diese Ziele noch um die Ziele Nichtverkettbarkeit, Transparenz und Intervenierbarkeit ergänzt werden.[636] Zur Sicherung der Vertraulichkeit sollten im Unternehmenskontext vorab feste Kommunikationswege festgelegt werden, welche auch in Krisenzeiten beibehalten werden können.[637]

Assume-Breach-Paradigma: Da immer wieder neue, zuvor noch unbekannte Sicherheitslücken (sog. „Zero-Day-Schwachstellen“) entdeckt werden, rät das Bundesamt für Sicherheit in der Informationstechnik (BSI) stets davon auszugehen, dass ein Produkt Schwachstellen enthält.[638] Insofern ist hervorzuheben, dass Sicherheitskonzepte eine ganzheitliche Sicherheitsarchitektur für den gesamten Produktlebenszyklus, angepasst an die jeweiligen Konfigurationsmöglichkeiten bieten sollten.[639] Trifft den Hersteller des Kommunikationssystems keine direkte Verpflichtung zur Umsetzung der Anforderungen aus Art. 32 DSGVO (sofern dieser als Produktlieferant nicht selbst Verantwortlicher oder Auftragsverarbeiter ist), sollten Unternehmen entsprechende Update-Services (ggf. gesondert) vereinbaren. Denn als Unternehmer i.S.d. § 14 BGB profitieren

[633] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 14; *Rockstroh/Kunkel*, MMR 2017, 77 (78); *Heckmann*, MMR 2006, 280 (281); *Bräutigam/Klindt*, NJW 2015, 1137 (1141). Vgl. auch § 2 Abs. 2 BSIG.
[634] Art. 2 Nr. 1 Cybersecurity Act.
[635] Siehe Abschnitt 2.4.4.2.5.1.
[636] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 15.
[637] vgl. *Gilga*, ZD-Aktuell 2020, 07113.
[638] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2017, S. 18; *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020, S. 22 ff.; BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 38.
[639] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 17.

sie nicht von der durch die Digitale-Inhalte-Richtlinie (Richtlinie (EU) 2019/770) sowie Warenkauf-Richtlinie (Richtlinie (EU) 2019/771) forcierten Novellierungen im BGB zu Update-Pflichten, da diese vornehmlich Verbraucher*innen i.S.d. § 13 BGB schützen.[640]

Überprüfung: Empfohlen wird die Umsetzung der Sicherheitsfunktionen durch vertrauenswürdige Dritte überprüfen zu lassen.[641] In diesem Sinne fallen auch sog. Penetrationstests (kurz: Pentests) unter Art. 32 Abs. 1 Buchst. d DSGVO.[642] Dabei sollte beachtet werden, ob Hersteller solche Pentests und ähnliche Sicherheitsüberprüfungen ausschließen oder explizit erlauben. Denn sowohl aus Urheber- als auch Strafrechtlicher Sicht kann es u.U. zu Implikationen kommen, wenn Nutzer*innen ohne Einverständnis der jeweiligen Rechteinhaber Softwaretests durchführen (bzw. von Dritten durchführen lassen), welche unterschiedliche Formen des Reverse-Engineerings beinhalten.[643] Handelt es sich um Open-Source-Code, ist damit in der Regel die Befugnis zur Bearbeitung und damit auch Formen der Sicherheitsüberprüfungen wie Disassemblieren oder Dekompilieren des Codes erlaubt.[644] Bei der Auswahl eines geeigneten Angebots kann auch darauf geachtet werden, ob der Anbieter über eine Responsible-Disclosure-Policy verfügt. Diese Policy regelt wie durch Dritte gefundene Sicherheitslücken an den Hersteller gemeldet werden können.[645]

Dokumentation: Der Stand der Technik sollte im Rahmen des IT-Sicherheitsmanagements nicht nur berücksichtigt, sondern auch dokumentiert werden.[646]

2.4.7.3 Data Breach Notification

Meldepflicht gegenüber Aufsichtsbehörden: Gemäß Art. 33 Abs. 1 DSGVO muss im Falle der Verletzung des Schutzes personenbezogener Daten der Verantwortliche diesen Vorfall unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden der Verletzung an seine zuständige Aufsichtsbehörde melden. Art. 55 DSGVO klärt, welche Aufsichtsbehörde zuständig ist. Nach seinem Wortlaut könnte „Verletzungen des Schutzes personenbezogener Daten“ jeden beliebigen Datenschutzverstoß umfassen – gemeint ist allerdings „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“ (Art. 4 Nr. 12 DSGVO). [647] Die englische Bezeichnung „personal data breach“ ist insofern passender, da deutlich wird, dass es um sog. „Datenpannen“ geht, also primär sicherheitsbezogene Vorfälle.[648]

Nach Art. 33 Abs. 2 DSGVO muss der Auftragsverarbeiter entsprechend an den Verantwortlichen melden. Art. 33 Abs. 3 DSGVO benennt einen Mindestsatz an Informationen, die eine Meldung enthalten muss. Die Bereitstellung der Informationen ist auch schrittweise möglich (Art. 33 Abs. 4 DSGVO). Art. 33 Abs. 5 DSGVO ver-

---

[640] Siehe zur Gesetzesnovelle: BT-Drs. 19/27653; BT-Drs. 19/27424.
[641] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 17.
[642] *Hladjk,* in: Ehmann/Selmayr - DSGVO Art. 32 Rn. 10; *Jandt,* in: Kühling/Buchner - DS-GVO/BDSG Art. 32 Rn. 29; *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 32 Rn. 44; *Mantz,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 32 Rn. 20; *Hansen,* in: NK Datenschutzrecht Art. 32 Rn. 56.
[643] *Maier u. a.*, DuD 2020, 511; *Wagner*, PinG 2020, 66 (71); *Wagner*, DuD 2020, 111.
[644] Vgl. zur GPL: *Hoeren,* in: Westphalen/Thüsing - Vertragsrecht und AGB-Klauselwerke, Kap. IT-Vertäge Rn. 210.
[645] *European Network and Information Security Agency (ENISA)*, Good practice guide on vulnerability disclosure, S. 56 ff.; *Pupillo u. a.*, Software vulnerability disclosure in Europe, S. 80; *National Cyber Security Centre*, Coordinated Vulnerability Disclosure: the Guideline, S. 21 ff.
[646] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik“, S. 9.
[647] *Bieker u. a.*, DuD 2018, 492 (496).
[648] *Bieker u. a.*, DuD 2018, 492 (496).

pflichtet zudem zur Dokumentation aller im Zusammenhang mit dem Vorfall stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen, sodass der Aufsichtsbehörde eine Überprüfung der Einhaltung der Data-Breach-Notification-Vorgaben möglich ist.

Ausnahmen von der Meldepflicht: Von der Meldepflicht ausgenommen sind Verletzungen des Schutzes personenbezogener Daten, die „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen". Hierbei ist gemeint, dass sich das Risiko voraussichtlich nicht realisiert: besteht kein hohes oder normales Risiko, sondern nur ein geringes Risiko, muss nicht gemeldet werden.[649]

Information betroffener Personen: Darüber hinaus sind unverzüglich alle betroffenen Personen gemäß Art. 34 Abs. 1 DSGVO zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Auch in diesem Zusammenhang ist wieder die Risikobeurteilung elementar.[650] Diese Benachrichtigung muss:

- In klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten umschreiben (Art. 34 Abs. 2 DSGVO) und
- Informationen zum Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen, eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten sowie eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen enthalten (Art. 34 Abs. 2 i.V.m. Art. 33 Abs. 3 Buchst. b, c und d DSGVO).

Art. 34 Abs. 3 DSGVO enthält wiederum Ausnahmen von der Benachrichtigungspflicht bei:

- Ergreifen geeigneter technischer und organisatorischer Sicherheitsvorkehrungen, die Daten unzugänglich machen (präventiv),[651]
- Sicherstellung durch nachfolgende Maßnahmen, dass ein hohes Risiko aller Wahrscheinlichkeit nicht mehr besteht,[652] oder
- Wenn die Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde.[653] Die Einzelbenachrichtigung kann dann durch eine öffentliche Bekanntmachung oder vergleichbar wirksam informierende Maßnahme ersetzt werden.

Der EDSA stellt in seinen Guidelines zur Data-Breach-Notification eine Übersicht bereit:[654]

[649] *Bieker u. a.*, DuD 2018, 492 (496); vgl. auch *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 18 ff.
[650] Zur Risikobeurteilung im Rahmen der datenschutzfreundlichen Technikgestaltung siehe Abschnitt 2.4.4.2.1.
[651] *Jandt,* in: Kühling/Buchner - DS-GVO/BDSG Art. 34 Rn. 14; vgl. auch *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 18 zur Frage der Meldepflicht bei verschlüsselten Daten.
[652] Zur Auslegung: *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 22 ff.
[653] Zur Unverhältnismäßigkeit des Aufwands: *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 22; *Jandt,* in: Kühling/Buchner - DS-GVO/BDSG Art. 34 Rn. 15a m.w.N.
[654] *European Data Protection Board*, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, S. 30.

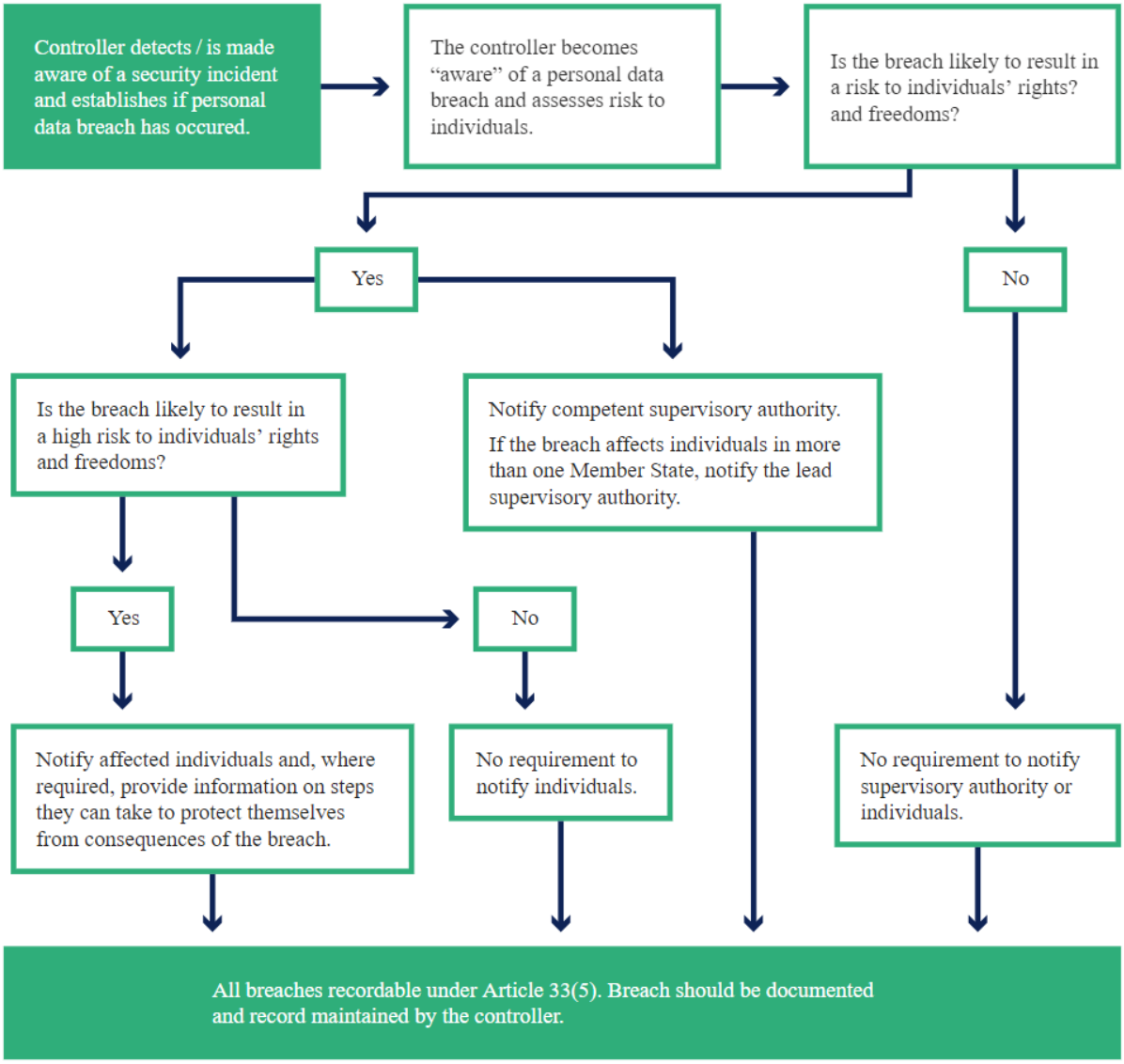


Abbildung 11 Flowchart zu Melde- und Benachrichtigungspflichten nach Artt. 33, 34 DSGVO des Europäischen Datenschutzausschusses (EDSA)

2.4.7.4 Einschränkbarkeit der Datensicherheit?

Die IT-Sicherheit wird erheblich dadurch beeinträchtigt, wenn bewusst sog. Backdoors bzw. Hintertüren bspw. für Strafverfolgungsbehörden und/oder Nachrichtendienste eingebaut werden (müssen), oder gefundene Sicherheitslücken offen gehalten werden.[655] Diese Jahr entbrannte mit der Ratsentschließung zu „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" erneut der Konflikt, wie die verschie-

[655] *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik", S. 17.

denen Sicherheitsbedürfnisse: IT- und Datensicherheit einerseits und öffentliche Sicherheit andererseits gelöst werden können.[656] Gerade Messengerdienste, die ein hohes Maß an Datensicherheit und Datensparsamkeit bieten, wären widersprüchlichen Anforderungen ausgesetzt, wenn sie einerseits bestmögliche Datenschutzkomponenten bieten (anonyme/pseudonyme Nutzungsmöglichkeit, Verschlüsselung, etc.) und andererseits gesetzlichen Regelungen unterworfen werden könnten, staatliche Behörden wie Strafverfolgungsbehörden oder Nachrichtendienste bei Abhörmaßnahmen unter Durchbrechung des Datenschutzsystems zu unterstützen. Dementsprechend sollen an dieser Stelle auch die verfassungsrechtlichen Grenzen solcher Initiativen aufgezeigt werden.

2.4.7.4.1 Gesetzliche Regelungen mit Bezug zur Sicherheit der Kommunikation über Messengerdienste

2021 stimmte der Bundestag für die Ausweitung des Einsatzes sog. Staatstrojaner.[657] Dies erlaubt Sicherheitsbehörden das Mitlesen auch von Messengernachrichten. Für solche Trojaner werden IT-Sicherheitslücken ausgenutzt. Zudem wurden die Mitwirkungspflichten von Telekommunikationsdiensten spezifiziert. Nach § 2 Abs. 1a Artikel 10-Gesetz (G10) muss, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, auf Anordnung Auskunft über die näheren Umstände der Telekommunikation erteilen, Inhalte ausleiten, Überwachung und Aufzeichnung der Telekommunikation ermöglichen und technische Unterstützung bei Maßnahmen nach § 11 Abs. 1a G10 leisten. Näheres soll eine Rechtsverordnung regeln. Nach der bisherigen Rechtslage habe eine „Aufklärungslücke bei Messengerdiensten“ bestanden. [658] Technisch müsse die „ruhende Kommunikation“ aus dem Speicherplatz des Endgerätes ausgelesen werden. Mit der Änderung des § 11 Abs. 1a S. 2 G10 wird dies nun rechtlich ermöglicht. Diese Regelung orientiere sich an dem Modell der Strafprozessordnung (§ 100a Abs. 1 S. 2 und 3 sowie Abs. 5 und 6 StPO).[659]

Gemäß § 100a Abs. 4 StPO muss jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, auf Grund der Anordnung einer Überwachung den Ermittlungspersonen diese Maßnahmen ermöglichen und die erforderlichen Auskünfte unverzüglich erteilen. Näheres ist in der TKÜV geregelt.

Erbringung / Mitwirkung Telekommunikationsdienst: Aufgrund des weiten Telekommunikationsbegriffs unterfällt laut BVerfG „der Zugriff auf E-Mail-Kommunikation, jedenfalls soweit es sich um die Übertragung der Nachricht vom Gerät des Absenders über dessen Mailserver auf den Mailserver des E-Mail-Providers und um den späteren Abruf der Nachricht durch den Empfänger handelt, unstrittig dem Anwendungsbereich des § 100a StPO“.[660] Dies dürfte auch für Messenger relevant sein.[661]

Geschäftsmäßige Erbringung / Mitwirkung Telekommunikationsdienste (G10): Bisher wurde auf die Legaldefinition des TKG zurückgegriffen.[662] Dabei sollen aber firmen- oder behördenintern betriebene Kom-

---

[656] *Rat der Europäischen Union,* Entschließung des Rates zur Verschlüsselung–Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung, 13084/1/20REV 1, Brüssel, den 24.11.2020.

[657] Vgl. *BMI,* Gesetz zur Anpassung des Verfassungsschutzrechts, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/anpassung-des-verfassungsschutzrechts.html; bitkom, Stellungnahme vom 30.06.2020, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/anpassung-des-verfassungsschutzrechts-bverfschg/bitkom.pdf;jsessionid=BE2B50C64E54EFF6BE84188DC8A8CD0D.2_cid287?__blob=publicationFile&v=1 [letzter Abruf 19.08.2021].

[658] BT-Drs. 19/24785, S. 22

[659] BT-Drs. 19/24785, S. 22

[660] BVerfG, Beschluss vom 20.12.2018 - 2 BvR 2377/16 – Posteo, Rn. 42.

[661] Der bestehende Konflikt mit der EuGH-Rechtsprechung in EuGH, Urteil vom 13.06.2019 - C-193/18 dürfte mit der Neufassung des TKG und der damit einhergehenden expliziten Erweiterung auf OTT-Dienste überwunden sein.

[662] *Roggan*, G-10-Gesetz, § 2 Rn. 4; *Günther,* in: Münchener Kommentar zur StPO, § 2 Rn. 8.

munikationsnetze (insbesondere Intranets und andere Corporate Networks) von einer Überwachung ausgenommen werden, da diese keinen Drittbezug besitzen.[663] Die Notwendigkeit eines Drittbezugs und damit Außenwirkung ergab sich aus § 3 Nr. 10 TKG.[664] Insofern seien auch Dienstleister, die lediglich ein geschlossenes System für den Eigenbedarf betreiben nicht unter § 2 G10.[665] Zwar fehlt im neuen TKG eine Entsprechung, die Einschränkung auf Geschäftsmäßigkeit folgt aus dem G10-Gesetz, weshalb dieses nach hier vertretener Ansicht nicht auf geschlossene Systeme anwendbar ist.

Bedeutung der Mitwirkungspflichten: Pflichten zur Auskunftserteilung beziehen sich nur auf Telekommunikationsumstände zeitlich nach einer entsprechenden Anordnung. [666] Konkrete Pflichten ergeben sich aus dem TKG i.V.m. der TKÜV. Die Reichweite der Pflichten der TK-Anbieter richtet sich danach, welche Daten tatsächlich in ihrem Herrschaftsbereich vorhanden sind.[667] Unklar ist, ob Datenzugriffsmöglichkeiten geschaffen werden müssten, um eine Überwachungsmaßnahme zu unterstützen. Im Hinblick auf die Frage, ob ein E-Mail-Anbieter IP-Adressen herausgeben müsse, selbst wenn diese nach der gewählten Systemstruktur nicht gespeichert werden, argumentierte das BVerfG, dass dieser die abgerufenen Datenpakete seiner Kundschaft gar nicht übersenden könne, ohne die öffentlichen IP-Adressen seiner Kundschaft wenigstens für die Dauer der Kommunikation flüchtig zu speichern.[668] Damit läge keine Anordnung zur Bereitstellung nicht vorhandener Daten vor – da die Daten zumindest kurzzeitig vorhanden sind. Selbst wenn die Protokollierung dieser Daten einem aus Datenschutzgründen bewusst gewählten Geschäftsmodells widerspreche, sei kein verfassungswidriger Eingriff in die Berufsfreiheit gegeben.[669] Ob dies auch eine Durchbrechung des Verschlüsselungskonzepts implizierte, ließ das Gericht allerdings offen. Da das Gericht eine subjektive Unmöglichkeit der Datenbereitstellung (aufgrund von hohem Zeit- und Kostenaufwand einer Systemumstellung) nicht gelten ließ, wurden mit dem Urteil durchaus Hürden für den Nachweis objektiver Unmöglichkeit gesetzt.[670] In der Literatur wird dagegen die Position vertreten, dass weder zusätzliche Daten auf Nutzerseite (wie kryptographische Schlüssel) erhoben werden müssen, noch eine Schwächung oder Umgehung von Verschlüsselungstechniken angeordnet werden kann. [671] Dem ist zuzustimmen. Da das Gericht die potentielle Verletzung von Datenschutzrechten gegenüber Drittnutzer*innen nicht ausreichend problematisierte, kann davon ausgegangen werden, dass eine die Datensicherheit von anderen Dienstnutzenden tangierende Wirkung der Entscheidung nicht beabsichtigt war. Zudem sind die staatlichen Schutzpflichten gegenüber den betroffenen Personen, welche einen TK-Dienst nutzen, zu bedenken.

2.4.7.4.2 Verletzung staatlicher Schutzpflichten

Erwägungen zur Schwächung der Datensicherheit im Rahmen der elektronischen Kommunikation begegnen erheblichen verfassungsrechtlichen Bedenken. Wie bereits in Abschnitt 2.1.3.3 dargelegt, begründen die Grundrechte als objektive Wertentscheidung der Verfassung staatliche Schutzpflichten. Insofern begründet das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG einen Auftrag an den Staat, Grundrechtsträger*innen vor

[663] *Roggan*, G-10-Gesetz, § 2 Rn. 5.
[664] "geschäftsmäßiges Erbringen von Telekommunikationsdiensten" ist das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht.
[665] *Günther,* in: Münchener Kommentar zur StPO, § 2 Rn. 8.
[666] *Günther,* in: Münchener Kommentar zur StPO, § 2 Rn. 9.
[667] *Brodowski,* in: BeckOK IT-Recht, § 100a StPO Rn. 26.
[668] BVerfG, Beschluss vom 20.12.2018 - 2 BvR 2377/16 – Posteo, Rn. 48.
[669] BVerfG, Beschluss vom 20.12.2018 - 2 BvR 2377/16 – Posteo, Rn. 41 ff.
[670] Vgl. *Seeger*, Newsdienst Compliance 2019, 23024.
[671] *Brodowski,* in: BeckOK IT-Recht, § 100a StPO Rn. 26.

dem Zugriff privater Dritter auf eine dem Fernmeldegeheimnis unterfallende Kommunikation zu schützen.[672] Auch dem Recht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kommt eine Schutzdimension zu, da das besondere, grundrechtlich erhebliche Schutzbedürfnis aus der Angewiesenheit auf die Nutzung informationstechnischer Systeme für die Freiheitsverwirklichung und die allgemeine Entfaltung der Persönlichkeit folgt.[673] Offene (und offen gehaltene) Lücken in der Sicherheit gefährden zudem des Recht auf informationelle Selbstbestimmung, da über Schwachstellen zumeist auch Zugang zu personenbezogenen Daten eröffnet wird. Sicherheitslücken entfalten ferner Schädigungspotenzial im betrieblichen Bereich und im Handel, wenn durch Infiltrationen Systeme manipuliert oder Abläufe gestört werden können.[674]

„Weiß der Staat von Sicherheitslücken, die den Herstellern und Nutzern unbekannt sind, verdichtet sich der allgemeine Schutzauftrag zu einer konkreten grundrechtlichen Verpflichtung, die Nutzerinnen und Nutzer informationstechnischer Systeme davor zu schützen, dass Dritte über unbekannte Sicherheitslücken die genutzten Systeme infiltrieren.“ [675] Diese konkrete Schutzpflicht beruht

- auf dem hohen Gefährdungs- und Schädigungspotenzial von Sicherheitslücken für die Grundrechte der Nutzer*innen informationstechnischer Systeme (natürliche wie juristische Personen),
- auf der fehlenden Möglichkeit der betroffenen Nutzerkreise, sich selbst effektiv zu schützen (fehlende Selbstschutzmöglichkeiten),
- und auf der Kenntnis von der Sicherheitslücke durch staatliche Stellen, die somit Abhilfe schaffen können – bei gleichzeitiger Unkenntnis des Herstellers bzw. Produktverantwortlichen.[676]

Diese vom BVerfG festgestellte konkrete grundrechtliche Schutzpflicht des Staates schließt allerdings nicht aus, eine Quellen-Telekommunikationsüberwachung mittels einer unbekannten Schutzlücke (sog. „Zero-Day-Schwachstellen“) durchzuführen. Sie verlangt aber eine Regelung zur Auflösung des Zielkonflikts zwischen dem Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung der staatlichen Überwachungsmaßnahme zum Zwecke der Gefahrenabwehr andererseits.[677] Das BVerfG verlangt insofern, dass Regelungen zum Umgang mit Sicherheitslücken klarstellen, dass

- Behörden bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke ermittelt und
- andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt,
- beides zueinander ins Verhältnis setzt und die Sicherheitslücke an den Hersteller meldet, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt.[678]

Daraus folgt kein generelles Verbot für Backdoors oder eine generelle Meldepflicht an die Hersteller bzw. Produktverantwortlichen im Sinne eines Responsible Disclosures Seitens deutscher Behörden, sofern sie in Kenntnis einer Sicherheitslücke gelangen. Andererseits werden die Hürden für ein staatliches Schwachstellenmanagement hoch gesetzt.

---

[672] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 32.
[673] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 33. Auch juristische Personen können sich nach Art. 19 Abs. 3 GG auf diese Grundrechte berufen.
[674] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 37.
[675] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 34.
[676] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 35 ff.
[677] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 34, 43 ff.
[678] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021 – 1 BvR 2771/18 -, Rn. 44.

2.4.7.5 Zwischenergebnis zur Datensicherheit und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Gerade kleine und mittelständische Unternehmen zeigten in der Vergangenheit wiederholt Schwierigkeiten, IT-Sicherheitsbedürfnisse und tatsächlich umgesetzte Sicherheitsmaßnahmen in Einklang zu bringen.[679] Insofern ist es bedeutsam, dass Angebote von Kommunikationslösungen essentielle Sicherheitsfunktionen aufweisen – welche nach einer Risikobewertung einen Einsatz im beruflichen Kontext zulässt – und diese auf transparente Weise kommunizieren. Einer Abschwächung dieses Sicherheitsniveaus (bspw. durch Backdoors, bewusst zurückgehaltene Information zu Sicherheitslücken durch staatliche Stellen, etc.) sind verfassungsrechtlich enge Grenzen gesetzt.

Praxistipp:

(1) Ein Messengerdienst sollte dem Stand der Technik entsprechende Ende-zu-Ende-Verschlüsselung sowie Transportverschlüsselung nutzen.
(2) Um zu ermitteln, ob ein Dienst bzw. eine Software ein hohes Sicherheitsniveau bietet, können folgende Aspekte Hinweise geben:
    a. Möglichkeit Anonymisierung / Pseudonymisierung
    b. Veröffentlichung externer Audits
    c. Veröffentlichung einer Responsible Disclosure Policy
    d. Dokumentation der Sicherheitskomponenten
    e. Sicherheitszertifikate

2.4.8 Rechenschaftspflicht

Der datenschutzrechtlich Verantwortliche unterliegt weitreichenden Rechenschaftspflichten, die sich unmittelbar aus datenschutzrechtlichen Vorgaben herleiten lassen. Gemäß Art. 5 Abs. 2, Alt. 2 DSGVO muss der Verantwortliche die Einhaltung aller datenschutzrechtlicher Grundsätze aus Art. 5 DSGVO nachweisen können. Da die Datenschutzgrundsätze zum einen für sich selbst stehen als auch in verschiedenen anderen Vorschriften ihre Konkretisierung finden, erstreckt sich die Rechenschaftspflicht des Verantwortlichen im Prinzip auf alle Datenverarbeitungsvorgänge mit Personenbezug.[680]

Für die Rechenschaftspflicht ergibt sich daher folgendes: Der Verantwortliche ist dazu angehalten alle Datenverarbeitungsprozesse in sein Verzeichnis der Verarbeitungstätigkeiten zu erfassen (Art. 30 DSGVO). Insbesondere die Dokumentation entsprechender Handlungsanweisungen, Betriebsvereinbarungen mithin alle organisatorischen Maßnahmen im Zusammenhang mit der Einführung und Nutzung von Kommunikations- und Kollaborationstools. Abschnitt IV der DSGVO gibt zudem Vorgaben, wann ein/e Datenschutzbeauftragte/r zu bestellen ist, welche Aufgaben diese/r erfüllt und wie seine/ihre Stellung aussieht. Ergänzt werden diese Vorschriften durch § 38 BDSG.

[679] *Ziegler*, DuD 2021, 330 (330) m.w.N.
[680] Vgl. zur Bedeutung der Rechenschaftspflicht: *Jung*, ZD 2018, 208 (208 ff.).

Ausnahmen im Hinblick auf die Pflicht ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen, gelten gemäß Art. 30 Abs. 5 DSGVO für:

- Unternehmen oder Einrichtung mit weniger als 250 Beschäftigten,
- Die vorgenommene Verarbeitung birgt kein Risiko für die Rechte und Freiheiten der betroffenen Personen und / oder erfolgt nur gelegentlich,
- Keine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO und personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.

2.4.8.1 Zuordnung von Verantwortlichkeit innerhalb eines Unternehmens

Vor der Inbetriebnahme einer Kommunikationslösung sollten Rollen und Verantwortlichkeiten im Unternehmen klar definiert werden, sofern dieses die datenschutzrechtliche Verantwortlichkeit trägt.[681] Sind im Rahmen von Unternehmensverbünden oder Projekten mit anderen Partnern mehrere bzw. zahlreiche Personen beteiligt, kann es mitunter Schwierigkeiten bereiten, Verantwortlichkeiten eindeutig zuzuweisen, wobei sich Unternehmen regelmäßig die Handlungen ihrer Beschäftigten zurechnen lassen müssen (vgl. Abschnitt 2.2.4.1). In anderen Kontexten wurden bereits Verantwortlichkeitsmatrizen wie die RACI[682] bzw. RASCI[683]-Matrix entwickelt.[684] Dabei handelt es sich um eine Technik zur Analyse und Darstellung von Verantwortlichkeiten. Diese Techniken könnten auch eingesetzt werden, um bei der Umsetzung der datenschutzrechtlichen Rechenschaftspflicht zu unterstützen. [685] Hierbei ist natürlich zu berücksichtigen, dass die Modelle ggf. an gesetzliche Vorgaben angepasst danach werden müssen, welche sich auf die Rollen auswirken, die im Unternehmen die Durchführungsverantwortung („Responsibility“) und welche die Gesamtverantwortung („Accountability“) tragen, wer gesetzlich verpflichtend beratend zu konsultieren ist (Datenschutzbeauftragter, Betriebsrat) und wie Einzelprozessschritte zu dokumentieren sind (Verfahrensverzeichnisse nach Art. 30 DSGVO).[686]

2.4.8.2 Datenschutzmanagementsysteme

Zur besseren Organisation, gerade bei komplexen Verarbeitungsketten und/oder mehreren Beteiligten, bieten sich Datenschutzmanagementsysteme (DSMS) an, um die Rechenschaftspflicht umzusetzen. Als weitere Vorteile werden Potentiale zur Einsparung digitaler wie analoger Speicherplätze genannt (z. B. durch Vermeidung von Doppelspeicherungen, übersichtliche Speicherpfade oder strukturierte Ablagesysteme).[687] Compliance-Management-Systeme (CMS) sowie Information Security Management Systems (ISMS) sind im unternehmerischen Alltag bereits etabliert. Durch die Rechenschaftspflicht der DSGVO steigt die Bedeutung, diese Ansätze um DSMS zu erweitern.[688] Dieses sollte Datenschutzleitlinien mit klaren Vorgaben zu Aufgaben und

[681] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 8.
[682] RACI steht für die jeweiligen Anfangsbuchstaben der Worte Responsible, Accountable, Consulted, Informed.
[683] Die Abkürzung RASCI leitet sich aus Responsible, Accountable, Supported, Consulted und Informed ab.
[684] *Jung/Hansch*, ZD 2019, 143 (143).
[685] *Jung/Hansch*, ZD 2019, 143 (143).
[686] *Jung/Hansch*, ZD 2019, 143 (144).
[687] *Lurtz*, ZD-Aktuell 2021, 05269.
[688] *Jung*, ZD 2018, 208 (208 ff.).

Rollen, Berichtswesen, Prozessgestaltung, etc., spezifizierende Datenschutzrichtlinien mit konkreten Vorgaben zu einzelnen Maßnahmen und Templates, Arbeitsanweisungen, Schulungsmaßnahmen und Audits umfassen.[689]

2.4.8.3 Zwischenergebnis zur Umsetzung der Datenschutzgrundprinzipien und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Die Datenschutzgrundprinzipien bieten für die Auswahl geeigneter Kommunikations- und Kollaborationslösungen einen guten Rahmen zur Erfassung der wesentlichen Pflichten. Starten sollten Verantwortliche mit einer genauen Definition der verfolgten Zwecke. Daraus leitet sich die einschlägige Rechtsgrundlage, die Risikobewertung im Hinblick auf Datenminimierung und Datensicherheit sowie das Löschkonzept ab. In organisatorischer Hinsicht ist sicherzustellen, dass u.a. Auskunftsersuchen, Berichtigungs- und Löschanfragen rechtzeitig erfüllt werden können. Alle wesentlichen Entscheidungen sollten nachvollziehbar dokumentiert werden.

[689] *Jung*, ZD 2018, 208 (212 f.).

Zweckbindung: Zwecke der Datenverarbeitung	- Zu welchen Zwecken sollen die personenbezogenen Daten verarbeitet werden? - Sind diese Zwecke eindeutig genug umschrieben?
Rechtmäßigkeit, Treu und Glauben: Auswahl der einschlägigen Rechtsgrundlage	- Welche Rechtsgrundlage(n) kommen in Frage? - Ist die Verarbeitung im Beschäftigtenkontext erforderlich? Muss der Betriebsrat einbezogen werden? - Besteht eine rechtliche Verpflichtung, ein Vertrag, ein überwiegendes berechtigtes Interesse? - Ist eine Einwilligung erforderlich und wäre diese wirksam? - Bestehen Sonderkonstellationen. Besondere Kategorien personenbezogener Daten? Regeln für - Telekommunikationsdienste? Telemediendienste?
Transparenz: Information & Auskunft	- Wurde eine Datenschutzerklärung erstellt? Ist diese vollständig, klar und verständlich? - Können Auskunftsersuchen in der vorgegebenen Zeit erfüllt werden bzw. greifen Ausnahmen ein?
Datenminimierung: Risikobewertung und technisch/ organisatorische Maßnahmen (TOMs)	- Welche Risiken bestehen bei der Datenverarbeitung? - Werden nur so viele Daten verarbeitet, wie zwingend erforderlich? Welche TOMs gewährleisten ein angemessenes Risiko? - Sind die Voreinstellungen datenschutzfreundlich gestaltet? - Bei Feststellung eines hohen Risikos muss eine DSFA durchgeführt werden, ggf. ist die Aufsichtsbehörde zu konsultieren.
Speicherbegrenzung	- Besteht ein Löschkonzept? - Können Verarbeitungen eingeschränkt werden, bis zur Entscheidung über Löschanfragen?
Datensicherheit	- Wie wird ein angemessenes IT-Sicherheitsniveau gewährleistet? - Sind Verantwortlichkeiten klar definiert, dass Meldungen / Benachrichtigungen im Fall von Datenschutzverstößen rechtzeitig erfolgen?
Richtigkeit	- Wie wird sichergestellt, dass unrichtige Daten berichtigt werden? - Können Berichtigungsanfragen betroffener Personen erfüllt werden? Können diese ggf. Daten selbst berichtigen?
Rechenschafts-pflicht	- Liegt ein Verzeichnis der Verarbeitungstätigkeiten vor? / Ist dieses entbehrlich? - Muss ein*e Datenschutzbeauftragte*r bestellt werden? - Sind alle nachzuweisenden Tatsachen ausreichend dokumentiert?

2.5 Komplementäre datenschutzrechtliche Anforderungen

Mit der DSGVO wurden weitere gesetzgeberische Neuerungen umgesetzt, die nicht unmittelbar Ausfluss der Datenschutzgrundprinzipien sind. So haben mit dem Recht auf Datenübertragbarkeit (auch Recht auf Datenportabilität genannt) wettbewerbsrechtliche Gedanken Einzug in die DSGVO erhalten (Art. 20 DSGVO).[690] Zielsetzung hier ist primär die Minimierung von Lock-in-Effekten, welche aber mittelbar Einfluss auf die effektive Umsetzung informationeller Selbstbestimmung haben kann.[691] Eine gewisse Skepsis gegenüber der Automatisierung im Zeitalter der künstlichen Intelligenz zeigt das Recht keiner automatisierten Entscheidung im Einzelfall einschließlich Profiling unterworfen zu werden (Art. 22 DSGVO). Als weitere Innovation kann die ausdifferenzierte Regelung zur Auftragsverarbeitung in Abgrenzung zur gemeinsamen Verantwortlichkeit gesehen werden. Diese Aspekte sollen im vorliegenden Abschnitt mit Bezug zur Kommunikation im Unternehmen diskutiert werden.

2.5.1 Neuerungen der DSGVO zur Stärkung der Datensouveränität betroffener Personen

Einige Innovationen der DSGVO lassen sich keinen der zentralen Datenschutzgrundprinzipien zuordnen, stellen nichtsdestotrotz wichtige Bausteine bei der Umsetzung eines adäquaten Datenschutzkonzepts dar und sollten – je nachdem ob die Norm im konkreten Fall einschlägig ist – bei der Umsetzung einer datenschutzgerechten Kommunikation im Unternehmenskontext beachtet werden.

2.5.1.1 Recht auf Datenübertragbarkeit

Dieses Betroffenenrecht soll den Anbieterwechsel erleichtern, indem betroffene Personen die von ihnen bereitgestellten Daten in einem strukturieren, gängigen und maschinenlesbaren Format herausverlangen können, wenn die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht und mithilfe automatisierter Verfahren erfolgt. Besteht der Wunsch diese Daten an einen neuen Verantwortlichen zu übermitteln, darf der bisherige Verantwortliche dies nicht behindern. Soweit dies technisch machbar ist, darf die betroffene Person nach Art. 20 Abs. 2 DSGVO auch verlangen, dass die personenbezogenen Daten direkt vom einen zum anderen Verantwortlichen übermittelt werden. Nicht adressiert ist allerdings die Frage einer „Annahmepflicht“ durch den neuen Verantwortlichen.[692] Das langfristige Ziel dieser Regelung liegt darin, dass im Ergebnis interoperable Formate verwendet werden (vgl. EG 68).[693]

Betroffene Daten: Betont werden muss, dass sich die Daten auch auf die Person beziehen müssen, die ihren Anspruch auf Datenübertragbarkeit geltend macht und keine personenbezogenen Daten Dritter übermittelt werden. Ausgenommen vom Anwendungsbereich der Datenübertragbarkeit sind zudem anonyme bzw. anonymisierte Daten, da sie schon aus dem Anwendungsbereich der DSGVO herausfallen und folglich die betroffene Person nicht unmittelbar betreffen können.[694] Dagegen fallen pseudonymisierte Daten, welche die Person betreffen, in den Anwendungsbereich (vgl. Abschnitt 2.3.1.2.4).

---

[690] *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 7 ff. *Jülicher u. a.*, ZD 2016, 358 (358).
[691] Vgl. *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 20 Rn. 2 ff. *Schantz*, NJW 2016, 1841 (1845).
[692] *Jülicher u. a.*, ZD 2016, 358 (362); *Brüggemann*, K&R 2018, 1 (5).
[693] So auch *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 20.
[694] Vgl. *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 10.

Die DSGVO enthält keine Legaldefinition für das „Bereitstellen“.[695] Nach Einschätzung des EDSA soll es sich bei den von der betroffenen Person bereitgestellten Daten einerseits um solche personenbezogene Daten handeln, die aktiv vom Benutzer eingegeben wurden.[696] Andererseits sollen aber auch solche personenbezogene Daten als „bereitgestellt“ erfasst sein, die durch Beobachtung der betroffenen Person erhoben werden können (auch als Nutzungsdaten bezeichnet).[697] Dagegen sollen solche Daten, die der Verantwortliche aus den bereitgestellten Daten erst abgeleitet hat, nicht vom Anspruch auf Erhalt oder Übermittlung erfasst sein.[698] Nicht betroffen sind daher solche personenbezogene Daten, die der Verantwortliche beispielsweise durch Analysen oder sonstige Verarbeitungsvorgänge gewonnen hat.[699]

Konstellationen: Der Anspruch ist beschränkt auf Konstellationen, in denen entweder die Einwilligung oder ein Vertrag die Rechtsgrundlage zur Datenverarbeitung bilden. Datenverarbeitungen auf Grundlage anderer Erlaubnistatbestände sind explizit ausgenommen. Zudem muss die Datenverarbeitung automatisiert erfolgen. Des Weiteren dürfen bei der Weitergabe personenbezogener Daten allerdings keine Recht Dritter verletzt werden, d.h. insbesondere keine personenbezogenen Daten ohne Legitimationsgrundlage übermittelt werden, die andere betroffene Personen betreffen.[700] Diese Problematik bezieht sich auf die Mehrrelationalität von Daten, die über Doppel- / Drittbezug verfügen können.[701] Würden sämtliche Daten mit Drittbezug vom Datenportabilitätsrecht ausgenommen, könnte dieses gerade in den wettbewerbspolitisch anvisierten Konstellationen der Social Media leer laufen.[702] Problematisch könnte auch der Schutz von Geschäftsgeheimissen im Hinblick auf Metadaten oder Interaktionsdaten werden, wenn sich daraus Unternehmensinterna wie interne Unternehmensstrukturen oder Berechnungsmodelle der Verarbeitungsprozesse ableiten lassen.[703]

Hier wird eine umfassende Abwägung und ggf. Bereitstellung eines eingeschränkten Datensatzes empfohlen.[704] Als technische Lösungsoptionen dieser Problematik werden der Einsatz von Algorithmen[705] zu Trennung der Daten oder Sticky Policies[706] zur eindeutigen Zuordnung zu einer Person vorgeschlagen. Die Artikel-29-Datenschutzgruppe schlägt hingegen Tools vor, die den betroffenen Personen ermöglichen, diejenigen Daten, die sie erhalten und übermitteln möchten, auszuwählen und etwaige Daten anderer Personen auszuschließen.[707] Daneben könnten Verantwortliche Einwilligungsmechanismen für Drittbetroffene einführen, um im Einzelfall selbst darüber zu entscheiden, ob personenbezogene Daten mit Mehrfachbezug übertragen werden sollen.[708]

Geltendmachung: Die betroffene Person muss bei der Geltendmachung ihres Rechts keine Formerfordernisse oder spezifische Fristen einhalten und muss keine Gründe angeben.[709] Der Verantwortliche sollte vor

---

[695] So auch *Jülicher u. a.*, ZD 2016, 358; *Brüggemann*, K&R 2018, 1 (2).
[696] Siehe *Artikel-29-Datenschutzgruppe,* Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 9 ff.
[697] *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 10 ff.; a.A. *Piltz,* in: Gola DS-GVO, Art. 20 Rn. 14. Siehe ausführlich zum Streit: *Westphal/Wichtermann*, ZD 2019, 191 (191 f.); *Brüggemann*, K&R 2018, 1 (2).
[698] Hierin besteht in der Literatur Einigkeit. Siehe *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 10 ff.; *Kamann/Braun,* in: Ehmann/Selmayr - DSGVO Art. 20 Rn. 13; *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 20 Rn. 11; *Brüggemann*, K&R 2018, 1 (2); *Westphal/Wichtermann*, ZD 2019, 191 (191).
[699] Vgl. *Herbst,* in: Kühling/Buchner - DS-GVO/BDSG Art. 20 Rn. 11; *Brüggemann*, K&R 2018, 1 (2).
[700] Für eine strenge Interpretation: *Piltz,* in: Gola DS-GVO, Art. 20 Rn. 40.
[701] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 20 Rn. 26; *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 94a.
[702] *Schantz*, NJW 2016, 1841 (1845).
[703] *Jaspers*, DuD 2012, 571 (573); *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 100.
[704] *Paal,* in: Paal/Pauly - DS-GVO BDSG Art. 20 Rn. 26.
[705] *Jülicher u. a.*, ZD 2016, 358 (362).
[706] *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 94.1a.
[707] *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 14.
[708] *Artikel-29-Datenschutzgruppe*, Leitlinien zum Recht auf Datenübertragbarkeit, WP 242 rev.01, S. 14.
[709] Vgl. *von Lewinski,* in: BeckOK DatenschutzR Art. 20 Rn. 62, 63; *Brüggemann*, K&R 2018, 1 (2).

der Übertragung, wie auch bei anderen Betroffenenrechten, eine sichere Identifikation der den Anspruch geltend machenden Person gewährleisten.[710] Das Recht auf Datenübermittlung findet folglich nach Art. 11 Abs. 2 DSGVO keine Anwendung, wenn eine Identifizierung nicht möglich ist.

2.5.1.2 Verbot automatisierter Entscheidungen im Einzelfall

Art. 22 DSGVO schützt betroffene Personen davor, nicht einer ausschließlich automatisierten Entscheidung, welche auf einer Verarbeitung ihrer personenbezogenen Daten beruht, ohne jegliches menschliche Eingreifen unterworfen zu werden. Darunter ist zu verstehen, dass ein lediglich algorithmenbasierter Datenverarbeitungsprozess, ohne Dazwischentreten eines Menschen einzelne, die Person betreffende persönliche Aspekte weder bewerten soll, noch, dass sich daraus rechtliche Wirkungen entfalten sollen oder andere Wirkungen, welche die betroffene Person erheblich beeinträchtigen können.[711] Art. 22 Abs. 1 DSGVO nennt zwei Alternativen: sofern diese Entscheidung gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Zunächst ist umstritten, ob im ersteren Fall auch eine erhebliche Beeinträchtigung vorliegen müsse, also das Verbot nur bei negativ wirkenden rechtlichen Wirkungen greift, oder ob jede rechtliche Wirkung erfasst ist, unabhängig von ihrer Einstufung als positiv oder negativ.[712] Die aktuell im Schrifttum vorherrschende Meinung, scheint eher zu letzterem zu tendieren.[713] EG 71 führt dazu exemplarisch die Beispiele der Ablehnung eines Online-Kreditvertrages oder Online-Einstellungsverfahrens auf.

Der Ausschluss der Verarbeitung soll nach Absatz 2 nicht gelten, wenn die Entscheidung

- für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,
- aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder
- mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.[714]

In jedem Fall sollte eine solche Verarbeitung mit angemessenen Garantien verbunden sein, einschließlich der spezifischen Unterrichtung der betroffenen Person und des Anspruchs auf direktes Eingreifen einer Person, auf Darlegung des eigenen Standpunkts, auf Erläuterung der nach einer entsprechenden Bewertung getroffenen Entscheidung sowie des Rechts auf Anfechtung der Entscheidung (EG 71 S. 4 DSGVO). In diesem Sinne regelt Art. 22 Abs. 3 DSGVO Pflichten des Verantwortlichen, sofern in den Fällen des Abs. 2 a) und c) automatisierte Einzelfallentscheidungen getroffen werden können. Art. 22 Abs. 4 DSGVO konkretisiert Art. 22 Abs. 2 DSGVO dahingehend, dass diese hier genannten Ausnahmen nicht auf Daten besonderer Kategorie im Sinne des Art. 9 Abs. 1 DSGVO Anwendung finden, sofern nicht besondere Umstände vorliegen.

Im BDSG finden sich die §§ 30, 31 und 37 BDSG, die konkretisierende Regelungen zu automatisierten Einzelfallentscheidungen bspw. bei Verbraucherkrediten und Profiling enthalten. Im Beschäftigtendatenschutz gibt

---

[710] *Brüggemann*, K&R 2018, 1 (2).
[711] *Brecht u. a.*, PinG 2018, 10 (12).
[712] *Brecht u. a.*, PinG 2018, 10 (13); *von Lewsinski,* in: BeckOK DatenschutzR Art. 22 Rn. 33.
[713] *Scholz,* in: NK Datenschutzrecht Art. 22 Rn. 32; *Helfrich,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 22 Rn. 48; *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 22 Rn. 26; *Hladjk,* in: Ehmann/Selmayr - DSGVO Art. 22 Rn. 9; a.A. sofern einem Begehren vollumfänglich stattgegeben wird: *Buchner,* in: Kühling/Buchner - DS-GVO/BDSG Art. 22 Rn. 25; *Schulz,* in: Gola DS-GVO, Art. 22 Rn. 22 ff. *Taeger,* in: Taeger/Gabel - DSGVO/BDSG Art. 22 Rn. 47.
[714] Zu beachten ist, dass es sich hierbei nicht um eine Rechtsgrundlage für die Datenverarbeitung selbst, sondern nur eine Verfahrensvorschrift handelt: *Schulz,* in: Gola DS-GVO, Art. 22 Rn. 3 ff. *Buchner,* in: Kühling/Buchner - DS-GVO/BDSG Art. 22 Rn. 11.

es keine spezielleren Regelungen. Da im Kontext der Unternehmenskommunikation weder für interne noch externe Kommunikation ein Sachverhalt ersichtlich ist, in dem eine automatisierte Einzelfallentscheidungen im Sinne des Art. 22 DSGVO getroffen wird, soll dieses Betroffenenrecht im Folgenden dieser Studie nicht weiter betrachtet werden. Insbesondere stellen sich bei den in Abschnitt 2.4.4.2.2.4 erwähnten State-of-the-Art-Angeboten eine solche Problematik nicht. Sollte ein Unternehmen dennoch eine automatisierte Entscheidungsfindung suchen, ist zu beachten, dass neben der Erfüllung der Anforderungen des Art. 22 DSGVO auch das Risiko der Datenverarbeitung für die Rechte und Freiheiten der Betroffenen steigt, sodass ggf. auch eine Datenschutz-Folgenabschätzung notwendig werden kann (vgl. Art. 35, EG 91 DSGVO, Abschnitt 2.4.4.5).

2.5.2 Anforderungen im Rahmen der Verteilung von Verantwortungssphären

Dieser Abschnitt widmet sich der konkreten Anforderungen im Hinblick auf die bereits eingeführten Konstellationen der gemeinsamen Verantwortung (Abschnitt 2.2.2) und der Auftragsverarbeitung (Abschnitt 2.2.3). Je nach konkreter Ausgestaltung der Kommunikationsinfrastruktur (Nutzung eines bestehenden Angebots, Betrieb On-Premise in Eigenregie, etc.) kann die Einbindung eines Kommunikationsdienstanbieters auf unterschiedliche Weise erfolgen:

- Verfolgen das dienstnutzende Unternehmen und der dienstanbietende Betreiber mit der Verarbeitung personenbezogener Daten eigene Zwecke, so wird regelmäßig eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DSGVO vorliegen.
- Unterliegt der dienstanbietende Betreiber hingegen den Weisungen des dienstnutzenden Unternehmens, kann eine Auftragsverarbeitung nach Art. 4 Nr. 8, 28 DSGVO vorliegen.
  - Wird ein System nach Vorstellungen des verantwortlichen Auftraggebers durch einen externen IT-Dienstleister erstellt bzw. betrieben, liegt i.d.R. ein Fall der Auftragsverarbeitung vor. Die Datenverarbeitung durch den Dienstleister muss auf die Erfüllung des Auftrags beschränkt sein.[715]
  - Wird ein bereits bestehender Dienst gewählt, ist abzugrenzen, ob eine Auftragsverarbeitung oder gemeinsame Verantwortung vorliegt: hierfür muss der Verantwortliche den/die vorgelegten Auftragsverarbeitungsverträge, Nutzungsbedingungen und Sicherheitsnachweise sowie die Datenschutzerklärung prüfen.[716]
- Betreibt das Unternehmen selbst den Kommunikationsdienst und der Dienstanbieter stellt lediglich Software bereit, ist das Unternehmen alleiniger Verantwortlicher. Den Softwarehersteller treffen keine unmittelbaren Pflichten aus dem Datenschutzrecht, es können sich aber vertragliche Pflichten ergeben, das verantwortliche Unternehmen bei der Umsetzung seiner Datenschutzpflichten zu unterstützen bzw. eine Technologie bereitzustellen, welche die Umsetzung der Datenschutzpflichten ermöglicht.[717]
  - Mit der Modernisierung des Kaufrechts anlässlich der Warenkauf-Richtlinie (WK-RL) wird der Mangelbegriff des § 434 BGB angepasst. Obwohl sich die WK-RL auf Verbraucherschutz bezieht, betrifft

[715] Vgl. zum vergleichbaren Fall der Videokonferenzsysteme: *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 6.
[716] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 7.
[717] siehe zum Streit über die Erstreckung auf Hersteller und Softwareproduzenten: *Baumgartner/Gausling*, ZD 2017, 308 (311); *Schuster/Hunzinger*, CR 2017, 141 (146); *Dümeland*, K&R 2019, 22 (24).

der Begriff des Sachmangels auch reine B2B-Konstellationen. Danach wird es künftig darauf ankommen, ob eine Sache[718] bei Gefahrübergang sowohl den subjektiven als auch objektiven Anforderungen sowie den Montageanforderungen entspricht.[719] Im Hinblick auf die subjektiven Anforderungen muss die Sache u.a. die vereinbarte Beschaffenheit haben und sich für die nach dem Vertrag vorausgesetzte Verwendung eignen, wobei zur Beschaffenheit auch Funktionalität, Kompatibilität und Interoperabilität zählen. Im Hinblick auf objektive Anforderungen, welche sich aus der gewöhnlichen Verwendung, Üblichkeit sowie berechtigten Erwartungen ableitet, sind u.a. Funktionalität, Kompatibilität und Sicherheit relevante Faktoren.[720]

- Die mit der Reform eingeführten Aktualisierungspflichten (§§ 475b f. BGB n.F.) sind allerdings auf Verbraucherverträge beschränkt. Hier können Unternehmen aber vereinbaren, dass diese nichtsdestotrotz Anwendung finden sollen.[721]

2.5.2.1 Herausforderungen der gemeinsamen Verantwortlichkeit

Bei der gemeinsamen Verantwortlichkeit müssen die zwei oder mehreren Verantwortlichen nach Art. 26 Abs. 1 S. 2 DSGVO in einer Vereinbarung in transparenter Form festlegen,

- wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Personen angeht, und
- wer welchen Informationspflichten nachkommt,

sofern und soweit die jeweiligen Aufgaben nicht bereits durch andere Vorschriften festgelegt sind. Diese Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln (Art. 26 Abs. 2 S. 1 DSGVO). Diese klare Zuteilung hat auch Folgen für die Haftung sowie Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden (vgl. EG 79). Die Vereinbarung hat keinen Einfluss darauf, ob eine gemeinsame Verantwortlichkeit anzunehmen ist: sie ist weder Voraussetzung noch kann sie eine solche begründen.[722] Die Detailtiefe der Aufgabenverteilung sollte in einem angemessenen Verhältnis zum Umfang der Verarbeitung sowie den damit für die betroffenen Personen verbundenen Risiken erfolgen.[723] Die Aufgaben sollten von der Stelle übernommen werden, welche am geeignetsten und effektivsten die Rechte und Pflichten umsetzen kann – die Aufgaben können dabei durchaus sehr ungleich verteilt sein.[724] Eine Pauschalübernahme sämtlicher Pflichten durch eine Stelle wird hingegen als nicht hinreichend transparent und konkret kritisiert.[725] Zudem muss das wesentliche der Vereinbarung der betroffenen Person zur Verfügung gestellt werden (Art. 26 Abs. 2 S. 2 DSGVO).

---

[718] Sachen sind gemäß § 90 BGB zwar nur körperliche Gegenstände, die Vorschriften über den Kauf von Sachen finden auf den Kauf von Rechten und sonstigen Gegenständen nach § 453 Abs. 1 BGB aber entsprechende Anwendung.

[719] Gesetz zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags, Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 37, ausgegeben zu Bonn am 30. Juni 2021.

[720] Grundsätzlich sollen subjektive und objektive Anforderungen gleichrangig zu berücksichtigen sein, zwischen Unternehmen seien aber abweichende ausdrückliche oder konkludente Vereinbarungen über die Beschaffenheit zulässig, die von den objektiven Anforderungen abweichen können: BT-Drs. 19/27424, S. 23.

[721] BT-Drs. 19/27424, S. 23.

[722] *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 26 Rn. 22; *Lang,* in: Taeger/Gabel - DSGVO/BDSG Art. 26 Rn. 27; *Piltz,* in: Gola DS-GVO, Art. 26 Rn. 10: „Ein ‚Outsourcing' an allein auf dem Papier Verantwortliche ist nicht möglich."

[723] *Lang,* in: Taeger/Gabel - DSGVO/BDSG Art. 26 Rn. 32.

[724] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 42.

[725] *DSK - Datenschutzkonferenz*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit; *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 54. Vgl. auch: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 42. Manche Anforderungen treffen alle Verantwortlichen und können nicht auf einen delegiert werden.

Art. 26 Abs. 1 DSGVO

[1]Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. [2]Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Art. 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. [3]In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

Hierbei werden die Informationspflichten besonders hervorgehoben sowie der Fakt, dass es aus Betroffenensicht sehr nützlich ist, eine Anlaufstelle für die Geltendmachung der Betroffenenrechte zu haben – selbst wenn diese ungeachtet dieser Vereinbarung ihre Rechte gemäß Art. 26 Abs. 3 DSGVO gegenüber jedem einzelnen der Verantwortlichen geltend machen kann.[726] Stellt die betroffene Person ein Auskunftsersuchen nach Art. 15 DSGVO an die Arbeitgeber, muss diese in der Lage sein, dies zu erfüllen, auch wenn die Daten durch den Messengerdienst verarbeitet werden.

Art. 26 Abs. 2 DSGVO

[1]Die Vereinbarung gemäß Absatz 1 muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln. [2]Das wesentliche der Vereinbarung wird der betroffenen Person zur Verfügung gestellt.

Pflichten der DSGVO	Aufgabenverteilung zwischen gemeinsam Verantwortlichen
Festlegung Zwecke und Mittel der Verarbeitung	Zentraler Startpunkt für die Annahme einer gemeinsamen Verantwortlichkeit ist die Verfolgung gemeinsamer Zwecke durch gemeinsam festgelegte Mittel. Ob dies der Fall ist, wurde bereits in Abschnitt 2.2.2 besprochen.
Rechtsgrundlagen, Umsetzung der Datenschutzgrundprinzipien	Bezüglich der Pflicht zur Umsetzung der Grundsätze aus Art. 5 DSGVO ist diese grundsätzlich nicht aufteilbar, sondern trifft alle Verantwortlichen gleichermaßen.[727] Fraglich ist, ob der Austausch von Daten zwischen den Verantwortlichen eine rechtfertigungsbedürftige Übermittlung darstellt.[728] Eine Privilegierung dürfte allerdings nicht bezweckt sein, sodass die Verantwortlichen für sämtliche Verarbeitungsschritte Rechtsgrundlagen vorweisen müssen.[729]
Informationspflichten	Bereitstellung der nach Art. 13 bzw. Art. 14 DSGVO erforderlichen Informationen gegenüber den betroffenen Personen

[726] *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 53.
[727] *Lang,* in: Taeger/Gabel - DSGVO/BDSG Art. 26 Rn. 31.; vgl. auch: *DSK - Datenschutzkonferenz*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit.
[728] *Piltz,* in: Gola DS-GVO, Art. 26 Rn. 8.
[729] *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 62; *Bertermann,* in: Ehmann/Selmayr - DSGVO Art. 26 Rn. 11; *Spoerr,* in: BeckOK DatenschutzR Art. 26 Rn. 23; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 42.

Dokumentationspflichten	Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO; ggf. Dokumentation von Einwilligungserklärungen
Datenschutzfreundliche Technikgestaltung, Datensicherheit und Datenschutz-Folgenabschätzung	Durchführung von Risikobeurteilungen, Umsetzung technischer und/oder organisatorischer Maßnahmen, Durchführung der DSFA
Umsetzung der Betroffenenrechte — Auskunftsrecht — Berichtigungsrecht — Recht auf Löschung — Recht auf Einschränkung der Verarbeitung — Widerspruchs-/Widerrufsrecht — Datenübertragbarkeit	Benennung eines/mehrerer Ansprechpartner für betroffene Personen. Nach Art. 26 Abs. 1 S. 3 DSGVO kann in der Vereinbarung zur gemeinsamen Verantwortlichkeit eine Anlaufstelle angegeben werden. Die betroffene Person kann ungeachtet dieser Vereinbarung ihre Rechte bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen (Art. 26 Abs. 3 DSGVO).
Meldepflichten	Meldung und Benachrichtigung bei Verletzung des Schutzes personenbezogener Daten (Art. 33 f. DSGVO)
Bei Auftragsverarbeitung:	Auswahl und Kontrolle eines Auftragsverarbeiters
Bei Drittstaatentransfers:	Umsetzung der Anforderungen nach Kapitel V DSGVO (siehe hierzu Abschnitt 4.2)

Tabelle 6 Überblick zur Aufgabenwahrnehmung bei gemeinsam Verantwortlichen

Hervorgehoben werden soll an dieser Stelle, dass auch ein Verstoß gegen Art. 26 DSGVO nach Art. 83 Abs. 4 Buchst. a DSGVO mit einem Bußgeld geahndet werden kann.[730] Zudem wären bei unzureichend konkretisierender Aufgabenzuweisung weitere Datenschutzverstöße zu befürchten, wenn die Verantwortlichen bestimmte Pflichten nicht oder nicht ausreichend umsetzen. Fraglich ist, welche Haftungsrisiken drohen, wenn einer der beteiligten Verantwortlichen seine zugewiesenen bzw. übernommenen Pflichten nicht erfüllt. Einerseits könnten mehrere Verantwortliche gesamtschuldnerisch haften, sodass sie nicht zur Entlastung auf den jeweils anderen nach der internen Verantwortungsverteilung verweisen können.[731] Andererseits könnte auch eine differenzierte Betrachtung angelegt werden, gerade wenn die Verantwortlichkeit nicht gleichwertig verteilt ist (bspw. ein Verantwortlicher hat keinen Zugang zu Daten), sodass eine wirksame Pflichtenverteilung auch gegenüber den Aufsichtsbehörden und potentiellen Sanktionen entlastend wirken würde.[732] Als Gegenargument kann ins Feld geführt werden, dass Verantwortliche die rechtskonforme Pflichtenumsetzung beim (Mit-)Verantwortlichen einfordern müssen.[733] Daher sollten ausdrückliche Regelungen über einen Ausgleich im Innenverhältnis in eine entsprechende Vereinbarung aufgenommen werden.

[730] *Piltz,* in: Gola DS-GVO, Art. 26 Rn. 28; *Spoerr,* in: BeckOK DatenschutzR Art. 26 Rn. 27.
[731] *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 26 Rn. 22; *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 64.
[732] Vgl. *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 26 Rn. 63 noch zur alten Rechtslage. Ähnlich wohl: *Jung/Hansch*, ZD 2019, 143 (144). Zur Störerauswahl: *Schwartmann/Burkhardt*, ZD 2021, 235 (237).
[733] Vgl. *DSK - Datenschutzkonferenz*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit, S. 2; siehe auch zur Kontrollmöglichkeit der Aufsichtsbehörden: *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 45.

2.5.2.2 Anforderungen bei einer Auftragsverarbeitung

Die Auftragsverarbeitung ist in Art. 28 und Art. 29 DSGVO geregelt. Eine Auftragsverarbeitung liegt vor, wenn die Datenverarbeitung auf Weisung des Verantwortlichen erfolgt, was allerdings nicht unter dessen direkter Autorität oder Kontrolle meint.[734] Es bedeutet aber, dass der Auftragsverarbeiter in fremdem Interesse tätig wird. Die Rechtsgrundlage der Datenverarbeitung durch den Auftragsverarbeiter folgt aus der Beziehung des Verantwortlichen zur betroffenen Person, sofern der Auftragsverarbeiter die Daten nicht anders als auf Anweisung des für die Verarbeitung Verantwortlichen verarbeitet.[735]

> **Art. 28 Abs. 1 DSGVO**
>
> Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Art. 28 Abs. 1 DSGVO richtet sich zunächst an den Verantwortlichen, der dazu verpflichtet wird, nur mit „geeigneten“ Auftragsverarbeitern zu arbeiten. Somit normiert Art. 28 Abs. 1 DSGVO vor allem die Anforderungen, die der Verantwortliche an seine Auftragsverarbeiter zu stellen hat.[736] Demnach hat der Verantwortliche nicht nur eine Sorgfaltspflicht hinsichtlich der Auswahl eines geeigneten Auftragsverarbeiters, sondern muss auch während der Verarbeitung überprüfen, dass der Auftragsverarbeiter in DSGVO-konformer Weise die Verarbeitung durchführt.[737] Als hinreichen Garantien für die Einhaltung der Abs. 1 und Abs. 4 können laut Art. 28 Abs. 5 die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSVO oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO als Faktor herangezogen werden.

Eine Auftragsverarbeitung wird dann verneint, wenn der Auftragsverarbeiter sich eigene Wertungs- und Entscheidungsspielräume einräumt und seine Tätigkeit über reine Hilfsfunktionen für die Erfüllung der Zwecke des Auftraggebers hinausgeht.[738] Selbst bei einer Beauftragung einer externen Stelle soll keine Auftragsverarbeitung im datenschutzrechtlichen Sinne vorliegen, wenn diese eigenständig und ohne Vorgaben über technische und organisatorische Mittel der Datenverarbeitung entscheiden kann.[739] Auf die Rechtsnatur der Betrauung des Auftragsverarbeiters nach Zivilrecht kommt es dabei nicht an.[740] Ob eine Stelle eine Doppelfunktion als Verantwortlicher und Auftragsverarbeiter einnehmen kann, hängt davon ab, ob es sich um einen einheitlichen Vorgang handelt oder ob sich der Vorgang in verschiedene, rechtlich selbständig bewertbare Teile zerlegen lässt.[741] Die Entscheidung über den Verarbeitungszweck impliziert stets die datenschutzrechtliche Verantwortlichkeit.[742]

Auftragsverarbeitungsvertrag (AV-Vertrag): Art. 28 Abs. 3 DSGVO verpflichtet zum Abschluss eins AV-

[734] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 24.
[735] *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, S. 24; *Felber*, ZD 2018, 382 (385).
[736] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 27 ff.
[737] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 41; vgl. auch *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 7.
[738] BGH, Urteil vom 13.7.2016 – IV ZR 292/14, Rn. 39; VGH München, Beschluss vom 26.09.2018 – 5 CS 18.1157, Rn. 16; VG Bayreuth, Beschluss vom 8.5.2018 – B 1 S 18.105, Rn. 48. Zur Übertragbarkeit auf die DSGVO: *Felber*, ZD 2018, 382 (386).
[739] VGH München, Beschluss vom 26.09.2018 – 5 CS 18.1157, Rn. 16.
[740] BGH, Urteil vom 13.7.2016 – IV ZR 292/14, Rn. 39; VG Bayreuth, Beschluss vom 8.5.2018 – B 1 S 18.105, Rn. 48.
[741] VG Bayreuth, Beschluss vom 8.5.2018 – B 1 S 18.105, Rn. 49.
[742] Vgl. EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 68; EuGH, Urteil vom 29.07.2019 – C-40/17 – Fashion ID, Rn. 68; *Felber*, ZD 2018, 382 (386).

Vertrags. Zu diesen inhaltlichen Mindestanforderungen gehören:

- Festlegung von Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen;
- eine Verpflichtung des Auftragsverarbeiters nur auf dokumentierte Weisungen des Verantwortlichen personenbezogene Daten zu verarbeiten (Buchst. a),
- eine Verschwiegenheitsklausel (Buchst. b),
- die Verpflichtung alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen zur Datensicherheit ergreifen (Buchst. c),
- die Einhaltung der Regelungen zur Subbeauftragung weiterer Unterauftragnehmer (Buchst. d),
- die Unterstützungspflicht bei Anträgen zur Geltendmachung von Betroffenenrechten durch geeignete TOM (Buchst. e),
- die Unterstützungspflicht zur Einhaltung der Art. 32- 36 DSGVO[743] (Buchst. f),
- zur Lösch- bzw. Rückgabepflicht (Buchst. g) und
- zum Nachweis der Einhaltung der Verpflichtungen aus Art. 28 DSGVO (Buchst. h).

Zusätzlich normiert Art. 28 Abs. 3 S.3 DSGVO eine Hinweispflicht des Auftragsverarbeiters gegenüber dem Verantwortlichen, sofern er der Auffassung ist, dass eine Weisung des Verantwortlichen gegen Datenschutzbestimmung verstößt.

Unterbeauftragung: Art. 28 Abs. 2 DSGVO regelt, in welcher Form Auftragsverarbeiter Unteraufträge erteilen dürfen. Grundsätzlich können Berechtigungen zur Unterbeauftragung im AV-Vertrag geregelt werden. Eine vorherige Genehmigung des Unterauftrags ist jedoch laut Art. 28 Abs. 2 DSGVO erforderlich.[744] Das weitere Vorgehen sowie die Haftung für Unterauftragsnehmer regelt Art. 28 Abs. 4 DSGVO.

Unterstützung des Verantwortlichen: Art. 28 Abs. 3 DSGVO verpflichtet die Auftragsverarbeiter dazu, Verantwortliche bei der Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Personen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Mittel zu unterstützen.[745] Unterstützungspflichten des Auftragsverarbeiters sind in den Art. 32 bis 36 DSGVO teilweise bereits normiert. Durch die Regelung wird sichergestellt, dass diese Pflichten auch vertraglich mit geregelt werden.[746] Diese vertraglichen Pflichten können über die gesetzlichen hinausgehen.[747] Sie sind allerdings nicht abdingbar. Im Hinblick auf die erforderlichen TOMs zur Gewährleistung der Datensicherheit muss geklärt werden, wer die Risikobewertung durchführt. Die Verantwortlichkeit für die Risikobewertung könnte beispielsweise Teil der vertraglichen Regelung sein, die Art. 28 Abs. 3 Buchst. f DSGVO vorsieht.[748] Damit Verantwortliche ihren Informations- und Auskunftspflichten nachkommen können, könnten sie Informationen

[743] Art. 32 bis 36 DSGVO verpflichten den Verantwortlichen, für eine angemessene Sicherheit der Verarbeitung zu sorgen (Art. 32), ggf. etwaige Datenschutzverletzungen an die Aufsichtsbehörde zu melden (Art. 33) bzw. betroffene Personen von solchen Verletzungen zu benachrichtigen (Art. 34), vor risikoträchtigen Verarbeitungen eine Datenschutz-Folgeabschätzung durchzuführen (Art. 35) und schließlich in bestimmten Zweifelfragen die Aufsichtsbehörde zu konsultieren (Art. 36).
[744] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 42.
[745] Eine ausführliche Übersicht über die Pflichten des Auftragsverarbeiters ist zu finden in: *Laue u. a.*, Das neue Datenschutzrecht in der betrieblichen Praxis, Kap. 5 Rn. 8.
[746] Vgl. *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 28 Rn. 75; *Klug,* in: Gola DS-GVO, Art. 28 Rn. 7.
[747] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 72.
[748] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 73; *Witt,* in: Koreng/Lachenmann - Formularhandbuch Datenschutzrecht, Kap. 6 Maßnahmenübersicht und deren risikobasierte Bewertung bei der Auftragsverarbeitung Rn 1-4 bietet eine Übersicht über vertraglich regelbare Maßnahme zur Sicherung der Datenverarbeitung.

vom Auftragsverarbeiter benötigen. Auch das Löschen, Berichtigen, Beschränken oder Übertragen muss durch den Auftragsverarbeiter technisch unterstützt werden, da der Verantwortliche ggfs. keinen Zugriff auf die Daten oder die entsprechenden Systeme hat, sofern die Daten beim Auftragsverarbeiter gespeichert werden.[749] Die Unterstützungspflicht muss technisch machbar sein und in das Aufgabenspektrum des Auftragverarbeiters fallen.[750] Bei hohem Aufwand käme eine Vergütungsregelung je nach Aufwand in Betracht.[751]

Form: In Art. 28 Abs. 6-8 DSGVO ist die Verwendung von Standardvertragsklauseln geregelt. Art. 28 Abs. 9 DSGVO schreibt die Schriftform sowohl für den Auftragsvertrag als auch für mögliche Unteraufträge vor, wobei hierunter auch ein elektronisches Format fällt.[752]

Folgen: Art. 29 DSGVO unterstreicht, dass der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten dürfen, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind. Art. 28 Abs. 10 DSGVO stellt klar, dass ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher gilt.

DSK, Orientierungshilfe Videokonferenzsysteme

Da die AV-Verträge in der Praxis häufig auf Musterverträgen der Dienstleister beruhen, sollte besonders darauf geachtet werden, dass

- die Weisungsgebundenheit des Auftragsverarbeiters umfassend geregelt wird und
- dem Verantwortlichen hinreichend Kontrollbefugnisse eingeräumt werden.

Verarbeitet der Dienstanbieter personenbezogene Daten der Betroffenen auch zu eigenen Zwecken oder Zwecken Dritter (z. B. Verarbeitung von Daten zum Nutzerverhalten, Einsatz von Analysetools, Tracking zu Werbezwecken), liegt keine Auftragsverarbeitung vor

2.5.3 Zwischenergebnis und Bedeutung für die Messengerdienstnutzung im Unternehmenskontext

Betreibt ein Unternehmen ein Kommunikationsnetzwerk nicht selbst „On Premise“, so sind unterschiedliche Verantwortungsverteilungen denkbar. Es müssen unterschiedliche Vereinbarungen getroffen werden – je

[749] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 70.
[750] *Petri,* in: NK Datenschutzrecht Art. 28 Rn. 70.
[751] *Bertemann,* in: Ehmann/Selmayr - DSGVO Art. 28 Rn. 27.
[752] Die Weisungen, auch mündliche, müssen dokumentiert sein und im Rahmen des Vertrags oder Rechtsinstruments konkret geregelt werden. Die Dokumentation der Weisungen kann in Textform im Sinne des 126b BGB oder in einem anderen elektronischen Verfahren, dass ein Mindestmaß an Manipulationsschutz aufbietet, erfolgen: *Bertemann,* in: Ehmann/Selmayr - DSGVO Art. 28 Rn. 3; *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 28 Rn. 99.

nachdem ob es sich um eine gemeinsame Verantwortung oder eine Auftragsverarbeitung handelt. Grundsätzlich gibt es zusätzlich Gestaltungsmöglichkeiten, dass eine Stelle eine Doppelfunktion einnimmt und nebeneinander zugleich Auftragsverarbeiter und verantwortliche Stelle ist.[753] So können die Beteiligten in unterschiedlichen Phasen einer Datenverarbeitung grundsätzlich mit unterschiedlichen Verantwortungsbeiträgen beteiligt sein. Eine solche Mischform könnte allerdings nicht triviale Herausforderungen bei der Informationsbereitstellung hervorrufen, da im Fall der gemeinsamen Verantwortung die Transparenz gegenüber der betroffenen Person sichergestellt werden muss, indem ihr die wesentlichen Aspekte der Vereinbarung über die Pflichtenverteilung zugänglich gemacht werden. Auch im Hinblick auf mögliche Haftungsfolgen sollte eindeutig festgestellt werden, in welcher Rolle die Stellen an einer Verarbeitung personenbezogener Daten beteiligt sind und welche Pflichten daraus resultieren.

2.6 Rechtsfolgen bei Verstößen

Werden Aufsichtsbehörden Verstöße gegen die Datenschutzvorgaben bekannt, gewährt ihnen Art. 58 DSGVO unterschiedliche Befugnisse beispielsweise zur Ergreifung von Maßnahmen, die Abhilfe schaffen sollen, als auch eine Geldbuße gemäß Art. 83 DSGVO zu verhängen (Art. 58 Abs. 2 Buchst. i DSGVO). Hierbei muss der Schadensersatzanspruch aus Art. 82 DSGVO von den Geldbußen durch die Behörden nach Art. 83 DSGVO unterschieden werden.

Seit der Corona-Pandemie werden zunehmend Kollaborationsdienste wie Microsoft Teams und Zoom verwendet. Die datenschutzrechtlichen Bedenken, die bei deren Einsatz immer wieder diskutiert werden, richten sich insbesondere auf den Verkehr der Daten außerhalb der EU (insbesondere in die USA, siehe Abschnitt 4.2.1.2). Die Aufsichtsbehörden haben hier zeitweise signalisiert, dass die Verwendung dieser Kollaborationstools keine Maßnahmen oder Sanktionen nach sich ziehen könnte. Diese Auffassung hat sich jedoch mittlerweile dahingehend geändert, dass die Behörden sehr wohl mit Abklingen der Pandemie eine Nutzung von datenschutzkonformen Kollaborationstools erwarten und hier verstärkt drauf achten wollen.[754]

Geldbußen: Allgemeine Bedingungen für das Verhängen von Bußgeldern sind in Art. 83 Abs. 1-3 DSGVO geregelt: Sanktionen sind im Einzelfall so zu bemessen, dass sie wirksam, verhältnismäßig und abschreckend sind. Sie können parallel zu anderen Maßnahmen verhängt werden. Obergrenze des Gesamtbetrags soll bei Verstößen gegen mehrere Bestimmungen durch gleiche bzw. miteinander verbundene Verarbeitungsvorgänge (Tateinheit) die Sanktion für den schwerwiegendsten Verstoß sein. Die Höhe der möglichen Sanktionen hängen dabei von der Art des Verstoßes sowie der Norm gegen welche verstoßen wurde ab (vgl. Tabelle 7).[755]

Norm	Höhe	Verstoß gegen
Art. 83 Abs. 4 DSGVO	bis zu 10.000.000 € oder 2 % des Umsatzes	Art. 8, 11, 25 bis 39, 42 und 43 für Verantwortliche und Auftragsverarbeiter

[753] Vgl. VG Bayreuth, Beschluss vom 08.05.2018 – B 1 S 18.105 –, Rn. 51.
[754] vgl. Kugelmann, Dieter: *Gesundheitsnot kennt Datenschutzgebot, VerfBlog*, 2020/3/26, https://verfassungsblog.de/gesundheitsnot-kennt-datenschutzgebot/, DOI: 10.17176/20200327-005643-0.
[755] Für eine vollständige Übersicht inkl. Straftatbestände und Folgen siehe: https://www.datenschutz.org/dsgvo-bussgeld/#bkat [letzter Abruf 28.07.2021].

Art. 83 Abs. 5 DSGVO	bis zu 20.000.000 € oder 4 % des Umsatzes	Grundsätze gemäß Art. 5, 6, 7 und 9 Betroffenenrechte nach Art. 12 bis 22 Drittlandübermittlung nach Art. 44 bis 49 Pflichten nach Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden Nichtbefolgung Anweisungen Aufsichtbehörde
Art. 83 Abs. 6 DSGVO	bis zu 20.000.000 € oder 4 % des Umsatzes	Nichtbefolgung einer Anweisung einer Aufsichtsbehörde gemäß Art. 58 Abs. 2 DSGVO

Tabelle 7 Sanktionsstufen

Gegen den größten Messengerdienst WhatsApp verhängte die irische Datenschutzbehörde ein Bußgeld in Höhe von 225 Millionen €.[756] Aktuell handelt es sich um die höchste von dieser Behörde verhängte Strafe. Begründet wird das Bußgeld mit der Nichteinhaltung von Transparenzpflichten.

Wegen der unzulässigen Überwachung und Ausspähung von Beschäftigten wurden bereits Bußgelder in Höhe von 10 bzw. 35 Millionen € gegen notebooksbiller.de und H&M verhängt.[757] In Spanien sah sich Vodafone diversen Geldbußen ausgesetzt, u.a. durch Auftragsverarbeiter begangene Fehler, welche aber dem Unternehmen als Pflichtverletzung in seiner Funktion als Verantwortlicher im Hinblick auf Kontroll- und Überwachungspflichten angelastet wurden.[758] Nach mehrfach wiederholten Verstößen wurden 8 Millionen € Bußgeld verhängt.[759] Bei einer Inspektion stellte die Aufsichtsbehörde fest, dass sowohl eine kontinuierliche Überwachung der Auftragsverarbeiter sowie technische / organisatorische Maßnahmen zur Durchführung des Auftrags fehlten, als auch eine internationale Datenübermittlung nach Peru stattfand, sodass Verstöße gegen Art. 28 und 44 DSGVO sanktioniert wurden. Mit unabhängig betriebenen Informationsportalen wie dem GDPR Enforcement Tracker[760], dem DSGVO-Portal[761] oder dem Projekt29[762] werden aktuelle Sanktionen EU-weit veröffentlicht.

Schadensersatz: Die Schadensersatzansprüche werden in Art. 82 DSGVO konkretisiert:

— Anspruchsberechtigt ist *jede* Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist (Abs. 1). Umstritten ist, ob dies auf betroffene Personen

[756] *Koch,* WhatsApp von irischer Datenschutzbehörde zu 225 Millionen Euro Strafe verurteilt, in: heise online, Stand 02.09.2021, https://www.heise.de/news/WhatsApp-von-irischer-Datenschutzbehoerde-zu-225-Millionen-Euro-Strafe-verurteilt-6180500.html [letzter Abruf 03.09.2021].

[757] *Neuerer/Kolf,* Mitarbeiter ausgespäht: Datenschutzbeauftragter verhängt Rekord-Bußgeld gegen H&M, 01.10.2020 in: Handelsblatt, https://www.handelsblatt.com/unternehmen/handel-konsumgueter/modehaendler-mitarbeiter-ausgespaeht-datenschutzbeauftragter-verhaengt-rekord-bussgeld-gegen-hundm/26234570.html; Kolf, Datenschützer verhängen Millionen-Buße gegen Notebooksbilliger, 08.01.2021, in: Handelsblatt, https://www.handelsblatt.com/unternehmen/handel-konsumgueter/videoueberwachung-datenschuetzer-verhaengen-millionen-busse-gegen-notebooksbilliger/26778902.html [letzter Zugriff 29.07.2021].

[758] AEPD – Agencia Española Protección Datos, abrufbar unter: https://www.aepd.es/es/documento/ps-00030-2021.pdf [letzter Zugriff 13.08.2021].

[759] EDPB, Spanish DPA Fines Vodafone Spain more than 8 Million Euros, Stand 31.03.2021, abrufbar unter: https://edpb.europa.eu/news/national-news/2021/spanish-dpa-fines-vodafone-spain-more-8-million-euros_en [letzter Zugriff 13.08.2021].

[760] https://www.enforcementtracker.com/, betrieben durch die CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB.

[761] https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php, betrieben durch die Compliance Essentials GmbH.

[762] https://www.projekt29.de/, Projekt 29 GmbH & Co. KG.

i.S.d. Art. 4 Nr. 1 DSGVO[763] oder natürliche Personen[764] beschränkt ist. In der Praxis dürften Schäden ohnehin zumeist bei der betroffenen Person entstehen.

- Anspruchsgegner sind Verantwortlicher oder Auftragsverarbeiter:
  - Jeder beteiligte Verantwortliche haftet für durch Verstöße verursachte Schäden (Abs. 2 S. 1)
  - Auftragsverarbeiter haften nur für Verletzung der ihnen speziell auferlegten Pflichten / Anweisungen der Verantwortlichen (Abs. 2 S. 2)
- Die Beweislast zum Nachweis eines fehlenden Verschuldens trägt der Verantwortliche / Auftragsverarbeiter (Abs. 3)
- Bei mehreren Verantwortlichen / Auftragsverarbeitern liegt eine gesamtschuldnerische Haftung vor (Abs. 4). Abs. 5 DSGVO regelt insoweit die Möglichkeit des Rückgriffsanspruchs der weiteren Haftungsschuldner, wenn einer für den gesamten Schaden aufgekommen ist.[765]

Für den Fall der Messengerdienstnutzung bedeutet dies, dass je nach Konstellation entweder das Unternehmen, das den Messengerdienst verwendet, oder der Dienstanbieter zur anteiligen Schadensersatzzahlungen herangezogen werden könnten.

Daneben können Ansprüche auf Unterlassung und Schadensersatz aus Verstoß gegen arbeitsvertragliche Pflichten gegenüber den Beschäftigten sowie aus dem Deliktsrecht wegen Verletzung des Persönlichkeitsrechts treten (§§ 823 Abs. 1, 1004 BGB).[766]

Strafbarkeit: Datenschutzverletzungen können zudem zu Strafverfahren führen (vgl. § 42 BDSG).[767] Schwere Verstöße können laut § 42 BDSG als Antragsdelikte strafrechtlich verfolgt werden. Hierzu zählt beispielweise die unberechtigte, wissentliche Weitergabe von personenbezogenen Daten einer großen Anzahl von Personen an Dritte.

Haftung der Leitungsorgane: Haftet das Unternehmen als juristische Person für Datenschutzverstöße, können unter Umständen auch die innerhalb des Unternehmens verantwortlichen Personen für das fahrlässige oder vorsätzliche Unterlassen von Aufsichtsmaßnahmen mit ihrem Privatvermögen haften (vgl. §§ 130, 9 OWiG).[768] Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen (§ 130 Abs. 1 S. 2 OWiG).

Sonstige Folgekosten: Entsprechende Geldbußen können darüber hinaus Folgekosten verursachen: Neben der kurzfristigen Einholung von kostenintensiven Datenschutz- und ggf. PR-Strategien, kann die Eintragung in das Gewerbezentralregister gemäß § 149 Abs. 2 Nr. 3 und 4 GewO Einfluss auf die Kreditwürdigkeit des Betriebs haben.[769]

[763] So: *Gola/Piltz,* in: Gola DS-GVO, Art. 82 Rn. 10.
[764] So: *Bergt,* in: Kühling/Buchner - DS-GVO/BDSG Art. 82 Rn. 13; *Moos/Schefzig,* in: Taeger/Gabel - DSGVO/BDSG Art. 82 Rn. 17.
[765] Zur Haftung als Gesamtschuldner: *Gola/Piltz,* in: Gola DS-GVO, Art. 82 Rn. 6 ff.
[766] BAG, Urteil vom 12. 9. 2006 - 9 AZR 271/06, Rn. 21.
[767] *Lurtz*, ZD-Aktuell 2021, 05269.
[768] *Faas*, ArbRAktuell 2018, 594 (595).
[769] *Lurtz*, ZD-Aktuell 2021, 05269.

3 Besonderheiten der elektronischen Kommunikation

Der Bereich der elektronischen Kommunikation wird von der ePrivacy-Richtlinie erfasst, diese bedarf allerdings der Umsetzung in mitgliedstaatliches Recht. Im Frühjahr 2021 wurden diese Umsetzungsrechtsakte im TTDSG und TKModG novelliert. Damit wurden die bisherigen datenschutzrechtlichen Regelungen in TKG a.F. und TMG a.F. in einem gemeinsamen Gesetz zusammengeführt. Teil 2 des TTDSG widmet sich der Telekommunikation, während Teil 3 eher Telemedien adressiert. Allerdings wird es sich dabei voraussichtlich nur um eine Zwischenlösung handeln, da der Plan einer unmittelbar geltenden ePrivacy-Verordnung noch nicht aufgegeben wurde.

3.1 Ursprüngliche Zielsetzung einer ePrivacy-Verordnung

Bislang war der Versuch, eine ePrivacy-VO für den Bereich der elektronischen Kommunikation zu schaffen, nicht von Erfolg gekrönt. Das Verfahren ist ins Stocken geraten und ein Abschluss nicht ersichtlich.[770] Selbst bei Vollendung dieses Reformvorhabens, wäre mit einer Übergangsfrist zu rechnen.

3.2 Novellierung des telekommunikations- und telemedienrechtlichen Datenschutzes

Zum 01.12.2021 tritt das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) in Kraft. Mit diesem Gesetz werden Teile des Telekommunikationsgesetzes (§§ 88-107 TKG), welche den Datenschutz und den Schutz des Fernmeldegeheimnisses in der Telekommunikation regelten, und das Telemediengesetz (§§ 11-15a TMG), deren Regelugen im Online-Bereich durch die DSGVO überlagert wurden,[771] in ein neues Stammgesetz überführt. Notwendig wurde dieser Schritt durch das Scheitern, parallel zur DSGVO den Telekommunikations- und Telemedienbereich ebenfalls im Rahmen einer Verordnung auf EU-Ebene zu harmonisieren (ePrivacy-VO). Folglich gilt neben der DSGVO die ePrivacy-RL 2002/58/EG[772] sowie das in Umsetzung dieser Richtlinie ergangene mitgliedstaatliche Recht weiter (vgl. Art. 95 DSGVO). Diese wurde allerdings gerade mit Blick auf die Cookie-Regelung (Art. 5 Abs. 3 ePrivacy-RL) nie umfassend im deutschen Recht umgesetzt, weshalb die deutschen Aufsichtsbehörden nach Inkrafttreten der DSGVO die Nichtanwendbarkeit des TMG annahmen.[773] Über das TTDSG soll die so entstandene Rechtsunsicherheit beseitigt werden und die Rechtslage an die aktuelle Rechtsprechung des EuGH angepasst werden.[774]

---

[770] Vgl. *Assion*, Stellungnahme als Sachverständiger zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG), BT-Drucksache 19/27441, Ausschussdrucksache 19(9)1039, S. 3; *Richter*, Stellungnahmen vom 20.04.2021, Ausschussdrucksache 19(9)1045, S. 2.

[771] *DSK - Datenschutzkonferenz*, Positionsbestimmung: Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, S. 2; *Jandt*, ZD 2018, 405 (407); a.A. *Gierschmann*, ZD 2018, 297 (299); *Breyer*, ZD 2018, 302 (303).

[772] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Amtsblatt Nr. L 201 vom 31/07/2002 S. 0037 – 0047.

[773] *DSK - Datenschutzkonferenz*, Positionsbestimmung: Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, S. 2.

[774] BT-Drs. 19/27441, S. 1, 30.

3.2.1 Sachliche und räumliche Anwendbarkeit des TTDSG

Relevanz entfalten die Regelungen des TTDSG im vorliegend betrachteten Kontext der Kommunikation im Unternehmen allerdings nur, wenn sie anwendbar sind. Die Frage der Anwendbarkeit stellt sich dabei sowohl aus der Perspektive eines Anbieters elektronischer Kommunikationsdienste als auch aus Perspektive des Unternehmens, welche elektronische Kommunikation im Unternehmen einsetzen will. Dafür bedarf es zunächst eines eindeutigen Verständnisses der „elektronischen Kommunikation“ sowie einer Klärung des Verhältnisses zur DSGVO.

3.2.1.1 Spezialregelungen für Telemedien und die Telekommunikation

Grundsätzlich geht der Gesetzgeber davon aus, dass nach der ePrivacy-Richtlinie auch im Bereich der elektronischen Kommunikation zunächst die DSGVO gilt.[775] § 1 TTDSG benennt zum Anwendungsbereich des neuen Gesetzes folgende Regelungskomplexe:

- Fernmeldegeheimnis, Abhörverbot und Geheimhaltungspflicht von Funkanlagenbetreibern,
- besondere Datenschutzvorschriften bei Telekommunikationsdienst- und Telemediennutzung,
- Privatsphärenschutz bei Mitteilung ankommender Verbindungen, Rufnummernunterdrückung und -anzeige und automatischer Anrufweiterschaltung,
- Aufnahme in Endnutzerverzeichnisse und Auskunftsdienste, Dienste zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers und Anbieter von Endnutzerverzeichnissen,
- von Telemedienanbietern zu beachtende technische und organisatorische Vorkehrungen,
- Auskunftserteilung über Bestands- und Nutzungsdaten durch Telemedienanbieter,
- Speicherung von und Zugriff auf Informationen in Endeinrichtungen der Endnutzenden (Cookies), und
- Aufsichtsbehörden und die Aufsicht.

Eine der wichtigsten Regelungen zum Anwendungsbereich findet sich in § 1 Abs. 1 Nr. 2 TTDSG, wonach dieses Gesetz besondere Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und Telemedien regelt. Die Begriffe „Telekommunikation“ und „Telemedien“ werden im Gesetz nicht selbst definiert. Insofern wird man auf die bisherigen Definitionen des TKG und TMG zurückgreifen müssen.

3.2.1.1.1 Telekommunikation

Neben dem TTDSG wird auch das TKG durch das Telekommunikationsmodernisierungsgesetz (TKMoG) überarbeitet.[776] Im Folgenden werden alte und neue Fassung vergleichend nebeneinandergestellt.

[775] BT-Drs. 19/27441, S. 33.
[776] BT-Drs. 19/26108, BT-Drs. 19/26964, BT-Drs. 19/28865.

Telekommunikation § 3 Nr. 22 TKG a.F.	Telekommunikation § 3 Nr. 59 TKG n.F.
der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen	der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen
Telekommunikationsanlage § 3 Nr. 23 TKG a.F.	**Telekommunikationsanlage § 3 Nr. 60 TKG n.F.**
technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können	technische Einrichtungen, Systeme oder Server, die als Nachrichten identifizierbare elektromagnetische oder optische Signale oder Daten im Rahmen der Erbringung eines Telekommunikationsdienstes senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können
Telekommunikationsdienste § 3 Nr. 24 TKG a.F.	**Telekommunikationsdienste § 3 Nr. 61 TKG n.F.**
in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen	in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen: a) Internetzugangsdienste b) Interpersonelle Telekommunikationsdienste und c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden
Dienstanbieter § 3 Nr. 6 TKG a.F.	**Anbieter von TK-diensten § 3 Nr. 1 TKG n.F.**
jeder, der ganz oder teilweise geschäftsmäßig a) Telekommunikationsdienste erbringt oder b) an der Erbringung solcher Dienste mitwirkt	jeder, der Telekommunikationsdienste erbringt;
	Neu: Interpersoneller Telekommunikationsdienst § 3 Nr. 24 TKG n.F.
	ein gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Telekommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen;

Tabelle 8 Synopse relevanter Definitionen das alten und neuen TKG

Die Definition des Telekommunikationsdienstes wurde in Umsetzung von Art. 2 Nr. 4 Richtlinie (EU) 2018/1972 grundlegend überarbeitet und orientiert sich nun verstärkt an einem funktionalen Ansatz und weniger der technischen Ausrichtung.[777] Die Ergänzung bei der Telekommunikationsanlage dient der Klarstellung zur Technologieneutralität, d.h. dass sämtliche technischen Einrichtungen, Systeme oder Server, die im Rahmen der Erbringung von Telekommunikationsdiensten eingesetzt werden, erfasst sind.[778] Der Telekommunikationsdienst wurde überarbeitet, um auch Online-Dienste, wie Internet-Telefonie, Messengerdienste und web-gestützte E-Mail-Dienste einzuschließen, die aus Sicht der Funktionalität gleichwertig zu klassischen Sprachtelefon-, Textmitteilungs- und E-Mail-Übertragungsdiensten sind (vgl. Erwägungsgrund 15 Richtlinie (EU) 2018/1972).[779] Aus Sicht des Gesetzgebers ist es für Endnutzer*innen nicht bedeutsam, ob der Anbieter selbst die Signalübertragung vornimmt oder ob die Kommunikation über einen Internetzugangsdienst übermittelt wird.[780]

Entgeltlichkeit liegt nicht nur bei einer direkten Zahlungspflicht vor, sondern ist auch dann gegeben, wenn eine andere wirtschaftliche Gegenleistung durch den Nutzenden oder Dritte den Dienst indirekt (mit-)finanziert, wie bspw. bei werbefinanzierten Angeboten.[781] Der EuGH hat die Entgeltlichkeit werbefinanzierter Dienste der Informationsgesellschaft mit der Begründung bestätigt, dass die Bezahlung nicht von der Person stammen muss, die den Dienst nutzt.[782] Andere Gerichte differenzierten zwischen der Zahlung eines Entgelts durch Dritte und der Preisgabe personenbezogener Daten als „Gegenleistung".[783] Auch die Gesetzesbegründung zum TKMoG verweist auf datenbasierte und werbefinanzierte Refinanzierungsmodelle als „Entgelt".[784]

Eine Übertragung von Signalen liegt nicht bei reinen Inhaltsdiensten wie bspw. Webseiten vor, diese können aber als Telemedien eingeordnet werden.[785] Die exakte Abgrenzung machte mitunter eine detaillierte Betrachtung der einzelnen Kommunikationsschichten erforderlich, wofür oftmals das sog. ISO/OSI-Referenzmodell herangezogen wurde.[786]

3.2.1.1.2 Telemedien

Eine inhaltliche Beschreibung der Telemedien findet sich nicht im Rahmen der Begriffsbestimmungen des TMG. Vielmehr werden Telemedien in § 1 Abs. 1 S. 1 TMG zum Anwendungsbereich in negativ abgrenzender Weise u.a. zum Telekommunikationsdienst legaldefiniert.

§ 1 Abs. 1 S. 1 TMG

Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikations-

[777] BT-Drs. 19/26108, S. 201.
[778] BT-Drs. 19/26108, S. 236.
[779] BT-Drs. 19/26108, S. 236.
[780] BT-Drs. 19/26108, S. 236.
[781] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 3 TKG Rn. 13; *Lünenbürger/Stamm,* in: Scheurle/Mayen - TKG, § 3 Rn. 63.
[782] EuGH, Urteil vom 11.9.2014 - C-291/13 – Papasavvas, Rn. 28 ff.
[783] OVG NRW, Vorlagebeschluss vom 26.2.2018 – 13 A 17/16, Rn. 19 f.
[784] BT-Drs. 19/26108, S. 237.
[785] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 3 TKG Rn. 15.
[786] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 3 TKG Rn. 16.

> dienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien).

Mit der Novelle des TKG, TTDSG und TMG werden die Worte „§ 3 Nr. 24 TKG, die *ganz* in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG“ durch die Wörter „§ 3 Nr. 61 TKG, telekommunikationsgestützte Dienste nach § 3 Nr. 63 TKG“ ersetzt.[787] Es bleibt somit bei der negativen Abgrenzung. Telemedien und Telekommunikationsdienste umfassen folglich elektronische Informations- und Kommunikationsdienste. Dienste, die bereits unter die Definition des Telekommunikationsdienstes fielen, konnten nach der alten Rechtslage gleichzeitig Telemedien i.S.d. TMG sein, solange nicht *ausschließlich* eine Übertragungsfunktion vorliegt.[788] Mit der Änderung bezweckte die Bundesregierung lediglich die Verweise auf das gleichzeitig novellierte TKG anzupassen.[789] Durch die Weglassung der Beschränkung „… die ganz in … bestehen“ wäre allerdings eine Abgrenzung dergestalt erfolgt, dass die Legaldefinition der Telemedien sämtliche Telekommunikationsdienste ausschließt.

3.2.1.2 OTT-Dienste

Die Differenzierung zwischen Telekommunikation und Telemedien konzentrierte sich bisher auf die Frage der Übertragung von Signalen über Telekommunikationsnetze. Lange umstritten war die Einordnung sog. Over-the-Top-Dienste (OTT-Dienste), die nicht selbst die Signalübertragung bewirken, sondern bestehende Internetverbindungen nutzen.[790] Auch Unternehmen nutzen zunehmend Internetdienste, „die eine interpersonelle Kommunikation ermöglichen, z. B. Voice-over-IP (VoIP-) Telefonie, Sofortnachrichtenübermittlung (Instant-Messaging) und webgestützte E-Mail-Dienste.“[791] Insbesondere für solche OTT-Dienste, bei denen es gerade auf die Übermittlung von Nachrichten ankommt, wie VoIP-Calls, Messenger und E-Mail-Dienste, und die herkömmliche TK-Dienste, wie Telefonate und SMS ersetzen, erschien die Qualifizierung problematisch.[792] Die Rechtsprechung kam zu unterschiedlichen Ergebnissen bezüglich der Frage, ob und welche OTT-Dienste unter die Definition des Telekommunikationsdienstes fallen.

E-Mail-Dienste (Gmail): In der Vorinstanz hatte das VG Köln Gmail als TK-Dienst i.S.v. § 3 Nr. 24 TKG subsumiert.[793] Der EuGH entschied dagegen, dass der E-Mail-Dienst Gmail nicht in den Anwendungsbereich der e-Privacy-RL fällt.[794] Zwar nimmt der Erbringer eines internetbasierten E-Mail-Diensts eine Übertragung von Signalen vor, allerdings qualifiziere dies nicht als Dienst, der ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze besteht.[795] Die Signalübertragung erfolge im Wesentlichen über die verschiedenen Netze, aus denen das offene Internet besteht.[796]

SkypeOut: Hier entschied der EuGH, dass die Bereitstellung einer Software mit einer Voice-over-Internet-Protocol-Funktion (VoIP – Stimmübertragung über Internetprotokoll), mit der die Nutzenden von einem End-

[787] BR-Drs. 325/21, S. 185.
[788] *Spindler,* in: Spindler/Schmitz - TMG, § 1 Rn. 31.
[789] BT-Drs. 19/26108, S. 394.
[790] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 3 TKG Rn. 12.
[791] BT-Drs. 19/27441, S. 33.
[792] Herrmann/Heilmann, in: BeckOK IT-Recht, § 3 TKG Rn. 18.
[793] VG Köln, Urteil vom 11.11.2015 - 21 K 450/15.
[794] EuGH, Urteil vom 13.6.2019 – C-193/18 – Google LLC/Bundesrepublik Deutschland.
[795] EuGH, Urteil vom 13.6.2019 – C-193/18 – Google LLC/Bundesrepublik Deutschland, Rn. 34 ff.
[796] EuGH, Urteil vom 13.6.2019 – C-193/18 – Google LLC/Bundesrepublik Deutschland, Rn. 36.

gerät über das öffentliche Telefonnetz eines Mitgliedstaats eine Festnetz- oder Mobilfunknummer eines klassischen Telefonanschlusses anrufen können, als „elektronischer Kommunikationsdienst“ einzustufen ist,[797] wenn ein Entgelt gezahlt wird und die Übertragung durch Vereinbarungen mit den Netzbetreibern erfolgt.[798] Da der EuGH selbst nicht auf das Gmail-Urteil Bezug nahm, interpretierten Stimmen aus der Literatur das Abgrenzungskriterium so, dass es auf die Übernahme der Verantwortung für die Übertragung dieser Signale durch Skype ggü. seinen Nutzenden ankomme.[799] Skype-interne VoIP-Anrufe sind von der Entscheidung hingegen nicht betroffen.[800]

Reine OTT-Dienste, internetbasierte VoIP-Anrufe (Sprache und Video), Instant Messaging, Screen-Sharing, File-Sharing, internetbasierte Fernsteuerung etc., die zur Signalübertragung allein das Internet nutzen und auf einen Internetzugang ihrer Nutzenden angewiesen sind, wurden daher nicht als Telekommunikationsdienste i.S.d. § 3 Nr. 24 TKG a.F. klassifiziert.[801] Die bisherige Differenzierung erscheint allerdings nicht mehr sachgerecht, da aus funktionaler Sicht eine Austauschbarkeit mit klassischen TK-Diensten vorliegt, die Regulierungsdichte aber unterschiedlich ausfällt.[802] Um Rechtssicherheit und Rechtsklarheit zu schaffen, sollte die ePrivacy-VO die OTT-Dienste klar einordnen.[803] Dieses Anliegen sieht der deutsche Gesetzgeber nun über Art. 2 Nr. 4b und Nr. 7 der Richtlinie (EU) 2018/1972 erreicht, dessen Anwendungsbereich ab dem 21.12.2020 auch für die ePrivacy-Richtlinie maßgeblich ist und welche mit der Aufnahme der Kategorie der interpersonellen Kommunikationsdienste als Unterfall der elektronischen Kommunikationsdienste die meisten nun von der bisherigen Definition der Telekommunikationsdienste ausgenommenen OTT-Dienste mit einbezieht.[804]

Interpersonelle Kommunikationsdienste: Dieser neu eingeführte Begriff dient der Umsetzung des Art. 2 Nr. 5 Richtlinie (EU) 2018/1972.[805] Adressiert werden insbesondere OTT-Online-Dienste wie Internettelefonie und web-gestützte E-Mail-Dienste insbesondere auch Messengerdienste, deren Funktionalität aus Perspektive der Endnutzenden gleichwertig zu „klassischen“ Telekommunikationsdiensten sind.[806] Ziel der Erweiterung ist einen wirksamen Schutz der Endnutzer*innen sicherzustellen, da es für diese selten relevant ist, ob die Signalübertragung durch den Anbieter selbst durchgeführt wird oder die Kommunikation über einen Internetzugangsdienst übermittelt wird. [807] Daher erfasst der Oberbegriff des TK-Dienstes nun:

- Internetzugangsdienste,
- Interpersonelle Telekommunikationsdienste und
- Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen.
- In Abgrenzung zu sozialen Medien ermöglicht der interpersonelle Telekommunikationsdienst einen Informationsaustausch zwischen einer endlichen und nicht potenziell unbegrenzten Anzahl von Personen, die vom Sender der Kommunikation oder von den daran Beteiligten bestimmt werden.[808]

Beispiele:

---

[797] Aufgrund der Umsetzung von EU-Recht gilt dies auch für den „Telekommunikationsdienst“ i.S.d. TKG: *Fokken*, NZA 2020, 629 (631 f.).
[798] EuGH, Urteil vom 5.6.2019 – C-142/18 – Skype Communications.
[799] *Spies*, MMR 2019, 516 (516); *Fokken*, NZA 2020, 629 (632).
[800] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 3 TKG Rn. 19; *Fokken*, NZA 2020, 629 (632).
[801] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 3 TKG Rn. 20.
[802] Siehe zur Kritik: *Jandt/Karg,* in: Datenschutz im Internet, Kap. A. II. Rechtliche Grundlagen Rn. 98 ff.
[803] Zur Einordnung von OTT-Diensten nach den ePrivacy-VO-Entwürfen siehe: *Engeler/Felber*, ZD 2017, 251 (252 ff.); *Specht,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § Verbraucherdatenschutz, Rn. 14.
[804] BT-Drs. 19/27441, S. 33; *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 3 TKG Rn. 21. Siehe auch Erwägungsgrund 17 RL (EU) 2018/1972.
[805] BT-Drs. 19/26108, S. 231.
[806] BT-Drs. 19/26108, S. 231.
[807] BT-Drs. 19/26108, S. 231.
[808] BT-Drs. 19/26108, S. 231; EG 17 RL (EU) 2018/1972.

- Sprachtelefonie, Internettelefonie
- E-Mails
- Messengerdienste und Gruppenchats

Dabei kann auch die Kommunikation zwischen natürlichen und juristischen Personen in den Anwendungsbereich fallen, wenn die juristische Person von einer natürlichen Person in deren Namen vertreten wird (vgl. Erwägungsgrund 17 Richtlinie (EU) 2018/1972) oder ein Postfach bereitstellt.[809] Ausgenommen sind Gespräche mit Maschinen, wie Sprachassistenten.[810]

Aus Sicht des Gesetzgebers ließen sich die vorgenannten Ausführungen weitestgehend bereits auf die bisherige Definition des „Telekommunikationsdienstes“ in § 3 Nr. 24 TKG übertragen, die neugefasste Definition „beseitigt allerdings bislang bestehende Unklarheiten“.[811] Folglich fallen nun Messengerdienste und vergleichbare Kommunikations- und Kooperationsdienste unter den Begriff des Telekommunikationsdienstes.[812]

3.2.1.2.1 Abgrenzung zur DSGVO

Die DSGVO genießt Anwendungsvorrang vor nationalem Recht – dieser wird allerdings in Art. 95 DSGVO zurückgenommen, damit die in Umsetzung der ePrivacy-Richtlinie ergangenen mitgliedstaatlichen Umsetzungsakte weiterhin anwendbar bleiben. Der Anwendungsbereich der ePrivacy-RL erstreckt sich dabei aber nur auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung *öffentlich zugänglicher* elektronischer Kommunikationsdienste in *öffentlichen* Kommunikationsnetzen in der Union.[813] Für geschlossene Benutzergruppen und damit auch rein innerbetriebliche Unternehmensnetze ist die Richtlinie hingegen nicht anwendbar.[814] „Öffentlichkeit“ wird nach hergebrachter Begriffsinterpretation von der geschlossenen Benutzergruppe abgegrenzt.[815] Kommunikationsnetze können als „öffentlich“ betrachtet werden, wenn sie einer vorher nicht definierbaren Anzahl Dritter zur Nutzung angeboten werden und die Kommunikation der Beteiligten dabei nicht oder nicht ausschließlich im Interesse oder für den Betreiber des Netzes erfolgt.[816] Für eine überschießende Regulierung solcher Fallkonstellationen, die gerade nicht öffentlich sind, gilt der Anwendungsvorrang DSGVO, sodass nationale Vorschriften verdrängt werden.[817] Allerdings besagt der Wortlaut des Art. 95 DSGVO nur, dass „keine zusätzlichen Pflichten“ durch die DSGVO aufgestellt werden. Dies ließe sich auch als ein lex-specialis-Verhältnis lesen, ohne dass die DSGVO Einfluss auf die Inhalte im Bereich ePrivacy nehmen will.[818] Nichtsdestotrotz wird der Anwendungsvorrang der DSGVO nach herrschender Meinung nur für den Anwendungsbereich der ePrivacy-RL zurückgenommen, nicht für über-

[809] BT-Drs. 19/26108, S. 231; EG 17 RL (EU) 2018/1972.
[810] BT-Drs. 19/26108, S. 231; EG 17 RL (EU) 2018/1972.
[811] BT-Drs. 19/26108, S. 237.
[812] vgl. *Schwartmann u. a.*, MMR 2021, 99 (99).
[813] *Holländer,* in: BeckOK DatenschutzR Art. 95 Rn. 4; *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 95 Rn. 2; *Karg,* in: NK Datenschutzrecht Art. 95 Rn. 6; siehe auch zu Unklarheiten der Regelung: *Piltz,* in: Gola DS-GVO, Art. 95 Rn. 5.
[814] *Holländer,* in: BeckOK DatenschutzR Art. 95 Rn. 4; *Karg,* in: NK Datenschutzrecht Art. 95 Rn. 6; *Sydow*, Sydow, Europäische Datenschutzgrundverordnung Art. 95 Rn. 12; *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 96 TKG Rn. 3; *Eckhardt,* in: Recht der elektronischen Medien, § 96 TKG Rn. 14.
[815] *Schütz,* in: Geppert/Schütz - TKG, § 6 Rn. 46 ff.
[816] *Karg,* in: NK Datenschutzrecht Art. 95 Rn. 6.
[817] *Holländer,* in: BeckOK DatenschutzR Art. 95 Rn. 4; *Kühling/Raab,* in: Kühling/Buchner - DS-GVO/BDSG Art. 95 Rn. 11; *Sydow*, Sydow, Europäische Datenschutzgrundverordnung Art. 95 Rn. 10; *Golland,* in: Taeger/Gabel - DSGVO/BDSG Art. 95 Rn. 17.
[818] *Piltz,* in: Gola DS-GVO, Art. 95 Rn. 11.

schießende Umsetzungen. Daran ändert nichts, wenn die „zusätzlich Pflichten“ nicht aus der DSGVO, sondern der ePrivacy-Umsetzung resultieren. Im Kontext der betriebsinternen Kommunikation *im* Unternehmen sind daher allein die DSGVO sowie das BDSG im Rahmen der Öffnungsklauseln maßgeblich.

3.2.1.2.2 Anwendbarkeit für öffentlich zugängliche elektronische Kommunikationsdienste

Die telekommunikations- und telemedienrechtlichen Datenschutzvorschriften, welche sich im Regulierungsbereich der ePrivacy-RL an öffentlich zugängliche Dienste richten, unterliegen nicht dem Anwendungsvorrang der DSGVO und sind folglich neben der DSGVO anwendbar. Auch im Hinblick auf das Angebot an Unternehmen als Endnutzer gilt zu bedenken, dass diese in den Schutzbereich der TK-Regeln fallen können.[819] Allerdings stellt sich auch hier die Problematik der OTT-Dienste: diese wurden von der ePrivacy-RL bisher nicht erfasst.[820] Der EuGH hatte in Bezug auf Art. 2 Buchst. c der Richtlinie 2002/21/EG (Rahmenrichtlinie) entschieden, dass ein internetbasierter E-Mail-Dienst keinen „elektronischen Kommunikationsdienst“ darstellt.[821] So bestätigt auch die EU-Kommission zu Sofortnachrichtenübermittlung (Instant-Messaging) und webgestützten E-Mail-Diensten, dass „solche Over-the-Top-Kommunikationsdienste („OTT-Dienste“) […] aber im Allgemeinen vom gegenwärtigen Rechtsrahmen der Union für die elektronische Kommunikation, einschließlich der e-Datenschutz-Richtlinie, nicht erfasst [werden].“[822] Die Aufnahme erfolge vielmehr über die Richtlinie (EU) 2018/1972 vom 11.12.2018 über den europäischen Kodex für die elektronische Kommunikation. Von dieser Richtlinie unberührt bleiben nach Art. 1 Abs. 3 Buchst. b der Schutz personenbezogener Daten und der Privatsphäre. Insofern wäre zunächst einmal festzuhalten, dass auch hier die Zurücknahme des Anwendungsvorrangs der DSGVO nicht für OTT-Dienste greift – auch für diese wäre weiterhin die DSGVO maßgeblich. Dagegen scheint der Gesetzgeber als auch der BfDI davon auszugehen, mit dem TTDSG auch Messenger als interpersonelle Telekommunikationsdienste zu regulieren.[823]

Nun wird im Hinblick auf die ohnehin geplante Ausdehnung der diskutierten ePrivacy-VO angemerkt, dass aus der Perspektive des Grundrechtsschutzes und aus funktionalen Erwägungen eine Angleichung der „klassischen“ TK-Dienste mit den OTT-Diensten sinnvoll sein könnte. Dies könnte über eine grundrechtskonforme Auslegung des Art. 95 DSGVO dergestalt erfolgen, dass dieser im Lichte der geänderten Rechtsauffassung auch OTT-Dienste als „öffentlich zugängliche elektronische Kommunikationsdienste“ erfasst.[824] Der EuGH hatte in seinem Verfahren über einen Bescheid aus dem Jahre 2012 zu entscheiden. Die Definition in Art. 2 Nr. 4 RL 2018/1972 wurde folglich noch nicht berücksichtigt. Danach sind „elektronische Kommunikationsdienste“:

> gewöhnlich gegen Entgelt über elektronische Kommunikationsnetze erbrachte Dienste, die — mit der Ausnahme von Diensten, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben — folgende Dienste umfassen:
>
> a) „Internetzugangsdienste“ im Sinne der Begriffsbestimmung des Artikels 2 Absatz 2 Nummer 2 der Verordnung (EU)

[819] *Holländer,* in: BeckOK DatenschutzR Art. 95 Rn. 6; vgl. auch *Klabunde/Selmayr,* in: Ehmann/Selmayr - DSGVO Art. 95 Rn. 4; *Sydow*, Sydow, Europäische Datenschutzgrundverordnung Art. 95 Rn. 11.
[820] EuGH, Urteil vom 12.06.2019 – C-193/18 – Google LLC/Bundesrepublik Deutschland; *Karg,* in: NK Datenschutzrecht Art. 95 Rn. 11.
[821] EuGH, Urteil vom 12.06.2019 – C-193/18 – Google LLC/Bundesrepublik Deutschland.
[822] *EU Kommission,* Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), Brüssel, den 10.01.2017, COM(2017) 10 final, Ziff. 1.1, S. 2.
[823] BT-Drs. 19/27441, S. 3, 32; BfDI, Stellungnahme zur öffentlichen Anhörung des Ausschusses für Wirtschaft und Energie, 21.04.2021, Ausschussdrucksache 19(9)1037, S. 5.
[824] So: *Karg,* in: NK Datenschutzrecht Art. 95 Rn. 12.

2015/2120,

b) interpersonelle Kommunikationsdienste und

c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für die Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden

Wie bereits zuvor in Abschnitt 3.2.1.1.1 angesprochen, sollen Messenger unter den Fall des interpersonellen Kommunikationsdienstes fallen, welcher in Art. 2 Nr. 5 definiert sowie in EG 17 beschrieben wird.

„interpersoneller Kommunikationsdienst“:

gewöhnlich gegen Entgelt erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über elektronische Kommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Kommunikation veranlassen oder daran beteiligt sind; dazu zählen keine Dienste, die eine interpersonelle und interaktive Kommunikation lediglich als untrennbar mit einem anderen Dienst verbundene untergeordnete Nebenfunktion ermöglichen

3.2.1.3 Betroffene Daten

Im Rahmen des Fernmeldegeheimnisses waren bereits bisher gemäß § 91 Abs. 1 S. 2 TKG auch Einzelangaben über juristische Personen und Personengesellschaften geschützt, soweit sie mit der Fähigkeit ausgestattet sind, Rechte zu erwerben oder Verbindlichkeiten einzugehen.[825]

§ 1 Abs. 2 TTDSG

Dem Fernmeldegeheimnis unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder Personengesellschaft, die mit der Fähigkeit ausgestattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, stehen den personenbezogenen Daten gleich.

Die bisherige Regelung wird nun in § 1 Abs. 2 TTDSG aufgegriffen und dient dabei der Umsetzung von Art. 1 Abs. 2 S. 2 RL 2002/58/EG.[826]

3.2.1.4 Persönlicher Anwendungsbereich

Die speziellen Regelungen des TKG und TTDSG sind nur von den jeweiligen Normadressaten zu erfüllen. Gerade im Unternehmenskontext stellen sich hier einige Abgrenzungsschwierigkeiten.

Anbieter von Telekommunikationsdiensten: Aufgrund des Merkmals der „geschäftsmäßigen“ Erbringung, welche in § 3 Nr. 10 TKG a.F. als „das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“ definiert war, folgte bisher die Notwendigkeit einer Außenwirkung bzw. eines Drittbezugs.[827] Dieses Kriterium wurde zwar bereits bei geschlossenen Benutzergruppen angenommen,

[825] *Eckhardt,* in: Recht der elektronischen Medien, § 91 TKG Rn. 42.
[826] BT-Drs. 19/27441, S. 33.
[827] *Ricke,* in: Recht der elektronischen Medien, § 3 Rn. 22.

sodass kein Angebot an die Öffentlichkeit verlangt wurde.[828] Ein Angebot von Telekommunikation musste aber zumindest an außerhalb der Sphäre des Dienstanbieters liegende Dritte gerichtet sein.[829] Damit waren firmenintern betriebene (geschlossene) Kommunikationssysteme vom Anwendungsbereich ausgenommen.[830]

Allerdings war umstritten, ob Beschäftigte ebenfalls als Dritte i.S.d. TKG anzusehen waren.[831] Eine höchstrichterliche Klärung dieser Frage ist nie erfolgt, sodass Arbeitgebern zumeist geraten wurde, die private Kommunikation vorsorglich zu untersagen, da bei Verletzung des Post- und Fernmeldegeheimnisses auch Strafbarkeit nach § 206 StGB droht.[832] Bei rein dienstlicher Nutzung wurde die Anwendbarkeit des TK-Rechts überwiegend verneint, da der Arbeitgeber sonst seinen unternehmerischen Pflichten, u.a. handels- und steuerrechtlichen Aufbewahrungspflichten, nicht nachkommen könnte.[833] Die dienstliche Kommunikation impliziert allerdings ebenso die Verarbeitung personenbezogener Daten wie die zu privaten Zwecken. [834] Eine solche Unterscheidung erscheint daher dogmatisch zweifelhaft. Allerdings treten Beschäftigte in ihrer dienstlichen Funktion regelmäßig als Vertreter*innen ihres Betriebs nach außen auf und bilden mit ihrem Unternehmen „eine Einheit“, sodass die Klassifikation als „Dritte“ fernliegend erscheint.[835] Sodann stellt sich die Frage, ob Beschäftigte zu Dritten werden, wenn die private Kommunikation erlaubt wird. Sowohl die Aufsichtsbehörden[836] als auch die herrschende Meinung im Schrifttum hatten diese Frage noch bejaht.[837] Verschiedene deutsche Arbeits- und Verwaltungsgerichte stuften den Arbeitgeber hingegen nicht als Dienstanbieter i.S.d. TKG ein, selbst wenn dieser seinen Beschäftigten die private Nutzung des dienstlichen E-Mail-Accounts gestattet.[838] Weder lokal noch zentral auf dienstlichen Rechnern gespeicherte oder über die Infrastruktur des Arbeitgebers übermittelte Daten der Beschäftigten unterliegen nach dieser Rechtsprechung dem Fernmeldegeheimnis.[839] Auf dem Arbeitsrechner gespeicherte Chatprotokolle, die Inhalt und Umstände einer abgeschlossenen Kommunikation sind, werden zwar über das Rechts auf informationelle Selbstbestimmung bzw. dem Recht auf Schutz personenbezogener Daten aber nicht dem Fernmeldegeheimnis geschützt.[840]

---

[828] *Ricke,* in: Recht der elektronischen Medien, § 3 Rn. 22; *Schütz,* in: Geppert/Schütz - TKG, § 3 Rn. 33; *Lünenbürger/Stamm,* in: Scheurle/Mayen - TKG, § 3 Rn. 27.

[829] *Schütz,* in: Geppert/Schütz - TKG, § 3 Rn. 33; *Lünenbürge/Stamm,* in: Scheurle/Mayen - TKG, § 3 Rn. 27.

[830] *Roggan*, G-10-Gesetz, § 2 Rn. 4; *Günther,* in: Münchener Kommentar zur StPO, § 2 Rn. 8.

[831] *Lünenbürger/Stamm,* in: Scheurle/Mayen - TKG, § 3 Rn. 27; *Baumgartner,* in: Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. IX. Rn. 71 ff.; *Fokken*, NZA 2020, 629 (633); *Wolf, de*, NZA 2010, 1206 (1208).; vgl. auch OLG Karlsruhe, OLG Karlsruhe, Beschluss vom 10.01.2005 – 1 Ws 152/04, Rn. 24.

[832] *Fokken*, NZA 2020, 629 (629).

[833] *Fokken*, NZA 2020, 629 (629).; ähnlich *Riesenhuber,* in: BeckOK DatenschutzR, § 26 BDSG, Rn. 168; *Brink/Schwab*, ArbRAktuell 2018, 111 (111); *Wybitul/Böhm*, CCZ 2015, 133 (133). vgl. auch *DSK - Datenschutzkonferenz*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, S. 6 ff.

[834] *Fokken*, NZA 2020, 629 (630).

[835] *Fokken*, NZA 2020, 629 (633); *Spindler,* in: Spindler/Schmitz - TMG, § 1 Rn. 39; *Baumgartner,* in: Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. IX. Rn. 14; *Wolf, de*, NZA 2010, 1206 (1208).

[836] *DSK - Datenschutzkonferenz*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, S. 4.

[837] *Tiedemann*, MMR 2010, 639 (641); *Brink*, jurisPR-ArbR 2011, Anm. 5; *Spindler,* in: Spindler/Schmitz - TMG, § 1 Rn. 39; *Wolf, de*, NZA 2010, 1206 (1207); *Brink/Schwab*, ArbRAktuell 2018, 111 (112).

[838] LAG Niedersachsen, Urteil vom 31.05.2010 – 12 Sa 875/09 –, Rn. 45; LArbG Berlin-Brandenburg, Urteil vom 16.02.2011 – 4 Sa 2132/10, Rn. 36; LAG Berlin-Brandenburg, Urteil vom 14.01.2016 - 5 Sa 657/15, Rn. 81; VG Karlsruhe, Urteil vom 27.05.2013, AZ: 2 K 3249/12, Rn. 87; VGH Baden-Württemberg, Urteil vom 30.07.2014 - 1 S 1352/13, Rn. 82; LG Erfurt v. 28.04.2021, 1 HK O 43/20; a.A. ArbG Hannover, Urteil vom 28. 4. 2005 - 10 Ca 791/04, Rn. 27.

[839] LAG Niedersachsen, Urteil vom 31.05.2010 – 12 Sa 875/09 –, Rn. 45; LArbG Berlin-Brandenburg, Urteil vom 16.02.2011 – 4 Sa 2132/10 –, Rn. 40; LAG Berlin-Brandenburg, Urteil vom 14.01.2016 - 5 Sa 657/15, Rn. 81; vgl. auch Hessischer VGH, Beschluss vom 19.05.2009 – 6 A 2672/08.Z –, Rn. 16 ff.; ArbG Düsseldorf, Urteil vom 29.10.2007 - 3 Ca 1455/07, Rn. 52.

[840] LAG Hamm, Urteil vom 10.07.2012 - 14 Sa 1711/10, Rn. 628.

Ausgehend vom Schutzzweck des Fernmeldegeheimnis nach Art. 10 GG sollen gerade Gefahren für die Vertraulichkeit der Kommunikation hinsichtlich des Übertragungsvorgangs begegnet werden, die sich aus dem Vorgang der *Fern*übermittlung, d.h. einer räumlich distanzierten Kommunikation, ergeben – und nicht gleichermaßen bei gemeinsamer Anwesenheit bestünden.[841] Auf den Endgeräten abgespeicherte Informationen aus dem Kommunikationsvorgang sind daher nicht vom Schutzbereich erfasst.[842] Insofern stellt sich in teleologischer Sicht die Frage, ob ein unterschiedliches Schutzregime für – zumeist auf Arbeitsrechnern – gespeicherte Daten und über arbeitgeberseitige Infrastruktur übermittelte Daten Sinn macht.[843] Als weiteres Argument dient das Merkmal der „in der Regel" vorliegenden Entgeltlichkeit, die bei bloßer Gestattung privater Nutzung gerade regelmäßig nicht gegeben ist.[844] Die Einordnung der Arbeitsgerichte erscheint daher wesentlich pragmatischer, Beschäftigte gegenüber ihrem Arbeitgeber nicht als „Dritte" zu sehen – unabhängig von der privaten oder beruflichen Natur der Kommunikation – und insofern nicht von einer Geschäftsmäßigkeit auszugehen.[845]

§ 3 Nr. 1 TKG n.F. definiert den „Anbieter von Telekommunikationsdiensten" nun als „*jeder*, der Telekommunikationsdienste erbringt". Im Hinblick auf die Verpflichtung zur Wahrung des Fernmeldegeheimnisses in § 3 Abs. 2 S. 2 TTDSG wird der Kreis der Verpflichteten allerdings wieder eingeschränkt auf:

- Anbieter *öffentlich zugänglicher* TK-Dienste[846]
- *Geschäftsmäßig* angebotene TK-Dienste
- Betreiber *öffentlicher* Telekommunikationsnetze
- Betreiber von TK-Anlagen zur *geschäftsmäßigen* Erbringung von TK-Diensten

Die Gesetzesbegründung nimmt Bezug auf § 3 Nr. 6 TKG a.F.[847] bezüglich des Verpflichteten. Bezweckt ist eine inhaltliche Übernahme des § 88 TKG a.F.[848] Dementsprechend dürfte keine Ausweitung auf bisher nicht Verpflichtete gewollt sein. Diese Einordnung ist insofern relevant, als bspw. § 9 ff. TTDSG weitere Pflichten an die „nach § 3 Abs. 2 S. 1 Verpflichtete" richtet. Da der Streit wohl bekannt war und keine Bezugnahme auf Arbeitgeber in der Gesetzesbegründung zu finden ist, erscheint es naheliegend den Anwendungsbereich nicht auf firmeninterne Betriebskommunikation zu erstrecken. Im Rahmen der Definition des interpersonellen Kommunikationsdienstes wird als Beispielsanwendungsfall die Kommunikation einer natürlichen Person mit einer juristischen Person über ein von dieser bereitgestelltes Postfach genannt.[849] Ist die Kommunikation allerdings „unbedeutend" oder „reine Nebensache" – wie oftmals bei Chatfunktionen von Online-Spielen – soll kein Telekommunikationsdienst vorliegen.[850] Als unbedeutend nennt EG 17 RL (EU) 2018/1972 einen Fall, „wenn es nur einen sehr begrenzten objektiven Nutzen für den Endnutzer aufweist und in der Realität von Endnutzern kaum verwendet wird." Gleichwohl die Ausnahme eng aus Sicht der Endnutzenden auszulegen ist,[851] dürfte die Gefahr einer Umgehung der telekommunikationsrechtlichen Vorschriften zur Motivation der

[841] *Fokken*, NZA 2020, 629 (630); *Wolf, de*, NZA 2010, 1206 (1209).
[842] BVerfGE 115, 116 (183 ff.); Hessischer VGH, Beschluss vom 19.05.2009 – 6 A 2672/08.Z, Rn. 15 ff.; LAG Berlin-Brandenburg, Urteil vom 16. 02. 2011 – 4 Sa 2132/10, Rn. 39; LAG Hamm, Urteil vom 10.07.2012 - 14 Sa 1711/10, Rn. 628; VG Frankfurt, Urteil vom 06.11.2008 – 1 K 628/08.F, Rn. 29.
[843] *Fokken*, NZA 2020, 629 (633).
[844] *Baumgartner,* in: Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. IX Rn. 82.
[845] Im Ergebnis auch: *Baumgartner,* in: Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. IX Rn. 82; *Fokken*, NZA 2020, 629 (633).
[846] Definiert in § 3 Nr. 44 TKG n.F.: „öffentlich zugängliche Telekommunikationsdienste" einem unbestimmten Personenkreis zur Verfügung stehende Telekommunikationsdienste.
[847] BT-Drs. 19/27441, S. 34.
[848] BT-Drs. 19/27441, S. 34.
[849] BT-Drs. 19/26108, S. 231.
[850] BT-Drs. 19/26108, S. 231.
[851] BT-Drs. 19/26108, S. 231; EG 17 RL (EU) 2018/1972

Einordnung unter die TK-Dienste bei Gestattung der privaten Nutzung innerbetrieblicher Kommunikationsinfrastruktur nicht gegeben sein.

EU-rechtskonforme Auslegung: Die telekommunikations- und telemedienrechtlichen Datenschutzbestimmungen stellen eine Umsetzung der Richtlinie 2002/58/EG dar (ePrivacy) dar. Diese Richtlinie gilt gemäß Art. 3 Abs. 1 „für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung *öffentlich zugänglicher* elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft." Bisher wurde keine Vollharmonisierung, sondern nur eine Mindestharmonisierung angenommen.[852] Insofern waren strengere und auch weiter gefasste nationale Regelungen möglich. Nun gilt aber zu bedenken, dass die DSGVO Anwendungsvorrang im Bereich des Datenschutzes vor mitgliedstaatlichem Recht genießt. Eine Auslegung der TTDSG-Regelungen sollte daher im Lichte der DSGVO erfolgen. Diese sieht zwar in Art. 95 DSGVO vor, dass die auf Grundlage der ePrivacy-RL ergangenen Regelungen bis zum Inkrafttreten einer ePrivacy-VO weiterhin Bestand haben sollen. Dies gilt aber eben nur für die in der ePrivacy-RL erfassten Sachverhalte.[853] Um Rechtssicherheit zu schaffen, sollten daher bereits im Rahmen der Begriffsinterpretation Fallkonstellationen ausgeschlossen werden, welche von der ePrivacy-RL nicht adressiert wurden und für welche die DSGVO nun Anwendungsvorrang genießt. Auch insofern wären alle nicht an die Öffentlichkeit gerichtete Angebote nicht erfasst.

Folgerichtig wurde im Gesetzgebungsverfahren eine Beschränkung auf öffentliche TK-Dienste gefordert, womit der Streit um den potentiellen Einbezug des Arbeitgebers vorerst beendet worden wäre.[854] Dabei wurde unterstrichen, dass durch die vorrangig anwendbare DSGVO keine Gefahr einer Schutzlosigkeit besteht.[855]

Anbieter von Telemedien: waren zuvor in § 2 Nr. 1 TMG definiert, als natürliche oder juristische Person, die „eigene oder fremde" Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Das Merkmal des „Bereithaltens" ist in der neuen Definition des TTDSG durch „erbringen oder an der Erbringung mitwirkt" ersetzt worden. Bietet ein Arbeitgeber bspw. Onlineforen zur Verfügung, konnte nach der bisherigen Rechtslage ein Telemedienangebot vorliegen.[856]

> § 2 Abs. 1 TTDSG „Anbieter von Telemedien" jede natürliche oder juristische Person, die eigene oder fremde Telemedien erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden Telemedien vermittelt

3.2.1.5 Räumlicher Anwendungsbereich

> **§ 1 Abs. 3 TTDSG**
>
> Diesem Gesetz unterliegen alle Unternehmen und Personen, die im Geltungsbereich dieses Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken oder Waren auf dem Markt bereitstellen. § 3 des Telemediengesetzes

[852] *Kühling/Raab,* in: Kühling/Buchner - DS-GVO/BDSG Art. 95 Rn. 11; *Sydow,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 95 Rn. 10; *Golland,* in: Taeger/Gabel - DSGVO/BDSG Art. 95 Rn. 17.
[853] *Holländer,* in: BeckOK DatenschutzR Art. 95 Rn. 4; *Kühling/Raab,* in: Kühling/Buchner - DS-GVO/BDSG Art. 95 Rn. 11; *Sydow*, Sydow, Europäische Datenschutzgrundverordnung Art. 95 Rn. 10; *Golland,* in: Taeger/Gabel - DSGVO/BDSG Art. 95 Rn. 17.
[854] Schwartmann, Stellungnahme vom 21.04.2021, Ausschussdrucksache 19(9)1043, S. 10.
[855] Schwartmann, Stellungnahme vom 21.04.2021, Ausschussdrucksache 19(9)1043, S. 10; vgl. auch *Riesenhuber* in: BeckOK DatenschutzR, § 26 BDSG, Rn. 169.
[856] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 BDSG, Rn. 169.1.

bleibt unberührt.

Auch im Rahmen des TTDSG gelten Sitzlandprinzip und Marktortprinzip. Die Norm hat Bedeutung für alle Bestimmungen, „die sich nicht auf die Verarbeitung personenbezogener Daten beziehen und die nicht unter § 3 TMG fallen, so dass das Marktortprinzip bei der Anwendung dieses Gesetzes gilt, soweit nicht § 3 TMG Anwendung findet."[857]

3.2.1.6 Zwischenergebnis in Bezug auf die Kommunikation im Unternehmenskontext

Insgesamt wird der Anwendungsbereich des TTDSG durch den Verweis auf die Begriffsbestimmungen des TKG determiniert, welche durch das TKMoG gegenüber der bisherigen Rechtlage um OTT-Dienste erweitert wurden.[858] Aus den zuvor angestellten Erwägungen folgt:

- Kommerziell betriebene OTT-Dienste wie z. B. Messengerdienste, die ihr Angebot grundsätzlich an die Allgemeinheit richten, fallen unter die TK-Dienste und müssten künftig die TK-Regeln zur Umsetzung des Fernmeldegeheimnisses umsetzen. Unklar bleibt, ob sie gleichzeitig den Anforderungen der telemedienrechtlichen Vorschriften nach TTDSG unterliegen können.
- Firmenintern betriebene Kommunikations- und Kollaborationsdienste dürften nicht unter die TK-Regulierung nach TTDSG fallen.
  - Dies gilt unstreitig für dienstliche Kommunikation.
  - Für die Duldung privater Kommunikation können sich Unternehmen als Arbeitgeber auf arbeitsgerichtliche Präzedenzfälle berufen, dass auch insoweit kein TK-Dienst vorliegt. Zudem dürfte das TTDSG von der DSGVO verdrängt werden, da hier keine öffentliche Zugänglichkeit vorliegt. Um sicherzugehen aus dem Schutzbereich des Fernmeldegeheimnisses herauszufallen, können Unternehmen dezentrale Lösungen einsetzen, bei denen Nachrichten nicht auf zentralen, arbeitgeberseitigen Servern zwischengespeichert werden müssen (und insofern noch ein Übermittlungsvorgang angenommen werden könnte).[859] Alternativ kann die private Nutzung untersagt werden.[860]

Firmenextern betriebene Kommunikations- und Kollaborationsdienste könnten ggf. unter die TK-Regulierung fallen, wenn sie auf gewisse Dauer angelegt (geschäftsmäßig) und öffentlich zugänglich sind: hier stellt sich die Frage, ob der Schutzbereich eröffnet ist, wenn die Kommunikation ausschließlich *mit* dem Unternehmen erfolgt und nicht *zwischen externen* Dritten.

[857] BT-Drs. 19/27441, S. 34.
[858] *Stroscher*, ZD-Aktuell 2021, 05222.
[859] Vgl. *DSK - Datenschutzkonferenz*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, S. 8. Sobald Daten im „Herrschaftsbereich" der betroffenen Personen liegen, endet der Schutzrahmen des Fernmeldegeheimnisses.
[860] Nach h.M. ist das TKG nicht bei verbotswidrig privater Nutzung einschlägig, ausnahmsweise kann die Duldung privater Nutzung aber zu einer betrieblichen Übung und damit zur Gestattung führen: *Baumgartner,* in: Weth/Herberger/Wächter/Sorge, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, Kap. IX Rn. 77.

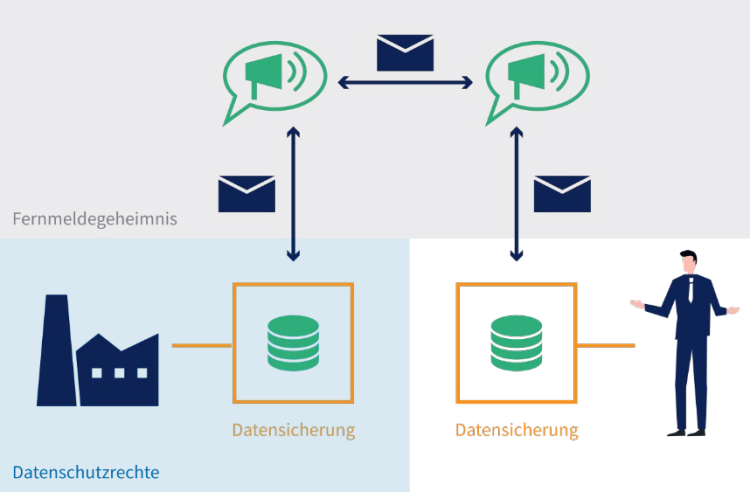


Abbildung 12 Schutzbereich des Fernmeldegeheimnisses

3.2.2 Rechtsgrundlagen auf Grundlage der mitgliedstaatlichen Umsetzung der ePrivacy-Richtlinie

Die Rechtslage kann, wie dargelegt, als relativ unübersichtlich bezeichnet werden. Es erscheint daher sinnvoll, sich einen groben Überblick über die Regelungen zu verschaffen, um eine vorsorgliche Umsetzung erwägen zu können. Denn im Hinblick auf nicht von der DSGVO erfasste Sachverhalte sind nationale Einordnungen der Messenger unter die TK-Regelungen ohne Konflikt mit Art. 95 DSGVO möglich – unabhängig davon, ob eine Pflicht durch EU-Vorgaben besteht. Neben einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten, enthalten die relevanten Vorgaben auch zahlreiche Einschränkungen. Die telekommunikationsrechtlichen Vorschriften des TTDSG differenzieren dabei nach der betroffenen Datenart nach Verkehrsdaten und Standortdaten.

Verkehrsdaten: Die als TK-Dienst Verpflichteten dürfen Verkehrsdaten nur verarbeiten, soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist. Verkehrsdaten werden in der ePrivacy-RL definiert als:

> **Art. 2 Buchst. b) RL 2002/58/EG**
>
> Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden

Gemäß § 9 Abs. 1 TTDSG zählen zu diesen Daten:

- Anschlussnummern/Kennungen, personenbezogene Berechtigungskennungen, Kundenkartennummern, Standortdaten bei mobilen Anschlüssen,
- Beginn und Ende der jeweiligen Verbindungen nach Datum/Uhrzeit/ggf. übermittelten Datenmengen,
- den vom Nutzer in Anspruch genommene Telekommunikationsdienst,
- die Endpunkte von festgeschalteten Verbindungen, Beginn und Ende nach Datum/Uhrzeit/ggf. übermittelten Datenmengen,
- sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

Dem liegt ein technologieneutrales Verständnis zugrunde.[861] Aufgrund des Schutzzwecks wird argumentiert, dass Verkehrsdaten regelmäßig solche mit Personenbezug sind, sodass rein technische Daten nicht erfasst wären.[862] Zur alten Rechtslage war noch umstritten, ob die Aufzählung abschließend ist – als Rechtsgrundlage greift die Regelung jedenfalls nur für die genannten Fälle von Verkehrsdaten. [863] Im Hinblick auf die Erforderlichkeit wird in der Literatur bisher ein strenger Maßstab angelegt, bezieht sich zwar auf die konkrete Ausgestaltung des Dienstes – dieser hat sich soweit zumutbar jedoch einer datenschutzfreundlichen Technikgestaltung zu bedienen.[864]

Im Übrigen sind Verkehrsdaten von den Verpflichteten nach Beendigung der Verbindung unverzüglich zu löschen. Eine darüberhinausgehende Verarbeitung der Verkehrsdaten ist unzulässig. Pflichten zur Verarbeitung nach anderen Rechtsvorschriften bleiben allerdings unberührt (§ 9 Abs. 1 S. 2-4 TTDSG).

§ 9 Abs. 2 TTDSG ergänzt, dass teilnehmerbezogene Verkehrsdaten vom Anbieter des TK-Dienstes zum Zweck der Vermarktung von TK-Diensten, zur bedarfsgerechten Gestaltung von TK-Diensten oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und im dazu erforderlichen Zeitraum nur verwendet werden dürfen, wenn der „Endnutzer“ in diese Verwendung eingewilligt hat. Daraus folgen im vorliegenden Kontext zwei Fragestellungen:

- Wer gilt bei der beruflichen Nutzung von TK-Diensten als „Endnutzer“? Diese Frage ist vor dem Hintergrund, dass auch juristische Personen grundsätzlich in den Schutzbereich fallen können, nicht trivial. Bei personenbezogenen Daten müsste es allerdings stets die betroffene Person sein, die in die Verarbeitung einwilligt.
- Können Beschäftigte wirksam (freiwillig) einwilligen? Insofern stellt sich wiederum die Problematik, ob in einer Dreieckskonstellation eines Unternehmens als Arbeitgeber, den Beschäftigten und einem Messengerdienst die Unfreiwilligkeit begründende Umstände dem Letzteren zuzurechnen sind (vgl. Abschnitt 2.4.1.2.1.3).

Daten derjenigen, welche nicht einwilligen, sind unverzüglich zu anonymisieren (§ 9 Abs. 2 S. 2 TTDSG). Strengere Anforderungen gelten bei einer zielnummernbezogenen Verwendung.

§ 10 TTDSG regelt die Verarbeitung von Verkehrsdaten zur Entgeltermittlung und Entgeltabrechnung. Im Hinblick auf die üblich gewordenen Pauschal- und Flatrate-Tarife, dürfte dieser Regelung im vorliegenden Kontext kaum Bedeutung zukommen. [865] Ebenso dürften Einzelverbindungsnachweise nach § 11 TTDSG kaum relevant sein.

§ 12 TTDSG erlaubt die Verarbeitung von Verkehrsdaten, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Wichtig ist zu beachten, dass nach § 12 Abs. 1 S. 4 TTDSG der Datenschutzbeauftragte des Verpflichteten unverzüglich über die Verfahren und Umstände der Maßnahme informiert werden muss, soweit die Verkehrsdaten nicht automatisiert erhoben und verwendet werden. Zudem sind nach S. 5 betroffene Endnutzer zu benachrichtigen, sofern sie ermittelt werden können. § 12 Abs. 4 TTDSG erlaubt darüber hinaus zur Aufdeckung von Betrug, Leistungserschleichung oder unzu-

[861] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 96 TKG Rn. 5.
[862] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 96 TKG Rn. 4; *Büttgen,* in: Scheurle/Mayen - TKG, § 96 TKG Rn. 4.
[863] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 96 TKG Rn. 6; *Braun,* in: Geppert/Schütz - TKG, § 96 Rn. 6.
[864] *Braun,* in: Geppert/Schütz - TKG, § 96 Rn. 12; *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 96 TKG Rn. 8; vgl. auch *Büttgen,* in: Scheurle/Mayen - TKG, § 96 Rn. 8.
[865] Vgl. auch zur alten Rechtslage: *Braun,* in: Geppert/Schütz - TKG, § 96 Rn. 12; *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 96 TKG Rn. 8; *Büttgen,* in: Scheurle/Mayen - TKG, § 96 Rn. 8.

mutbaren Belästigungen Verkehrsdaten zu verarbeiten, wenn tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme des Telekommunikationsdienstes vorliegen.

Standortdaten: Nach der Definition der ePrivacy-RL handelt es sich um:

> **Art. 2 Buchst. c RL 2002/58/EG**
>
> Daten, die in einem elektronischen Kommunikationsnetz verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben

Nicht im Zusammenhang mit TK-Netzen oder TK-Diensten entstehende Standortdaten fallen nicht unter die Regelung, deren Verarbeitung richtet sich (bei Personenbezug) nach dem allgemeinen Datenschutzrecht (insbes. DSGVO).[866] Zu den von der Regelung erfassten Daten zählen grundsätzlich neben Funkzellenangaben, GPS-Daten sowie festnetzbezogene Standorte.[867] Dabei können Standortdaten je nach Fallkonstellation gleichzeitig auch Verkehrsdaten sein.[868] Gemäß § 13 Abs. 1 TTDSG dürfen telekommunikationsbezogenen Standortdaten nur in eingeschränktem Umfang verarbeitet werden.

> § 13 Abs. 1 S. 1 TTDSG
>
> Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder Telekommunikationsdiensten verarbeitet werden, dürfen nur in dem zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Nutzer vom Anbieter des Dienstes mit Zusatznutzen gemäß der Verordnung (EU) 2016/679 informiert wurde und eingewilligt hat.

Dienste mit Zusatznutzen sind gemäß § 2 Abs. 2 Nr. 5 TTDSG „jeder von einem Anbieter eines Telekommunikationsdienstes bereitgehaltene zusätzliche Dienst, der die Verarbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder für die Entgeltabrechnung des Telekommunikationsdienstes erforderliche Maß hinausgeht“. Bei jeder Ermittlung des Standortes ist nach § 13 Abs. 1 S. 2, 3 TTDSG eine Textmitteilung an das Endgerät zu senden, es sei denn der Standort wird nur auf dem Endgerät angezeigt. Als Umsetzungsbeispiele werden SMS oder Push-Nachrichten genannt, die konkret Aufmerksamkeit erzeugen.[869] Bei der Fremdortung, also einer Weitergabe von Standortdaten an andere Nutzer oder Dritte, bedarf es einer ausdrücklich, gesondert und schriftlich gegenüber dem Anbieter des Dienstes mit Zusatznutzen erteilten Einwilligung (§ 13 Abs. 1 S. 4 TTDSG). Diese konnte zumindest unter der alten Rechtslage weder elektronisch noch im Rahmen von AGB erteilt werden.[870] Trotz Einwilligung muss eine zeitweise Untersagung die Verarbeitung von Standortdaten nach § 13 Abs. 2 TTDSG möglich sein. Ausnahmen gelten nach § 13 Abs. 3 TTDSG für Notrufnummern. Gemäß § 13 Abs. 4 TTDSG muss die Verarbeitung von Standortdaten auf das erforderliche Maß und personell beschränkt sein.

[866] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 98 TKG Rn. 4.
[867] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 98 TKG Rn. 4; *Eckhardt,* in: Recht der elektronischen Medien, § 98 TKG Rn. 9.
[868] *Braun,* in: Geppert/Schütz - TKG, Teil 98 Rn. 8 ff.; *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 98 TKG Rn. 4.
[869] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 98 TKG Rn. 13.
[870] *Herrmann/Heilmann,* in: BeckOK IT-Recht, § 98 TKG Rn. 15; *Braun,* in: Geppert/Schütz - TKG, § 98 Rn. 22.

3.2.3 Impulse des TTDSG für die Umsetzung der Datenschutzgrundprinzipien im Unternehmenskontext

Die wesentlichen Anforderungen im Hinblick auf Transparenz, Zweckbindung, Richtigkeit und Speicherbegrenzung folgen auch für Telekommunikationsdienste und Telemedien i.S.d. TTDSG weitgehend aus der DSGVO. Besondere Anforderungen sollen im Folgenden im Hinblick auf Datensicherheit und Datenminimierung vorgestellt werden.

3.2.3.1 Datenminimierung im Rahmen der Nutzung von Telemedien- und Telekommunikationsdiensten

Aufgrund der Unklarheiten bezüglich des persönlichen und sachlichen Anwendungsbereichs für Anbieter von Telekommunikationsdiensten und Anbietern von Telemediendiensten sollen im Folgenden beide Aspekte beleuchtet werden. Denn sofern datenschutzfreundliche Messenger ohnehin auch die Anforderungen des TTDSG erfüllen würden, kann der Streit um den Anwendungsbereich dahinstehen. Im TTDSG wurden die datenschutzrechtlichen Regelungen des TKG a.F. und des TMG a.F. weitgehend ohne wesentliche Veränderungen übernommen.

3.2.3.1.1 Telemedien

In § 19 TTDSG wurden die bisherigen Regelungen aus § 13 Abs. 4-7 TMG a.F. übernommen.[871] Hierzu zählen die Pflichten, dafür Sorge zu tragen, dass:

- Telemediennutzende die Dienstnutzung jederzeit beenden können (Abs. 1)
- die Inanspruchnahme gegen Kenntnisnahme Dritter geschützt ist (Abs. 1)
- Ermöglichung anonymer / pseudonymer Nutzung – soweit möglich / zumutbar (Abs. 2)
- Anzeige bei Weitervermittlung zu anderen Telemedienanbietern (Abs. 3)
- Sicherstellung angemessener Datensicherheit (Abs. 4)

Im Zusammenhang mit dem hier besprochenen Datenminimierungsgrundsatz von besonderem Interesse ist Abs. 2, welcher auf § 13 Abs. 6 TMG a.F. beruht.

> **§ 19 Abs. 2 S. 1 TTDSG**
>
> Anbieter von Telemedien haben die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

Die Nutzer*innen von Telemedien sind über diese Möglichkeit zu informieren (§ 19 Abs. 2 S. 2 TTDSG). Knackpunkt der Regelung und damit deren effektive Reichweite sind die Merkmale der technischen Möglichkeit und Zumutbarkeit. Im Hinblick auf die technische Möglichkeit lässt sich festhalten, dass Messengerdienste am Markt angeboten werden, welche eine anonyme bzw. pseudonyme Nutzungsmöglichkeit bieten. Diese ist somit gegeben. Hierbei wurde von der herrschenden Meinung eine anonymisierte/pseudonymisierte Telemediennutzung nach außen für ausreichend erachtet – während eine Identifizierungspflicht intern zum

[871] BT-Drs. 19/27441, S. 37.

Dienstanbieter nicht als Verstoß erachtet wurde.[872] Andere legten die Regelung enger aus als ein „Recht auf Anonymität".[873] Im Beschäftigtenkontext wird eine Anonymität im rechtlichen Sinne kaum herstellbar sein, da zumeist identifizierende Informationen im kommunikativen Kontext immanent sind.[874] Allerdings können sich Unternehmen für die Nutzung von Kommunikations- und/oder Kollaborationstools aussprechen, welche eine eindeutige Identifizierung gegenüber dem Dienstanbieter nicht fordern. Da das Zumutbarkeitskriterium weite Auslegungsspielräume bietet, dürfte der praktische Nutzen dieser Regelung kaum über den des allgemeinen Datenminimierungsgrundsatzes hinausgehen.[875] Vielmehr dürfte es sich bloß um eine Konkretisierung handeln.

3.2.3.1.2 Telekommunikation

Schutz des Fernmeldegeheimnisses: Die Vertraulichkeit der Kommunikation haben nach § 3 Abs. 2 TTDSG Verpflichtete entsprechend der Vorgaben in § 3 Abs. 3 TTDSG besonders zu wahren. Nach der hier in Abschnitt 3.2.1.4 dargelegten Ansicht wird vertreten, dass zu den geschäftsmäßigen Anbietern von TK-Diensten des § 3 Abs. 2 Nr. 2 TTDSG höchstens „klassische" Messengerdienste aber nicht unternehmensintern betriebene Kommunikationssysteme zählen. Zudem ist unklar, ob der Anwendungsvorrang der DSGVO die TTDSG-Regelungen für OTT-Dienste verdrängt (vgl. Abschnitt 3.2.1.2.1). Allerdings sind diese Fragen höchst umstritten und aktuell noch nicht abschließend gerichtlich geklärt.

> § 3 Abs. 2 S. 1 TTDSG
>
> Den [..] Verpflichteten ist es untersagt, sich oder anderen über das für die Erbringung der Telekommunikationsdienste oder für den Betrieb ihrer Telekommunikationsnetze oder ihrer Telekommunikationsanlagen einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder von den näheren Umständen der Telekommunikation zu verschaffen.

Diese Regelung entspricht dem bisherigen Kenntnisnahmeverbot in § 88 TKG.[876] Allerdings war bereits nach der alten Rechtslage unklar, welche Maßnahmen als Erforderlich einzustufen waren. [877] Weit bedeutender im Beschäftigungskontext ist die zweckgebundene Kenntnisnahme: diese ist auf den TK-Betrieb fokussiert.

Mit dieser Regelung wird deutlich, dass mit den Verpflichteten nicht (auch) ein an einem Kommunikationsprozess als Absender oder Rezipient beteiligtes Unternehmen gemeint sein kann, sondern vielmehr die Stelle, welche die Nachrichten*übermittlung anbietet.* Empfangen oder senden Beschäftigte Nachrichten im Namen des Unternehmens, ist eine Kenntnisnahme bezweckt. Dies wäre zwar bei der viel diskutierten privaten Nutzung anders gelagert. Allerdings gilt zu bedenken, dass privat und beruflich – insbesondere bei Heimarbeit – oft kaum trennbar sind. Auch in Chat-Gruppen mit überwiegend privatem Charakter können leitende

[872] OLG Düsseldorf, Urteil vom 07.06.2006 – I-15 U 21/06, Rn. 27; *Konferenz der Justizministerinnen und Justizminister der Länder*, Digitaler Neustart, S. 314; *Schmitz*, JIPITEC 2013, 190 (193); *Kersten*, JuS 2017, 193 (195 f); *Kluge*, K&R 2017, 230 (233); *Stadler*, ZD 2011, 57 (58); *Müller-Broich,* in: TMG, § 13 Rn. 10; vgl. auch Hanseatisches Oberlandesgericht Hamburg, Urteil vom 04.02.2009 – 5 U 180/07 – Long Island Ice Tea, Rn. 53.

[873] *Fritsch u. a.*, DuD 2005, 592 (592); *Schnabel/Freund*, CR 2010, 718 (720); *Caspar*, ZRP 2015, 233 (234); vgl. auch LG München I, Urteil vom 03. Juli 2013 – 25 O 23782/12 –, Rn. 42.

[874] Vgl. auch die Forderungen im Gesetzgebungsverfahren „anonym" als ohnehin nicht erreichbar zu streichen: *Benedikt*, Stellungnahme vom 21.04.2021, Ausschussdrucksache 19(9)1042, S. 3; *Schwartmann* Stellungnahme vom 21.04.2021, Ausschussdrucksache 19(9)1043, S. 3; *Schwartmann u. a.*, MMR 2021, 99 (100); a.A. *Engeler*, Stellungnahme vom 21.04.2021, Ausschussdrucksache S. 11.

[875] Vgl. *Wagner*, Datenökonomie und Selbstdatenschutz, S. 506 ff.; ähnlich wohl: *Schwartmann u. a.*, MMR 2021, 99 (100).

[876] Zur alten Rechtslage: *Bock,* in: Geppert/Schütz - TKG, § 88 Rn. 26.

[877] *Bock,* in: Geppert/Schütz - TKG, § 88 Rn. 26.

Angestellte, welche als Unternehmensvertreter*innen zu werten sind, beteiligt sein. Werden hingegen Beschäftigten Räume mit vertraulichem Charakter eröffnet, sollte vorsorglich eine klare Trennung zu den betrieblichen Foren vorgenommen werden. Einblicke in diese privaten Räume wären im Zweifel strikt untersagt.

Verpflichtete dürfen zudem nach § 3 Abs. 2 S. 2 TTDSG Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. „Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 StGB hat Vorrang." Hierin liegt eine sehr strenge Umsetzung des Zweckbindungsrundsatzes. Fraglich wäre, ob Art. 6 Abs. 4 DSGVO eine solche „andere gesetzliche Vorschrift" wäre. Diese Frage soll im Rahmen dieser Studie dahingestellt bleiben.

Umgang mit Verkehrsdaten: Im Rahmen des § 9 Abs. 1 TTDSG dürfen Verkehrsdaten nur zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist, verarbeitet werden.

Im Prinzip liegt hierin eine konkretisierende Umsetzung eines streng verstandenen Erforderlichkeitsprinzips, welcher auch bei der Datenverarbeitung zur Vertragserfüllung besteht (vgl. Abschnitt 2.4.1.2.2.1). Klargestellt wird, dass für die Umsetzung von TK-Diensten erforderliche Daten nur im hierfür erforderlichen Maß verarbeitet werden dürfen und danach unverzüglich – also ohne schuldhaftes Zögern – zu löschen sind.

Werden weitere Zwecke wie die Vermarktung von Telekommunikationsdiensten, die bedarfsgerechte Gestaltung von Telekommunikationsdiensten oder die Bereitstellung von Diensten mit Zusatznutzen verfolgt, müssen die Daten anonymisiert werden oder es bedarf einer gesonderten Einwilligung (§ 9 Abs. 2 TTDSG). Kommt man zur Anwendbarkeit dieser Regelung, wäre ein Rückgriff auf die Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO ausgeschlossen.

Umgang mit Standortdaten: Aufgrund der besonderen Datenschutzrisiken, welche über die Erstellung von Bewegungsprofilen entstehen können, unterliegen TK-Dienste sehr strengen Anforderungen bei der Verarbeitung von Standortdaten: entweder dürfen diese als Verkehrsdaten nach § 9 TTDSG verarbeitet werden, wurden zuvor anonymisiert oder es liegt eine Einwilligung vor. Für Telemedien gilt hingegen nach § 19 Abs. 2 TTDSG die Anonymisierungspflicht nur unter dem Vorbehalt technischer Möglichkeit und Zumutbarkeit. Dies deutet auf unterschiedliche Schutzniveaus hin. § 13 TTDSG scheint seinen Anwendungsbereich allerdings auf die Bereitstellung von „Diensten mit Zusatznutzen" i.S.d. § 2 Abs. 2 Nr. 5 TTDSG zu beschränken. Gemäß EG 18 der ePrivacy-RL können dies bspw. die Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersage oder touristische Informationen umfassen. Ist der Messengerdienst als TK-Dienst einzustufen und möchte derartige Zusatzdienste anbieten, wäre dies folglich problematisch. Ob die Regelung auch für Unternehmen als Arbeitgeber einschlägig wäre, bleibt fraglich.

Unter beiden Regimen müssen sich Unternehmen die Frage stellen, ob die Verarbeitung von Standortdaten erforderlich ist. Sofern sich eine Notwendigkeit aus dem Einsatzzweck ergibt, ist zu klären, ob eine Anzeige der genauen Standorte, Schätzungen oder andere datenschutzfreundliche Gestaltungen zielführend sind: so könnte es ausreichen, bei mobilen Beschäftigten die Nähe bzw. Distanz zum anvisierten Einsatzort in Kilometer und/oder Fahrtzeit zu verwenden, um eine effiziente Zuteilung zu erreichen. Bei der Organisation von Gruppen von Beschäftigten können aggregierte Anzeigeformen gewählt werden. Von entscheidender Relevant ist auch die Frage, gegenüber welchen Personen im oder außerhalb des Unternehmens Standortdaten angezeigt werden sollen. Insgesamt gilt der Grundsatz: je weniger Personen über genaue Standorte der betroffenen Personen informiert sind, desto geringer fallen die Datenschutzrisiken aus.

Praxistipp:

(1) Die Rechtslage bezüglich der Einordnung von Unternehmen als TK-Dienstanbieter gegenüber ihren Beschäftigten ist unsicher. Dies betrifft auch das Zusammenspiel zwischen DSGVO und TTDSG. Deshalb sollten Unternehmen bei der Nutzung oder dem Betrieb von Messengerlösungen (internen wie externen) im Zweifel auch einen Nachweis der Umsetzung der spezifischen Pflichten für Telekommunikationsdienstanbieter und Telemediendienstanbieter führen können.

(2) Bei der Auswahl von Diensten bzw. Software sollte daher darauf geachtet werden, dass diese einen strengen Datenminimierungsansatz verfolgen:
   a. Ermöglichung anonymer oder pseudonymer Nutzung (ggü. Dritten)
   b. Ausschluss zweckändernder Weiterverarbeitung
   c. Minimierung der Datenerhebung auf das zwingend notwendige Maß
   d. Unverzügliche Datenlöschung (sofern nicht bewusst archiviert)
   e. Keine Erhebung von Standortdaten

3.2.3.2 Datensicherheitsanforderungen nach TTDSG

Ungeachtet der Unsicherheit bezüglich des Anwendungsbereichs des TTDSG sollen an dieser Stelle auch die Regelungen des TTDSG im Hinblick auf Datensicherheit vorgestellt werden.

Technische und organisatorische Vorkehrungen bei Telemedien: Die Datensicherheit bei Telemedien regelt § 19 Abs. 4 TTDSG. Diese Norm entspricht dem früheren § 13 Abs. 7 TMG und richtet sich an „Anbieter von Telemedien“. Hinzu kommt die Einschränkung für „*geschäftsmäßig* angebotene Telemedien“. Insofern ist wiederum der Streit relevant, ob auch Arbeitgeber geschäftsmäßige Anbieter sind, was im Rahmen dieser Studie verneint wird (Abschnitt 3.2.1.4).

Ohnehin kommt es zu einem gewissen Gleichlauf mit Art. 32 DSGVO: beide Regelungen fordern die Berücksichtigung des Stands der Technik und nennen als Beispiel die Verschlüsselung. Dass eine Verschlüsselung nur dann als TOM in Betracht kommt, wenn sie „als sicher anerkannt“ ist, bedarf wohl keiner näheren Begründung. Mit der wirtschaftlichen Zumutbarkeit werden die Implementierungskosten mit einbezogen. Gemäß § 7d BSIG kann das Bundesamt für Sicherheit in der Informationstechnik (BSI) in begründeten Einzelfällen zur Abwehr konkreter erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von Telemedienangeboten ausgehen und welche unzureichend gesichert sind, Anordnungen gegenüber den jeweiligen Dienstanbietern treffen.

---

§ 19 Abs. 4 TTDSG

Anbieter von Telemedien haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen

> Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass
>
> 1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
> 2. diese gesichert sind gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind.
>
> Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Vorkehrung nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens. Anordnungen des Bundesamtes für Sicherheit in der Informationstechnik nach § 7d Satz 1 BSI-Gesetz bleiben unberührt.

Umgang mit Fehlübermittlungen: Gemäß § 6 Abs. 2 TTDSG haben nach § 3 Abs. 2 S. 1 Nr. 1 und 2 TTDSG Verpflichtete (Anbieter / Mitwirkende bei *öffentlich zugänglichen* / *geschäftsmäßig* angebotenen TK-Diensten) die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um Fehlübermittlungen und das unbefugte Offenbaren von Nachrichteninhalten innerhalb des Unternehmens des Anbieters und an Dritte auszuschließen.

> Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Soweit es im Hinblick auf den angestrebten Schutzzweck erforderlich ist, sind die Maßnahmen dem jeweiligen Stand der Technik anzupassen.

§ 6 TTDSG führt § 107 TKG fort. Messengerdienste, welche § 6 Abs. 2 TTDSG erfüllen, dürften gleichzeitig auch Art. 32 DSGVO entsprechen.

Insgesamt ist davon auszugehen, dass solche Messengerdienste, welche die Anforderungen des Art. 32 DSGVO bestmöglich umsetzen, nicht in Konflikt mit §§ 6 Abs. 2 und/oder 19 Abs. 4 TTDSG geraten werden und damit Haftungsrisiken von vorneherein abgewendet werden können – unabhängig davon, ob diese Normen im Einzelfall anwendbar sind. Lediglich bei einem Verstoß könnte es insoweit fraglich werden, unter welchem Regime Sanktionen bzw. Bußgelder verhängt werden.

3.2.4 Weitere Neuerungen des TTDSG

An dieser Stelle sollen nun weiter Regelungen vorgestellt werden, welche für die elektronische Kommunikation insgesamt von Interessen sein können.

3.2.4.1 Die Cookie-Regelung

Ein dringender Anlass zur Schaffung nationaler Regelungen für die Zwischenperiode zur ePrivacy-VO lag in der nicht ausreichend umgesetzten Regelung zu Art. 5 Abs. 3 ePrivacy-RL. Diese wird gern als „Cookie-Regelung“ bezeichnet, erfasst aber generell die Speicherung von Informationen in Endeinrichtungen.

> **§ 25 Abs. 1 S. 1 TTDSG**
>
> Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der

> Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat.

Information und Einwilligung richten sich nach der DSGVO (§ 25 Abs. 1 S. 2 TTDSG). Ausnahmen vom Einwilligungserfordernis gewährt § 25 Abs. 2 TTDSG für:

- Den alleinigen Zweck der Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz.
- Die unbedingte Erforderlichkeit, damit der Anbieter eines Telemediendienstes einen vom Nutzenden ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

Die Regelung greift unabhängig vom Personenbezug.[878] Die Umsetzung der sog. „Cookie-Banner" stand immer wieder in der Kritik, sodass nun Aufsichtsbehörden wie in Berlin Aktionen starten, um gegen intransparente Einwilligungsabfragen vorzugehen.[879] Bei der Gestaltung von Einwilligungserklärungen sollte beachtet werden, dass die Ablehnung der Datenverarbeitung genauso leicht sein muss, wie die Zustimmung. Diese darf nicht aufwendiger gestaltet sein (insbesondere durch sog. „Dark Patterns"), versteckt oder eingebettet in unvollständige oder missverständliche Angaben und Beschriftungen.[880]

3.2.4.2 Personal Information Management Systems (PIMS)

Nach § 25 TTDSG erteilte Einwilligungen können künftig durch unabhängige Stellen verwaltet werden. Die Anforderung an solche Stellen, wie bspw. Treuhandstellen, sind in § 26 Abs. 1 TTDSG geregelt. Konkretisierende Anforderungen sollen durch eine Rechtsverordnung nach § 26 Abs. 2 TTDSG zusätzlich geschaffen werden. Die Frage, ob und wie solche Intermediäre gesetzlich vorgesehen werden sollten, war eine im Gesetzgebungsverfahren höchst umstrittene Position.[881] Für den in dieser Studie spezifisch betrachteten Fall des Messengereinsatz im Unternehmenskontext ist derzeit noch nicht ersichtlich, ob PIMS eine größere Bedeutung erlangen werden, sodass die Erwähnung an dieser Stelle nicht weiter vertieft werden soll.

3.3 Zwischenergebnis

Der Versuch des deutschen Gesetzgebers, die mit der DSGVO entstandene Rechtsunsicherheit im Hinblick auf den telekommunikations- und telemedienrechtlichen Datenschutz zu beheben, kann als misslungen bezeichnet werden. Aktuell gehen die Autor*innen dieser Studie davon aus, dass der deutsche Gesetzgeber seinen Regelungsspielraum überschritten hat, Teile der Regelungen damit weiterhin europarechtswidrig sind und aufgrund des Vorrangs des Europarechts nicht anwendbar sind.[882] Nichtsdestotrotz wurden diese im Rahmen der Rechtsgrundlagen, Datenminimierung und Datensicherheit vorgestellt, um einen Vergleich der datenschutzrechtlichen Pflichten des TTDSG und der DSGVO ziehen zu können. Dies bietet einen Überblick,

[878] *Schwartmann u. a.*, MMR 2021, 99 (100).
[879] *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Pressemitteilung, vom 09.08.2021, abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210809-PM-Tracking-de.pdf [letzter Abruf 10.08.2021].
[880] *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Pressemitteilung, vom 09.08.2021, abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210809-PM-Tracking-de.pdf [letzter Abruf 10.08.2021].
[881] *Benedikt*, Stellungnahme vom 21.04.2021, Ausschussdrucksache 19(9)1042, S. 6; *Schwartmann*, Stellungnahme vom 21.04.2021, Ausschussdrucksache 19(9)1043, S. 6 ff.; *Richter*, Stellungnahme vom 20.04.2021, Ausschussdrucksache 19(9)1045; S. 2 ff.; *Engeler*, Stellungnahme vom 21.04.2021, Ausschussdrucksache 19(9)1056, S. 3; *Schwartmann u. a.*, MMR 2021, 99 (101).
[882] *Assion,* Stellungnahme als Sachverständiger zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG), BT-Drucksache 19/27441, Ausschussdrucksache 19(9)1039, S. 4 ff.

wann Rechtsunsicherheit durch Auswahl geeigneter Lösungen in praktischer Hinsicht dergestalt begegnet werden kann, indem vorsorglich die Pflichten des TTDSG miterfüllt werden.

4 Chancen und Risiken von Messengerdiensten in der Unternehmenskommunikation

Nachdem die Grundlagen der Datenverarbeitung unter Berücksichtigung der Besonderheiten des Beschäftigungsverhältnisses aufgefächert wurden, erfolgt nun die Ableitung konkreter Schlussfolgerungen mit besonderer Relevanz für den Einsatz von Messengerdiensten in der Unternehmenskommunikation. Hierfür wird zunächst ein Blick auf die allgemeine Datenschutzsituation bei Messengerdiensten mit praktischen Beispielen geworfen, wobei über die bereits in Kapitel 2 vorgestellten Datenschutzgrundprinzipien und allgemeinen Anforderungen hinaus nun der Fokus auf spezifischen Fragen des technischen Datenschutzes, der Datensicherheit sowie der Transparenz liegt. Als eine besondere Herausforderung bilden die rechtlichen Implikationen beim Einsatz international operierender Messenger einen weiteren Schwerpunkt dieses Abschnitts.

4.1 Datenschutz bei Messengerdiensten

Für die Auswahl einer Kommunikationslösung sind neben praktischen Erwägungen, wie erforderlicher Funktionsumfang und Bedienungsfreundlichkeit, die rechtlichen Dimensionen insbesondere im Hinblick auf Datensicherheit und Datenminimierung relevant, welche durch die konkrete technische Ausgestaltung der Datenverarbeitung bedingt sind. Der gesetzlich gebotene Schutz personenbezogener Daten im Zuge der Übermittlung von Nachrichten erstreckt sich dabei sowohl auf die personenbezogenen Kommunikationsinhalte als auch die Umstände der Kommunikation (Metadaten), soweit sich aus letzteren Informationen über natürliche Personen ableiten lassen.[883] Im Folgenden sollen Besonderheiten dieser Datenkategorien nichtsdestotrotz getrennt betrachtet werden. Als weitere wesentliche Entscheidungsparameter für den Einsatz eines Messengerdienstes im Unternehmenskontext sollten die Transparenz bezüglich der Datenverarbeitung sowie die Nutzungsbedingungen einbezogen werden.

4.1.1 Anwendbarkeit der DSGVO

Personenbezug: Wie in Abschnitt 2.3.1.2 dargelegt, liegen bei der Verarbeitung von Kommunikationsinhalten sowie Metadaten regelmäßig personenbezogene Daten vor.

Automatische Verarbeitung: Im Kontext von Messengerdiensten müsste eine automatisierte oder zumindest teilautomatisierte Verarbeitung angenommen werden. Der Hauptzweck des Messengerdienstes liegt in der Zustellung von Nachrichten in Echtzeit, ggf. verbunden mit einer Zwischenspeicherung auf eigenen Servern. Bei vielen Messengerdiensten kann der Dienstanbieter zudem auf die im Adressbuch bzw. Kontaktverzeichnis des Nutzenden gespeicherten Kontakte zugreifen, um zu überprüfen, welche Kontakte des Nutzenden bereits bei dem entsprechenden Dienst registriert sind. Die dadurch gewonnenen personenbezogenen Daten werden dann ggf. anschließend weiterverarbeitet. Allein dadurch liegt schon die automatisierte Verarbeitung personenbezogener Daten vor.

Ausnahmen (Haushaltsprivileg): Die Anwendbarkeit der DSGVO wäre ausgeschlossen, wenn eine Ausnahme wie bspw. das Haushaltsprivileg eingreift (siehe Abschnitt 2.3.1.5). Explizit hervorgehoben wird im

[883] Zum vergleichbaren Fall der E-Mail-Kommunikation: *DSK - Datenschutzkonferenz*, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, S. 2 ff.

Hinblick auf nicht von der DSGVO erfasste Sachverhalte der rein privaten und/oder familiären Tätigkeit in EG 18 S. 2 DSGVO die Nutzung sozialer Netzwerke.[884] Handelt es sich um reine private und/oder familiäre Kontakte des Netzwerknutzenden, greift hier die Haushaltsausnahme und hat dann zur Rechtsfolge, dass die DSGVO im Verhältnis zwischen den Privatpersonen keine Anwendung findet. Bei einigen Messengerdiensten wird der Zugriff auf die im Kontaktverzeichnis des Nutzenden gespeicherten Daten eingeräumt. Allerdings ist darauf zu achten, dass sich der Betreiber eines solchen Messengerdienstes laut EG 18 Satz 3 DSGVO hingegen nicht auf die Haushaltsausnahme berufen kann, auch wenn die Messengernutzung aus der Perspektive der Nutzenden eine rein private Tätigkeit betrifft.[885]

Erwägungsgrund 18 S. 3 DSGVO

Diese Verordnung gilt jedoch für die Verantwortlichen oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen.

Damit das Haushaltsprivileg nicht leerläuft, wird folgende Abgrenzung vorgeschlagen: Die Nutzenden unterfallen der DSGVO hinsichtlich der von ihnen erhobenen und übermittelten personenbezogenen Daten nicht, selbst bei Weitergabe an den Dienstanbieter.[886] Die DSGVO ist aber auf die Verarbeitung dieser Daten durch den Dienstanbieter anzuwenden.[887]

Befinden sich im Kontaktverzeichnis des Nutzenden sowohl private als auch berufliche, oder nur berufliche Kontaktdaten (zum Beispiel von Kunden, Lieferanten, eigenen und fremden Beschäftigten sowie sonstigen Ansprechpartner*innen), ist die Lage anders zu beurteilen, da die Haushaltsausnahme dann nicht mehr greift.[888] Die DSGVO findet dann im dienstlichen Kontext Anwendung bei allen Beziehungen mit den Betroffenen.[889]

Messenger	WhatsApp	Facebook Messenger	MS Teams	Signal	Wickr	Telegram	Threema	Wire	Skype	ginlo	stashcat	Teamwire
Hauptsitz	USA					Dubai, VAE	Schweiz		Luxemburg	Deutschland		
EU-Niederlassung	Irland			-	-	-	-	-				

Tabelle 9 Niederlassungen bekannter Messengerdienste (Auswahl)

[884] Dagegen entschied der EuGH noch zur alten Rechtslage, dass eine Veröffentlichung im Internet, bei der die veröffentlichten Daten einer unbegrenzten Zahl von Personen verfügbar gemacht werden, „offensichtlich“ nicht der Haushaltsausnahme unterfalle: EuGH, Urteil vom 6.11.2003 - Rs. C-101/01 Lindqvist/Schweden, Rn. 47.
[885] Bei der privaten Nutzung von Firmengeräten siehe: *Jung/Hansch*, ZD 2019, 143 (145).
[886] *Bäcker,* in: BeckOK DatenschutzR Art. 2 Rn. 22.
[887] *Bäcker,* in: BeckOK DatenschutzR Art. 2 Rn. 22.
[888] Für eine Beurteilung nach dem Schwerpunkt: *Gola/Lepperhoff*, ZD 2016, 9 (10).
[889] *Faas*, ArbRAktuell 2018, 594 (595); *Jung/Hansch*, ZD 2019, 143 (145); *Piltz*, K&R 2016, 557 (558).

Räumliche Anwendbarkeit: Mit dem Blick auf den Sitz der derzeit dominierenden Messengerdienste am Markt, ist zu erkennen, dass die Mehrheit der Dienstanbieter ihren (Haupt-)Sitz nicht in der EU hat. Im Hinblick auf die typische Tätigkeit von Messengerdiensten spielt dies allerdings keine Rolle bezüglich der Anwendbarkeit der DSGVO. Aufgrund der Erweiterung des Sitzlandprinzips um das Marktortprinzip bestehen keine Bedenken bezüglich der räumlichen Anwendung. Aus diesem Grund spielt es keine Rolle, ob der Anbieter eines Messengerdienstes seinen Sitz in der Schweiz, in den USA oder in einem anderen Land der Welt hat. Sobald sich die Dienste auch an natürliche Personen richten, die sich in der Union befinden, gelten die Regelungen der DSGVO weiterhin für deren Verarbeitung personenbezogener Daten.

4.1.2 Schutz der Kommunikationsinhalte und Umsetzung des Prinzips der Datensicherheit

Der Inhalt der Nachrichten und damit das Sensibilitäts- und Vertraulichkeitsbedürfnis, wird durch die betroffene Person bzw. den Nutzenden der Anwendung bestimmt. Um Datenschutzrisiken zu vermeiden, indem der Dienstanbieter keinen Zugang zu personenbezogenen Daten erhält, können Verschlüsselungslösungen zum Einsatz kommen, über die auch die Sicherheit der Daten gewährleistet werden. Mittlerweile bieten die Mehrzahl der Messenger standardmäßig eine Ende-zu-Ende-Verschlüsslung für vertrauliche Kommunikation an, die gewährleistet, dass weder der Messenger noch Dritte auf Chat-Inhalte zugreifen können.[890] Da einige Messengerdienste auch Video-Calls ermöglichen, bietet die Orientierungshilfe der DSK zu Videokonferenzsystemen relevante Anhaltspunkte. Im Vergleich zu Messengern stellte die DSK allerdings fest, dass zum Zeitpunkt der Erstellung des Papiers kaum Konferenzsysteme mit Ende-zu-Ende-Verschlüsselung marktgängig waren. Wird nur eine Transportverschlüsselung bereitgestellt, verlangt die DSK weitere kompensierende Schutzmaßnahmen.[891]

DSK, Orientierungshilfe Videokonferenzsysteme

Videokonferenzsysteme müssen eine Verschlüsselung nach dem Stand der Technik implementieren, hierzu zählen:

- mindestens Transportverschlüsselung
- ggf. Ende-zu-Ende-Verschlüsselung
- Verschlüsselung gespeicherter Daten

„Eine wirksame Ende-zu-Ende-Verschlüsselung setzt voraus, dass die Endgeräte der Teilnehmenden sich gegenseitig nachprüfbar authentisieren und für jede Konferenz neue flüchtige Verschlüsselungsschlüssel unter Kontrolle der Konferenzteilnehmer so erzeugt, ausgehandelt bzw. verteilt werden, dass dem Betreiber keine Kenntnisnahme des Schlüsselmaterials möglich ist.“

[890] Bereits: *Schrey u. a.*, MMR 2017, 736 (737).
[891] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 19.

In Tabelle 10 werden Informationen und Besonderheiten aus den Datenschutzerklärungen sowie Untersuchungen von dritter Seite zusammengetragen. Eine Untersuchung, inwieweit die technischen Angaben tatsächlich effektiv umgesetzt wurden oder zur Sicherheit der einzelnen Verschlüsslungsverfahren, konnte im Rahmen dieser Studie nicht durchgeführt werden. Insofern ist aber hervorzuheben, wenn Anbieter ihre Produkte durch Dritte, wie bspw. Sicherheitsforscher*innen untersuchen lassen und dies öffentlich dokumentieren. Zum Vergleich werden zunächst 4 international bekannte Messengerdienste präsentiert, die sich vorallem im Rahmen der Privatnutzung etabliert haben. Diese werden 5 Anbietern gegenübergestellt, die sich auch bzw. nur auf die Nutzung im Unternehmenskontext spezialisiert haben und aus dem europäischen Raum heraus angeboten werden.

	Transportverschlüsselung	Ende-zu-Ende-Verschlüsselung (E2EE)	Lokale Nachrichtenverschlüsselung	Speicherort	Externe Sicherheitsaudits
Beispiele für Messenger mit Fokus auf Privatnutzung					
Facebook Messenger	Nicht bekannt	X Aktivierbar für geheime Unterhaltungen, nicht bei Gruppenchats[892]	Nicht bekannt	Nicht bekannt	Nicht bekannt
Signal	✓ überprüfbar, da Quellcode öffentlich zugänglich auf GitHub[893]	✓ Signal-Protokoll (ehemals Axolotl-Protokoll) mit Perfect Forward Secrecy (PFS), von WhatsApp, Wire übernommen[894]	✓	Lokal, auf Servern, wenn Nachrichten unzustellbar[895]	✓ Letzter Audit 2017[896]
Telegram	✓	nur Einzelchats (optional) über das MTProto 2.0-Protokoll[897]	X	Cloud (außer geheime Chats)[898]	Letzter Audit 2017[899]
WhatsApp WhatsApp	✓ dokumentiert im Whitepaper[900]	+/- Signal-Protokoll (nicht prüfbar)[901] aber Backupdaten in	+/-, ja aber bei Backups lokal und in Cloud,	i.d.R. lokal, 30 Tage auf Servern, wenn Nachricht	Sicherheitsmeldungen veröffentlicht

[892] *Verbraucherzentrale,* WhatsApp-Alternativen: Messenger im Überblick, Stand 31.05.2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055 [letzter Abruf 06.07.2021].
[893] Zwischenzeitlich wohl aktuelle Produktivversion nicht öffentlich verfügbar: *Kuketz,* Signal: Server-Sourcecode auf GitHub älter als 9 Monate, Stand 26.01.2021, abrufbar unter https://www.kuketz-blog.de/signal-server-sourcecode-auf-github-aelter-als-9-monate/; mittlerweile aber regelmäßige Releases: https://github.com/signalapp/Signal-Server/releases [letzter Abruf 01.09.2021].
[894] *Kuketz,* Signal: Hohe Sicherheit und Zero-Knowledge-Prinzip – Messenger Teil9, 08.12.2020, in: Kuketz IT-Security Blog, https://www.kuketz-blog.de/signal-hohe-sicherheit-und-zero-knowledge-prinzip-messenger-teil9/ [letzter Abruf 30.07.2021].
[895] https://signal.org/legal/#privacy-policy [letzter Zugriff 28.07.2021].
[896] *Kuketz,* Messenger Stand: 15.06.2021, https://www.messenger-matrix.de/messenger-matrix.html [letzter Abruf 18.08.2021].
[897] *Kuketz,* Messenger Stand: 15.06.2021, https://www.messenger-matrix.de/messenger-matrix.html [letzter Abruf 18.08.2021]. Eine ausführliche Beschreibung der Technik findet sich unter: https://core.telegram.org/techfaq [letzter Abruf 18.08.2021].
[898] *Kuketz,* Messenger Stand: 15.06.2021, https://www.messenger-matrix.de/messenger-matrix.html [letzter Abruf 18.08.2021].
[899] Laut *Kuketz,* Messenger Stand: 15.06.2021, https://www.messenger-matrix.de/messenger-matrix.html [letzter Abruf 18.08.2021]. Der Sicherheitsaudit selbst konnte nicht gefunden werden.
[900] WhatsApp Encryption Overview Technical white paper, Version 3 Updated October 22, 2020 abrufbar unter: https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-5&_nc_sid=2fbf2a&_nc_ohc=u59c-vv-H4cAX9tRFR1&_nc_ht=scontent.whatsapp.net&oh=075fbd2236fb0ab6417ec5d78fe249aa&oe=61220FD9 [letzter Abruf 18.08.2021].
[901] *Kuketz,* Messenger Stand: 15.06.2021, https://www.messenger-matrix.de/messenger-matrix.html [letzter Abruf 18.08.2021].

Business		Cloud nicht sicher verschlüsselt[902]	Schlüssel beim Anbieter[903]	unzustellbar	[904]
Beispiele für Messenger mit Angebot für Privatpersonen und Unternehmen					
ginlo (Privat)ginlo Business	✓ Hinweis zur Datensicherheit unklar[905]	✓	✓	Lokal, 90 Tage auf Servern, wenn Nachricht unzustellbar[906]	Nicht bekannt
Threema Threema Work	✓ dokumentiert im Whitepaper[907] und überprüfbar, da Quellcode öffentlich zugänglich auf GitHub	✓[908] Nutzt quelloffene Kryptobibliothek NaCl, die eine Verifikation der E2EE ermöglicht, [909] PFS auf dem Transport-layer sowie dem E2EE-Layer bei Sprach- und Videoanrufen	✓	Lokal, 14 Tage auf Servern, wenn Nachricht unzustellbar	✓ Letzter Audit 2019, 2020
Wire	✓	✓ Wire nutzt das Proteus-Protokoll, eine eigene Implementation des Signal-Protokolls[910]	✓	Lokal, temporär auf Server, wenn Nutzende offline, Speicherung von Log-Files für 72 Stunden	✓ Letzter Audit 2017, 2018
Beispiele für Messenger mit Fokus auf innerbetriebliche Kommunikation					
Stashcat	✓	Unklare Angaben: Wohl nicht standardmäßig,	Unklare Angaben: Datentrennung umgesetzt[911]	Servern, verschlüsselt in Deutschland	Sicherheits-meldungen veröffentlicht[912]

[902] *Rentrop,* WhatsApp-Datenschutz: Was zu beachten ist, in: heise online, Stand 24.08.2020, abrufbar unter: https://www.heise.de/tipps-tricks/WhatsApp-Datenschutz-Was-zu-beachten-ist-4422720.html [letzter Abruf 01.09.2021].
[903] *Kuketz,* Messenger Stand: 29.08.2021, https://www.messenger-matrix.de/messenger-matrix.html [letzter Abruf 01.09.2021].
[904] Sicherheitsmeldungen werden veröffentlicht unter: https://www.whatsapp.com/security/advisories/2021/ [letzter Abruf 18.08.2021].
[905] „In bestimmten Fällen werden Ihre persönlichen Daten während der Übertragung durch die Secure Socket Layer-Technologie (SSL) verschlüsselt […] Der Inhalt von E-Mail-Nachrichten kann von Dritten gelesen werden, Wir empfehlen Ihnen daher, uns vertrauliche Informationen nur auf dem Postweg zukommen zu lassen" Datenschutzerklärung (Stand Feb. 2020): https://app-help.ginlo.net/consumer/de/privacy/ [letzter Zugriff 28.07.2021].
[906] Datenschutzerklärung für ginlo Business (Stand Mai 2020) https://app-help.ginlo.net/business/de/privacy/ [letzter Zugriff 28.07.2021].
[907] Threema, Cryptography Whitepaper, Version: June 2021, abrufbar unter: https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf [letzter Abruf 30.07.2021].
[908] Unternehmen haben optionale Möglichkeit zur Erfüllung von Compliance-Anforderungen bei der Threema Work-Ersteinrichtung ein vorberechnetes Schlüsselpaar festzulegen: https://threema.ch/privacy_policy/index.php?lang=de&version=1k [letzter Abruf 18.08.2021].
[909] *Kuketz,* Threema: Instant-Messaging-Dienst aus der Schweiz – Messenger Teil2, 04.02.2020, in: Kuketz IT-Security Blog, https://www.kuketz-blog.de/threema-instant-messaging-dienst-aus-der-schweiz-messenger-teil2/ [letzter Abruf 30.07.2021]. Forward Secrecy wird dagegen auf dem Transportlayer umgesetzt: Threema, Cryptography Whitepaper, Version: June 2021, S. 14.
[910] *Kuketz,* Wire: Vertrauen verspielt – Messenger Teil4, 10.03.2020, in: Kuketz IT-Security Blog, https://www.kuketz-blog.de/wire-vertrauen-verspielt-messenger-teil4/ [letzter Abruf 30.07.2021]; Wire Swiss GmbH, Wire Security Whitepaper (Stand 19.07.2021), abrufbar unter: https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf [letzter Abruf 19.08.2021].
[911] Windelband/Ertel, Messenger im Gesundheitswesen – Teil 2 stashcat, in: Datenschutznotizen, abrufbar unter: https://www.datenschutz-notizen.de/messenger-im-gesundheitswesen-teil-2-stashcat-3625090/ [letzter Abruf 19.08.2021].
[912] Siehe zum Schwachstellenreport auch: CIPHRON, Advisory für StashCat vom 31. Juli 2017, https://www.ciphron.de/information-security/ciphron-lab-blog/ciph-2017-1-stashcat; Krempl, Polizeilicher Kryptomessenger mit Problemen, vom 28.05.2018, in: golem.de, https://www.golem.de/news/nimes-polizeilicher-kryptomessenger-mit-problemen-1805-134596.html [letzter Abruf 18.08.2021].

		Algorithmen und Protokoll nicht eindeutig dokumentiert			
Teamwire	✓	Unklare Angaben: Metadaten-Verschlüsselung	Unklare Angaben: Verschlüsselung von „Data-at-Rest“	auf den Servern verschlüsselt abgespeichert	Nicht gefunden

Tabelle 10 Datensicherheitsaspekte zum Schutz der Kommunikationsinhalte bei ausgewählten Beispielen von Messengerdiensten[913]

Im Hinblick auf die Dokumentation der Datensicherheitsmechanismen wurde folgendes festgestellt: Threema,[914] Wire[915] und WhatsApp[916] haben jeweils Whitepaper zu ihren kryptografischen Lösungen publiziert. Signals Protokolle wurden in der Wissenschaft besprochen. [917]

Einige Messenger haben selbst Audits durchführen lassen, bei denen gezielt nach Sicherheitslücken geforscht werden, und die Ergebnisse hierzu veröffentlicht. So ließ Threema 2019 ein Quellcode-Audit durch die FH Münster durchführen.[918] Im Jahr 2020 folgte ein Audit durch Cure53.[919] Auch bei Wire sind Überprüfungen einzelner Komponenten durch Kudelski Security und X41 D-Sec auf der Homepage abrufbar.[920] Beide Messenger bieten Kommunikationskanäle zur Meldung von Sicherheitslücken. Ein Nachweis der formalen bzw. kryptografischen Korrektheit des Signal-Protokolls erfolgten in den Jahren 2016 und 2017 durch internationale Forschungseinrichtungen.[921] Transparenz bietet auch andere Anbieter wie bspw. Stashcat durch die Veröffentlichung von Sicherheitsmeldungen.[922]

Verwirrend erscheint der Hinweis in der ginlo-Datenschutzerklärung für einen als sicher beworbenen Messengerdienst auf den Postweg zu verweisen. Für die bisher noch weniger bekannten Anwendungen stashcat und Teamwire lassen sich kaum unabhängige Informationen finden, sodass sich kaum nähere Aussagen machen lassen.

[913] Die Auswahl ist nach den folgenden Kriterien motiviert: Bekanntheitsgrad, Verortung in Europa und Datenschutzstandards sowie spezifische Fokussierung auf den Unternehmenskontext.
[914] Threema, Cryptography Whitepaper, Version: June 2021, abrufbar unter: https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf [letzter Abruf 30.07.2021].
[915] Wire Swiss GmbH, Wire Security Whitepaper, July 2021, abrufbar unter: https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf [letzter Abruf 30.07.2021].
[916] WhatsApp Encryption Overview Technical white paper, Version 3 Updated October 22, 2020 abrufbar unter: https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-5&_nc_sid=2fbf2a&_nc_ohc=u59c-vv-H4cAX9tRFR1&_nc_ht=scontent.whatsapp.net&oh=075fbd2236fb0ab6417ec5d78fe249aa&oe=61220FD9 [letzter Abruf 18.08.2021].
[917] *Cohn-Gordon u. a.*, Journal of Cryptology 2020, 1914; *Kobeissi u. a.*, Automated Verification for Secure Messaging Protocols and Their Implementations.; *Kuketz,* Signal: Hohe Sicherheit und Zero-Knowledge-Prinzip – Messenger Teil9, 08.12.2020, in: Kuketz IT-Security Blog, https://www.kuketz-blog.de/signal-hohe-sicherheit-und-zero-knowledge-prinzip-messenger-teil9/ [letzter Abruf 30.07.2021].
[918] *Ising/Poddebniak/Schinzel,* FH Münster, Security Audit Report Threema 2019, 2019-03-28, abrufbar unter: https://threema.ch/press-files/2_documentation/security_audit_report_threema_2019.pdf [letzter Abruf 30.07.2021].
[919] *Heiderich/Wege/Kean u.a.,* Cure53, Pentest- & Audit-Report Threema Mobile Apps 10.2020, abrufbar unter: https://threema.ch/press-files/2_documentation/security_audit_report_threema_2020.pdf [letzter Abruf 30.07.2021].
[920] Siehe https://wire.com/de/security/#audits [letzter Abruf 30.07.2021].
[921] *Cohn-Gordon u. a.*, Journal of Cryptology 2020, 1914; *Kobeissi u. a.*, Automated Verification for Secure Messaging Protocols and Their Implementations.; *Kuketz,* Signal: Hohe Sicherheit und Zero-Knowledge-Prinzip – Messenger Teil9, 08.12.2020, in: Kuketz IT-Security Blog, https://www.kuketz-blog.de/signal-hohe-sicherheit-und-zero-knowledge-prinzip-messenger-teil9/ [letzter Abruf 30.07.2021].
[922] https://stashcat.com/sicherheitsmeldungen/ [letzter Abruf 30.07.2021].

Negativ fällt die nicht standardmäßig eingestellte Verschlüsselung bei anderen Anbietern ins Gewicht. Die Erhebung der Verbraucherzentrale NRW zu Messengerdiensten ergab, dass mit Facebook-Messenger, Skype und Telegram drei sehr bekannte Messenger zwar eine Ende-zu-Ende-Verschlüsselung anbieten, allerdings nur aktivierbar durch den Nutzenden und nicht als voreingestellte Standardeinstellung.[923]

4.1.3 Schutz der Metadaten und Umsetzung des Prinzips der Datenminimierung

Im Kontext von Messengerdiensten kann das Prinzip der Datenminimierung umgesetzt werden, indem so wenig wie möglich personenbezogene Daten der Dienstnutzenden durch den Dienstbetreiber erfragt oder durch die Anwendung verarbeitet werden. Im Hinblick auf die datenschutzrechtliche Relevanz der Metadaten stellen sich zwei essentielle Weichenstellungen:

- Wie viele Daten sind zur Dienstnutzung erforderlich? Ist der Umfang auf das Mindestmaß beschränkt und sind nur nützliche Daten optional?
- Wie werden die Daten vom Dienstanbieter verarbeitet und insbesondere gespeichert? Welche Datensicherungsmechanismen werden ergriffen?

4.1.3.1 Umsetzung des Datenminimierungsgrundsatzes

Zunächst kann festgestellt werden, dass die Messengerdienste zur Registrierung unterschiedliche Daten verlangen. Bei einigen ist eine Mobiltelefonnummer und/oder eine E-Mail-Adresse erforderlich (vgl. Tabelle 11). Teilweise können Daten auch optional angegeben werden, um durch andere Nutzer*innen leichter auffindbar zu sein. Bei wenigen Anbietern, wie bspw. der schweizer Messenger-App Threema, erfolgt die Identifikation der Nutzer*in weder über E-Mail-Adresse noch über die Telefonnummer, sondern über eine zufällig erzeugte ID. Daraus wird geschlussfolgert, dass die Nutzung anonym ist (vgl. zu den Anforderungen der Anonymisierung: Abschnitt 2.3.1.2.3).[924] So gelangte die Verbraucherzentrale zur Einschätzung, dass Threema im Vergleich „der einzige Messenger, der vollkommen ohne personenbezogene Angaben einsatzfähig ist," sei.[925] Losgelöst von der Frage, ob der Einsatz einer ID eine anonyme oder (nur) pseudonyme Nutzung gewährleistet, ist dies aus Sicht des Datenminimierungsgrundsatzes sowie der datenschutzfreundlichen Technikgestaltung positiv zu bewerten. Dies betrifft nicht die anonyme oder pseudonyme Nutzbarkeit gegenüber anderen Nutzenden, sondern gegenüber dem App-Anbieter. Dagegen ziehen solche Anbieter Kritik auf sich, die Zugriff auf die Metadaten der Kommunikation (Absender*in, Empfänger*in, Zeitpunkt, Nachrichtengröße etc.) haben, insbesondere bei unverschlüsselter Speicherung im Rahmen von Cloud-Backups, unverschlüsselter Speicherung auf den jeweiligen Endgeräten und/oder die Speicherung von Nachrichten-Anhängen (wie z.B. Fotos, Videos) in der jeweiligen Smartphone-Mediathek. [926] Bei Letzterem könnten – je nach erteilten Berechtigungen – gegebenenfalls andere Apps Zugriff auf die Daten erhalten.[927]

---

[923] Verbraucherzentrale NRW, Datenschutz bei Messengern im Überblick, Stand 19.04.2021, abrufbar unter: https://www.verbraucherzentrale.de/sites/default/files/2021-04/Messenger-Vergleiche_Tabelle_2021_VZNRW.pdf [letzter Zugriff 30.07.2021].

[924] *Faas*, ArbRAktuell 2018, 594 (596). Verbraucherzentrale, WhatsApp-Alternativen: Messenger im Überblick, Stand 31.05.2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055 [letzter Abruf 06.07.2021].

[925] Verbraucherzentrale, WhatsApp-Alternativen: Messenger im Überblick, Stand 31.05.2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055 [letzter Abruf 06.07.2021]. Dem Vergleich gehörten der Facebook-Messenger, Ginlo, Signal, Skype, Telegram, Threema, WhatsApp und Wire an.

[926] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/ [letzter Zugriff 06.07.2021].

[927] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/ [letzter Zugriff 06.07.2021].

	Umfang der Datenerhebung	Schutzmaßnahmen
Beispiele für Messenger mit Fokus auf Privatnutzung		
Facebook Messenger	Erforderlich: Klarname,[928] zahlreiche Zugriffsberechtigungen[929] Optional: Profilbild Daten können zur Personalisierung genutzt werden.[930]	Keine eindeutigen Angaben
Signal	Erforderlich: Telefonnummer[931] und "Randomly generated authentication tokens, keys, push tokens, and other material that is necessary to establish calls and transmit messages"[932]	Optional können Adressbücher auf Signal-Kontakte geprüft werden, diese werden gehasht an Signal-Server übermittelt. Signal verfolgt das Zero-Knowledge-Prinzip: Der Betreiber hat keine Informationen darüber, wer mit wem wann kommuniziert.[933]
Telegram	Erforderlich: Telefonnummer, gewählter Name Optional: Profilbild, Benutzername (öffentlich), E-Mail-Adresse, Standort Bindet Tracker ein[934]	Bei Kontaktsynchronisation: Speicherung Telefonnummern, Vor- und Nachnamen von Kontakten aus Adressbuch auf Telegram-Servern[935]
WhatsApp WhatsApp Business	Erforderlich: Telefonnummer, Profilname, Nutzungs- und Protokollinformationen, Geräte- und Verbindungsdaten (inkl. IP-Adresse, Batteriestand, etc.); zzgl. Unternehmensinformationen bei Business-Account, Nutzungs-, Protokoll- und funktionale Informationen, Performance-, Diagnose- und Analyseinformationen Optional: Profilbild, Standort teilen, Statusinformationen, Sichtbarkeit einstellbar für Jeder, Meine Kontakte, Niemand	Hochladen von Kontakten mittlerweile optional, Verwaltung der Kontakte in einer Form „in der sichergestellt ist, dass solche Kontakte nicht identifiziert werden können" mithilfe kryptografischer Hash-Werte[937] zuvor noch als Klartext[938] Allerdings ist die Zustimmung zum Teilen der erhobenen Daten mit den Facebook-Unternehmen zur Weiterentwicklung eigener Dienste und Produkte laut Business Nutzungsbedingungen nicht ablehnbar.

[928] Zur Klarnamenpflicht: KG Berlin, Urteil vom 20.12.2019 - Az. 5 U 9/18; OLG München, Urteil vom 8.12.2020 – 18 U 2822/19.
[929] Verbraucherzentrale NRW, Facebook-Messenger umgehen: Nachrichten lesen ohne Zwangs-App, Stand 21.01.2021, https://www.verbraucherzentrale.nrw/wissen/digitale-welt/soziale-netzwerke/facebookmessenger-umgehen-nachrichten-lesen-ohne-zwangsapp-13735 [letzter Abruf 18.08.2021].
[930] Verbraucherzentrale, WhatsApp-Alternativen: Messenger im Überblick, Stand 31.05.2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055 [letzter Abruf 06.07.2021].
[931] *Kuketz,* Signal: Hohe Sicherheit und Zero-Knowledge-Prinzip – Messenger Teil9, 08.12.2020, in: Kuketz IT-Security Blog, https://www.kuketz-blog.de/signal-hohe-sicherheit-und-zero-knowledge-prinzip-messenger-teil9/ [letzter Abruf 30.07.2021].
[932] https://signal.org/legal/#privacy-policy [letzter Abruf 30.07.2021].
[933] *Kuketz,* Signal: Hohe Sicherheit und Zero-Knowledge-Prinzip – Messenger Teil9, 08.12.2020, in: Kuketz IT-Security Blog, https://www.kuketz-blog.de/signal-hohe-sicherheit-und-zero-knowledge-prinzip-messenger-teil9/ [letzter Abruf 30.07.2021].
[934] *Kuketz,* Messenger, Stand 29.08.2021, abrufbar unter: https://www.messenger-matrix.de/messenger-matrix.html; *Kuketz,* Telegram: »Sicherheit« gibt es nur auf Anfrage – Messenger Teil3, Stand 08.03.2020, abrufbar unter: https://www.kuketz-blog.de/telegram-sicherheit-gibt-es-nur-auf-anfrage-messenger-teil3/ [letzter Abruf 01.09.2021].
[935] Verbraucherzentrale, WhatsApp-Alternativen: Messenger im Überblick, Stand 31.05.2021, https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-messenger-im-ueberblick-13055 [letzter Abruf 06.07.2021].
[937] Beschrieben unter: https://faq.whatsapp.com/general/contacts/about-contact-upload [letzter Abruf 19.08.2021]. Allerdings besagt Punkt 7 „Deine Kundenkontakte" der Nutzungsbedingungen (Stand 29.10.2020): „Das Unternehmen stellt WhatsApp Kontaktinformationen wie Telefonnummern zu Verfügung („Kundendaten")".
[938] Kuketz, WhatsApp, Telegram, Signal: Großflächiger Missbrauch von Contact-Discovery möglich, Stand 21.04.2021, abrufbar unter: https://www.kuketz-blog.de/whatsapp-telegram-signal-grossflaechiger-missbrauch-von-contact-discovery-moeglich/ [letzter Abruf 01.09.2021].

	(Defaulteinstellung: Jeder)[936] ggf. Transaktions- und Zahlungsdaten	Zudem ist einem Datentransfer in die USA zuzustimmen[939]
Beispiele für Messenger mit Angebot für Privatpersonen und Unternehmen		
ginlo (Privat) ginlo Business	Erforderlich: Mobilnummer, achtstellige ginlo-ID Optional: Profilname, Profilbild; Telefonbuch-Kontaktabgleich, E-Mail-Adresse	Mobilnummer (sowie Telefonbuch-Kontakte, E-Mail-Adresse) gehascht auf ginlo-Server gespeichert,[940] Information an Kontakte; Verschlüsselte Speicherung Log-In-Daten und Kommunikationsdaten lokal
Threema Threema Work[941]	Erforderlich: Nutzername, Passwort, Threema-ID, öffentlicher Schlüssel, Datum (ohne Uhrzeit), Betriebssystem, App-Version Optional: Nickname, Mobilnummer, E-Mail-Adresse Profilbild, optional möglich: Standortfreigabe (ohne Bezug zu Threema-ID)	Neben Nachrichteninhalten auch Header-Informationen (Absender, Empfänger, etc.) verschlüsselt Optionaler Adressbuchabgleich: einwegverschlüsselt (gehasht), SSL-verschlüsselt temporär an Server übertragen und unmittelbar gelöscht
Wire[942]	Erforderlich: Name, Mobilnummer oder E-Mail-Adresse Ggf. zahlungsrelevante Daten zu Abrechnungszwecken	Optionaler Adressbuchabgleich: Telefonnummern gehasht, nur flüchtig verarbeitet; Anonyme Nutzungsstatistiken und Crash-Logs
Beispiele für Messenger mit Fokus auf innerbetriebliche Kommunikation		
Stashcat[943]	Erforderlich: Name, E-Mail-Adresse, Benutzerrolle, Kommunikationsdaten (inkl. Aktivität), Logfiles Optional: Profilbild, Standort	Server in „gesicherten Hochsicherheitsrechenzentrum“ (mit Ausnahme Übersetzungsdienst); Beschränkung ausschließlich auf firmeninterne / organisationsinterne Kommunikation
Teamwire[944]	Email-Adresse und Telefonnummer, weitere Daten „können“ verarbeitet werden u.a.: Klarname, Firma, Position, Benutzername/Passwort, Adressbuch, IP-Adresse, Mac-Adresse / UDID, Standort	Verschlüsselung, Anonymisierung „so weit wie möglich“, Hashfunktion Einweg-verschlüsselt; Beschränkung ausschließlich auf firmeninterne / organisationsinterne Kommunikation

Tabelle 11 Schutz der Metadaten bei Beispielen ausgewählter Messengerdienste

Schwierigkeiten bereitet die Informationsgewinnung beim Facebook-Messenger, welcher allerdings auch nicht auf den betrieblichen Kontext ausgerichtet ist. Wire gibt in seiner Datenschutzerklärung an, für die Verarbeitung von geschäftlichen Interessenten und Nutzern von geschäftlichen Konten auf Dienstleistungen von

[936] *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021, S. 7.
[939] WhatsApp, Business Nutzungsbedingungen (Stand 29.10.2020), https://www.whatsapp.com/legal/business-terms/?lang=de [letzter Abruf 18.08.2021].
[940] Ginlo Datenschutzerklärung, (Stand Mai 2020) https://app-help.ginlo.net/business/de/privacy/ [letzter Zugriff 28.07.2021]
[941] Threema Datenschutzerklärung (Stand: 01.09.2020), https://threema.ch/privacy_policy/index.php?lang=de&version=1k [letzter Abruf 18.08.2021].
[942] Wire Datenschutzerklärung (Stand 30.06.2020), abrufbar unter: https://wire.com/de/legal/#privacy [letzter Abruf 18.08.2021].
[943] Stashcat, Datenschutzerklärung für den Messenger-Dienst stashcat, abrufbar unter: https://stashcat.com/datenschutz-portal/ [letzter Abruf 18.08.2021].
[944] Datenschutz und Sicherheit von Teamwire, https://teamwire.eu/funktionen-sicherheit/ [letzter Abruf 18.08.2021].

Drittanbietern aus den USA zurückzugreifen.[945] Leider wird hier noch auf die Zertifizierung nach „Privacy Shield“ verwiesen, welches aber für ungültig erklärt wurde.[946] Auch stashcat bindet einen Dienstanbieter aus den USA ein und verweist auf dessen Schutzmaßnahmen.[947] Interessant ist die Angabe auf der Homepage von Teamwire, die ePrivacy-*Verordnung* umzusetzen[948] – dieser Messenger lebt bereits in der Zukunft. Anbieter, die mit der DSGVO-Konformität werben, sollten zudem in ihren Cookie-Bannern keine Dark Patterns oder Nudging einsetzen.

Auf Anfrage einer US-Staatsanwaltschaft teilte Signal mit, außer Account-Erstelldatum und letztem Zugriff auf keine weiteren Daten ihrer Nutzenden zugreifen zu können.[949] Allerdings legte eine Forschergruppe sowohl bei WhatsApp und Telegram als auch bei Signal schwerwiegende Datenschutzprobleme bei den derzeit eingesetzten Methoden zum Adressbuchabgleich auf.[950] So konnten bspw. mit Hilfe großformatiger Crawling-Attacken interessante cross-messenger Nutzungsstatistiken durchgeführt werden, die zeigen, dass Nutzende oftmals die Standardeinstellungen nicht ändern.[951] So stellten die Forschenden u. a. fest, dass ca. 42% Signal-User*innen und 46% Telegram-User*innen der untersuchten Profile aus dem Raum USA auch WhatsApp nutzen.[952] Dort präsentierten sich für Jedermann sichtbar fast 50% mit Profilbild und fast 90% mit Info-Text (vgl. die Defaulteinstellungen).[953] Nutzername und Profilbild bei Signal waren bei der Untersuchung hingegen verschlüsselt. [954] Dass der Missbrauch von Schwachstellen des Messengerdesigns beim Schutz von Metadaten für Betroffene weitreichende Konsequenzen haben kann, zeigte die Meldung, dass Telefonnummern Hongkonger Protestierender über die Adressbuchsynchronisation bei Telegram ermittelbar waren.[955]

4.1.3.2 Automatisches Auslesen des Adressbuchs

Einige Messengerdienste zeichnen sich dadurch aus, dass sie automatisch das Adressbuch des Smartphones auslesen. Ist dies nicht einmal durch die Nutzenden steuerbar, stellt es aus datenschutzrechtlicher Sicht den größten Kritikpunkt an solchen Diensten dar, insbesondere wenn eine regelmäßige Übertragung der Tele-

[945] Wire Datenschutzerklärung (Stand 30.06.2020), abrufbar unter: https://wire.com/de/legal/#privacy [letzter Abruf 18.08.2021].
[946] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II.
[947] Stashcat, Datenschutzerklärung für den Messenger-Dienst stashcat, abrufbar unter: https://stashcat.com/datenschutz-portal/ [letzter Abruf 18.08.2021]. Neben EU-Standardvertragsklauseln „hinaus werden ergänzende Garantien technischer, organisatorischer und vertraglicher Natur wie Verschlüsselung, Zugriffskontrollen und Zusicherungen der Benachrichtigung des Verantwortlichen im Fall der Anfrage einer Ermittlungsbehörde ebenfalls implementiert.“
[948] https://teamwire.eu/funktionen-sicherheit/ [letzter Zugriff 12.08.2021].
[949] Signal, Grand jury subpoena for Signal user data, Central District of California, 27.04.2021, https://signal.org/bigbrother/central-california-grand-jury/ [letzter Abruf 06.07.2021].
[950] *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021. Als Reaktion wurden von Signal und Facebook weitere Schutzmaßnahmen gegen Crawling implementiert – das Problem der sog. Enumeration Attacks im Hinblick auf die Kontaktsynchronisation sei aber nicht vollständig vermeidbar (vgl. *Hagen u.a.,* S. 13).
[951] *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021.
[952] *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021, S. 8.
[953] *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021, S. 8.
[954] *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021, S. 8.
[955] Berger, Telegram-Schwachstelle gefährdet Aktivisten in Hongkong, in: heise-online, Stand 28.08.2019, abrufbar unter: https://www.heise.de/newsticker/meldung/Telegram-Schwachstelle-gefaehrdert-Aktivisten-in-Hongkong-4508687.html [letzter Abruf 08.09.2021].

fonnummern aus dem Smartphone-Adressbuch an den Dienstanbieter erfolgt und dieser Vorgang undifferenziert nach Status des Telefonbucheintrags automatisch sämtliche Kontakte erfasst.[956] In der rechtswissenschaftlichen Literatur wurde dies bereits kritisch als „Zwangsvernetzung“ bezeichnet.[957] Zu den bereitgestellten Daten zählen sowohl die Telefonnummern anderer Messengerdienst-Nutzer*innen als auch sonstige Kontakte des Smartphone-Nutzenden, d.h. von Personen, die mit dem konkreten Messenger in keinerlei Verbindung stehen. [958]

In diesem Zusammenhang erzielte das Amtsgericht in Bad Hersfeld sehr viel Aufmerksamkeit, obwohl es sich zum einen nur um ein erstinstanzliches Urteil und zum anderen um ein familiengerichtliches Verfahren handelte.[959] Nichtsdestotrotz hatte das Urteil Sprengkraft mit praktischer Auswirkung.[960]

AG Bad Hersfeld, Beschluss vom 20.3.2017 – F 111/17 EASO

„Wer den Messenger-Dienst "WhatsApp" nutzt, übermittelt nach den technischen Vorgaben des Dienstes fortlaufend Daten in Klardaten-Form von allen in dem eigenen Smartphone-Adressbuch eingetragenen Kontaktpersonen an das hinter dem Dienst stehende Unternehmen. Wer durch seine Nutzung von "WhatsApp" diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden.“

Kritisiert wurde an dieser Entscheidung, dass die Einschätzung „fälschlicherweise“ den privaten Einsatz des Messengerdienst adressiert.[961] Diese Kritik zielt auf die Haushaltsausnahme nach Art. 2 Abs. 2 Buchst. c DSGVO ab, wonach das Datenschutzrecht nicht für ausschließlich persönliche oder familiäre Tätigkeiten anwendbar ist (siehe Abschnitte 2.3.1.5 und 4.1.1). Die Weitergabe von Daten an ein internationales Unternehmen könnte allerdings die Grenzen der Haushaltsausnahme sprengen. Zudem sind Unterlassungsansprüche nach Deliktsrecht möglich.

4.1.3.2.1 Verantwortlichkeit

Der Messengerdienstanbieter WhatsApp will die Verantwortung auf seine Nutzer*innen verlagern, indem diese mit der Anerkennung der Nutzungsbedingung bestätigen, zur Weitergabe der Daten autorisiert zu

[956] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/ [letzter Zugriff 06.07.2021].*Schrey u. a.*, MMR 2017, 736 (737); *Jung/Hansch*, ZD 2019, 143 (145); *Faas*, ArbRAktuell 2018, 594.
[957] *Faas*, ArbRAktuell 2018, 594 (594).
[958] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/[letzter Zugriff 06.07.2021]; *Faas*, ArbRAktuell 2018, 594 (594).
[959] AG Bad Hersfeld, Beschluss vom 20.3.2017 – F 111/17 EASO.
[960] Vgl. *Faas*, ArbRAktuell 2018, 594 (595).
[961] *Ulbricht,* in: Messenger Marketing, S. 75.

sein.[962] Datenschutzexpert*innen kritisieren allerdings, dass eine solche Abstimmung eher praxisfern ist. [963] Befürchtet wird, dass in der Mehrzahl der Fälle Daten ohne Kenntnis und Zustimmung betroffener Personen an WhatsApp übermittelt werden, sodass eine rechtskonforme Nutzung dieses Messengerdienstes nur mit einer Unterbindung der Datenübermittlung bspw. durch Einsatz von Selbstdatenschutzlösungen[964] möglich ist. [965] Für Unternehmen gilt zu bedenken, dass sie im Hinblick auf die beruflich geführten Adressbücher ihrer Beschäftigten, in denen personenbezogene Kontaktdaten bspw. von Kundschaft, Lieferanten, Kolleg*innen und Geschäftskontakten für Zwecke und mithilfe von Mitteln des Unternehmens verwaltet werden, Verantwortliche i.S.v. Art. 4 Nr. 7 DSGVO sind, sodass sie für die Weiterleitung dieser Daten an einen Dritten einer Rechtsgrundlage bedürfen.[966]

4.1.3.2.2 Mögliche Rechtsgrundlagen

Einwilligung: Im Messengerdienstkontext versuchen einige Dienstanbieter die Erteilung einer Einwilligung zur Weitergaben von personenbezogenen Daten der Nutzenden sowie von Dritten über ihre AGB bzw. Datenschutzerklärungen an die Installation der App zu koppeln, sodass der Zugriff auf das Adressbuch des Nutzenden eine Rechtsgrundlage hätte.[967] Abgesehen davon, dass es bisher gerichtlich noch nicht geklärt ist, ob eine solche Kopplung an die Möglichkeit einer Dienstnutzung in den AGB oder Datenschutzerklärungen als eine freiwillige sowie eindeutige bestätigende Einwilligungshandlung des Nutzenden einzuordnen ist, kann eine solche Einwilligung allenfalls die personenbezogenen Daten der Messengerdienstnutzenden selbst erfassen, nicht aber die personenbezogenen Daten anderer Kontakte im Adressbuch, welche die Messengerdienst-App nicht installiert haben und somit nicht nutzen. Die Einholung freiwillig, informiert und individuell zu erteilenden Einwilligungen sämtlicher betroffener Kommunikationspartner*innen in die Datenweitergabe ist gerade bei größeren beruflichen Datenbeständen meist illusorisch.[968] Allenfalls bei solchen Kontakten, die ihrerseits den gleichen Dienst nutzen oder eigeninitiativ über den Dienst kommunizieren, wäre über eine konkludente Einwilligung nachdenkbar. In der bloßen Offenbarung der Telefonnummer im geschäftlichen Verkehr lässt sich eine solche Einwilligung keinesfalls konstruieren.[969]

Berechtigtes Interesse: Im Rahmen der Frage, ob die Erforderlichkeit zur Erfüllung eines berechtigten Interesses angenommen werden kann, bestehen erhebliche Bedenken. Liegt das verfolgte Interesse in der Nutzung eines Messengerdienstes, so lässt sich schnell feststellen, dass datensparsamere Alternativen gegeben sind (siehe Abschnitt 2.4.4.2.2.4). Insofern müsste schon argumentiert werden, dass das Unternehmen ein gewichtiges Interesse verfolgt, gerade diesen Dienst nutzen zu wollen.

Es ist davon auszugehen, dass es in der Verantwortung des Unternehmens liegt, sicherzustellen, dass eine Übertragung sämtlicher Kontaktdaten technische oder organisatorisch unterbunden wird.[970] Für entsprechende WhatsApp-Szenarien kann das Unternehmen separate dienstliche Mobiltelefone beschaffen, die eine

---

[962] Vgl. auch zur gemeinsamen Verantwortung: *Jung/Hansch*, ZD 2019, 143 (145).
[963] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/[letzter Zugriff 06.07.2021].
[964] Zu rechtlichen Möglichkeiten und Grenzen von Selbstdatenschutzlösungen siehe: *Wagner*, Datenökonomie und Selbstdatenschutz.
[965] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/[letzter Zugriff 06.07.2021].
[966] *Faas*, ArbRAktuell 2018, 594 (595).
[967] Dies ist der Fall bei der WhatsApp Datenschutzrichtlinie https://www.whatsapp.com/legal/privacy-policy-eea?eea=1 [letzter Zugriff 16.08.2021].
[968] *Faas*, ArbRAktuell 2018, 594 (595).
[969] *Faas*, ArbRAktuell 2018, 594 (595).
[970] *Jung/Hansch*, ZD 2019, 143 (145); *Schrey u. a.*, MMR 2017, 736 (737).

Vermischung privater und dienstlicher bzw. geschäftlicher Kontakte vermeiden und deren Adressbücher ausschließlich Telefonnummern der WhatsApp-Kontakte enthalten (bzw. des jeweiligen Dienstanbieters).[971] Zudem können professionelle Mobile-Device-Management-Lösungen zur Einrichtung separater Benutzerprofile bzw. Container für berufliche und private Kommunikation auf demselben Smartphone genutzt werden.[972] Technische Maßnahmen bieten Selbstdatenschutzapps (z.B. XPrivacy, SRT Appguard[973]) für feingranulare Einstellungen von Datenzugriffsberechtigungen mit Filtermechanismen oder Containerlösungen, sodass Datenbestände getrennt gehalten und vor Zugriffen geschützt werden können.[974] Kommunikationspartner*innen in WhatsApp separat anzulegen verringert zwar Bequemlichkeit und Komfort der Messengernutzung, diese Einbuße rechtfertigt allerdings keine Datenweitergabe.[975]

4.1.3.2.3 Schlussfolgerung

Die Einschätzung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz zum meistgenutzten Dienst in Deutschland, welcher bekannt für das automatische Auslesen des Adressbuchs ist (WhatsApp), lautet wie folgt:[976]

„WhatsApp als Messenger-Dienst ist nicht a priori datenschutzwidrig, aktuelle Probleme resultieren weniger aus der Gestaltung des Dienstes, sondern aus dessen Einsatzbedingungen in der Praxis. Ein datenschutzkonformer WhatsApp-Einsatz ist unter bestimmten **Voraussetzungen** möglich. Hierzu zählen

- der Einsatz aktueller Software-Versionen, um eine Verschlüsselung der Kommunikationsinhalte zu gewährleisten
- der Einsatz dienstlicher/geschäftlicher Mobiltelefone; eine Nutzung privater Endgeräte kommt nur ausnahmsweise und verbunden mit tragfähigen Container-Lösungen in Betracht
- die Nutzung eines „one-record-Adressbuchs“ mit ausschließlich der Telefonnummer des Dienstanbieters, eines Telefonbuchs mit ausschließlich WhatsApp-Kontakten oder eine Sperre des Adressbuchzugriffs durch WhatsApp
- die Deaktivierung von Cloud-Backups
- die Sicherstellung, dass Chat-Anhänge nicht in der Mediathek des Mobiltelefons gespeichert werden bzw. Dritt-Applikationen keinen Zugriff darauf haben
- eine ausreichende Absicherung der Endgeräte (Zugriffssperre, Verschlüsselung)“

Aus Sicht des Bundesdatenschutzbeauftragen überwiegen die Bedenken, dass die Übermittlunge von Metadaten an WhatsApp (und damit auch Facebook) einen Beitrag zur Profilbildung liefert, sodass für Behörden,

[971] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/[letzter Zugriff 06.07.2021].
[972] *Schrey u. a.*, MMR 2017, 736 (736).
[973] Bei dieser Lösung bestehen allerdings urheberrechtliche Bedenken: *Brummund*, GI-Jahrestagung 2014, 539.
[974] *Ulbricht,* in: *Mehner*, Messenger Marketing, S. 75.
[975] *Faas*, ArbRAktuell 2018, 594 (596).
[976] Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/[letzter Zugriff 06.07.2021].

„die in besonderem Maße an die Einhaltung von Recht und Gesetz gebunden sind und denen in diesem Zusammenhang eine Vorbildfunktion zukommt“ eine Verwendung dieses Dienstes nicht tragbar ist.[977]

4.1.3.3 Optionaler Adressbuchabgleich mittels Hash-Algorithmen

Über die Möglichkeit hinausgehend, einen Adressbuch-Zugriff zu verweigern, stellen mittlerweile die Mehrheit der Messenger Optionen zur Verfügung, optional Adressbücher mit Kontakten abzugleichen. Hierfür wird im Fall der Einräumung eines Adressbuch-Zugriffs ein sog. „Hash“ erstellt. Hierbei handelt es sich um das Ergebnis einer kryptographischen Hashwert-Berechnung aus den Rufnummern in eine Zeichenfolge mit fester Länge, sodass die Rufnummern aus dem Adressbuch nicht im Klartext an den Server des Messengerdienstes übertragen werden.[978] Der Hash-Algorithmus wird auch Einweg-Funktion genannt, da eine Berechnung des ursprünglichen Klartextes als unmöglich bezeichnet wird, allerdings werden gleiche Klartexte durch gleiche Hash-Werte abgebildet. [979] Fraglich ist, ob es sich bei den Hash-Werten um anonyme Daten handelt, die gemäß EG 26 S. 5 und 6 nicht vom Anwendungsbereich der DSGVO erfasst sind. Anonyme Daten sind Informationen, die sich entweder von Beginn an nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder nachträglich in einer Weise anonymisiert wurden, sodass die betroffene Person nicht oder nicht mehr identifiziert werden kann.[980]

Es stellt sich daher die Frage, ob sich aus dem Hash-Wert tatsächlich die ursprüngliche Rufnummer nicht mehr wiederherstellen lässt. In der Tat ist es für einen Angreifer möglich, den Hash-Wert abzuhören und durch eine sog. Brute-Force-Attacke (= Durchprobieren aller Möglichkeiten) auf die Rufnummer zurückzuschließen.[981] Anders als z. B bei Passwörtern (wo u.a. Groß- und Kleinbuchstaben und Sonderzeichen vorkommen können) sind bei Rufnummern nur Ziffern von 0 bis 9 gegeben, was den Aufwand einer Brute-Force-Attacke erheblich reduziert und damit die Möglichkeiten für eine vollständige Enumeration innerhalb einer akzeptablen Zeit aufweisen könnte.[982] Mit viel Rechenpower und Speicherkapazität hätte der Messengerdienstanbieter oder ein Angreifer prinzipiell die Möglichkeit, alle Rufnummern für ein bestimmtes Hash-Verfahren zurück zu berechnen.[983] Auch registrierte Messengerdienstnutzer*innen können mittels Crawling-Attacken Rückschlüsse auf Nutzerdaten ziehen, sofern keine weiteren Schutzmaßnahmen vorliegen.[984] Um zu verhindern sämtliche Rufnummern vorab zu berechnen und in Datenbanken vorzuhalten (sog. „Rainbow Tables“) wird der Hash-Funktion ein Salt, d.h. ein Initialisierungswert beigefügt, welcher bei jedem gespeicherten Wert anders ist.[985] Allerdings bestehen auch hier Bedenken, dass ein Durchprobieren aller Kombinationen möglich bleibt.[986]

---

[977] *BfDI*, Tätigkeitsbericht 2020, S. 33.
[978] *Voitel*, DuD 2017, 686 (686).
[979] *Voitel*, DuD 2017, 686 (686); *Martini,* in: Paal/Pauly - DS-GVO BDSG Art. 32 Rn. 34e.
[980] *Armin/Rothkegel,* in: Taeger/Gabel - DSGVO/BDSG Art. 4 Rn. 47.
[981] *Voitel*, DuD 2017, 686 (686); *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021, S. 2. Siehe bspw. die Funktionsbeschreibung von Threema, unter: https://threema.ch/de/faq/addressbook_data [letzter Abruf 18.08.2021].
[982] *Voitel*, DuD 2017, 686 (686). Ob dies einen nicht unverhältnismäßigen Aufwand bedeuten würde, muss im Einzelfall entschieden werden: *Felber*, ZD 2018, 382 (385).
[983] *Voitel*, DuD 2017, 686 (687); vgl. auch *Marx u. a.,* IT-Sicherheit 2018, 55 (56 ff.).
[984] *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021, S. 2 ff.
[985] *Voitel*, DuD 2017, 686 (687).
[986] *Voitel*, DuD 2017, 686 (687).

Aus diesem Grund dürfte es sich bei den Hash-Werten nicht um anonyme, sondern um pseudonyme Daten nach Art. 4 Nr. 5 DSGVO handeln, auf die mithin laut EG 26 S. 2 die DSGVO weiter Anwendung findet.[987] In diesem Sinne entschieden das VG Bayreuth sowie der bayerische Verwaltungsgerichtshof, dass das Hashen von E-Mail-Adressen den Personenbezug nicht entfallen lässt, wenn es weiterhin mit verhältnismäßigem Aufwand möglich ist, die Hashwerte einer natürlichen Person zuzuordnen.[988] Der Personenbezug entfalle nicht vollständig, da ein Datenabgleich auch bei gehashten Mailadressen möglich bleibe (vgl. bereits Abschnitt 2.3.1.2.3).[989]

Die Umwandlung in Hashwerte dürfte aber als technische Schutzmaßnahme im Sinne des Privacy by Design eingeordnet werden, insbesondere wenn die Verarbeitung nur flüchtig erfolgt. Zudem sollten großflächige Crawling-Attacken durch Begrenzungsmaßnahmen abgewehrt werden.[990] Nichtsdestotrotz bleibt es erforderlich, eine Rechtsgrundlage einzuholen.

Praxistipp:

(1) Bei der Auswahl eines Messengerdienstes sollte darauf geachtet werden, dass dieser das Kontaktverzeichnis des Endgeräts nicht automatisch ausliest und Kontaktdaten nicht im Klartext übermittelt und / oder auf Servern speichert
   a. Nutzung eines Dienstes mit Möglichkeit Kontakte manuell einzugeben oder
   b. Einsatz getrennter Adressbücher für unterschiedliche Dienste

(2) Trotz Hashen von Telefonnummern / Mailadressen sollten Sie davon ausgehen, dass es sich um personenbezogene Daten handelt. Wird eine Kontaktsynchronisation angeboten, muss stets eine Rechtsgrundlage gegeben sein.

4.1.3.3.1 Mögliche Rechtsgrundlage

In Abschnitt 4.1.3.2 wurde bereits dargestellt, dass das automatische Auslesen des Adressbuches und/oder die Übermittlung der Kontaktdaten in Klartext datenschutzrechtlich höchst problematisch sind. Wie in Tabelle 11 gezeigt, bieten viele Messengerdienste dies als Service optional an und übermitteln die Daten nur in gehashter Form, wobei eine Verarbeitung zumeist nur flüchtig erfolgt. Festzuhalten ist, dass nach herrschender Meinung das hashen allein nicht zur Annahme anonymer Daten ausreicht. Insofern soll der Frage nachgegangen werden, wie unter der Prämisse, dass es sich um personenbezogene Daten handelt, eine Legitimationsgrundlage gefunden werden kann.

Verarbeitung personenbezogener Daten: Bei einer nur flüchtigen Datenverarbeitung, bei der die Daten nur temporär erfasst und unmittelbar wieder überschrieben werden, wird diskutiert, ob überhaupt eine Datenverarbeitung vorliegt.[991] Allerdings enthält Art. 4 Nr. 2 DSGVO keinerlei Einschränkungen auf die Dauer des

[987] Vgl. noch zur alten Rechtslage: *Felber*, ZD 2018, 382 (385); *Marx u. a.,* IT-Sicherheit 2018, 55 (56).
[988] VG Bayreuth, Beschluss vom 8.5.2018 – B 1 S 18.105, Rn. 45; bestätigt durch BayVGH, Beschluss vom 26.9.2018 – 5 CS 18.1157
[989] VG Bayreuth, Beschluss vom 8.5.2018 – B 1 S 18.105, Rn. 45.
[990] *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021.
[991] *Klink-Straub/Straub*, NJW 2018, 3201 (3202).

Verarbeitungsvorgangs.[992] Dagegen spricht, dass im Zeitalter automatisierter Datenverarbeitung erhebliche Schutzlücken sowie Abgrenzungsprobleme zu befürchten wären.[993] Die Auslegung der Definitionen durch den EuGH ließ zumeist die Intention durchscheinen, dass ein weiter Anwendungsbereich des Datenschutzrechts erreicht werden soll.[994]

Einwilligung der Kommunikationskontakte: Die Schwierigkeit im Hinblick auf die Einholung einer wirksamen Einwilligung beruht auf dem Aspekt, dass betroffene Person hier nicht nur die Person ist, welche den Messengerdienst nutzt, sondern auch die Personen, welche im Adressbuch des Endgeräts verzeichnet sind. Dass diese jeweils einwilligen, dürfte eher die Ausnahme bilden (vgl. Abschnitt 4.1.3.2.2).

Erforderlichkeit im Beschäftigungskontext: Gerade im Rahmen der innerbetrieblichen Kommunikation wäre es denkbar, dass von einem Abgleich von Adressbuchdaten ausschließlich Beschäftigte des Betriebs betroffen sind und es zur Organisation betrieblicher Abläufe erforderlich ist, dass sich die Beschäftigten ohne großen Zeitaufwand durch manuelle Eingabe von Kontaktdaten vernetzen können. Dies wäre möglich, wenn auf Dienstgeräten ausschließlich innerbetriebliche Kontakte verzeichnet sind oder getrennte Adressbücher genutzt werden.

Berechtigte Interessen: Im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO sind auch die Interessen Dritter berücksichtigungsfähig. Insofern besteht ein Interesse der Person, die den Messengerdienst nutzt, anstelle einer manuellen Eingabe sämtlicher Kontakte einen automatischen Adressbuchabgleich zu nutzen. Dies gilt nur, wenn die Option aktiv ausgewählt wurde. Ein Abgleich der Kontaktdaten in Form von Hashes stellt dabei grundsätzlich ein geeignetes Mittel dar, wobei jedenfalls im Hinblick auf einen automatisierten Abgleich derzeit kein datenschutzfreundlicheres Verfahren bekannt ist. Im Einzelfall sollten allerdings unterschiedliche Umsetzungen bedacht werden.[995] So sollten Maßnahmen ergriffen werden, um die beschriebene Gefahr von Brute-Force-Angriffen oder Crawling-Attacken zu minimieren. Personenbezogene Daten sollten nach einem Abgleich zudem unmittelbar wieder gelöscht werden. Werden schutzwürdige Belange der betroffenen Personen kaum tangiert, gelingt die Legitimation.[996] Wesentlich ist, dass eine Kenntnisnahme sowie Weiternutzung der Daten ausgeschlossen ist, dann könnte von einem überwiegenden Interesse an einem automatischen Adressbuchabgleich ausgegangen werden.

4.1.3.3.2 Information über Datenverarbeitung

Problematisch bleibt an dieser Stelle die Umsetzung der Informationspflichten gegenüber den betroffenen Personen, deren Kontakte im Adressbuch verzeichnet sind. Einschlägig wäre Art. 14 DSGVO, da die Daten nicht bei der betroffenen Person selbst erhoben werden (vgl. Abschnitt 2.4.2.2.2). Hier wäre zu erwägen, ob eine Ausnahmesituation eingreift. So bedarf es keiner Information, wenn sich die Erteilung der Information als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte der betroffenen Personen, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit.

---

[992] *Roßnagel*, in: NK Datenschutzrecht Art. 4 Nr. 2 Rn. 11.
[993] *Wagner*, Das neue Mobilitätsrecht, S. 142.
[994] Vgl. zur Verantwortlichkeit bspw.: EuGH, Urteil vom 10.07.2018 – C-25/17 – Jehovan todistajat, Rn. 66.
[995] Vgl. bspw. Vorschläge für Abhilfemaßnahmen für Hash-Umkehrungen bei *Hagen u.a.,* Proceedings 2021 Network and Distributed System Security Symposium 2021, S. 10 ff.
[996] Vgl. auch BGH, Urteil vom 16.05.2017 – VI ZR 135/13, Rn. 43 zur Berücksichtigungsfähigkeit fehlender Identifizierbarkeit bei Verarbeitung dynamischer IP-Adressen.

4.1.4 Transparenz

In der Praxis wird der Grundsatz der Transparenz vornehmlich durch die Datenschutzerklärungen umgesetzt. Diese müssen im jeweiligen App-Store vor Installation der App einsehbar sein. Eine Verlinkung ist dabei ausreichend. Es sollte allerdings darauf geachtet werden, dass nicht zu viele Klicks oder ein intensives Scrollen erforderlich ist, um an die Erklärung zu gelangen.[997] Des Weiteren muss die Datenschutzerklärung innerhalb der App verfügbar gehalten werden. Trifft das Unternehmen die Verantwortlichkeit für die Datenverarbeitung via Messengerdienst, muss es grundsätzlich selbst über die Verarbeitung informieren und darf nicht lediglich auf die Datenschutzbestimmungen des Dienstes verweisen.[998]

Datenschutzerklärungen: Wie in Abschnitt 2.4.2 dargestellt, sollte die Informationsbereitstellung präzise, verständlich und leicht zugänglich sein und dabei in einer klaren und einfachen Sprache gehalten sein. Optimal ist eine kurze und bündige Darstellung mit einer gut strukturierten Gliederung, um eine Informationsüberflutung zu vermeiden.[999] Hierfür sollte auch eine klare Trennung von anderen Sachverhalten (wie bspw. den Nutzungs- und Lizenzbestimmungen) gegeben sein.[1000] Im Hinblick auf die Verständlichkeit und den Zuschnitt auf die Zielgruppe ist zu verlangen, dass für den deutschsprachigen Raum auch eine Datenschutzerklärung in deutscher Sprache vorgehalten wird.[1001]

Datenschutzerklärung ist …					
	vorhanden	in Deutsch	getrennt von anderen Erklärungen	präzise, verständlich, vollständig	Sonstiges
Beispiele für Messenger mit Fokus auf Privatnutzung					
Facebook Messenger	– ✓	– ✓	– ✓	umfasst alle Facebook-Produkte	nutzt Cookies
Signal	– ✓	– X	Signal Terms & Privacy Policy	– X	
Telegram	– ✓	– X	– ✓	– ✓	
WhatsApp WhatsApp Business	– ✓ – (✓)[1002]	– ✓ – ✓	– ✓ – ✓	Aufzählung aller Rechtsgrundlagen aus Art. 6 DSGVO	nutzt Cookies, Information zu „Datenschutzschild“[1003] aktuell?
Beispiele für Messenger mit Angebot für Privatpersonen und Unternehmen					
ginlo (Privat)	– ✓	– ✓	– ✓	– ✓	kleine Kurz-Gesagt-

[997] *Artikel-29-Datenschutzgruppe*, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 8.
[998] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 15.
[999] *Artikel-29-Datenschutzgruppe,* Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 7. Eine Datenschutzerklärung mit mehr als 50 Bildschirmseiten für einen Smart-TV ist unzumutbar: LG Frankfurt, Urteil vom 10.06.2016 – 2-3 O 364/15.
[1000] *Artikel-29-Datenschutzgruppe*, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 7.
[1001] *Artikel-29-Datenschutzgruppe*, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, S. 10.
[1002] Im Rahmen der WhatsApp Business Nutzungsbedingungen finden sich auch die WhatsApp Business Richtlinie, Datenverarbeitungsbedingungen, Richtlinie zum geistigen Eigentum und Markenrichtlinien. Zusätzlich sind Datensicherheitsbedingungen verlinkt. Die Datenverarbeitungsbedingungen enthalten lediglich die Pflichten als Auftragsverarbeiter.
[1003] Unklar ist, ob sich die Information auf den Privacy Shield bezieht, welches seit Juli 2020 für unwirksam erklärt wurde (siehe Abschnitt 4.2.1.2).

ginlo Business	– ✓	– ✓	– ✓	– ✓	Blöcke[1004]
Threema Threema Work	– ✓ – ✓	– (✓)[1005] – (✓)	– ✓ – ✓	– ✓ – ✓	
Wire	– ✓	– ✓	– ✓	– ✓	Verweis auf Zertifizierung nach Privacy Shield
Beispiele für Messenger mit Fokus auf innerbetriebliche Kommunikation					
Teamwire	– (✓)[1006]	– ✓	– ✓	Aufzählung fast aller Rechtsgrundlagen Art. 6 DSGVO[1007]	nutzt Cookies
stashcat	– ✓	– ✓	– ✓	Aufzählung fast aller Rechtsgrundlagen Art. 6 DSGVO	Kein Ausschluss Datenübermittlung in USA durch Übersetzungsdienst

Tabelle 12 Umsetzung der Transparenzpflichten bei ausgewählten Messengerdiensten[1008]

Besonders negativ fallen unter dem Gesichtspunkt der leichten Zugänglichkeit solche Messengerdienste auf, welche die Zugänglichkeit zu ihrer Datenschutzerklärung von der Zustimmung zu Cookies abhängig machen. Des Weiteren umfassen Erklärungen zumeist nicht nur spezifisch die Messenger-App, sondern die gesamte Produkt-Palette oder unterschiedliche Kontexte (Webseite, App, sonstige [E-Mail]-Kommunikation), sodass sich Informationen aus Nutzersicht nur schwierig zuordnen lassen. Einen klaren Vorteil bieten hier Angebote, die auf einen Messenger beschränkt sind. Nur hier ist es möglich, tatsächlich konkret und detailliert über anfallende Daten, die Zwecke der Verarbeitung und die einschlägigen Rechtsgrundlagen aufzuklären. Ebenfalls wenig Aussagekräftig ist die Bezugnahme auf sämtliche der Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO bei WhatsApp und dem Facebook Messenger. Bei Teamwire erfolgt zumindest eine Konkretisierung im Verlauf der einzelnen Erhebungskontexte (Webseite, Newsletter, App). Die Ausführungen übernehmen jedoch weite Passagen der DSGVO fast wörtlich, bleiben im Hinblick auf die Information über den konkreten Kontext allerdings sehr vage oder gar missverständlich. Bei anderen Messengern wird wesentlich eindeutiger differenziert zwischen zur Erbringung der Leistungen des Messengerdienstes erforderlichen Daten (Vertragserfüllung, Art. 6 Abs. 1 Buchst. b DSGVO) und der Bereitstellung optionaler Daten (Einwilligung, Art. 6 Abs. 1 Buchst. a DSGVO). Langatmige Erklärungen zu Datenschutzrechten ohne konkreten Bezug zur Anwendung sollten aus Sicht des datenschutzrechtlich Verantwortlichen nach Möglichkeit vermieden werden. Vielmehr sind kurze Erklärungen bei gleichzeitiger Detailtiefe anzustreben. Wird eine Einwilligung eingeholt, sollte ausreichend Klarheit bestehen, welche Verarbeitungsvorgänge auf die Einwilligung der teilnehmenden Person gestützt

[1004] Datenschutzhinweise Stand Mai 2020, abrufbar unter https://app-help.ginlo.net/business/de/privacy/ [letzter Abruf 28.07.2021].
[1005] Über den Playstore war zum Testzeitpunkt die Erklärung in Englisch verlinkt.
[1006] Fehlermeldung bei Zugriffsversuch vom Playstore; Webseite bietet allgemeine Erklärung zur Webseite, Newsletter sowie App.
[1007] Bezüglich der Registrierung und Bereitstellung der Apps und Services wird als Rechtsgrundlage konkretisierend „bei Vorliegen einer Einwilligung“ Art. 6 Abs. 1 Buchst. a DSGVO genannt. Die Speicherdauer richtet sich hingegen nach der „Dauer des Vertragsverhältnisses“.
[1008] Die Auswahl ist nach den folgenden Kriterien motiviert: Bekanntheitsgrad, Verortung in Europa und Datenschutzstandards sowie spezifische Fokussierung auf den Unternehmenskontext. Der Abruf der Datenschutzerklärungen erfolgte aus dem Playstore von einem Android-Endgerät.

werden, damit sich diese ihrer Dispositionsbefugnisse bewusst werden.[1009] Fehlen eindeutige Informationen zum Umfang der Einwilligung, handelt es sich nicht um eine *informierte* Einwilligung, wodurch Verantwortliche das Risiko der Rechtswidrigkeit der Datenverarbeitung tragen.[1010] Auch die Datenschutzerklärung sollte daher transparent reflektieren:

- um welche Daten es sich konkret handelt,
- welche diese Daten erforderlich zur Erbringung des Dienstes sind und
- welche dieser Daten optional sind und auf einer jederzeit widerrufbaren Einwilligung basieren.

Sonstige Informationen: Um eine Einschätzung zur Datenschutzkonformität eines Systems treffen zu können, helfen Aussagen über die technischen Implementierungen, die eingesetzten Standards, Software-Bibliotheken und Lizenzen. Dabei weist die DSK darauf hin, dass:[1011]

- Quelloffene Systeme können gegenüber proprietärer Software Transparenz fördern. Insbesondere haben Expert*innen so Möglichkeiten tiefergehende Analysen einzelner Funktionen durchzuführen.
  - Der veröffentlichte Quellcode sollte vollständig, aktuell und (zumindest für Expert*innen) reproduzierbar sein.
- Für ein besseres Verständnis der technischen Struktur und wichtigsten Systemkomponenten bieten technische Erläuterungen wie Whitepaper Hintergrundwissen.
- Berichte über Sicherheitsprüfungen sowie zur Beseitigung aufgefundener Sicherheitsprobleme sollten frei zugänglich veröffentlicht werden.
  - Auch bei diesen sollte darauf geachtet werden, ob diese umfassend und aktuell sind und damit die im Einsatz befindliche Produktivversion, also keine veraltete Version, betreffen.

4.1.5 Nutzungsbedingungen

Aus datenschutzrechtlicher Perspektive erhöht sich durch den Einbezug des Beschäftigungskontextes die Komplexität der rechtlichen Anforderungen beim Einsatz von Messengerdienste als Kommunikationstools. Des Weiteren stellen Unternehmen oftmals gesteigerte Anforderungen an die Datensicherheit zum Schutz ihrer Geschäftsgeheimnisse (hierzu später unter Kapitel 6). Daher erscheint es naheliegend, dass einige Anbieter von Messengerlösungen die Domänen des Privatkundenbereichs und der Business-Lösungen getrennt halten. Folglich wird in vielen Nutzungsbedingungen der „Standard“-Anwendung die Nutzung zu beruflichen Zwecken ausgeschlossen. Zunächst einmal kann hierin eine inhaltliche Beschränkung des Nutzungsrechts der urheberrechtlich geschützten Software liegen (vgl. §§ 69a ff., 31 Abs. 1 S. 3 UrhG), sodass das Unternehmen eine Urheberrechtsverletzung begeht, wenn das eingeräumte Recht zur privaten Nutzung überschritten wird.[1012] Ordnet ein Unternehmen nichtsdestotrotz den Einsatz eines auf die Nutzung zu privaten Zwecken konzipierten Messengerdienstes durch seine Beschäftigten an, so besteht zudem die Gefahr, dass ein datenschutzwidriger Zustand entsteht, wenn bspw. die Rechtsgrundlagen nicht greifen.[1013] Kommt es zu einem

[1009] vgl. zu Videokonferenzsystemen: *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 14.
[1010] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 14.
[1011] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 24.
[1012] *Schrey u. a.*, MMR 2017, 656 (657).
[1013] Bspw. schließen selbst die WhatsApp Business Nutzungsbedingungen einen innerbetrieblichen Einsatz im Unternehmen aus: WhatsApp, Business Nutzungsbedingungen (Stand 29.10.2020), https://www.whatsapp.com/legal/business-terms/?lang=de [letzter Abruf 18.08.2021].

Schaden oder einer behördlichen Sanktion, wäre zu bedenken, inwieweit das Unternehmen den Messengerdienst schadlos stellen müsste. In jedem Fall sollten Unternehmen die Nutzungsbedingungen aufmerksam studieren: ein Ausschluss zur beruflichen Nutzung sollte als deutlicher Hinweis verstanden werden, dass die (datenschutz-)rechtlichen Anforderungen für diesen Fall nicht gewährleistet werden können.

Enthalten die Nutzungsbestimmungen hingegen keine Beschränkung auf private oder gewerbliche Zwecke, kann von einem unbeschränkten Nutzungsrecht ausgegangen werden.[1014] Machen Dienste die Nutzung zu betrieblichen Zwecken davon abhängig, dass die Einzelnutzer*innen befugt sind, das Unternehmen an die Bestimmungen der Nutzungsbedingungen zu binden, stellt sich die Problematik, dass – sofern nicht zuvor eine Befugnis eingeräumt wurde – dies für „einfache" Beschäftigte kaum realistisch möglich ist. [1015] Um die Beschäftigten vor Vertrags- und Urheberrechtsverletzungen zu schützen, müssen die Unternehmen folglich die jeweiligen Nutzungsbedingungen analysieren und entsprechende Berechtigungen erteilen oder eine betriebliche Nutzung des nicht rechtskonform nutzbaren Messengers durch Beschäftigte untersagen.

4.1.6 Hinweise zur Auswahl und zum Betrieb von Messengerdiensten

Der BfDI veröffentlichte Anfang April 2020 auf seiner Website Leitfragen zur Auswahl und zum sicheren Betrieb von Messenger- und Videokonferenzdiensten veröffentlicht.[1016] Diese werden im Folgenden leicht verkürzt zusammengefasst:

Datenschutzniveau nach DSGVO:

- Hat der Anbieter seinen **Sitz in der EU**? Welche Informationen stellt der Anbieter ohne Sitz in der EU über das **Datenschutzniveau** und die Einhaltung der DSGVO bereit (Angemessenheitsbeschluss, Standardvertragsklauseln)?
  - Stellt der Anbieter Informationen dazu zur Verfügung, in welchen Ländern die einzelnen Komponenten seiner Infrastruktur lokalisiert sind?
  - Stehen die Server der Dienstleister in der EU / gibt es ausreichend **Garantien** für den Serverstandort für eine DSGVO-konforme Verarbeitung?

Transparenz & Sicherheit:

- Stellt der Anbieter eine **Datenschutzerklärung** zur Verfügung (die nicht zu vage oder verwirrend formuliert ist)?
- Welche Informationen gibt es zu den eingesetzten **Protokollen** und **Verschlüsselungsverfahren**?
  - Stellt das Angebot eine **Ende-zu-Ende-Verschlüsselung** der Kommunikation sicher?
  - Das Fehlen einer durchgehenden Transportverschlüsselung der Verbindung zwischen den Clients und den Servern des Anbieters sollte als Ausschlusskriterium gewertet werden.
  - Je mehr Informationen bereitgestellt werden, desto eher deutet dies auf eine ausreichende Sicherheit hin, da eine **unabhängige Überprüfung** möglich ist.
  - Gibt es Informationen zur Sicherheit der Infrastruktur allgemein? Bspw. eine **Zertifizierung** nach einem allgemein anerkannten Standard wie ISO/IEC 27001?

[1014] *Schrey u. a.*, MMR 2017, 656 (657).
[1015] *Schrey u. a.*, MMR 2017, 656 (657).
[1016] BfDI, Leitfragen zur Beurteilung von Angeboten, abrufbar unter https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Datenschutzpraxis/Beurteilung_Angebote_Messenger.html [letzter Abruf 08.08.2021].

Umfang Datenverarbeitung:

- Stellt der Anbieter ausreichend konkrete und hinreichend umfangreiche Informationen zur **Weitergabe von Daten an Dritte** (Auftragsverarbeiter, Partnerunternehmen) bereit?
- **Welche identifizierenden Daten** müssen angegeben werden, um den Dienst nutzen zu können?
  - frei wählbare ID und E-Mail-Adresse sind datenschutzfreundlicher als Mobilfunknummer, welche andererseits wieder für Authentisierung und Identifikation der Gesprächskontakte erforderlich sein könnten.
  - Insgesamt gilt: je mehr Daten die Dienstnutzung erfordert, desto problematischer im Hinblick auf den Datenschutz
- Welche Möglichkeiten gibt es zur **sicheren Identifikation** der Kommunikationskontakte?
  - Wie stellt die Anmeldung sicher, dass Kommunikationsbeteiligte nicht über ihre Identität täuschen können?
- **Wo** werden die Daten (Kommunikationsinhalte, Adressbücher, Metadaten) **gespeichert**?
  - Je mehr Daten zentral auf Servern des Anbieters gespeichert werden, desto eher problematisch aus Sicht des Datenschutzes.
- Wie werden Daten (Nutzerinfos, Adressbücher, Chatverläufe, Dokumente, Anrufprotokolle, etc.) auf **Endgeräten gesichert**?
  - Von Vorteil ist eine verschlüsselte Speicherung unabhängig von der allgemeinen Geräteverschlüsslung.
- Welche Möglichkeiten der **gezielten Löschung** bietet die Anwendung?

Sofern die anvisierten Angebote zur Beantwortung der Leitfragen nicht ausreichend Informationen bereitstellen, können Unternehmen die Organisation von Infrastruktur und Betrieb „selbst in die Hand nehmen“. Aber auch dabei bieten die Leitfragen Orientierungspunkte worauf Unternehmen bei der Umsetzung achten sollten.

4.2 Datenschutzrechtliche Herausforderungen beim Einsatz von international operierenden Messengerdiensten

Nutzt ein datenschutzrechtlich verantwortliches Unternehmen ein System, welches es nicht selbst vor Ort innerhalb der EU/des EWR betreibt, sondern das von einem Dienstleister betrieben wird, der seinen Sitz außerhalb der EU/des EWR hat, muss beachtet werden, dass auch der Dienstleister die in der EU geltenden datenschutzrechtlichen Vorgaben berücksichtigt.[1017] Wie bereits die Übersicht in Abschnitt 4.1.1 zeigt, werden Messengerdienste aus unterschiedlichsten Ländern angeboten.

[1017] *BfDI*, Tätigkeitsbericht 2020, S. 32.

4.2.1 Datenübermittlung in Drittländer

Der universelle Schutzanspruch der EU-Grundrechte, insbesondere des Schutzes personenbezogener Daten nach Art. 8 EU-GrCh, wird durch die „Vererbung“ des datenschutzrechtlichen Pflichtenkanons auch beim Verlassen des territorialen Geltungsgebiets der DSGVO deutlich.[1018] Zudem werden hohe Anforderungen gesetzt, wenn personenbezogene Daten in Drittländer außerhalb der EU/des EWR übermittelt werden sollen.

4.2.1.1 Grundsätzliche Anforderungen an Drittstaatentransfers

Die Zulässigkeit des Datentransfers an Drittstaaten richtet sich nach den Art. 44 ff. DSGVO. Der Begriff des „Drittlands“ bzw. „Drittstaates“ ist in der DSGVO nicht eindeutig definiert. Im europarechtlichen Kontext wird damit ein Staat bezeichnet, der nicht Mitglied der EU ist.[1019] Eine Ausnahme bilden die drei EWR-Staaten (Island, Lichtenstein, Norwegen), da diese ihre nationalen Gesetze an den EU-Rahmen angepasst haben. [1020] Übermittlung in diese Staaten sind Übermittlungen in andere EU-Mitgliedstaaten gleichgestellt.[1021] Da EU-Mitgliedstaaten als auch EWR-Staaten somit bereits an die Regelungen der DSGVO gebunden sind, finden die einen angemessenen Datenschutz oder geeignete Garantien verlangenden Art. 44 ff. DSGVO nur auf den Datentransfer in Staaten außerhalb der EU/des EWR Anwendung.[1022]

> Art. 44 DSGVO
>
> Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation.

Die Rechtmäßigkeit einer Datenübermittlung folgt einer Zwei-Stufen-Prüfung:[1023]

- Der Übermittlungsvorgang muss nach den allgemeinen Regeln der DSGVO rechtmäßig sein.
- Zusätzlich müssen die besonderen Bedingungen der Art. 44 ff. DSGVO erfüllt sein.

Dies bedeutet, dass zusätzlich zu den allgemeinen Regelungen zur Datenverarebeitung der DSGVO die Bestimmungen des Kapitels 5 der DSGVO (Art. 44-50 DSGVO) anzuwenden sind, um sicherzustellen, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen bei Datenverarbeitungen mit internationalem Kontext nicht unterschritten wird. [1024] Somit ist zu prüfen, ob ein Angemessenheitsbeschluss oder geeignete Garantien vorliegen, die die Angemessenheit des Datenschutzniveaus gewährleisten.[1025] Sollte dabei festgestellt werden, dass keine von beiden Voraussetzungen gegeben sind, kann eine Prüfung der Ausnahmevorschriften erfolgen.[1026]

[1018] *Ambrock/Karg*, ZD 2017, 154 (155).
[1019] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 44 Rn. 6; *Kamp/Beck,* in: BeckOK DatenschutzR Art. 44 Rn. 23.
[1020] *Kamp/Beck,* in: BeckOK DatenschutzR Art. 44 Rn. 24.
[1021] *Kamp/Beck,* in: BeckOK DatenschutzR Art. 44 Rn. 24.
[1022] *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 44 Rn. 17; *Auer-Reinsdorff/Conrad*, Auer-Reinsdorff/Conrad IT-R-HdB, § 35 Grenzüberschreitende Datenverarbeitung, Rn. 20.
[1023] *Ambrock/Karg*, ZD 2017, 154 (155); *Voigt/von dem Bussche,* in: Konzerndatenschutz, Kap. 3 Rn. 1.
[1024] *Ambrock/Karg*, ZD 2017, 154 (155).
[1025] *Ambrock/Karg*, ZD 2017, 154 (156).
[1026] *Ambrock/Karg*, ZD 2017, 154 (156).

4.2.1.1.1 Datenübermittlung in Drittstaaten mit einem angemessenen Schutzniveau

Liegt ein Angemessenheitsbeschluss der EU-Kommission vor, handelt es sich um einen Drittstaat mit angemessenem Schutzniveau und eine Datenübermittlung darf ohne weitere Genehmigung erfolgen (Art. 45 Abs. 1 S. 2, EG 103 S. 2).[1027]

Art. 45 Abs. 1 DSGVO

Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlungen bedarf keiner besonderen Genehmigung.

Die EU-Kommission hat eine Reihe von Staaten mit einem angemessenen Schutzniveau anerkannt. Im Einzelnen handelt es sich derzeit um die folgenden Staaten: [1028]

- Andorra (Kommissionsbeschluss 2010/625/EU vom 19.10.2010, ABl. EU vom 21.10.2010, Nr. L 277/27.)
- Argentinien (Kommissionsbeschluss 2003/490/EG vom 30.03.2003, ABl. EG vom 5.7.2003, Nr. L 168/19.)
- Australien, Sonderfall PNR-Daten (ABl. EU v. 8.8.2008, Nr. L 213/47)
- Canada (Kommissionsbeschluss 2002/2/EG vom 20.12.2001, ABl. EG vom 4.1.2002, Nr. L 2/13.)
- Färöer-Inseln (Kommissionsbeschluss 2010/146/EG vom 05.03.2010, ABl. EU vom 9.3.2010, Nr. L 58/17.)
- Guernsey (Kommissionsbeschluss 2003/821/EC vom 21.11.2003, ABl. EG vom 25.11.2003, Nr. L 308/27.)
- Isle of Man (Kommissionsbeschluss 2004/411/EC vom 28.04.2004, ABl. EU vom 30.4.2004, Nr. L 151/51)
- Israel (Kommissionsbeschluss 2011/61/EU vom 31.01.2011, ABl. EU vom 1.2.2011, Nr. L 27/39.)
- Japan (Durchführungsbeschluss (EU) 2019/419 der Kommission vom 23.1.2019, ABl. vom 19.3.2019, Nr. L 76/1)[1029]
- Jersey (Kommissionsbeschluss 2008/393/EC vom 08.05.2008, ABl. EU vom 28.5.2008, Nr. L 138/21.)
- Neuseeland (Kommissionsbeschluss 2013/65/EU vom 19.12.2012, ABl. EU vom 30.1.2013, Nr. L 28/12.)
- Schweiz (Kommissionsbeschluss 2000/518/EC vom 26.07.2000, ABl. EG vom 25.8.2000, Nr. L 215/1.)
- Uruguay (Kommissionsbeschluss 2012/484/EU vom 21.08.2012, ABl. EU vom 23.8.2012, Nr. L 227/11.)

Bei diesen Staaten ist es nicht mehr erforderlich, in eine Prüfung einzutreten, ob diese ein angemessenes Datenschutzniveau aufweisen. Als Folge ist eine Datenübermittlung in diese Staaten ohne eine weitere eigene Überprüfung datenschutzrechtlich zulässig. Allerdings ist aus den obengenannten Angemessenheitsbeschlüssen zu erkennen, dass diese Entscheidungen der EU-Kommission relativ lange zurückliegen (zwischen 2000-2013, als die DSGVO noch nicht existierte). Die EU-Kommission ist nach dem Inkrafttreten der DSGVO verpflichtet, alle Angemessenheitsbeschlüssen dahingehend zu überprüfen, ob in den jeweiligen Staaten ein der EU vergleichbares Datenschutzniveau anerkannt werden kann.[1030]

[1027] *Beck*, in: BeckOK DatenschutzR Art. 45 Rn. 1; *Ambrock/Karg*, ZD 2017, 154 (156).
[1028] Beschlüsse abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [letzter Abruf 18.08.2021].
[1029] Erster Angemessenheitsbeschluss nach Inkrafttreten der DSGVO.
[1030] EU Commission, Adequacy decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [letzter Abruf 28.05.2021].

4.2.1.1.2 Datenübermittlung vorbehaltlich angemessener Garantien

Liegt kein Angemessenheitsbeschluss vor, können Garantien die Angemessenheit des Datenschutzniveaus gewährleisten (Art. 46, 47 DSGVO). Fehlen auch diese, kommen einige Ausnahmen in Betracht (Art. 49 DSGVO). Dabei sind die Vorschriften mit dem Ziel anzuwenden und auszulegen, dass das durch die DSGVO gewährleistete Schutzniveau auch bei Datenübermittlungen im internationalen Kontext aufrechterhalten wird.[1031] Der Ausdruck „angemessenes Schutzniveau" bedeutet nach der Rechtsprechung des EuGHs dabei nicht, dass das Drittland ein identisches Schutzniveau gewährleisten muss, es wird aber verlangt, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleistet, das dem in der Union im Licht des in der Grundrechtecharta garantierten Niveaus der Sache nach gleichwertig ist.[1032]

Garantien: Wenn kein Angemessenheitsbeschluss durch die EU-Kommission vorliegt, ist gemäß Art. 46 Abs. 1 DSGVO zu prüfen, ob andere geeignete Garantien für eine Datenübermittlung in die betreffenden Drittstaaten vorliegen. Als zusätzliche Bedingung müssen die betroffenen Personen auf Grundlage dieser Garantien durchsetzbare Rechte zugestanden werden und wirksame Rechtsbehelfe zur Verteidigung dieser Rechte bestehen.[1033] In Art. 46 Abs. 2 DSGVO ist eine nicht abschließende Aufzählung geeigneter Garantien aufgelistet, bei deren Vorliegen Daten übermittelt werden dürfen, ohne dass hierzu noch eine besondere Genehmigung einer Aufsichtsbehörde notwendig ist. Das sind folgende Instrumente:

- Rechtlich bindende und durchsetzbare Verwaltungsvereinbarungen
- Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) gemäß Art. 47 DSGVO
- Standarddatenschutzklauseln der EU-Kommission (Standardvertragsklauseln)
- Genehmigte Verhaltensregeln nach Art. 40 DSGVO und genehmigte Zertifizierungsmechanismen nach Art. 42 DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen

Vorbehaltlich der Genehmigung der zuständigen Aufsichtsbehörde können Garantien zudem bestehen in:

- Einzeln ausgehandelte Vertragsklauseln und
- Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen

Aus Unternehmensperspektive sind die Standardvertragsklauseln (engl. Standard Contractual Rules, SCC) und genehmigten verbindlichen internen Datenschutzvorschriften (engl. Binding Corporate Rules, BCR) die relevantesten Fallgruppen:

Standard Contractual Clauses (SCC) Hierbei handelt es sich um von der EU-Kommission „vorgenehmigte" Mustervertragsklauseln über die sichergestellt werden soll, dass Vertragspartner im Drittstaat ein angemessenes Schutzniveau einhalten.[1034] Im Juni 2021 veröffentlichte die Kommission modernisierte Standardvertragsklauseln unter der DSGVO für Datenübertragungen von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern, die der DSGVO unterliegen, an nicht der DSGVO-unterliegende Verantwortliche oder Auftragsverarbeiter (insbesondere mit Sitz außerhalb der EU/des EWR).[1035] Bei individuell ausgehandelten Vertragsklauseln nach Art. 46 Abs. 3 Buchst. a DSGVO bedarf es einer Genehmigung durch die zuständige

[1031] *Ambrock/Karg*, ZD 2017, 154 (156).
[1032] EuGH, Urteil vom 06.10.2015 – C-362/14 – Schrems I, Rn. 73.
[1033] *Ambrock/Karg*, ZD 2017, 154 (156). So auch die Feststellungen des EuGHs zum Safe-Harbour-Abkommen: EuGH, Urteil vom 06.10.2015 – C-362/14 – Schrems I, Rn. 95.
[1034] *Voigt*, in: Konzerndatenschutz, Kap. 2 Rn. 13.
[1035] Abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de [letzter Abruf 18.08.2021].

Aufsichtsbehörde. Bei der Nutzung der SCC ist hingegen keine weitere Genehmigung erforderlich.[1036] Im Rahmen der SCC ist ausdrücklich festzulegen, welche Vertragsparteien in welchen Rollen beteiligt sind (Datenexporteur und Datenimporteur), sowie nach Möglichkeit die konkreten Datenflüsse den jeweiligen Vertragsparteien eindeutig zuzuordnen.[1037] SCC gehen von einem Vertragsmodell aus, in welchem die Vertragspartner die Einhaltung der Vertragsklauseln überwachen.[1038] Der EuGH hatte die bisher geltenden, bereits unter der Datenschutz-Richtlinie erlassenen SCC als gültig bestätigt, dabei aber anklingen lassen, dass diese nicht für jeden denkbaren Fall des Datentransfers in Drittländer schon alle zur Herstellung eines gleichwertigen Datenschutzniveaus erforderlichen Vereinbarungen und Maßnahmen enthalten (insbesondere können sie aufgrund ihres Vertragscharakters keine drittstaatlichen Behörden binden), sondern in Abhängigkeit von der Rechtslage im Empfängerland insbesondere hinsichtlich von Datenzugriffen dortiger Behörden gegebenenfalls durch zusätzliche Maßnahmen ergänzt werden müssen.[1039]

Binding Corporate Rules (BCR): bieten Spielräume für multinationale Konzerne für grenzüberschreitende Datentransfers innerhalb von Konzernunternehmen.[1040] Eine genaue Definition bietet Art. 4 Nr. 20 DSGVO. Solche Regeln müssen alle allgemeinen Datenschutzgrundsätze und einklagbare Rechte enthalten, um angemessene Garantien für Datenübertragungen zu gewährleisten.[1041] Sie müssen rechtsverbindlich sein und von jedem betroffenen Mitglied der Unternehmensgruppe durchgesetzt werden.[1042] Die Unternehmen müssen der zuständigen Datenschutzbehörde BCR zur Genehmigung vorlegen, welche dann nach dem Kohärenzverfahren gemäß Art. 63 DSGVO erfolgt. BCR kommen folglich nur in Frage, wenn die Kommunikation unternehmensintern erfolgt.

4.2.1.1.3 Ausnahmen für bestimmte Fälle

Falls weder ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt noch geeignete Garantien nach Art. 46 DSGVO bestehen, ist eine Übermittlung personenbezogener Daten in ein Drittland nur auf Basis der in Art. 49 Abs. 1 DSGVO genannten Ausnahmen zulässig. Der Ausnahmekatalog aus dem Art. 49 Abs. 1 S. 1 Buchst. a-g DSGVO lautet wie folgt:

- Ausdrückliche Einwilligung der betroffenen Person nach Unterrichtung
- Erforderlichkeit zur Erfüllung eines Vertrags mit der betroffenen Person oder zur Durchführung vorvertraglichen Maßnahmen
- Erforderlichkeit zum Abschluss oder zur Erfüllung eines Vertrags im Interesse der betroffenen Person mit einer anderen Person
- Zur Wahrung eines wichtigen öffentlichen Interesses
- Erforderlichkeit zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Zum Schutz lebenswichtiger Interessen bei Unmöglichkeit einer Einwilligung
- Daten aus Registern zur Information der Öffentlichkeit
- Begrenzte Übermittlung nach Interessenabwägung bei „zwingenden berechtigten Interessen“ (Art. 49 Abs. 1 S. 2 DSGVO)

[1036] *Voigt/von dem Bussche,* in: Konzerndatenschutz, Kap. 3 Rn. 1; *Schantz,* in: NK Datenschutzrecht Art. 46 Rn. 31.
[1037] *Voigt/von dem Bussche,* in: Konzerndatenschutz, Kap. 3 Rn. 5.
[1038] *Schantz,* in: NK Datenschutzrecht Art. 46 Rn. 35.
[1039] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 132 ff.; *Lange/Filip,* In: BeckOK DatenschutzR Art. 46 Rn. 25; *Schwartmann/Burkhardt*, ZD 2021, 235 (235); *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 46 Rn. 12a ff.
[1040] *Voigt,* in: Konzerndatenschutz, Kap. Rn. 15.
[1041] *Schneider,* in: Forgó/Helfrich/Schneider - Betrieblicher Datenschutz, Kap. 2 Rn. 158.
[1042] *Towfigh/Ulrich,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 47 Rn. 14 ff.

Einwilligung: Ein Datentransfer in ein unsicheres Drittland ist gemäß Art. 49 Abs. 1 Buchst. a DSGVO zulässig, wenn die betroffenen Personen wirksam in die Datenübermittlung in das Drittland eingewilligt haben. Die Wirksamkeit und damit legitimierende Wirkung der Einwilligung setzt dabei voraus, dass die betroffene Person (1) über bestehende Risiken derartiger Datenübermittlungen (2) ohne Vorliegen eines Angemessenheitsbeschlusses und geeigneter Garantien unterrichtet wurde und (3) in Kenntnis dieser Umstände ausdrücklich einwilligt.[1043] In diesem Fall benötigt das Unternehmen zur Rechtfertigung des Übermittelns personenbezogener Daten in das Drittland keine zusätzlichen Garantien. [1044]

Verwendet eine Kund*in oder Geschäftspartner*in aus eigenem Antrieb eine Kommunikationslösung mit Datentransfer in ein unsicheres Drittland, dessen Schutzniveau nicht mit dem der EU gleichwertig ist, ohne dieses Defizit ausgleichende Schutzgarantien, so kann hierin eine selbstbestimmte und souveräne Entscheidung liegen, sofern die erhöhten Transparenzanforderungen tatsächlich erfüllt sind und damit die Tragweite der Entscheidung verstanden wurde.[1045] Insofern können sich auch Unternehmen mit unmittelbarem Kundenkontakt auf die Ausnahme berufen.[1046] Umstritten ist hierbei, wie weit über die Rechtslage im Zielland informiert werden muss.[1047] So verlangen einige Literaturstimmen, konkrete Erkenntnisse zu Datenmissbrauchsrisiken oder typische Risiken wie z.B. erschwerte Durchsetzung von Betroffenenrechten, fehlende Kontrolle der Weiterverarbeitung und Übermittlung der Daten, fehlende Datenschutzaufsicht oder Zugriffe durch staatliche Stellen den betroffenen Personen vor Augen zu führen.[1048] Anderen genügt abstrakt auf das Risiko eines fehlenden angemessenen Datenschutzniveaus und fehlender Garantien zu verweisen.[1049] Der Europäische Datenschutzausschuss verlangt als Beispiele die konkrete Information über ein mögliches Fehlen von Aufsichtsbehörden, von Datenverarbeitungsgrundsätzen oder von Datenschutzrechten der betroffenen Personen.[1050]

Umstritten ist ferner, ob die Einwilligungsfähigkeit ausscheiden muss, wenn der Wesensgehalt der Grundrechte der Artt. 7, 8 EU-GrCh betroffen ist, also eine Missachtung fundamentaler und grundlegender Rechte der Betroffenen zu befürchten ist.[1051] Da die Einwilligung das Instrument zur Wahrnehmung der eigenen Autonomie und eigener Gestaltungsinteressen bietet, ist bei Überlegungen zur Einschränkbarkeit der Einwilligung Vorsicht geboten.[1052] Andererseits wird gerade bei „leicht“ erteilten Einwilligungen die bloße Fiktion der Freiwilligkeit bemängelt.[1053] Insofern ist es bedeutsam, dass die Auslegung und Anwendung der Regelungen zur Einwilligung stets im Lichte der Autonomiesicherung dem Selbstbestimmungsgedanken Rechnung

[1043] *Ulbricht,* in: *Mehner*, Messenger Marketing, S. 76; *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 4 f.
[1044] *Ulbricht,* in: *Mehner*, Messenger Marketing, S. 76.
[1045] Bietet das Unternehmen ausschließlich diesen Kommunikationsweg ohne alternative Optionen, kann dies Zweifel an der Freiwilligkeit begründen: *Ambrock/Karg*, ZD 2017, 154 (157) gehen von Unfreiwilligkeit erst bei gewisser Marktmacht aus, wenn Verbraucher:innen keine gleichwertigen Alternativen zur Verfügung stehen.
[1046] *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 49 Rn. 14.
[1047] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 8.
[1048] *Schantz,* in: NK Datenschutzrecht Art. 49 Rn. 14; *Ambrock/Karg*, ZD 2017, 154 (157).
[1049] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 49 Rn. 6; *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 49 Rn. 15.
[1050] *European Data Protection Board*, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, S. 9.
[1051] *Ambrock/Karg*, ZD 2017, 154 (158).
[1052] Vgl. zu Verboten zum Schutz der Menschenwürde: VG Neustadt, NVwZ 1993, 98 – Zwergenweitwurf, BVerwGE 64, 274 – Peepshow I; BVerwGE 115, 189 – Omega, welche selbst wiederum dem Vorwurf eines Eingriffs in die Menschenwürde ausgesetzt sind: VG Weimar, Urteil vom 06.04.2016 – 3 K 1422/14 We, Rn. 18; vgl. auch OVG Lüneburg, Urteil vom 18.02.2010 – 1 LC 244/07, Rn. 71.
[1053] *Buchner/Kühling*, DuD 2017, 544 (545); *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 108; *Kamp/Rost*, DuD 2013, 80 (82); *Krauß u. a.*, DuD 2017, 217 (219); *Rihaczek*, DuD 2003, 667 (667); *Roßnagel u. a.*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, S. 91; *Seidel*, ZG 2014, 153 (155); *Simitis*, NJW 1984, 398 (401); *Veil*, NVwZ 2018, 686 (688).

trägt.[1054] Wesentliche Kriterien hierfür sind die Informiertheit, Freiwilligkeit und Reversibilität.[1055] Ist eine Entscheidung (rechtlich oder zumindest praktisch) unabänderlich, wäre es durchaus diskutierbar, neben einer ausdrücklichen Einwilligung weitere Schutzmaßnahmen zu fordern.[1056] Andererseits wäre ebenfalls eine Autonomieeinschränkung gegeben, wenn betroffenen Personen das Recht abgesprochen würde, die sie betreffenden Daten zu teilen.[1057] Insofern reflektiert Art. 9 Abs. 2 Buchst. e DSGVO die Veröffentlichung besonderer Kategorien personenbezogener Daten. Folglich kann betroffenen Personen nicht verwehrt werden, einen aus einem unsicheren Drittland betriebenen Kommunikationsdienst ohne besondere Schutzgarantien zu nutzen, solange sie tatsächlich ausreichend über diesen Umstand informiert sind. Dementsprechend erscheint es auch sachgerecht einen strengen Maßstab an die Bereitstellung der Information zu stellen.

Im Hinblick auf Beschäftigten stellt sich wiederum die Frage der Freiwilligkeit, also ob sie eine echte Wahl haben und ohne Nachteile zu erleiden die Einwilligung verweigern oder widerrufen können. [1058] Die Übertragung des Grundsatzes der differenzierten Einwilligung auf die Auswahl von Zielländern dürfte zwar zu weit gehen, da dann eine Datenverarbeitung jeweils in und außerhalb der EU angeboten werden müsste.[1059] Allerdings eignet sich die Einwilligung wegen ihrer Widerruflichkeit nicht für wiederholte, routinemäßige oder systematische Datenübermittlungen.[1060] Im Rahmen von Messengerdiensten gilt zu bedenken, dass die bekanntesten nicht interoperabel ausgestaltet sind, sodass keine parallelen Strukturen aufgebaut werden können. Dementsprechend wären diejenigen Beschäftigten, die in einen Drittstaatentransfer nicht einwilligen oder ihre Einwilligung widerrufen von diesem Kommunikationsweg ausgeschlossen. Aufgrund der auftretenden Gruppendynamik kann eine Freiwilligkeit kaum begründet werden, wenn einzelne Mitarbeitende von einem Kommunikationskanal ausgeschlossen werden. Daher scheidet die Einwilligung für die Einführung von Messengerdiensten mit Datentransfer in unsichere Drittstaaten für die interne Unternehmenskommunikation aus.[1061]

Kommunizieren Mitarbeitende im Namen eines Unternehmens extern mit Kundschaft und/oder Geschäftskontakten, welche in einen Drittstaatentransfer wirksam eingewilligt haben, gelten die gleichen Bedenken bezüglich der Beschäftigtenseite: kann eine Person einen bestimmten Jobzuschnitt im Bereich Kundenkontakt ohne Einwilligung nicht ausüben und müsste eine Versetzung oder schlimmstenfalls Kündigung fürchten, ist eine Einwilligung nicht freiwillig.

[1054] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 174 ff.; 307 ff.

[1055] *Picot u. a.*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 169 (174).

[1056] Neben der Sicherung von Individualrechten kommt dem Datenschutz auch ein objektiv-rechtlicher Gehalt zu: *Bäcker*, Der Staat 2012, 91 (95); *Boehme-Neßler*, International Data Privacy Law 2016, 222 (226); *Winter*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 37 (46).

[1057] Gewisse Beschränkungen wären hingegen mit dem Argument der Mehrrelationalität möglich: Daten beziehen sich oftmals nicht nur auf eine betroffene Person, sondern erlauben oftmals Rückschlüsse auf weitere Betroffene, vgl. *Wagner*, Datenökonomie und Selbstdatenschutz, S. 200 f.

[1058] *Schwartmann/Burkhardt*, ZD 2021, 235 (236); *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 11; *Schantz,* in: BeckOK DatenschutzR Art. 49 Rn. 16; *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 49 Rn. 10; *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 49 Rn. 16; *Ambrock/Karg*, ZD 2017, 154 (157). Von einer echten Wahl bei karriereföndernden Verarbeitungsvorgängen ausgehend: *Klug,* in: Gola DS-GVO, Art. 49 Rn. 5.

[1059] *Schantz,* in: BeckOK DatenschutzR Art. 49 Rn. 18. *Ambrock/Karg* sprechen demgegenüber von zwei getrennten Einwilligungen: in den Datenverarbeitungsvorgang selbst und in den Drittstaatentransfer: *Ambrock/Karg*, ZD 2017, 154 (158). Sind beide Vorgänge untrennbar verknüpft, dürfte der ersten Einwilligung allerdings keinerlei Bedeutung zukommen.

[1060] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 11. Aufgrund des Ausnahmecharakters gehen *Ambrock/Karg* darüber hinaus davon aus, dass Art. 49 DSGVO nur für Ausnahmesituationen mit einmaligem Charakter einschlägig sei: *Ambrock/Karg*, ZD 2017, 154 (157). Dies würde durch die im Singular formulierten Erwägungsgründe 111-113 deutlich.

[1061] Im Ergebnis so auch für Bürosoftware: *Schwartmann/Burkhardt*, ZD 2021, 235 (236).

Sonstige Ausnahmen im Beschäftigtenkontext: Im Hinblick auf die Erforderlichkeit zur Erfüllung des Arbeitsvertrags gelten ebenfalls strenge Maßstäbe: Nützlichkeit alleine reicht nicht aus, es müsste ein „direkter und objektiver Zusammenhang“ zum Vertrag bestehen und zudem ist fraglich, ob „Ausnahmen für bestimmte Fälle“ über Einzelausnahmen hinausgehen und damit wiederkehrende Übermittlungen legitimieren können.[1062] Stimmen aus der Literatur sehen hingegen dort den Ausnahmecharakter als erfüllt an, wenn die Pflege zu Auslandskontakten in Drittländern und damit die Übermittlung von Daten bereits im Arbeitsvertrag zwischen Beschäftigten und Unternehmen hinreichend deutlich zum Ausdruck kommt, bspw. wenn Beschäftigte spezifisch für Einkaufs- oder Verkaufskontakte mit Drittländern eingestellt wurden.[1063] Umstritten ist, ob bei Matrixstrukturen, auch regelmäßige Kommunikation zwischen konzernangehörigen Einheiten wie bspw. Berichtspflichten an Fachvorgesetze in internationalen Konzernstrukturen auf Grundlage des Arbeitsvertrags erfüllt sowie konzernweite Kontaktdatenverzeichnisse gepflegt werden dürfen.[1064] Kritisiert wird hierbei, dass keine „gelegentliche“ Übermittlung mehr gegeben wäre (vgl. EG 111 S. 1 DSGVO).[1065] Im Ergebnis ist davon auszugehen, dass wiederholte, gleichgelagerte Übermittlungen innerhalb von Konzernen und Unternehmensgruppen auf geeignete Garantien nach Art. 46 DSGVO gestützt werden sollten oder unterbleiben müssten.[1066]

Der Einsatz von Messengern mit Drittstaatentransfer wäre auch nicht über „zwingende berechtigte Interessen“ legitimierbar, da wiederholte oder routinemäßige Übermittlungen explizit nicht darunter fallen sollen.[1067] Mindestens wären geeignete und angemessene Schutzgarantien zu ergreifen, wie bspw. eine Datentrennung durch Softwarelösungen oder separate Endgeräte, sodass keine personenbezogenen Daten der Beschäftigten von Datentransfers in Drittstaaten durch einen Messengerdienstanbieter betroffen sind; Auftreten in Unternehmensrollen (wie bspw. IT-Support, Kundenservice, Rechtsabteilung, etc.), sodass eine Zuordnung der Meta- und Inhaltsdaten zu einer konkreten Person nicht möglich ist oder zumindest erschwert ist sowie Hinweise auf andere, mögliche Kommunikationskanäle. Da es sich bei der Interessenabwägung in diesem Kontext um eine „Ausnahme unter den Ausnahmen“ handelt,[1068] dürfte sie in der Praxis kaum Drittlandübermittlungen rechtfertigen.[1069]

Daraus folgt:

- Der Rückgriff auf einen der Ausnahmetatbestände des Art. 49 DSGVO scheidet zur Nutzung eines Messengerdienstes, der aus einem unsicheren Drittland betrieben wird, für die Kommunikation *innerhalb* eines Unternehmens ohne internationale Unternehmensstruktur kategorisch aus.
- Bei internationalen Unternehmen bestehen erhebliche Zweifel, ob die Abwicklung der *gesamten* Unternehmenskommunikation über Drittlanddienste das Kriterium der Erforderlichkeit erfüllt. Angesichts der restriktiven Auslegung sollten Datenübermittlungen auf Informationen beschränkt werden, die auch mit Kolleg*innen im Drittland ausgetauscht werden müssen.[1070] Hier können On-Premise-Lösungen oder Angebote innerhalb der EU oder eines Staates mit Angemessenheitsbeschluss genutzt werden.

[1062] *European Data Protection Board*, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, S. 10; *Schwartmann/Burkhardt*, ZD 2021, 235 (236); *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 49 Rn. 19; *Rohrlich*, ZAP 2020, 1265 (1269).
[1063] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 15; *Gabel,* in: Taeger/Gabel - DSGVO/BDSG Art. 49 Rn. 8.
[1064] bejahend: *Klug,* in: Gola DS-GVO, Art. 49 Rn. 6; *Schantz,* in: NK Datenschutzrecht Art. 49 Rn. 23; *Gabel,* in: Taeger/Gabel - DSGVO/BDSG Art. 49 Rn. 8.
[1065] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 16.
[1066] *Lange/Filip,* in: BeckOK DatenschutzR Art. 49 Rn. 16; ähnlich *Schantz,* in: NK Datenschutzrecht Art. 49 Rn. 24; *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 49 Rn. 19.
[1067] *Klug,* in: Gola DS-GVO, Art. 49 Rn. 12; *Pauly* in: Paal/Pauly - DS-GVO BDSG Art. 49 Rn. 28; *Voigt,* in: Konzerndatenschutz, Kap. 2 Rn. 32.
[1068] *Schantz,* in: NK Datenschutzrecht Art. 49 Rn. 52.
[1069] *Voigt,* in: Konzerndatenschutz, Kap. 2 Rn. 34.
[1070] Vgl. das vom EDSA angeführte Beispiel der Zentralisierung von Verwaltungsfunktionen, welches nicht als Erforderlich eingestuft wird: *European Data Protection Board*, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, S. 12; *Gabel,* in: Taeger/Gabel - DSGVO/BDSG Art. 49 Rn. 8; *Klug,* in: Gola DS-GVO, Art. 49 Rn. 6; *Zerdick,* in: Ehmann/Selmayr - DSGVO Art. 49 Rn. 10.

- Sollen/müssen über einen Messengerdienst Informationen mit Kundschaft oder Geschäftskontakten im Drittland ausgetauscht werden, welche (auch) eine Übermittlung von Beschäftigtendaten impliziert, so sollte dies bereits bei Einstellung und im Arbeitsvertrag ausreichend kommuniziert werden. Reine Praktikabilitätsgründe hierfür Drittlanddienste ohne geeignete Garantien zu nutzen, dürften das Erforderlichkeitskriterium nicht erfüllen.
- Soll ein Kommunikationskanal eröffnet werden, um auch auf besonders beliebten oder sämtlichen Messengerdiensten präsent zu sein, ohne dass ein spezifischer Auslandsbezug gegeben ist und weder ein Angemessenheitsbeschluss vorliegt noch geeignete Garantien nach Art. 46 DSGVO umsetzbar sind, gilt folgendes:
  - Betroffene Personen, die einen Drittlanddienst freiwillig in informierter Weise nutzen, können ausdrücklich einwilligen, sofern keine die Freiwilligkeit und Transparenz beschränkende Umstände vorliegen (z.B. besonders marktmächtige Stellung, fehlende alternative Optionen zur Kontaktaufnahme, fehlender Gefahrenhinweis etc.). Für routinemäßige Kommunikationsvorgänge bestehen allerdings bedenken im Hinblick auf den Ausnahmecharakter. Der/die Verantwortliche(n) sollte die Einwilligung dokumentieren, um diese nachweisen zu können.
  - Erfolgt die Drittlanddatenübermittlung zur Vertragserfüllung, ist ein restriktiver Maßstab an die Erforderlichkeit anzulegen: so fallen Follow-Up-Maßnahmen, d.h. Marketingmaßnahmen im Anschluss an die eigentliche Vertragserfüllung nicht mehr unter den Ausnahmetatbestand.[1071]
  - Im Hinblick auf betroffene Beschäftigtendaten muss der Drittlandbezug sowie die Erforderlichkeit bereits im Arbeitsvertrag hinreichend deutlich zum Ausdruck kommen, sodass die Betreuung bestimmter Kommunikationskanäle Gegenstand der geschuldeten Tätigkeit sein müsste. Um Risiken entsprechend des risikobasierten Ansatzes zu minimieren, können unterschiedliche technisch-organisatorische Maßnahmen ergriffen werden, wie die Gewährleistung der Nichtverkettbarkeit durch Datentrennung und Nutzung von Pseudonymen/Unternehmensrollen.

Der Europäische Datenschutzausschuss veröffentlichte Hilfestellungen im Hinblick auf Drittstaatentransfers:[1072]

[1071] *Gabel,* in: Taeger/Gabel - DSGVO/BDSG Art. 49 Rn. 8; *Klug,* in: Gola DS-GVO, Art. 49 Rn. 6.
[1072] *European Data Protection Board*, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0.

European Data Protection Board, Recommendations 01/2020

- **Step 1:** Kenne deine Datentransfers
- **Step 2:** Identifiziere die Transferregeln (Angemessenheitsbeschluss, SCC, BCR, etc.)
  - ➔ Sichern diese ein im Wesentlichen gleichwertiges Schutzniveau?
- **Step 3:** Bewerte, ob das Übermittlungsinstrument nach Art. 46 DSGVO, auf das sich der Transfer stützt, unter Berücksichtigung aller Umstände des Einzelfalls wirksam ist.
  - ➔ Unterliegt der Empfänger im Drittland Rechtsvorschriften und Praktiken, welche die Durchsetzung der Datenschutzrechte hindern?
- **Step 4:** Umsetzung von Zusatzschutzmaßnahmen: diese sollten technischer Natur sein und können durch vertragliche und/ oder organisatorische Maßnahmen ergänzt werden
  - ➔ Die Auswahl orientiert sich an den zu kompensierenden Risiken um Drittland sowie Art und Umfang der Datenübermittlung
- **Step 5:** Umsetzung der Verfahrensschritte, inkl. wirksamer zusätzlicher Maßnahmen (ggf. Einholung erforderlicher Erklärungen/Genehmigungen, etc.)
- **Step 6:** Re-Evaluation in angemessenen Abständen

Als nicht abschließende Beispiele technischer Maßnahmen – welche je nach Kontext und spezifischer Schutzwirkung auszuwählen sind – nennt der EDSA folgende Maßnahmen:[1073]

- **Verschlüsselung:** Bei Datenspeicherung für Sicherungszwecke und andere Zwecke, die keinen Zugriff auf die Daten im Klartext erfordern: Nutzung eines Verschlüsselungsalgorithmus, der z. B. im Hinblick auf Schlüssellänge, Betriebsmodus, etc. dem Stand der Technik entspricht und robust gegen Brute-Force-Angriffe ist. Die Stärke der Verschlüsselung und die Schlüssellänge müssen dem spezifischen Zeitraum Rechnung tragen, in dem die Vertraulichkeit der verschlüsselten personenbezogenen Daten gewahrt bleiben muss. Der Verschlüsselungsalgorithmus muss korrekt und durch ordnungsgemäß gewartete Software ohne bekannte Schwachstellen implementiert sein, deren Konformität mit der Spezifikation des gewählten Algorithmus überprüft wurde, z. B. durch Zertifizierung. Die Schlüssel müssen zuverlässig verwaltet werden und dürfen ausschließlich in der Kontrolle des Datenexporteurs stehen.
- **Pseudonymisierung:** in einer Weise, dass die personenbezogenen Daten weder einer bestimmten betroffenen Person zugeordnet werden können noch dazu verwendet werden können, die betroffene Person ohne die Verwendung zusätzlicher Informationen aus einer größeren Gruppe herauszugreifen. Identifizierende Informationen dürfen ausschließlich beim Exporteur vorhanden sein und durch diesen kontrolliert werden. Die Weitergabe oder unbefugte Nutzung dieser zusätzlichen Informationen muss durch geeignete technische und organisatorische Garantien verhindert werden. Der Verantwortliche

[1073] *European Data Protection Board*, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, S. 28 ff.

muss durch eine gründliche Analyse der betreffenden Daten feststellen, dass die pseudonymisierten Daten auch bei einem Abgleich mit sonstigen Informationen nicht einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

European Data Protection Board, Recommendations 01/2020

Es ist zu beachten, dass in vielen Situationen Faktoren, die für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität einer natürlichen Person, ihren physischen Standort oder ihre Interaktion mit einem internetbasierten Dienst zu bestimmten Zeitpunkten spezifisch sind, die Identifizierung dieser Person ermöglichen können, auch wenn ihr Name, ihre Adresse oder andere eindeutige Identifikatoren weggelassen werden. Dies gilt insbesondere dann, wenn die Daten die Nutzung von Informationsdiensten betreffen (Zeitpunkt des Zugriffs, Reihenfolge der abgerufenen Funktionen, Merkmale des verwendeten Geräts usw.). Diese Dienste könnten, wie der Importeur personenbezogener Daten, verpflichtet sein, denselben Behörden in ihrem Zuständigkeitsbereich Zugang zu gewähren, die dann wahrscheinlich über Daten über die Nutzung dieser Informationsdienste durch die Zielperson(en) verfügen werden.

- **Transportverschlüsselung:** sofern Gefahren eines unzulässigen Datenzugriffs den Transportweg betreffen und die Verschlüsselungsprotokolle dem Stand der Technik entsprechen sowie wirksamen Schutz gegen aktive und passive Angriffe mit bekannten Mitteln bieten und
  - sich die an der Kommunikation beteiligten Parteien auf eine vertrauenswürdige Zertifizierungsstelle oder Infrastruktur für öffentliche Schlüssel einigen,
  - spezifische Schutzmaßnahmen nach dem Stand der Technik gegen aktive und passive Angriffe auf die sendenden und empfangenden Systeme angewandt werden, einschließlich Tests auf Software-Schwachstellen und mögliche Hintertüren,
  - für den Fall, dass die Transportverschlüsselung aufgrund von Erfahrungen mit Schwachstellen der Infrastruktur oder der verwendeten Software allein keine angemessene Sicherheit bietet, personenbezogene Daten auch auf der Anwendungsschicht mit dem Stand der Technik entsprechenden Verschlüsselungsverfahren Ende-zu-Ende verschlüsselt werden,
  - der Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. Schlüssellänge, ggf. Betriebsmodus) dem Stand der Technik entsprechen und unter Berücksichtigung der ihnen zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute-Force-Angriffe) als robust gegenüber einer Kryptoanalyse durch Dritte bei der Übermittlung von Daten in dieses Drittland angesehen werden können,
  - die Stärke der Verschlüsselung dem spezifischen Zeitraum Rechnung trägt, in dem die Vertraulichkeit der verschlüsselten personenbezogenen Daten gewahrt bleiben muss,
  - der Verschlüsselungsalgorithmus korrekt und durch ordnungsgemäß gewartete Software ohne bekannte Schwachstellen implementiert wird, deren Konformität mit der Spezifikation des gewählten Algorithmus überprüft wurde, z. B. durch Zertifizierung,
  - die Schlüssel werden vom Exporteur oder von einer Stelle, der der Exporteur vertraut und die ein

im Wesentlichen gleichwertiges Schutzniveau bietet, zuverlässig verwaltet (d. h. erzeugt, verwaltet, gespeichert, gegebenenfalls mit der Identität des vorgesehenen Empfängers verbunden und widerrufen).

— **Split oder multi-party processing:** Die Daten werden zwischen unabhängigen Auftragsverarbeitern in unterschiedlichen Rechtsordnungen so aufgeteilt, dass kein Teil, den ein einzelner Verarbeiter erhält, ausreicht, um die personenbezogenen Daten ganz oder teilweise zu rekonstruieren und damit Personen zu identifizieren. Der Datenexporteur erhält das Ergebnis der Verarbeitung von jedem der Auftragsverarbeiter unabhängig und fügt die erhaltenen Teile zusammen, um das Endergebnis zu erhalten, das personenbezogene oder aggregierte Daten darstellen kann. Hierfür können auch sicherer Mehrparteienberechnungen zum Einsatz kommen, und zwar so, dass keinem von ihnen Informationen offenbart werden, die sie nicht schon vor der Berechnung besitzen. Der für die gemeinsame Berechnung verwendete Algorithmus muss gegen aktive Angreifer sicher sein. Der Verantwortliche muss nachweisen können, dass selbst mit Abgleich weiterer (im Drittland) verfügbarer Daten, kein Personenbezug hergestellt werden kann.

4.2.1.2 Datenübermittlung in die USA

Im Hinblick auf Datenübermittlungen in die USA besteht zunächst die Problematik, dass kein einheitlich normiertes Datenschutzrecht existiert und auch kein den EU-Standards entsprechendes angemessenes Datenschutzniveau angenommen werden kann.[1074] Bis zum Safe-Harbor-Urteil (bzw. Schrems I) des EuGHs konnten Datenübermittlungen trotzdem auf das Safe-Harbor-Abkommen gestützt werden.[1075] Das Nachfolgeabkommen wurde Privacy Shield getauft.[1076] Bis zum 16.07.2020 konnten personenbezogenen Daten aus der EU auf Grundlage dieses Privacy Shield-Abkommens, das datenschutzrechtlich als eine Garantie für eine Datenübermittlung nach Art. 46 Abs. 2 Buchst. c DSGVO zu betrachten war, in die USA übermittelt werden.[1077] Mit dem Schrems II-Urteil vom 16.07.2020 hat der EuGH auch dieses Abkommen für unwirksam erklärt.[1078] Das Gericht begründet seine Entscheidung damit, dass das US-Recht – insbesondere die Überwachungsprogramme und Zugriffsbefugnisse der US-Behörden, welche nach Ansicht des EuGHs unverhältnismäßig geregelt sind, – für die vom US-Recht adressierten Datenverarbeiter gegenüber den Grundsätzen des Privacy Shield Vorrang genießen.[1079] Daraus folgt, dass es an wirksamen Rechtsschutzinstrumenten für EU-Bürger*innen mangele, gegen Maßnahmen von US-Behörden vorzugehen und Rechte durchzusetzen.[1080] Die Entscheidung führt zur Rechtsfolge, dass Datenübermittlungen, die bis dahin auf Grundlage des Privacy Shield-Abkommens erfolgten, nun entweder auf eine andere alternative Rechtsgrundlage gestützt oder ausgesetzt werden müssen.[1081]

Im Hinblick auf den Einsatz von Standardvertragsklauseln betonte der EuGH, dass es dem Verantwortlichen bzw. seinem Auftragsverarbeiter obliegt, in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem

[1074] *Voigt,* in: Konzerndatenschutz, Kap. 2 Rn. 8.
[1075] EuGH, Urteil vom 06.10.2015 – C-362/14 – Schrems I.
[1076] Ausführlich zum Privacy Shield: *Spies,* in: Konzerndatenschutz, Kap. 3.
[1077] *Ulbricht,* in: *Mehner*, Messenger Marketing, S. 76.
[1078] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II.
[1079] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 163 ff.
[1080] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 176 ff.
[1081] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 45 Rn. 24c.

Empfänger der Übermittlung – zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und erforderlichenfalls mehr Garantien als die durch diese Klauseln gebotenen zu gewähren.[1082] Sie sind verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auszusetzen oder zu beenden, wenn das Recht dieses Drittlands dem Empfänger aus der Union übermittelter personenbezogener Daten Verpflichtungen auferlegt, die den genannten Klauseln widersprechen und daher geeignet sind, die vertragliche Garantie eines angemessenen Schutzniveaus hinsichtlich des Zugangs der Behörden dieses Drittlands zu diesen Daten zu untergraben.[1083] Damit etablierte der EuGH eine fortlaufende Prüfpflicht des Verantwortlichen in Zusammenarbeit mit dem Empfänger, das Recht sowie Entwicklungen des Rechts im Bestimmungsland zu analysieren und dabei besonderes Augenmerk auf die nationalen Sicherheitsgesetze des jeweiligen Bestimmungsdrittlands und deren praktische Handhabung zu legen.[1084] Im Anschluss an die Entscheidung betonte der EDSA die einzelfallbezogene Überprüfung des Datenschutzniveaus in dem betreffenden Drittland auf seine Angemessenheit, wofür die Kriterien des Art. 45 Abs. 2 DSGVO als Maßstab herangezogen werden können, sowie die Berücksichtigung der Umstände der Übermittlung sowie potentiell einzubeziehende Maßnahmen.[1085] Die DSK kommt zur Ansicht, dass Standarddatenschutzklauseln ohne zusätzliche Maßnahmen für Datenübermittlungen in die USA grundsätzlich nicht mehr ausreichend seien.[1086] Insbesondere wird angesichts der Rechtslage in den USA bezweifelt, dass Regelungen der SCC vor Ort wirksam durchsetzbar sind.[1087] Eine Schritt-für-Schritt-Anleitung zur Umsetzung der Prüfungspunkte inklusiver grafischer Übersicht wird vom Landesdatenschutzbeauftragten für Rheinland-Pfalz bereitgestellt.[1088] Schlussendlich wird konstatiert, der EuGH habe Datenübermittlungen in die USA unter SCC unter kaum erfüllbare Bedingungen gestellt.[1089] Diese Wertungen der Schrems-II-Entscheidung sind auch auf andere Garantien nach Art. 46 DSGVO genannten Garantien übertragbar, sodass diese auch bei Binding Corporate Rules Anwendung finden dürften.[1090]

Unklar war, welche zusätzlichen Maßnahmen eine Datenübermittlung in die USA legitimieren können. Der EuGH hat diese Frage offengelassen.[1091] Vertragliche Lösungen allein dürften auch nach Ansicht des EDSA ausscheiden.[1092] Technische Maßnahmen wie Verschlüsselung und/oder Pseudonymisierung könnten Risiken gegenüber Zugriffen drittstaatlicher Behörden mitigieren.[1093]

[1082] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 134.
[1083] EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 135
[1084] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 46 Rn. 12b.
[1085] *European Data Protection Board*, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems, S. 2 ff.; *Schwartmann/Burkhardt*, ZD 2021, 235 (235).
[1086] DSK, Pressemitteilung vom 28.7.2020: Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II“) stärkt den Datenschutz für EU-Bürgerinnen und Bürger; abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf [letzter Abruf 18.08.2021].
[1087] *Rohrlich*, ZAP 2020, 1265 (1269).
[1088] Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz, Datenübermittlung in Drittländer, Stand: 24.7.2020; abrufbar unter: https://www.datenschutz.rlp.de/de/themenfelder-themen/datenuebermittlung-in-drittlaender/, sowie grafische Übersicht unter: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Pruefschritte_Datenuebermittlung_in_Drittlaender_nach_Schrems_II.pdf [letzter Abruf 18.08.2021].
[1089] *Schwartmann/Burkhardt*, ZD 2021, 235 (235).
[1090] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 46 Rn. 12d.
[1091] *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 46 Rn. 12a; *Schwartmann/Burkhardt*, ZD 2021, 235 (235).
[1092] *European Data Protection Board*, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems, S. 5; *Schwartmann/Burkhardt*, ZD 2021, 235 (235).
[1093] *European Data Protection Board*, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0.

Zusammenfassend bliebt festzuhalten:

- Für Datenübermittlungen in die USA besteht kein Angemessenheitsbeschluss oder Äquivalent.
- Der Abschluss von Standardvertragsklauseln und Binding Corporate Rules reichen allein nicht aus, um Datenübermittlungen in die USA zu legitimieren. Zusätzlich muss über geeignete technische und/oder organisatorische Maßnahmen auch sichergestellt werden, dass diese eingehalten werden können.

BfDI FAQ zur Nutzung von Skype for Business

https://www.bfdi.bund.de/DE/Buerger/Inhalte/Arbeit-Besch%C3%A4ftigung/Besch%C3%A4ftigtendaten-schutz/FAQ_Besch%C3%A4ftigtendatenschutz.html

- „Bei der Übermittlung personenbezogener Daten an ein Unternehmen in den USA bestehen aktuell grundsätzliche Bedenken hinsichtlich der Nutzung von Skype for Business. Dies insbesondere wegen des potenziellen **Abflusses von Daten an den Mutterkonzern Microsoft** sowie der damit verbundenen Verarbeitung an Orten außerhalb des Geltungsbereichs der DSGVO."
- „In Einzelfällen und unter Anwendung umfangreicher technisch-organisatorischer Maßnahmen kann die Nutzung von Skype for Business möglich sein. Hierzu zählen beispielsweise das Hosting von Skype for Business auf **eigenen Servern** ohne die Möglichkeit des Zugriffs von außerhalb des Netzwerkes und die Verhinderung des Abflusses von Daten an Microsoft. Die Verhinderung des Abflusses von Daten ist technisch-organisatorisch sicherzustellen und **nachvollziehbar darzulegen**."

4.2.1.3 Datenübermittlung in die Schweiz

Datenverarbeitungen in Drittländern, zu denen ein Angemessenheitsbeschluss der EU-Kommission vorliegt, können unter den gleichen Anforderungen wie eine EU-interne Datenweitergabe erfolgen. Unter Berücksichtigung der gesamten nationalen Rechtsordnung im Drittland sowie der gelebten Rechtspraxis vor Ort fasst die EU-Kommission den Angemessenheitsbeschluss unter den Anforderungen des Art. 45 Abs. 2 DSGVO.[1094] Angemessenheitsbeschlüsse müssen regelmäßig überprüft werden. Bei negativem Ausgang ist ein Widerruf möglich.

Zunächst bleiben die unter der Datenschutzrichtlinie 95/46/EG erlassenen Angemessenheitsbeschlüsse der EU-Kommission auch unter der DSGVO in Kraft – darunter auch der Beschluss für die Schweiz. [1095] Allerdings muss die Schweiz auch in Zukunft über ein angemessenes Schutzniveau verfügen, um weiterhin eine Anerkennung der EU-Kommission zu erhalten. Angesichts der nachhaltigen Novellierungen des Datenschutzrechts in der EU in Form der Richtlinie (EU) 2016/680 über den Datenschutz im Bereich der Strafverfolgung (Schengen-RL) sowie der DSGVO, wurde auch für das schweizerische Recht die Anpassung der Datenschutzgesetzgebung notwendig.[1096] Die Annäherung an das EU-Recht ist dabei sowohl aus völkerrechtlichen Verträgen (Datenschutzübereinkommen SEV 108 des Europarats [Europarats-Konvention]) als auch aufgrund der

[1094] *Scheja/Reibach/Reichert,* in: Leupold/Wiebe/Glossner - IT-Recht, Teil 6.6 Rn. 298.
[1095] *Scheja/Reibach/Reichert,* in: Leupold/Wiebe/Glossner - IT-Recht, Teil 6.6 Rn. 299.
[1096] *Widmer,* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 35 Rn. 28.

engen wirtschaftlichen Verflechtung mit EU-Staaten geboten.[1097] Mit diesem Ziel legte der Schweizerische Bundesrat (Regierung der Schweizerischen Eidgenossenschaft) dem Parlament bereits 2017 eine Botschaft[1098] über die „Totalrevision" des Datenschutzgesetzes (DSG) zu Beratung vor.[1099] Das DSG sowie einzelne Regelungen der Kantone sollten zeitnah an die DSGVO angepasst werden. Allerdings geriet das Projekt ins Stocken, sodass zunächst der Datenschutz betreffend den Bereich des Strafrechts und der Strafvollstreckung abgetrennt und vorab geregelt wurde.[1100] Im Hinblick auf die Angemessenheit des Datenschutzniveaus zog das Revisionsprojekt wesentliche kontrovers diskutierte Kritikpunkte auf sich:

- Anders als die DSGVO soll der DSG-Entwurf nicht alle Verstöße mit Sanktionen belegen und Bußgelder nur bei Vorsatz vorsehen.[1101] Als Maximalbetrag werden lediglich CHF 250.000 vorgesehen (Art. 60 ff. nDSG). Die Sanktionen richten sich allerdings primär gegen die handelnden natürlichen Personen und nur subsidiär gegen Unternehmen, sodass auch von einem schärferen Strafcharakter gesprochen werden kann.[1102]
- Die Bestellung eines Datenschutzbeauftragten (Datenschutzberater) soll freiwillig sein (Art. 10 nDSG).[1103] Muss nach einer DSFA die Datenschutzaufsichtsbehörde konsultiert werden, kann dies bei Konsultation der Datenschutzberater*in unterbleiben (Art. 23 Abs. 4 nDSG).

Andere Kritikpunkte, welche eine Abweichung vom DSGVO-Konzept bedeutet hätten, wurden nach Beratungen im Nationalrat und Ständerat noch angepasst.[1104] So wurde eine Definition des Profilings sowie ein Recht auf Datenherausgabe und -übertragung aufgenommen.[1105] Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) begrüßte diese Annäherungen.[1106]Die Vernehmlassung zur Totalrevision der Verordnung zum Bundesgesetz über den Datenschutz wurde im Juni 2021 vom Bundesrat eröffnet.[1107] Sodann wurde das neue Datenschutzgesetz (nDSG) in der Herbstsession 2020 vom Parlament verabschiedet. Allerdings müssen vor Inkrafttreten noch die entsprechenden Ausführungsbestimmungen in der Verordnung zum Bundesgesetz über den Datenschutz (VDSG) angepasst werden, denn zahlreiche Bestimmungen des nDSG müssen auf Verordnungsebene konkretisiert werden. Die im Juni 2021 eröffnete Vernehmlassung wird laut Bundesrat voraussichtlich bis am 14. Oktober 2021 dauern.[1108] Die VDSG soll gleichzeitig mit dem neuen DSG in der zweiten Jahreshälfte 2022 in Kraft treten.[1109]

[1097] *Bühlmann/Metin*, ZD 2019, 356 (356); *Weber/Suter,* in: Forgó/Helfrich/Schneider - Betrieblicher Datenschutz, Kap. 5 Rn. 177.
[1098] Hierbei handelt es sich um eine Begründung des Entwurfs durch den Gesetzgeber, vergleichbar mit den Bundestags-Drucksachen. Zu weiteren Hintergründen siehe: *Bühlmann/Metin*, ZD 2019, 356 (356).
[1099] Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941. Alle Ratsunterlagen zur Totalrevision des Datenschutzgesetzes und Änderung weiterer Erlasse abrufbar unter: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/ratsunterlagen?AffairId=20170059&k=PdAffairId:20170059 [letzter Abruf 13.08.2021].
[1100] *Widmer,* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 35 Rn. 30. Bundesamt für Justiz BJ, Stärkung des Datenschutzes, Stand 23.06.2021, abrufbar unter: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html [letzter Zugriff 13.08.2021].
[1101] *Widmer,* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 35 Rn. 32.
[1102] *Bühlmann/Metin*, ZD 2019, 356 (359).
[1103] *Widmer,* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 35 Rn. 32.
[1104] Synopse abrufbar unter: https://www.parlament.ch/centers/eparl/curia/2017/20170059/S3-2%20D.pdf [letzter Abruf 16.08.2021].
[1105] Zur Kritik am Fehlen dieses Rechts im Entwurf: *Widmer,* in: Auer-Reinsdorff/Conrad IT-R-HdB, § 35 Rn. 33; *Bühlmann/Metin*, ZD 2019, 356 (359).
[1106] ZD-Aktuell 2020, 06921
[1107] Bundesamt für Justiz BJ, Stärkung des Datenschutzes, Stand 23.06.2021, abrufbar unter: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html [letzter Zugriff 13.08.2021].
[1108] Der Bundesrat, Revision der Datenschutzverordnung: Bundesrat eröffnet Vernehmlassung, Stand 23.06.2021, abrufbar unter https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-84103.html [13.08.2021].
[1109] Der Bundesrat, Revision der Datenschutzverordnung: Bundesrat eröffnet Vernehmlassung, Stand 23.06.2021, abrufbar unter https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-84103.html [13.08.2021].

Die noch zu konkretisierenden Bestimmungen betreffen u.a. die Mindestanforderungen an die Datensicherheit, die Modalitäten der Informationspflichten und des Auskunftsrechts, die Meldung von Verletzungen der Datensicherheit, Ausnahmen für private Verantwortliche mit weniger als 250 Beschäftigten ein Verzeichnis der Verarbeitungstätigkeiten anzulegen sowie Kriterien für die Übermittlung personenbezogener Daten ins Ausland. Zudem sollen Stellung und Unabhängigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) mit dem nDSG gestärkt werden und die Aufgaben der Datenschutzberater*innen in der Bundesverwaltung präzisiert werden.[1110]

Für Unternehmen in der Schweiz ist die DSGVO zwar grundsätzlich nicht unmittelbar anwendbar, allerdings kann sich eine Anwendbarkeit aus dem Marktortprinzip (vgl. Abschnitt 2.3.2.2) ergeben.[1111] Dann wären für Schweizer Unternehmen sowohl DSGVO als auch nDSG zu beachten.[1112] Hier sollten die – wenn auch geringfügigen – Abweichungen im Detail bedacht werden. Aufgrund der noch ausstehenden Reformarbeiten lässt sich aktuell noch keine Prognose im Hinblick auf die Erneuerung des Angemessenheitsbeschlusses der EU-Kommission abgeben.[1113] Es wird aber davon ausgegangen, dass alle Beteiligten in der Schweiz daran arbeiten werden, die Gefahr eines Widerrufs des bestehenden Beschlusses zu vermeiden.[1114]

4.2.2 Datenzugriffe aus Drittländern

Ebenso problematisch wie nach EU-Recht als unzulässig zu bewertende Zugriffe auf Daten *in* Drittländern (insbesondere durch lokale Behörden), sind solche Zugriffe *aus* Drittländern auf personenbezogene Daten, die innerhalb der EU bzw. des EWR verarbeitet werden.

4.2.2.1 USA

Ob eine Lösung der Datenübermittlungsproblematik für US-amerikanische Kommunikations- und Cloudanbieter über eine Verortung der gesamten Serverinfrastruktur innerhalb der EU (des EWR) gesucht werden kann, erscheint ebenfalls fraglich. Denn im Wege des sog. CLOUD-Acts („Clarifying Lawful Overseas Use of Data Act“) könnte von US-amerikanischen Unternehmen durch Ermittlungsbehörden verlangt werden, dass (auch personenbezogene) Kundendaten an amerikanische Behörden preisgegeben werden müssen, unabhängig davon, wo die Daten gehostet werden.[1115] Das Sicherheitsproblem, welches zur Feststellung des nicht angemessenen Schutzniveaus in den USA führte,[1116] bleibt folglich bestehen. Unternehmen könnten in den USA zu einer Datenübermittlung verpflichtet werden, die nicht mit EU-Recht vereinbar ist.[1117] Adressaten des CLOUD-Acts sind Anbieter elektronischer Kommunikationsdienste sowie Remote-Computing-Dienste, die US-Recht unterfallen.[1118] Gleichzeitig fordert Art. 48 DSGVO, das Datenübermittlungsersuchen drittstaatlicher

[1110] Der Bundesrat, Revision der Datenschutzverordnung: Bundesrat eröffnet Vernehmlassung, Stand 23.06.2021, abrufbar unter https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-84103.html [13.08.2021].
[1111] *Mausbach*, ZD 2019, 450 (451 ff.); *Bühlmann/Metin*, ZD 2019, 356 (357).
[1112] Laut Schweizer Lehre galt (zumindest bisher) das sog. „Auswirkungsprinzip“, sodass es zur Anwendbarkeit Schweizer Rechts kommt, wenn sich die Datenverarbeitung in der Schweiz auswirkt: *Bühlmann/Metin*, ZD 2019, 356 (357); *Weber/Suter,* in: Forgó/Helfrich/Schneider - Betrieblicher Datenschutz, Kap. 5 Rn. 15.
[1113] Mit Blick auf Abweichungen sowie das Sanktionsmodell skeptisch: *Weber/Suter,* in: Forgó/Helfrich/Schneider - Betrieblicher Datenschutz, Kap. 5 Rn. 187.
[1114] *Mausbach*, ZD 2019, 450 (454).
[1115] *Schwartmann/Burkhardt*, ZD 2021, 235 (236); *Gausling*, MMR 2018, 578 (579).
[1116] Vgl. EuGH, Urteil vom 16.07.2020 – C-311/18 – Schrems II, Rn. 178 ff.; *Pauly,* in: Paal/Pauly - DS-GVO BDSG Art. 45 Rn. 24c.
[1117] *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 48 Rn. 25; *Jansen*, ZD 2018, 149 (150).
[1118] *Gausling*, MMR 2018, 578 (579).

Behörden auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sein müssen, um anerkannt und vollstreckt zu werden. Ein solches Rechtshilfeabkommen sieht der CLOUD-Act hingegen nicht als Bedingung.[1119] Die Heranziehung anderer Legitimationsgrundlagen kommt nach Einschätzung des Europäischen Datenschutzausschusses und dem Europäischen Datenschutzbeauftragten (mit Ausnahme extrem gelagerter Einzelfälle) in der Regel kaum zur Zulässigkeit einer Datenübermittlung.[1120] Daher wird auch hier geschlussfolgert, dass für die Legitimation von Kommunikations- oder Cloud-Angeboten die Lösung ausschließlich über eine europäische Datenverarbeitung durch Serverstandorte in der EU nicht funktioniert. [1121] Zusätzlich müssten weitere technischen oder organisatorischen Maßnahmen ergriffen werden. Als Lösungsoptionen werden im Schrifttum unterschiedliche Optionen vorgeschlagen:

- Abspaltung von Unternehmensteilen, um dem Geltungsbereich des US-Rechts zu entgehen und somit nicht mehr als Adressat des CLOUD-Acts zu gelten.[1122]
- Implementierung eines Modells einer Datentreuhand durch einen europäischen Dienstleister: der Zugriff auf personenbezogene Daten erfolgt ausschließlich durch den europäischen Dienstleister, während dem US-Recht unterfallenden Verantwortlichen das Verfügungsrecht entzogen ist.[1123] Die personenbezogenen Daten sind dann nicht mehr „im Besitz, Gewahrsam oder unter der Kontrolle“ des vom CLOUD Act Verpflichteten.
- Implementierung einer clientseitigen Verschlüsselung, sodass es schlicht unmöglich ist, unverschlüsselte und damit lesbare Informationen an amerikanische Behörden herauszugeben.[1124]

Nach eigenen Angaben verfolgt der amerikanische Messengerdienst Signal einen entsprechenden Weg die eigenen Zugriffsmöglichkeiten auf Nutzerdaten technisch zu beschränken: auf der eigenen Webseite wird der Fall einer US-behördlichen Anfrage geschildert, welcher der Dienst nicht nachgekommen sei, da die Daten dem Dienstanbieter schlicht nicht vorliegen.[1125] Lediglich das Datum der Erstellung des Accounts und des letzten Zugriffs auf diesen Account sei der Behörde zurückgemeldet worden.[1126] Entscheidend hierbei ist, dass nicht nur (Kommunikationsinhalts-)Daten auf dem Transportweg verschlüsselt werden, sondern auch die Metadaten nicht oder nur in verschlüsselter (und nicht entschlüsselbarer) Form vorliegen.

4.2.2.2 Schweiz

Auch im Hinblick auf potentielle Datenzugriffe drittstaatlicher Behörden soll als Vergleich zu den USA die Rechtslage in der Schweiz beleuchtet werden. Hier sah sich der schweizer Messenger-App-Anbieter Threema

[1119] *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 48 Rn. 25.
[1120] *European Data Protection Board/European Data Protection Supervisor*, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex), S. 8; *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 48 Rn. 26 ff.
[1121] *Schwartmann/Burkhardt*, ZD 2021, 235 (236).
[1122] *Gausling*, MMR 2018, 578 (582); *Jansen*, ZD 2018, 149 (150).
[1123] *Gausling*, MMR 2018, 578 (582); *Schwartmann/Burkhardt*, ZD 2021, 235 (236). Ein solches Modell haben Microsoft und Deutsche Telekom allerdings bereits wieder beendet: *Schröder,* in: Kühling/Buchner - DS-GVO/BDSG Art. 48 Rn. 29.
[1124] *Schwartmann/Burkhardt*, ZD 2021, 235 (236).
[1125] Signal, Grand jury subpoena for Signal user data, Central District of California, 27.04.2021, https://signal.org/bigbrother/central-california-grand-jury/: Looking back at how Signal works, as the world moves forward, 05.06.2020, https://signal.org/blog/looking-back-as-the-world-moves-forward/ [letzter Abruf 06.07.2021].
[1126] Signal, Grand jury subpoena for Signal user data, Central District of California, 27.04.2021, https://signal.org/bigbrother/central-california-grand-jury/ [letzter Abruf 06.07.2021].

einer Zugriffsanfrage einer Überwachungsbehörde ausgesetzt, welche einen Teil der Verschlüsselung aushebeln wollte.[1127] Der Streit bezog sich zwar nicht auf die Kommunikationsinhalte, allerdings können auch aus einer Echtzeitüberwachung der Metadaten (in der Schweiz als „Randdaten“ bezeichnet), also wer wann mit wem kommuniziert hat, sehr detaillierte Informationen über betroffene Personen abgeleitet werden. Threema verschlüsselt hierbei nicht nur die Chats, sondern auch die Metadaten, wobei die nutzerseitige Verschlüsselung bewirkt, dass selbst der App-Anbieter keine Zugriffsmöglichkeiten auf die Informationen hat. Das Bundesverwaltungsgericht entschied, dass Anbieter*innen von OTT-Diensten, zu welchen auch Threema zählt, nicht den Überwachungspflichten für Anbieter von Fernmeldediensten (Art. 2 Bst. b BÜPF, Art. 3 Bst. b FMG), sondern den weniger weitreichenden Pflichten für Anbieter*innen abgeleiteter Kommunikationsdienste (AAKD) unterstehen (Art. 2 Bst. c BÜPF).[1128] Bei Fernmeldediensten, die eine „fernmeldetechnische Übertragung von Informationen für Dritte“ ermöglichen, steht die technische Vornahme des Informationstransports im Vordergrund.[1129] Diese Dienste unterliegen schweizerischen Vorgaben zur Vorratsdatenspeicherung. Ein Messengerdienst wie Threema hingegen nicht. Die Entscheidung wurde vom Bundesgericht bestätigt.[1130]

4.2.3 Zwischenergebnis zum internationalen Datentransfer

Aufgrund der Schutzpflichten der Datenschutzgrundrechte sowie der Gefahr des Unterschreitens eines angemessenen, grundrechtlich gebotenen Datenschutzniveaus durch Übermittlung personenbezogener Daten in Drittstaaten außerhalb des Geltungsbereichs der DSGVO, stellt diese hohe Legitimationsanforderungen an solche Drittstaatentransfers. Der in der Praxis unkomplizierteste Fall – da ohne weitere Genehmigungen oder Prüfungen umsetzbar – ist der Austausch personenbezogener Daten mit Beteiligten in Drittstaaten, für die ein Angemessenheitsbeschluss der EU-Kommission vorliegt (so bspw. für die Schweiz). Für andere Drittstaaten eröffnen Standardvertragsklauseln und Binding Corporate Rules Wege für eine Datenübermittlung. Für die USA besteht allerdings insofern erhebliche Rechtsunsicherheit, da unklar ist, wieweit US-amerikanische Anbieter von Kommunikations- und Cloudlösungen die notwendigen Klauseln der SCC nach dem zusätzlich für sie maßgeblichen US-amerikanischen Recht einhalten können. Ein Datentransfer an als auch Datenzugriffsmöglichkeiten durch US-amerikanische Unternehmen unterliegen daher weiteren Bedingungen, die ein angemessenes Datenschutzniveau sicherstellen und dabei insbesondere Datenzugriffe US-amerikanischer Behörden, welche aus EU-rechtlicher Perspektive als unverhältnismäßig eingestuft werden, ausschließen. Welche das konkret sind, um Datenschutzrisiken effektiv zu mitigieren, ist noch Grundlage aktueller Diskussionen. Behalten sich US-amerikanische Unternehmen vor, Datenübermittlungen ohne besondere Sicherheitsvorkehrungen in die USA durchzuführen, bestehen erhebliche Bedenken an einem datenschutzkonformen Einsatz dieser Produkte.[1131] Weitere Ausnahmeregelungen für Drittstaatentransfers sind für den vorliegenden Kontext nur in sehr engen Grenzen einschlägig. Insbesondere die Einwilligung als Legitimationsgrundlage

[1127] Netzwoche, Im Streit zwischen Threema und dem Bund steht es 1:0 für den Datenschutz, 30.06.2020, https://www.netzwoche.ch/news/2020-06-03/im-streit-zwischen-threema-und-dem-bund-steht-es-10-fuer-den-datenschutz; Sieber (SRF), Threema muss Behörden keine Daten bereitstellen, 18.05.2021, https://www.srf.ch/news/schweiz/ueberwachung-von-metadaten-threema-muss-behoerden-keine-daten-bereitstellen [letzter Abruf 06.07.2021].
[1128] Bundesverwaltungsgericht (Schweiz), Urteil vom 19.05.2020 – A-550/2019.
[1129] Vgl. Botschaft des Bundesrates vom 27.02.2013 zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), BBl 2013 2683, S. 2707.
[1130] Bundesgericht, Urteil vom 29.04.2021 - 2C_544/2020.
[1131] *Schwartmann/Burkhardt*, ZD 2021, 235 (237).

dürfte im Beschäftigtenkontext mangels Freiwilligkeit regelmäßig ausscheiden. Achtung ist auch dann geboten, wenn Anbieter zwar selbst in der EU/EWR verortet sind, aber Unterauftragnehmer aus den USA zum Einsatz kommen.[1132]

Praxistipp:

(1) Datenlokalität wahren: Verarbeitung personenbezogener Daten physisch innerhalb der EU/des EWR sowie Staaten mit Angemessenheitsbeschluss der EU-Kommission
(2) Vorkehrung treffen gegen Datenherausgabeersuchen von Drittstaaten durch technische Datenminimierungs- und Datenkontrollmaßnahmen, z.B.
    a. Ermöglichung anonymisierter Nutzung
    b. Nutzerseitige Verschlüsselung von Kommunikations- und Metadaten

[1132] *Rohrlich*, ZAP 2020, 1265 (1270).

5 Fallspezifische Einsatzszenarien von Messengerdiensten im Unternehmenskontext

In diesem Kapitel werden im Hinblick auf die Kommunikation im Unternehmenskontext einzelne Fallszenarien aufgeschlüsselt nach interner Kommunikation *im* Unternehmen und externer Kommunikation *mit dem* Unternehmen betrachtet.

5.1 Mitbestimmungsrechte des Betriebsrats

Entscheiden sich Unternehmen für den Einsatz von Messengerdiensten zur internen und / oder externen Kommunikation und Kollaboration, müssen zwingend die Mitbestimmungsrechte des Betriebsrats berücksichtigt werden.

5.1.1 Verhaltensregeln

Im Hinblick auf die Anordnung oder Duldung der Nutzung bestimmter Kommunikationsmittel gilt die Rechtsprechung des Bundesarbeitsgerichts (BAG) zu berücksichtigen: Danach greift auch im Rahmen unverbindlicher Verhaltensregeln (wie bspw. einem „Code of Conduct“ oder Ethik-Richtlinien) das Mitbestimmungsrecht aus § 87 Abs. 1 BetrVG, wenn die Maßnahme des Arbeitgebers darauf gerichtet ist, das Verhalten der Beschäftigten zu steuern oder die Ordnung des Betriebs zu gewährleisten.[1133] § 87 Abs. 1 Nr. 1 BetrVG berechtigt die Betriebsparteien hingegen nicht, in die private Lebensführung der Beschäftigten einzugreifen. Regelungen über private Beziehungen im Betrieb sind aber nicht von vornherein der Mitbestimmung entzogen.[1134] „Betrieb“ ist insofern nicht räumlich, sondern funktional zu verstehen.[1135] Daher kann das Mitbestimmungsrecht auch dann bestehen, wenn es um das Verhalten der Beschäftigte außerhalb der Betriebsstätte, wie bspw. gegenüber Kundschaft und Lieferanten, geht.[1136]

5.1.2 Überwachungssysteme

Bei Einsatz technischer Systeme, die eine Überwachung der Arbeitnehmer ermöglichen, ist ebenfalls der Betriebsrat vorab einzuschalten (§ 87 Abs. 1 Nr. 6 BetrVG).[1137] Das Mitbestimmungsrecht nach § 87 Abs.1 Nr. 6 BetrVG wird allerdings erst ausgelöst, wenn eine Leistungs- oder Verhaltenskontrolle durch eine technische Einrichtung ermöglicht wird. Dies sei laut BAG bspw. der Fall beim Fahrtenschreiber,[1138] nicht jedoch beim Einsatz eines internetbasierten Routenplaners zur Überprüfung einer Fahrtkostenabrechnung.[1139]

- **„Überwachung“** i.S.d. § 87 Abs.1 Nr. 6 BetrVG ist ein Vorgang, durch den Informationen über das Verhalten oder die Leistung der Arbeitnehmer*in erhoben und so aufgezeichnet werden, dass sie zumin-

[1133] BAG, Beschluss vom 22.07.2008 – 1 ABR 40/07, Rn. 57 ff.
[1134] BAG, Beschluss vom 22.07.2008 – 1 ABR 40/07, Rn. 58 m.w.N.
[1135] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03.
[1136] BAG, Beschluss vom 22.07.2008 – 1 ABR 40/07, Rn. 58; BAGE 109, 235, Beschluss vom 27.01.2004 - 1 ABR 7/03.
[1137] *Fitting,* in: Betriebsverfassungsgesetz, § 87 Rn. 225; *Weisser/Färber*, MMR 2015, 506 (509).
[1138] BAG, Beschluss vom 08.11.1994 - 1 ABR 20/94; BAGE 51, 143, Beschluss vom 18.2.1986 - 1 ABR 21/84.
[1139] BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 20 ff.

dest für eine gewisse Dauer verfügbar bleiben, um sie auch späterer Wahrnehmung zugänglich zu machen.[1140] Dabei muss die Überwachung durch die technische Einrichtung selbst bewirkt werden, indem sie auf Grund ihrer technischen Natur unmittelbar, d.h. wenigstens in ihrem Kern das Verhalten oder die Leistung der Beschäftigten kontrolliert.[1141] Dabei ist ausreichend, dass die technische Einrichtung zumindest einen Teil des Überwachungsvorgangs ausführt, sofern sie selbst und automatisch die Daten über bestimmte Vorgänge verarbeitet.[1142]

- Zur Überwachung **„bestimmt“** sind technische Einrichtungen dann, wenn sie objektiv geeignet sind, Verhaltens- oder Leistungsinformationen der Beschäftigten zu erheben und aufzuzeichnen.[1143] Hierbei kommt es auf eine subjektive Überwachungsabsicht des Arbeitgebers nicht an.[1144]
- Ein technisches Überwachungssystem gilt auch dann durch den Arbeitgeber als **„angewendet“**, wenn er bloß im Einvernehmen mit einem Dritten seine Beschäftigten anweist, sich der Überwachung durch dessen technische Einrichtung zu unterwerfen – selbst wenn diese Überwachung in erster Linie oder gar ausschließlich im Interesse des Dritten erfolgt und der Arbeitgeber keinen Zugriff auf die erfassten Daten nehmen kann.[1145] Der Arbeitgeber ist verpflichtet durch entsprechende Vertragsgestaltung mit dem Dritten sicherzustellen, dass der Betriebsrat sein Mitbestimmungsrecht ausüben kann.[1146]

Ob die Einführung und Nutzung eines Kooperations- oder Kommunikationstools wie eines Messengerdienstes das Mitbestimmungsrecht des Betriebsrats auslöst, hängt also entscheidend davon ab, ob mit diesem Werkzeug Daten mit Leistungs- bzw. Verhaltensbezug zu den Beschäftigten aufgezeichnet werden und somit eine Kontrollmöglichkeit entsteht – unabhängig davon, ob der Arbeitgeber diese Option tatsächlich zur Überwachung nutzen will. Hintergrund dieses Mitbestimmungsrechts ist die Gefährdung des Persönlichkeitsrechts der Beschäftigten durch eine technisierte Ermittlung von Verhaltens- und Leistungsdaten, wobei auf diese Weise praktisch ununterbrochen und für die betroffenen Personen oft nicht wahrnehmbar und damit weniger durchschaubar eine ungleich größere Anzahl von Daten erhoben werden kann als bei der Überwachung durch Menschen.[1147] Technische Kontrolleinrichtungen können in Bereiche eindringen, die einer menschlichen Überwachung nicht zugänglich sind und so die Beschäftigten zum Objekt einer Überwachungstechnik machen, der sie sich nicht entziehen können, sodass diese Technologien nur bei gleichberechtigte Mitbestimmung des Betriebsrats zugelassen werden sollen.[1148] Allein das Wissen darum, dass man zum Objekt einer Überwachungstechnik gemacht wird, kann zu erhöhter Abhängigkeit führen und damit die freie Entfaltung der eigenen Persönlichkeit hindern.[1149]

Auch ist darauf hinzuweisen, dass sich der Arbeitgeber der Mitbestimmungspflicht nicht mit dem Argument entziehen kann, ihm seien Verhaltensregeln oder technische Überwachungseinrichtungen von einem Vertragspartner vorgegeben. Vielmehr liegt es in seinem Verantwortungsbereich bspw. über entsprechende Vertragsgestaltung sicherzustellen, dass die ordnungsgemäße Wahrnehmung der Mitbestimmungsrechte des Betriebsrats gewährleistet ist.[1150] Wird eine Technologie im Betrieb eingeführt, die eine Datenverarbeitung

[1140] BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 20; BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03, Rn. 27.
[1141] BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 20; BAG, Beschluss vom 08.11.1994 – 1 ABR 20/94.
[1142] BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 20.
[1143] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03; BAG, Beschluss vom 06.12.1983 - 1 ABR 43/81, NJW 1984, 1476 (1483 f.).
[1144] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03; BAG, NJW 1984, 1476 (1484).
[1145] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03.
[1146] BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03 m.w.N.
[1147] BAG, Beschluss vom 08.11.1994 – 1 ABR 20/94.
[1148] BAG, Beschluss vom 10.12.2013 – 1 ABR 43/12, Rn. 27; BAGE 51, 143, Beschluss vom 18.2.1986 - 1 ABR 21/84.
[1149] BAG, Beschluss vom 08.11.1994 – 1 ABR 20/94.
[1150] BAG, Beschluss vom 27. 1. 2004 – 1 ABR 7/03.

nach § 26 Abs. 1 BDSG erforderlich macht oder auf Grundlage einer Einwilligung umgesetzt werden soll, welche objektiv zur Überwachung der Beschäftigten geeignet ist, muss der Betriebsrat als Vertretung der Arbeitnehmerinteressen zuvor eingebunden werden.

Beispielsweise kann nach der BAG-Rechtsprechung, eine arbeitgeberseitig betriebene Facebookseite, die Postings zum Verhalten und zur Leistung der Beschäftigten ermöglicht, eine technische Einrichtung sein, die zur Überwachung der Beschäftigten im Sinne des § 87 Abs. 1 Nr. 6 BetrVG bestimmt ist.[1151] Sind dabei anfallende Daten einzelnen Beschäftigten nicht zuordenbar (bspw. bei Verwendung einer nicht individualisierten Zugangskennung), kann bei Aufzeichnung der Gesamtleistung einer Gruppe ausnahmsweise eine dem Mitbestimmungsrecht unterliegende Einrichtung vorliegen, wenn der auf die Gruppe ausgeübte Überwachungsdruck auf die einzelnen Gruppenmitglieder durchschlägt. [1152] Ebenfalls als Mitbestimmungspflichtig wurde vom LAG Hamburg die Einrichtung eines Twitter-Accounts eingestuft.[1153] Je nach dem Inhalt der (öffentlich) einsehbaren Antworten auf einen Tweet kann die Arbeitgeberin diese namentlich oder situationsbedingt einer bestimmten Beschäftigten zuordnen und zur Verhaltens- und Leistungskontrolle verwenden, sofern die Nachricht entsprechende Aussagen beinhaltet.[1154] Je nach Gestaltung der Kommunikation und Kollaboration über Messengersysteme können diese Erwägungen ebenfalls relevant sein. Bei Verletzung der Mitbestimmungsrechte besteht ein Anspruch auf Unterlassung der mitbestimmungswidrigen Maßnahmen.

5.1.3 Betriebsvereinbarungen

Der Betriebsrat kann als Interessenvertretung der Beschäftigten mit dem Arbeitgeber eine Betriebsvereinbarung über die Nutzung des Messengerdienstes vereinbaren. Hierbei sind bestimmte Grenzen (Beispielsweise geltende tarifvertraglich Regelungen, Einbezug von relevanten Personen (Datenschutzbeauftragten)) zu beachten. Eine Betriebsvereinbarung ist laut EG 155 bzw. Art. 88 DSGVO („Kollektivvereinbarungen einschließlich Betriebsvereinbarungen“) eine Legitimationsgrundlage für die Verarbeitung von Beschäftigtendaten (analog siehe § 26 Abs. 1 BDSG).[1155]

Soll eine Betriebsvereinbarung über die Nutzung eines Messengerdienstes abgeschlossen werden, entfaltet der Schutz der Persönlichkeitsrechte der Beschäftigten als höherrangiges Recht Rahmenbedingungen bezüglich der Wirksamkeit dieses Gestaltungsinstruments, welche zu parallelen Erwägungen wie der Abwägung unter § 26 BDSG führen.[1156] So stellte das BAG fest, dass der Umstand einer Zustimmung zu einer Überwachungsmaßnahme durch den Betriebsrat allein jedenfalls dann keine legitimierende Wirkung entfalten kann, wenn keine den Eingriff in die Persönlichkeitsrechte rechtfertigenden Tatsachen vorliegen. [1157] Eingriffe sind gerechtfertigt, wenn diese einer Abwägung der widerstreitenden Interessen nach dem Grundsatz der Verhältnismäßigkeit standhalten.[1158] Betriebsratsvereinbarungen sollen die Grenzen eines rechtlich zulässigen Eingriffs insofern nicht zulasten der Beschäftigten verschieben.[1159]

[1151] BAG, Beschluss vom 13.12.2016 – 1 ABR 7/15, Rn. 33 ff.
[1152] BAG, Beschluss vom 13.12.2016 – 1 ABR 7/15, Rn. 27.
[1153] LAG Hamburg, Beschl. v. 13.9.2018 – 2 TaBV 5/18, die Entscheidung wurde mit BAG, Beschluss vom 25.02.2020 - 1 ABR 40/18 allerdings wegen fehlender Antragsbefugnis aufgehoben.
[1154] LAG Hamburg, Beschl. v. 13.9.2018 – 2 TaBV 5/18, Rn. 45.
[1155] Vgl. Zur Wirksamkeit: BAG, Urteil vom 21.6.2012 – 2 AZR 153/11, Rn. 41; BAG, Beschluss vom 26. August 2008 – 1 ABR 16/07 –, BAGE 127, 276-297, Rn. 14 ff.; BAG, Beschluss vom 29.06.2004 – 1 ABR 21/03 –, BAGE 111, 173-190, Rn. 13 ff.
[1156] Vgl. BAG, Beschluss vom 29.06.2004 – 1 ABR 21/03 –, BAGE 111, 173-190, Rn. 13 ff.
[1157] BAG, Urteil vom 21.6.2012 – 2 AZR 153/11, Rn. 41; BAG, Beschluss vom 26. August 2008 – 1 ABR 16/07 –, BAGE 127, 276-297, Rn. 14 ff.
[1158] BAG, Urteil vom 27.03.2003 – 2 AZR 51/02; BAG 17.11.2016 - 2 AZR 730/15, Rn. 31; BAG, Beschluss vom 15.04.2014 – 1 ABR 2/13 (B) –, BAGE 148, 26-41, Rn. 41; LAG Berlin-Brandenburg, Urteil vom 30.08.2018 - 26 Sa 1151/17, Rn. 80.
[1159] BAG, Urteil vom 21.6.2012 – 2 AZR 153/11, Rn. 41 m.w.N.

5.1.4 Zwischenergebnisse: Mitbestimmungsrechte bei der Nutzung von Messengerdiensten im Unternehmenskontext

Aus § 87 Abs. 1 Nr. 6 BetrVG folgt das Mitbestimmungsrecht des Betriebsrats. Hat das Unternehmen Zugriff auf Chat-Verläufe, ergeben sich daraus relevante Daten über Ort, Zeit und Inhalt der Kommunikation, sodass die Einführung einer technischen Einrichtung, die zur Überwachung von Mitarbeiterverhalten bzw. -leistungen objektiv geeignet ist, anzunehmen ist.[1160] Besonders ausgeprägte Überwachungsmöglichkeiten bieten Dienste mit Attention-Tracking-Funktionen, bei denen die Aktivität des Beschäftigten angezeigt wird.[1161]

Sofern das Unternehmen durch Auswahl einer technisch abgesicherten Lösung gewährleistet, dass dem Messengereinsatz keine solche objektive Eignung zu Kontrollzwecken zukommt, könnte hingegen auch die Mitbestimmung entfallen. Hierbei gilt allerdings zu bedenken, ob eine Dokumentation der Daten für eine gewisse Dauer vorgesehen ist (bspw. automatisierte Backups), und hieraus nichtsdestotrotz Möglichkeiten eines Zugriffs resultieren. [1162] Zudem darf nicht vernachlässigt werden, dass die Beschäftigten als Kommunikationsbeteiligte lokale Kopien der Kommunikationsverläufe auf ihren Endgeräten gespeichert haben. [1163] Diese können gleichzeitig als Vertreter*innen des Unternehmens fungieren, sodass eine Mitbestimmung im Zweifel eher zu bejahen ist. Zudem könnte auch § 87 Abs. 1 Nr. 1 BetrVG einschlägig sein, wenn es sich bei Regelungen zur Nutzung von Messengern im Unternehmen um die Arbeitspflicht konkretisierende, allgemeine verbindliche Verhaltensregeln handelt.[1164] Regelungen zur Nutzung von Telefon, Internet oder E-Mail können grundsätzlich hierunter fallen,[1165] sodass im Hinblick auf Messenger und vergleichbare Kommunikationsformen kein Unterschied bestehen dürfte.[1166]

Die Mitwirkung des Betriebsrats kann aber auch aktiv gesucht werden, um eine Betriebsvereinbarung abzuschließen. Betriebsvereinbarungen sind eine taugliche Legitimationsgrundlage.[1167] Die Wirksamkeit einer Betriebsvereinbarung impliziert die Einhaltung der Verhältnismäßigkeitsgrundsätze. Insofern ist es auch im Rahmen einer Betriebsvereinbarung von Relevanz, ob es sich um eine datenschutzfreundliche oder datenintensive Lösung handelt.

5.2 Interne Kommunikation im Unternehmen

In diesem Abschnitt werden Konstellationen untersucht, in denen primär die Beschäftigten eines Unternehmens miteinander kommunizieren. Betroffene Daten sind in diesem Kontext vornehmlich Beschäftigtendaten entsprechend § 26 BDSG.

5.2.1 Verantwortlichkeit des Unternehmens

Bei der Nutzung von Messengerdiensten im Unternehmenskontext stellt sich die Frage, ob sich abhängig

[1160] *Schrey u. a.*, MMR 2017, 736 (738).
[1161] *Dietrich u. a.*, DuD 2021, 5 (7).
[1162] Vgl. *Schrey u. a.*, MMR 2017, 736 (739).
[1163] *Schrey u. a.*, MMR 2017, 736 (739).
[1164] *Schrey u. a.*, MMR 2017, 736 (739); zu den Anforderungen: *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 179.
[1165] vgl. auch *Selk,* in: *Forgó u. a.*, Forgó/Helfrich/Schneider - Betrieblicher Datenschutz, Kap. 3 Rn. 66 (allerdings unter § 87 Abs. 1 Nr. 6 BetrVG).
[1166] *Schrey u. a.*, MMR 2017, 736 (739).
[1167] *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 87; *Schrey u. a.*, MMR 2017, 736 (739). Zudem könnte eine ggf. entstandene betriebliche Übung beseitigt werden: *Schrey u. a.*, MMR 2017, 736 (740).

vom jeweiligen Kontext, eine Verschiebung der datenschutzrechtlichen Verantwortlichkeit bei der Nutzung von Messengerdiensten ergeben könnte. Um zu beurteilen, welche datenschutzrechtlichen Verantwortlichkeiten bei dem Unternehmen, dem Dienstanbieter oder auch bei den Beschäftigten selbst liegen könnten, ist es zweckmäßig verschiedene klar abgrenzbare Fallgruppen zu bilden.

5.2.1.1 Anordnung eines am Markt verfügbaren Messengerdienstes

In diesem Szenario werden die Beschäftigten verpflichtet, den Dienst zu nutzen. Alternativen werden keine angeboten, dem Beschäftigten wird es nicht freigestellt, einen anderen oder einen unternehmenseigenen Messengerdienst zu nutzen.

- Hier ist das Unternehmen selbst Verantwortlicher. Entsprechend der Rechtsprechung des EuGHs, welche bereits in Abschnitt 2.2 vorgestellt wurde, ist hierein eine kausale Ermöglichung der Datenverarbeitung zu erblicken. Denn das Unternehmen entscheidet über das „Warum“ der Kommunikation und durch die Auswahl eines konkreten Drittanbieters auch über das „Wie“. [1168]
- Im Hinblick auf die Beziehung zum Messengerdienst könnte eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO oder eine Auftragsverarbeitung i.S.d. Art. 4 Nr. 8 DSGVO vorliegen.
  - **Gemeinsame Verantwortlichkeit:** Sofern sich Anbieter der Kommunikationssysteme eine Nutzung der bei der Kommunikation anfallenden, personenbezogenen Daten für *eigene* Zwecke (bspw. im Rahmen ihrer AGB) vorbehalten, liegt eine eigene Verantwortung dieses Anbieters vor (vgl. Abschnitte 2.2.2 und 2.5.2.1). [1169] Anders hingegen bei Diensten, welche eine anonyme Nutzung ermöglichen und auch keine über die Diensterbringung hinausgehenden Daten verarbeiten: bei Anonymität im Rechtssinne würde mangels Anwendbarkeit der DSGVO für den Messengerdienst die Verantwortlichkeit allein beim Unternehmen liegen (sofern dieses Daten einzelnen Personen zuordnen kann). [1170] Zur Absicherung sollte nichtsdestotrotz ein Auftragsverarbeitungsvertrag geschlossen werden.
  - **Auftragsverarbeitung:** könnte insbesondere dann gegeben sein, wenn das Unternehmen ein Kommunikationssystem durch einen Dritten betreiben lässt. [1171] Das Unternehmen muss einen Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO abschließen. Dabei ist insbesondere im Hinblick auf die TOMs darauf zu achten, dass der Auftragsverarbeiter die personenbezogenen Daten nicht vertragswidrig für eigene Zwecke nutzt. [1172]

Die Nutzung eines kommerziellen Angebots, das besonders schnell und einfach verfügbar ist, kann auf den ersten Blick mit wenig Aufwand verbunden sein – praktische Hürden bestehen allerdings im Prüfaufwand bei der Auswahlentscheidung eines geeigneten Dienstes, insbesondere wenn die Angebote nicht ausreichend Transparenz bieten. [1173]

[1168] Zu Videokonferenzsystemen: *Bühr*, K&R 2021, 221 (221).
[1169] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 6 f.; *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten; *Bühr*, K&R 2021, 221 (221).
[1170] Zu der Bestimmung von (Re-)Identifizierungsrisiken siehe: Abschnitte 2.3.1.2.3 sowie 4.1.3.3.
[1171] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 6 f; *Bühr*, K&R 2021, 221 (221).
[1172] *Bühr*, K&R 2021, 221 (221). Siehe Abschnitt 2.5.2.2.
[1173] Vgl. *BfDI*, Tätigkeitsbericht 2020, S. 33.

5.2.1.2 Bereitstellung eines Messengerdienstes On-Premise

In diesem Szenario betreibt das Unternehmen den Messengerdienst im eigenen Unternehmen mithilfe eigener Serverinfrastruktur. Man spricht hierbei von einer sog. „On-Premise-Lösung", in Abgrenzung zu einer sog. „cloudbasierten"-Lösung, die nicht vom Unternehmen selbst betrieben wird.

- Hier ist das Unternehmen selbst Verantwortlicher.
- Stellt der Messengerdienstanbieter lediglich Software zur Verfügung, ohne selbst in die Verarbeitung personenbezogener Daten involviert zu sein, dürfte keine Verantwortlichkeit gegeben sein. Die Produkthersteller von Softwarelösungen können allenfalls mittelbar von Datenschutzverpflichtungen im Rahmen der vertraglichen Gewährleistungspflichten oder deliktischen Ansprüchen betroffen sein.[1174] Unterstützt der Anbieter hingegen bei der Umsetzung On-Premise wäre an eine Auftragsverarbeitung zu denken.

Wird entsprechende Software auf eigenen Systemen betrieben, dürfte es sich aus datenschutzrechtlicher Sicht um die „einfachste" Variante handeln, da eine Einbindung von Dritten nicht erforderlich ist.[1175] Dieser Frage soll im weiteren Verlauf der Studie nachgegangen werden.

„Während der Eigenbetrieb eines Systems den Verantwortlichen einerseits die volle Kontrolle über praktisch alle datenschutzrelevanten Parameter gibt, bürdet er ihnen andererseits die komplette Verantwortung für den sicheren und performanten Betrieb auf."[1176] Bei einer Auftragsverarbeitung wäre der Auftragsverarbeiter nach Artt. 28, 29 DSGVO gesetzlich verpflichtet Unterstützungsleistungen zu bieten. Andererseits können die gesamtschuldnerische Haftung sowie die Frage der Insolvenzgefahr bei Regressansprüchen in der Praxis diese theoretische Erwägung überlagern. So kommt es für eine Bewertung als positiv oder negativ entscheidend darauf an, inwiefern der Dienst tatsächlich Garantien bietet, sodass den Verantwortlichen kein Auswahlverschulden nach Art. 8 Abs. 1 DSGVO trifft. Stellt der Messengeranbieter lediglich Software zum Selbstbetrieb zur Verfügung, kann sich das Unternehmen im Rahmen der privatautonomen Gestaltungsmöglichkeit ebenfalls entsprechende Mithilfe bei der Erfüllung von datenschutzrechtlichen Verpflichtungen zusichern lassen. In diesem Zusammenhang wurde bereits das Beispiel einer Muster-Datenschutz-Folgenabschätzung durch den Sofwarehersteller genannt (siehe Abschnitt 2.4.4.5). Insofern kommt es auch hier wieder darauf an, welche Informationen und Einstellungsmöglichkeiten die Angebote bereitstellen.

5.2.1.3 Duldung von Kommunikationsformen

In diesem Szenario nutzen die Beschäftigten einen Messengerdienst und das Unternehmen duldet die Nutzung dieses Dienstes. Diese Nutzung kann sowohl auf privaten als auch auf dienstlichen Endgeräten erfolgen:

- **Corporate-Owned, Personally Enabled devices (COPE)**: steht für die Nutzung von Firmengeräten auch zu privaten Zwecken. Im Falle der Nutzung von Messengerdiensten auf dem unternehmenseigenen Firmengerät bei erlaubter/geduldeter Privatnutzung, stellt sich die Frage, ob das Verhalten von Beschäftigten am Firmengerät dem Arbeitgeber zugerechnet wird. Das Gerät dürfte wohl vorwiegend für die geschäftliche Nutzung überlassen worden sein und das Unternehmen bzw. der Arbeitgeber könnte

[1174] siehe zum Streit über die Erstreckung auf Hersteller und Softwareproduzenten: *Baumgartner/Gausling*, ZD 2017, 308 (311); *Schuster/Hunzinger*, CR 2017, 141 (146); *Dümeland*, K&R 2019, 22 (24).
[1175] *Bühr*, K&R 2021, 221 (221).
[1176] *BfDI*, Tätigkeitsbericht 2020, S. 33.

damit selbst als Verantwortlicher anzusehen sein, nicht dessen Beschäftigte.[1177] Allerdings ist es anders zu beurteilen, wenn Beschäftigte des Unternehmens personenbezogene Daten aus dem dienstlichen Adressbuch zu eigenen Zwecken verarbeiten. Dann gelten sie selbst als Verantwortliche, wobei das Unternehmen als Arbeitgeber ebenfalls eine Verantwortlichkeit wegen unterbliebener, aber zu ergreifender technischer und organisatorischer Maßnahmen treffen könnte.[1178]

- **Bring your Own Device (BYOD):** Für die Verarbeitung personenbezogener Daten auf Privatgeräten ist der Arbeitgeber verantwortlich, nur soweit es sich um dienstliche Daten handelt.[1179] Die Beschäftigten stellen insofern nur die Mittel, über den Zweck entscheidet aber der Arbeitgeber.

Beispiele

- 1. Beschäftigte einer Abteilung richten eine Chatgruppe in einem vom Unternehmen nicht verwendeten Messengerdienst ein, in der sie sich zur Mittagspause und/oder dienstlichen Treffen verabreden.
- 2. Beschäftigte einer Abteilung verwenden einen unternehmensweit genutzten Messengerdienst zur Organisation einer privaten Geburtstagsfeier.

Beispiel 1:

Es liegt zwar ein dienstlicher Kontext vor, durch die Nutzung eines durch das Unternehmen nicht freigegebenen Dienstes werden die Beschäftigten jedoch selbst zu Verantwortlichen (vgl. Abschnitt 2.2.4.2, Mitarbeiterexzess). Die Haushaltsausnahme nach Art. 2 Abs. 2 Buchst. c DSGVO greift nicht, da es sich nicht um die Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten handelt (vgl. Abschnitt 2.3.1.5). Im ersten Beispiel stellt sich allerdings die Frage, ob das Unternehmen eine (Mit-)Verantwortung trifft – insbesondere, wenn durch die Installation einer Messenger-App auch personenbezogene Unternehmenskontakte übermittelt werden.[1180] Eine Zurechnung des Mitarbeiterverhaltens wäre denkbar, wenn es im Verantwortungsbereich des Unternehmens liegt – gerade bei der Herausgabe von Firmengeräten oder Kenntnis der Speicherung von beruflichen Unternehmenskontakten auf Privatgeräten – technische und organisatorische Maßnahmen zu ergreifen. Schwieriger erscheint eine Zuordnung, wenn der/die Arbeitnehmer*in außerhalb ihres Tätigkeitsbereichs und der Kontrollmöglichkeit des Unternehmens Messengerdienste nutzt.[1181]

Beispiel 2:

Es liegt die private Nutzung eines dienstlichen Messengerdienstes vor. Sofern diese Art der Nutzung nicht von einer bestehenden Unternehmensrichtlinie untersagt ist, bleibt das Unternehmen Verantwortlicher.

Im zweiten Beispiel erfolgt eine durch das Unternehmen vorgegebenen App zu anderen (privaten) Zwecken. Um einen Mitarbeiterexzess annehmen zu können – welcher die Verantwortung des Unternehmens ausschließt oder überlagert – sollte das Unternehmen explizit die private Nutzung untersagen. Oftmals wird eine Vermischung beruflicher und privater Kommunikation nicht gänzlich ausschließbar sein – insofern dürfte auch hier eher eine (Mit-)Verantwortlichkeit des Unternehmens anzunehmen sein.

[1177] *Schrey u. a.*, MMR 2017, 736 (737); vgl. *Rohrlich*, ZAP 2020, 1265 (1267).
[1178] *Jung/Hansch*, ZD 2019, 143 (145).
[1179] *Jung/Hansch*, ZD 2019, 143 (146).
[1180] Ausführlich: *Jung/Hansch*, ZD 2019, 143 (145).
[1181] *Jung/Hansch*, ZD 2019, 143 (145).

5.2.1.3.1 Arbeitsrechtliche Implikationen

Fehlen Regelungen zum Umgang mit Messengerdiensten oder anderen Kommunikationslösungen im Betrieb, besteht die Gefahr, dass Ansprüche aus einer „betrieblichen Übung“ geltend gemacht werden könnten.[1182] Von einer betrieblichen Übung spricht man bei einer regelmäßigen Wiederholung bestimmter Verhaltensweisen, aus denen die Beschäftigten schließen können, eine Leistung oder Vergütung solle auf Dauer gewährt werden.[1183] Eine solche wiederholte Leistung kann aus einer neutralen Perspektive dahingehend gewertet werden, dass der Arbeitgeber stillschweigend eine Ergänzung des Arbeitsvertrags einräumt, welche die Beschäftigten ebenso stillschweigend annehmen. [1184] Das BAG hat bereits Duldungen eines bestimmten Verhaltens darunter gefasst.[1185] Wann und wie weit im Einzelfall solche Ansprüche abgeleitet werden können, ist allerdings umstritten. [1186] Dies betrifft vor allem die Nutzung dienstlicher IT-Infrastruktur zu privaten Zwecken. Der Duldung muss ein rechtsgeschäftlicher Erklärungswert beigemessen werden können, welcher voraussetzt, dass der Arbeitgeber Kenntnis von der privaten Nutzung hat.[1187]

In der Praxis wird daher empfohlen Regelungen zum Umgang mit Messengerdiensten im Unternehmen aufzustellen (z.B. im Wege einer „Messenger-Policy“).[1188] Bei der Ausgestaltung und Umsetzung sollten mindestens folgende Punkte bedacht werden: [1189]

- Datenschutzrechtliche Hinweise zu Datenschutzmaßnahmen, -Einstellungen und Sicherheitsgarantien sollten in dokumentierter Weise an die Beschäftigten kommuniziert werden.
- Sachverhalte, welche eine (jederzeitige) Einsichtnahme in die Kommunikation (bspw. externe Kontakte zu Kunden) erforderlich machen, sollten klar von privater Kommunikation getrennt sein. Alternativ wäre die private Kommunikation gänzlich und konsequent zu unterbinden, sodass keine betriebliche Übung entsteht.
- Die Nutzung eines Messengerdienstes sollte die Nutzungsbedingungen (bspw. Beschränkung auf private Zwecke) nicht verletzen. Soll/muss das Unternehmen für eine betriebliche Nutzung an Nutzungsbedingungen des Messengers gebunden werden, ist eine entsprechende Freizeichnung gegenüber den Beschäftigten notwendig.

5.2.1.3.2 Rechtsfolgen eines Mitarbeiterexzesses

Ein Mitarbeiterexzess kann für das Unternehmen als Arbeitgeber verschiedene Folgen haben: Zum einen kann ein Datenschutzverstoß, der öffentlich bekannt wird, mit einem Imageschaden einhergehen. Zum anderen gerät der Arbeitgeber in die Position, seine organisatorischen Maßnahmen rechtfertigen zu müssen, damit sich der Beschäftigte nicht darauf berufen kann, dass er / sie lediglich im Rahmen des Erlaubten bzw. im Rahmen der zugewiesenen Tätigkeit gehandelt habe.

[1182] *Schrey u. a.*, MMR 2017, 736 (737); *Brink/Schwab*, ArbRAktuell 2018, 111 (113). Vgl. auch zur Duldung privater Nutzung betrieblicher Infrastruktur: *DSK - Datenschutzkonferenz*, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, S. 4.
[1183] BAG, Urteil vom 11. 4. 2006 - 9 AZR 500/05, Rn. 14; *Schrey u. a.*, MMR 2017, 736 (737); *Brink/Schwab*, ArbRAktuell 2018, 111 (113).
[1184] BAG, Urteil vom 11. 4. 2006 - 9 AZR 500/05, Rn. 14; *Schrey u. a.*, MMR 2017, 736 (737).
[1185] BAG, Urteil vom 11. 4. 2006 - 9 AZR 500/05, Rn. 14.
[1186] *Schrey u. a.*, MMR 2017, 736 (737 f.); gegen die Folgerung aus bloßer Duldung: *Riesenhuber,* in: *Wolff/Brink*, BeckOK DatenschutzR, § 26 BDSG Rn, 170.
[1187] LAG Berlin-Brandenburg, Urteil vom 14.01.2016 - 5 Sa 657/15, Rn. 85.
[1188] *Schrey u. a.*, MMR 2017, 736 (738); *Brink/Schwab*, ArbRAktuell 2018, 111 (113).
[1189] *Schrey u. a.*, MMR 2017, 736 (738).

Der Arbeitgeber als primärer Haftungsadressat bzw. Adressat eines Bußgeldverfahrens[1190] muss somit einen Entlastungsbeweis führen, dass seine Beschäftigten im Exzess als eigene Verantwortliche gehandelt haben. Datenabrufe durch Beschäftigte im Exzess sind zudem meldepflichtige Datenschutzverstöße gemäß Art. 33 DSGVO, die in der Regel der Datenschutzbehörde zu melden sind.

5.2.2 Einschlägige Rechtsgrundlagen

5.2.2.1 Anordnung eines am Markt verfügbaren Messengerdienstes

Im Rahmen der Nutzung eines bestehenden Messengerdienstes werden in der Regel die Server des jeweiligen Anbieters verwendet und es muss – sofern der Zugriff nicht ausschließlich über den Browser erfolgt – eine App durch die jeweiligen Endnutzer*innen installiert werden.[1191] Für eine Einwilligung dürfte im Rahmen einer verbindlichen Anordnung mangels Freiwilligkeit kein Raum sein. Für die Arbeitgeber richtet sich folglich die Rechtsgrundlage nach § 26 Abs. 1 S. 1 BDSG.

Erfordert eine Messenger-App hingegen eine Einwilligung zur Registrierung, kommen Probleme mit dem Kopplungsverbot hinzu (vgl. Abschnitt 2.4.1.2.1.1.4).[1192] Die Messengerdienstnutzung muss auch ohne Einwilligung möglich sein – beruhen hingegen wesentliche Funktionen auf einer Einwilligung, kommt dieser Messenger im Arbeitskontext nicht in Frage (vgl. Abschnitt 2.4.1.2.1.3). Allenfalls optional nutzbare Features oder die Angabe optionaler Daten können auf eine Einwilligung gestützt werden.

5.2.2.1.1 Anordnung zur Nutzung auf einem Privatgerät

Ein Einsatz auf privaten Endgeräten der Beschäftigten kann nicht verpflichtend angeordnet werden.[1193] Sofern das Unternehmen keine Endgeräte dienstlich bereitstellt, sollte ein Einsatz unterbleiben.[1194] Die Einräumung der Nutzung auf Privatgeräten auf Wunsch der Beschäftigten im Sinne des Bring Your Own Device muss stets freiwillig sein. Der Ansatz des BYOD wird allerdings auch aus IT-Sicherheitsgesichtspunkten kritisiert.[1195] Dabei kommt es darauf an, wie sicherheitskritisch der Einsatzbereich ist und welche Softwarelösungen zur Trennung des privaten und beruflichen Bereichs verfügbar sind. So könnte auf den privaten Smartphones ein sog. „Mobile Device Management“ aufgesetzt werden, um den Sicherheitsbedenken zu begegnen. Dies würde aber voraussetzen, dass ausnahmslos alle Beschäftigten, dieser Veränderung an ihrem Privateigentum ohne Bedingung zustimmen.[1196]

[1190] *Ambrock*, ZD 2020, 492.
[1191] *Brüggemann/Hölzel,* in: Kipker/Voskamp - Sozialdatenschutz, Kap. 4 Rn. 82.
[1192] *Brüggemann/Hötzel,* in: Kipker/Voskamp - Sozialdatenschutz, Kap. 4 Rn. 127.
[1193] *Kremer/Sander,* in: Koreng/Lachenmann - Formularhandbuch Datenschutzrecht, Kap. D. III. 4. Rn. 1; *Helfrich,* in: Forgó/Helfrich/Schneider - Betrieblicher Datenschutz, Kap. 2 B II. 2 Rn. 18.vgl. auch Kuntz, ZD-Aktuell 2021, 05135; Pressemitteilung der LfD Niedersachsen: Thiel: Umstellung auf dienstliche Geräte bei der Polizei fördert Datenschutz, muss aber schneller gehen, vom 24.03.2021, abrufbar unter https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/nimes-stellungnahme-198834.html [letzter Abruf 13.08.2021].
[1194] a.A. wohl *Schrey u. a.*, MMR 2017, 656 (660) (allerdings mit der Einschränkung einer strikten Trennung der privaten und dienstlichen Daten).
[1195] Pressemitteilung der LfD Niedersachsen: Thiel: Umstellung auf dienstliche Geräte bei der Polizei fördert Datenschutz, muss aber schneller gehen, vom 24.03.2021, abrufbar unter https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/nimes-stellungnahme-198834.html [letzter Abruf 13.08.2021].
[1196] Pressemitteilung der LfD Niedersachsen: LfD Niedersachsen beanstandet Polizei-Messenger NIMes wegen Einsatz auf privaten Geräten, vom 17.03.2021 (Stand: 18.03.2021), abrufbar unter: https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-beanstandet-polizei-messenger-nimes-wegen-einsatz-auf-privaten-geraten-197397.html [letzter Abruf: 13.08.2021].

5.2.2.1.2 Anordnung zur Nutzung auf einem Dienstgerät aus Perspektive der Arbeitgeber

Die Anordnung zur Verwendung eines bestimmten Messengerdienstes ist an §26 Abs. 1 BDSG zu messen. Im Hinblick auf die in diesem Rahmen durchzuführende Verhältnismäßigkeitsprüfung, sollten folgende Aspekte bedacht werden:

Kommunikationsinhalte: Im Hinblick auf die in Abschnitt 2.1.1 beschriebenen Daten, stellt sich insbesondere die Frage, ob es auch erforderlich i.S.d. § 26 BDSG bewertet werden kann, im Rahmen von Video-Calls und Voice-Calls Bild- und Tondaten zu übertragen.[1197] Zum Teil könnten Netiquette-Regeln zur Schaffung einer vertrauten und konstruktiven Diskussionsatmosphäre dies gebieten.[1198] Für eine Erforderlichkeit ließe sich argumentieren, dass nicht nur das geschriebene oder gesprochene Wort von Relevanz ist, sondern auch die Gestik, Mimik und Körpersprache Informationsträger sind. [1199] Zudem kann die kommunikative und freundlichen Atmosphäre leiden. Befindet sich die Person in privaten Räumen, sollten Lösungen gewählt werden, welche eine Verschleierung oder Ersetzung des Hintergrunds ermöglichen (Blurring).[1200]

Metadaten: Innerhalb eines Unternehmens dürfte es regelmäßig erforderlich sein, die Gesprächspartner eindeutig identifizieren zu können. Zudem dürfte es – je nach Organisationsstruktur – erforderlich sein, zu jeder Abteilung und Unterabteilung einen Kommunikationskanal eröffnen zu können.

Datensparsamere Varianten können darin bestehen, sofern die personale Identifikation hinter der funktionalen Zuordnung zu einer Aufgabe zurücktritt, nichtpersonalisierte Nutzernamen einzuführen wie bspw. Kontakt_Presseabteilung, info@RECHT, Helpdesk-IT etc. Insofern müsste der Messengerdienst die freie Wahl des Nutzernamens unterstützen.

Überwachungspotential entfalten zudem Kommunikationslösungen, welche die Aktivität des jeweils Nutzenden anzeigen (auch „Attention-Tracking-Funktionen“ genannt).[1201] Diese können einen praktischen Nutzen haben: so sehen Kolleg*innen auf einen Blick, ob der/die andere gerade ansprechbar, beschäftigt oder abwesend ist. Die grundsätzliche Arbeitszeiterfassung im Arbeitsverhältnis wird vom EuGH sogar vorgeschrieben.[1202] Attention-Tracking geht allerdings über die bloße Erfassung von Start- und Endzeitpunkt hinaus. Fraglich ist, ob hierin eine unzulässige „Totalüberwachung“ (vgl. Abschnitt 2.4.1.3.3.2.3 zum Begriff) zu erblicken ist. Zu befürchten wäre, dass ein erheblicher Überwachungsdruck entsteht, insbesondere wenn diese Daten ausgewertet und/oder dokumentiert werden. Eine Deaktivierbarkeit kann hingegen Selbstbestimmungsspielräume eröffnen – allerdings nur, wenn diese im Betrieb tatsächlich auch gelebt werden.

Auswahl technischer Lösungen: Da im Rahmen des Erforderlichkeitskriteriums des § 26 Abs. 1 S. 1 BDSG eine Verhältnismäßigkeitsprüfung stattfindet, hat es durchaus bereits auf der Ebene der Auswahl eines entsprechenden Dienstes bedeutsame Implikationen, ob und wie Datenschutzbelange durch den Kommunikati-

---

[1197] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 11; *Bühr*, K&R 2021, 221 (222); *Bertram/Falder*, ArbRAktuell 2021, 95 (98).
[1198] Siehe bspw. https://www.uni-leipzig.de/fileadmin/ul/Dokumente/2020_Lehre-digital_Netiquette-Videokonferenz.pdf; https://www.uni-regensburg.de/medien/netiquette_videokonferenzen.pdf für Videokonferenzen wie Seminarteilnahmen an Universitäten in Pandemiezeiten.
[1199] *Bühr*, K&R 2021, 221 (222).
[1200] *Bertram/Falder*, ArbRAktuell 2021, 95 (98); *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 12; *Suwelack*, ZD 2020, 561 (565).
[1201] *Dietrich u. a.*, DuD 2021, 5 (7).
[1202] EuGH, Urteil vom 14.05.2019 – C-55/18 – CCOO.

onsdienst erfüllt werden. Da sich Softwarelösungen zur Kommunikation oder für eine kollaborative Zusammenarbeit oftmals auch zweckentfremdet zur Überwachung und Kontrolle einsetzen lassen,[1203] können solche Risiken – neben rechtlichen Verboten – auch auf technischem Weg einschränken.

Dienst ist geeignet kommunikative Anforderungen zu erfüllen	
Ist die Maßnahme überhaupt geeignet, das verfolgte Ziel zu erreichen oder zumindest zu fördern?	— Anforderungsanalyse — Definition der Zielstellungen
Erforderlichkeit eines speziellen Dienstes	
Existieren andere weniger eingriffsintensive Mittel zur Zielerreichung?	— Überblick über Stand der Technik
Bestehen Abstriche bei der Qualität zur Zweckerreichung?	— Mapping Funktionen mit Zielsetzung
Ist die grundrechtsschonendere Verarbeitungsmethode wirtschaftlich nicht zweckmäßig oder technisch nicht umsetzbar?	— Einschätzung Realisierbarkeit — Abwägung zwischen Risiken und Kosten
Angemessenheit des gewählten Dienstes	
In welchem Verhältnis steht das Gewicht der rechtfertigenden Gründe zur Schwere des Eingriffs in Arbeitnehmerrechte?	— Risikobewertung — Gesamtabwägung Ziele & Risiken

Tabelle 13 Erforderlichkeitsprüfung nach § 26 Abs. 1 BDSG

Daneben sind die Mitbestimmungsrechte sowie die Möglichkeit einer Betriebsvereinbarung mit dem Betriebsrat zu beachten (siehe Abschnitt 5.1).

Betriebsvereinbarung: Im Rahmen der Möglichkeit der Regelung des Beschäftigtendatenschutzes durch Kollektivvereinbarungen können allgemeine Rechtsvorschriften für bestimmte Anwendungsfälle individuell und unternehmensspezifisch konkretisiert werden.[1204] Diese Konkretisierung darf allerdings das Schutzniveau der aus den grundrechtlichen Wertungen fließenden und durch eine Verhältnismäßigkeitsprüfung zu ermittelnden, gesetzlichen Standards nicht unterschreiten (vgl. Abschnitt 5.1.3).

5.2.2.1.3 Perspektive des Messengerdienstes

5.2.2.1.3.1 Messengerdienst als Auftragsverarbeitung

Im Fall einer Auftragsverarbeitung wäre der Messengerdienst-Anbieter als der „verlängerte Arm“ des Unternehmens dazu berechtigt, die Daten von Mitarbeiter*innen (bzw. Kundschaft) im Interesse des Unterneh-

[1203] *Dietrich u. a.*, DuD 2021, 5 (9).
[1204] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 11.

mens zu verarbeiten. Hierzu müsste ein entsprechender Vertrag zwischen dem Unternehmen und dem externen Messengerdienst-Anbieter geschlossen werden (AV-Vertrag, siehe Abschnitt 2.5.2.2). Vorbedingung ist allerdings, dass der Messengerdienst-Anbieter keine eigenen Zwecke mit der Datenverarbeitung verfolgt.

Gerade bei Angeboten aus dem internationalen Raum werden allerdings Zweifel geäußert, ob die angebotenen AV-Verträge den Anforderungen der Art. 28 ff. DSGVO erfüllen.[1205] Setzen Messenger Analyse- oder Trackingsoftware ein, ist eine Auftragsverarbeitung ausgeschlossen. Zudem könnten sie vorsorglich die Vorgaben zum Schutz des Fernmeldegeheimnisses, der Verkehrs- und Standortdaten sowie technische und organisatorischer Vorkehrungen nach TTDSG umsetzen, um ein hohes Datenschutzniveau zu belegen. Ähnliche Anforderungen ergeben sich ohnehin aus Art. 32 DSGVO sowie Art. 28 DSGVO.

5.2.2.1.3.2 Messengerdienst als gemeinsame Verantwortliche

Sofern der Messengerdienstanbieter mit der Datenverarbeitung eigene Zwecke verfolgt, scheidet eine Auftragsverarbeitung aus. Die Verarbeitung personenbezogener Daten muss folglich auf eine eigene Rechtsgrundlage gestützt werden.

Aus Sicht des Unternehmens ist in dieser Konstellation wichtig, eine Vereinbarung nach Art. 26 DSGVO mit dem Dienstanbieter zu schließen, die es hinreichend in Kenntnis über die Verarbeitungsvorgänge setzt, um zu bewerten, ob die Verarbeitungstätigkeiten rechtskonform durchgeführt werden.[1206] Zweifel gehen aus Sicht der DSK zu Lasten des Verantwortlichen (hier: dem Unternehmen), der die Möglichkeit hat, auf intransparente Datenverarbeitungen zu verzichten.[1207] Da die Zwecksetzung bei der gemeinsamen Verarbeitung nicht identisch sein muss, kann diese sich auch wechselseitig ergänzen.[1208] Insofern dürften regelmäßig sowohl gemeinsame Zwecke als auch eigene Zwecke gegeben sein. Auch im Hinblick auf die Offenlegung der personenbezogenen Daten an den Dienstanbieter, benötigt das Unternehmen – anders als bei der Auftragsverarbeitung – eine eigene Rechtsgrundlage.[1209] Eine Privilegierung ist hier nicht intendiert.[1210]

[1205] *Brüggemann/Hötzel,* in: Kipker/Voskamp - Sozialdatenschutz, Kap. 4 Rn. 83.
[1206] Vgl. *DSK - Datenschutzkonferenz*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit, S. 2.
[1207] *DSK - Datenschutzkonferenz*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit, S. 2.
[1208] *Jung/Hansch*, ZD 2019, 143 (147).
[1209] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 9.
[1210] *Felber*, ZD 2018, 382 (386).

DSK, Orientierungshilfe Videokonferenzsysteme

- Anders als bei der Auftragsverarbeitung bedarf sowohl die Übermittlung der personenbezogenen Daten an den Dienstanbieter als auch die Verarbeitung durch diesen zu eigenen Zwecken (bzw. Zwecken Dritter) einer Rechtsgrundlage.
- Die Vereinbarung über die gemeinsame Verantwortlichkeit ist keine Rechtsgrundlage, sondern eine zusätzliche Anforderung.
- In der Praxis ist eine Rechtsgrundlage für die Offenlegung personenbezogener Daten an Dienstanbieter regelmäßig schwierig zu begründen.

Durch die Novellierung des Datenschutzes im Rahmen der elektronischen Kommunikation im TTDSG, besteht aufgrund des Anwendungsvorrangs der DSGVO und dem komplexen Nebeneinander zwischen DSGVO und ePrivacy-RL die Problematik, dass unklar ist, ob die neu geschaffenen Regelungen auch für die Verarbeitung personenbezogener Daten durch OTT-Dienstanbieter anwendbar sind (vgl. Abschnitt 3). Wären sie anwendbar, würden sie einerseits eine Rechtsgrundlage bieten, andererseits auch Einschränkungen beinhalten. Daneben schützen sie auch das Fernmeldegeheimnis im Hinblick auf juristische Personen, sodass sie im Verhältnis Messengerdienst – Unternehmen als Nutzer anwendbar sind. Um dieser Rechtsunsicherheit Rechnung zu tragen, sollten Anbieter von Messengerdiensten sowohl die Vorgaben des TTDSG als auch der DSGVO parallel im Blick haben:

Erforderlichkeit zu Erfüllung der Nachrichtenübermittlung: Installieren Beschäftigte des Unternehmens Messenger-Applikationen auf einem ihnen überlassenen Endgerät und kommt es dabei zu einem direkten Vertragsschluss zur betroffenen Person, wäre Art. 6 Abs. 1 Buchst. b DSGVO als Rechtsgrundlage einschlägig. Wird die DSGVO hingegen vom TTDSG als die ePrivacy-RL umsetzendes lex specialis verdrängt, kann die Verarbeitung von Verkehrsdaten auf § 9 Abs. 1 TTDSG gestützt werden. Zwar werden von dieser Regelung die der Rechtsgrundlage unterfallenden Daten einschränkend gelistet. Allerdings gewährt § 9 Abs. 1 S. 1 Nr. 5 TTDSG „sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten“ zu verarbeiten. Es ist somit in doppelter Hinsicht die Erforderlichkeit zu prüfen:

(1) Sind die Daten bereits in Nr. 1-4 gelistet oder zur TK-Erbringung erforderlich?
(2) Werden sie in einem zur TK-Diensterbringung erforderlichem Maß und Umfang verarbeitet?

Die Erforderlichkeit sollte dabei objektiv bestimmt werden. Daten, welche für den Zweck der Erbringung der Leistungen des Messengerdienstes erforderlich sind, dürfen verarbeitet werden, soweit und solange dies erforderlich ist.

Vermarktungszwecke, bedarfsgerechte Gestaltung, Zusatzdienste: Folgt man der engen Auslegung des Erforderlichkeitskriteriums im Rahmen des Art. 6 Abs. 1 DSGVO, würden lediglich zur Erbringung vertraglicher Leistungen nützliche Daten nicht als „erforderlich“ von Art. 6 Abs. 1 Buchst. b DSGVO erfasst. Eindeutig regelt § 9 Abs. 2 TTDSG, dass solche über die eigentliche Erbringung des Telekommunikationsdienstes hinausgehende Zwecke einer Einwilligung bedürfen.

Somit stellt sich wiederum die Problematik, ob die Einwilligung im Dreiecksverhältnis gegenüber Messengern wirksam ist, wenn sie gegenüber Arbeitgebern mangels Freiwilligkeit nicht wirksam wäre. Insofern kommt eine Einwilligung allenfalls in Betracht, wenn sie sich auf optionale Funktionen oder Daten bezieht und der Dienst gleichermaßen auch ohne Einwilligung nutzbar ist.

Die Verfolgung berechtigter Interessen, welche die schutzwürdigen Belange der betroffenen Personen überwiegen, wäre nach dem Regime der DSGVO unter Art. 6 Abs. 1 Buchst. f DSGVO möglich, unter den engeren Bedingungen des § 9 TTDSG hingegen nicht. Verfolgen Messengerdienste mit der Verarbeitung personenbezogener Daten eigene Zwecke ohne, dass diese zur Diensterbringung selbst erforderlich sind, einer rechtlichen Verpflichtung unterliegen oder durch eine Einwilligung getragen werden, kommt es entscheidend darauf an, ob die DSGVO vorrangig anzuwenden ist und ob die Interessenabwägung zugunsten des Messengerdienstes ausfallen würde.

Fraglich bleibt daher, ob ein Messengerdienst, welcher im Beschäftigungskontext eingesetzt werden soll, überhaupt in datenschutzkonformer Weise eigene Zwecke verfolgen kann, welche nicht in der Diensterbringung sowie diese absichernden Maßnahmen liegen.

Standortdaten: Im Rahmen der Legitimation nach DSGVO würde keine Besonderheit im Hinblick auf Standortdaten greifen – unter dem Regime des TTDSG wären hingegen die engeren Anforderungen des § 13 TTDSG zu bedenken. Bietet eine Messengerdienst einen (weiteren) Dienst mit Zusatznutzen an, welcher die Verarbeitung von Standortdaten erforderlich macht, müssten die Daten entweder anonymisiert werden oder eine (wirksame) Einwilligung vorliegen. Letzteres wäre allenfalls denkbar, wenn die betroffenen Beschäftigten auf diesen Zusatzdienst verzichten können, also ihre Einwilligung verweigern oder widerrufen können ohne Nachteile befürchten zu müssen. Das bloße Abbestellen solcher Dienste im Sinne eines Opt-Out erfüllt nicht die DSGVO-Standards an eine wirksame Einwilligung.

Beschäftigtendatenschutz als Rechtsgrundlage? § 26 Abs. 1 BDSG begrenzt seinen Anwendungsbereich im Hinblick auf die betroffenen Personen auf Beschäftigte, macht allerdings keine Aussage über den Verantwortlichen.[1211] Diskutiert werden könnte daher darüber, ob sich ausschließlich Arbeitgeber als Verantwortliche auf diese Rechtsgrundlage berufen können.[1212] Allerdings kann kaum davon gesprochen werden, dass die Leistungen eines Messengerdienstes zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erfolgen. Der Anbieter als verantwortliche Stelle verfolgt regelmäßig eigene Verarbeitungszwecke.

5.2.2.1.4 Zwischenergebnis

Plant ein Unternehmen für die unternehmensinterne Kommunikation einen Messengerdienst anzuordnen, richtet sich die Rechtmäßigkeit nach § 26 Abs. 1 BDSG oder einer Betriebsvereinbarung. Umsetzbar ist dies im Wege einer Auftragsverarbeitung. In diesem Fall ist ein Messengerdienst auszuwählen, welcher den Abschluss eines AV-Vertrags anbietet und keine eigenen Verarbeitungszwecke, die über die Erfüllung der Auftragsverarbeitung hinausgehen, verfolgt. In der Praxis stellen sich allerdings oftmals Abgrenzungsprobleme zur gemeinsamen Verantwortlichkeit, insbesondere wenn der Dienstanbieter eigenverantwortlich die Diensterbringung gestaltet und sich hierfür eigene Wertungs- und Entscheidungsspielräume vorbehält oder

[1211] *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 28.
[1212] So: *Ströbel/Wybitul,* in: Handbuch Europäisches und deutsches Datenschutzrecht, § 10 Rn. 28.; ähnlich *Wolff/Kosmider*, ZD 2021, 13 (15); a. A. *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 12.

eigene Zwecke verfolgt.[1213] Ob eine Rechtsgrundlage an einen (Mit-)Verantwortlichen für die Übermittlung personenbezogener Daten der Beschäftigten eingreift, ist allerdings äußerst fraglich. Daher wird die Nutzung eines Drittangebots in gemeinsamer Verantwortung eher ausscheiden.

5.2.2.2 Bereitstellung eines Messengerdienstes On Premise

Erfolgt eine Anordnung eines unternehmensseitig On Premise bereitgestellten Messengerdienstes bestehen im Hinblick auf die Rechtsgrundlage keine Unterschiede zu Abschnitt 5.2.2.1.2. Liegt eine Bereitstellung in der Form vor, dass Beschäftigten eine Nutzung freigestellt ist, gelten folgende Erwägungen:

Einwilligung: Auch im Rahmen der Bereitstellung eines Dienstes ohne explizite Anordnung diesen zu nutzen, bestehen weiterhin Zweifel an der Freiwilligkeit einer Einwilligung, da dies nur über eine echte Wahlmöglichkeit sicherzustellen wäre. Würden die Beschäftigten die Informationen auch auf anderem Wege – ohne Nutzung dieses Kommunikationskanals – erhalten und dabei keinerlei persönlichen Nachteile erleiden, würde dies für Freiwilligkeit sprechen.[1214] Dann müsste die Alternative aber ohne Verarbeitung der in Frage stehenden personenbezogenen Daten auskommen.[1215]

Erforderlichkeit im Beschäftigungsverhältnis: Eine Legitimation kann über § 26 Abs. 1 BDSG erfolgen. Insofern gelten vergleichbare Erwägungen wie unter Abschnitt 5.2.2.1.2, mit dem Unterschied, dass keine Daten an einen externen Messengerdienstanbieter fließen (als Auftragsverarbeiter oder gemeinsam Verantwortlicher), sondern innerhalb der Unternehmensinfrastruktur verbleiben. Die Abwägungskriterien bei der Auswahl, Anpassung und Implementierung einer Software zum allein verantworteten Betrieb, sind vergleichbar. Auch hier muss im Rahmen der Umsetzung einer Kommunikationslösung, welche mit der Verarbeitung personenbezogener Daten der Beschäftigten verbunden ist, auf ihre Geeignetheit, Erforderlichkeit und Angemessenheit geprüft werden. In der Praxis wären Vorteile bei der technischen Beschreibung der Verarbeitungsprozesse zu erwarten, welche das Unternehmen dann besser nutzen kann, um seine datenschutzrechtlichen Pflichten, insbesondere im Rahmen der Risikobewertung sowie den Informationspflichten zu erfüllen.

Betriebsvereinbarung: Bietet das Unternehmen seinen Beschäftigten eine datenschutzfreundliche Alternative zu den bestehenden Kommunikationswegen, wäre auch der Weg über eine Betriebsvereinbarung mit dem Betriebsrat in Erwägung zu ziehen (hierzu in Abschnitt 5.1.3). Gerade wenn das Interesse sowohl auf Arbeitnehmer- als auch auf Arbeitgeberseite an einer geeigneten Kommunikationsform besteht, jedoch gewisse Restzweifel an der Freiwilligkeit der Einwilligung oder der Erforderlichkeit zur Durchführung des Beschäftigungsverhältnisses bleiben, bietet sich eine Betriebsvereinbarung an, um die Datenverarbeitung auf ein sicheres Gerüst zu stellen. Die Betriebsvereinbarung kann Konkretisierungen enthalten, darf das Schutzniveau der Datenschutzvorgaben, insbesondere der DSGVO, aber nicht unterschreiten.[1216]

Zusammenfassend lässt sich festhalten: Bei der Bereitstellung zur freiwilligen Nutzung ist die Einwilligung nicht von vorneherein ausgeschlossen (allerdings mit Aufwand verbunden), möglich sind zudem die Erfor-

[1213] Vgl. *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten., abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf [letzter Abruf 12.08.2021].
[1214] *Bühr*, K&R 2021, 221 (222); *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 10.
[1215] *Bühr*, K&R 2021, 221 (222).
[1216] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 11.

derlichkeit im Beschäftigungsverhältnis nach § 26 Abs. 1 BDSG sowie eine Betriebsvereinbarung als Rechtsgrundlage. Bedenken sollten Unternehmen, dass es auch in dieser Konstellation erforderlich werden kann, einen AV-Vertrag abzuschließen, wenn ein Service-/Wartungsvertrag vereinbart wird, bei dessen Erfüllung ein Zugang zu personenbezogenen Daten erfolgt.

5.2.2.3 Duldung von beschäftigtenseitig gewählten Messengerdiensten

Anders als im ersten Szenario liegt hier keine Anordnung vor, sondern eine freie Wahl der Beschäftigten, sich einer speziellen Kommunikationsform zu bedienen. Selbst bei Verfolgung eigener Zwecke der Beschäftigten sollte der Vorgang nicht vorschnell unter die Einwilligung nach § 26 Abs. 2 BDSG subsumiert werden. Denn es können rechtliche Implikationen durch den Drittbezug von Daten (zu Personen, die nicht eingewilligt haben) sowie der Weitergabe von privaten Nachrichten an die Arbeitgeberseite verbunden sein. Zwar können sich auch im Rahmen des Arbeitsverhältnis Beschäftigten grundsätzlich frei entscheiden, wie sie ihr Grundrechte auf informationelle Selbstbestimmung (sowie die anderen IT- und Datenschutzgrundrechte) ausüben wollen.[1217] Auch mit einem Ausschluss der Einwilligungsmöglichkeit würden abhängig Beschäftigten ihre Grund- und Persönlichkeitsrechte eingeschränkt. [1218] Da zudem die von der EU-Kommission geforderte pauschale Annahme fehlender Freiwilligkeit im Arbeitsverhältnis nicht in die DS-GVO übernommen wurde, ist eine Einzelfallbetrachtung der Freiwilligkeit der Einwilligungen von Beschäftigten auch aus EU-rechtlicher Perspektive möglich.[1219]

Handelt es sich um Kommunikationszwecke, die nicht i.S.d. § 26 Abs. 1 BDSG erforderlich sind, werden von der gewählten Kommunikationslösung personenbezogene Daten Dritter (wie Kontakte im Adressbuch) betroffen (und als Klardaten übermittelt), sind Datentransfers in unsichere Drittländer vorgesehen, werden Datenschutzstandards im Hinblick auf Privacy-by-Design und Datensicherheit nicht erfüllt oder bestehen vergleichbare risikobehaftete Verarbeitungsvorgänge, kann es für Unternehmen mitunter riskant werden, wenn sie die Auswahl eines Messengerdienstes auf Basis einer Einwilligung ihren Beschäftigten überlassen und gleichzeitig in der (Mit-)Verantwortung stehen. Um diesen Gefahren zuvorzukommen, kann es sich anbieten unternehmensseitig aktiv eine Kommunikationsplattform bereitzustellen:

- Bereitstellung oder Benennung von Kommunikationsformen, welche keine Verletzung von Datenschutzrechten Dritter befürchten lassen (d.h. Übermittlung von Drittdaten nur in anonymisierter Form)
- Auswahl dieser Kommunikationslösung mit der Zielsetzung auch bei privater Nutzung keine Datenschutzrisiken zu erzeugen:
  - Ausschluss von Datentransfers in unsichere Drittländer
  - Einhaltung des aktuellen Stands der Technik im Hinblick auf datenschutzfreundliche Technikgestaltung und Voreinstellung sowie Datensicherheit
  - Begrenzung der Weitergabe personenbezogener Daten auf das erforderliche Minimum
- Auswahl danach, ob eine den beteiligten Verantwortungssphären und Verarbeitungsbeiträgen angemessenes Angebot auf Abschluss einer Vereinbarung nach Art. 26 Abs. 1 DSGVO oder eines AV-Vertrags unterbreitet wird

[1217] BAG, Urteil vom 11.12.2014 – 8 AZR 1010/13, Rn. 32.
[1218] So wohl: BAG, Urteil vom 11.12.2014 – 8 AZR 1010/13, Rn. 32. Vgl. auch zum Wunsch der Beschäftigten auf aktive Einwilligungsmöglichkeiten: *Polst u. a.*, DuD 2021, 19 (22).
[1219] *Ambrock/Karg*, ZD 2017, 154 (157); *Schantz*, NJW 2016, 1841 (1845).

Erfolgt die Nutzung im Eigeninteresse der Beschäftigten ohne, dass in irgendeiner Weise (sozialer oder beruflicher) Druck aufgebaut wird, so könnten die Anforderungen an die Freiwilligkeit der Einwilligung nach § 26 Abs. 2 BDSG erfüllt sein. Dies bedarf aber stets einer Betrachtung im Einzelfall.

5.2.2.4 Sonderfälle und Einzelfragen zur Reichweite der Rechtsgrundlagen

5.2.2.4.1 Weitergabe privater Nachrichten aus geschlossenen Gruppen an Arbeitgeber

In bestimmten Konstellationen kann es vorkommen, dass geschlossene Chat-Gruppen innerhalb eines Betriebs eingerichtet oder eigenverantwortlich durch die Beschäftigten eingeführt werden, in denen sich die Beschäftigten privat austauschen. Werden solche privaten Nachrichten an den Arbeitgeber weitergegeben, kann hierin eine Verletzung der Datenschutz- und Persönlichkeitsrechte der betroffenen Beschäftigten liegen.[1220] Allein die Tatsache, dass mehrere Personen an einer Chat-Gruppe teilnehmen oder auch dienstliche Belange behandelt werden, macht diese nicht öffentlich.[1221] Bestehen berechtigte Erwartungen, dass der Adressatenkreis beschränkt ist, darf der Inhalt solcher Nachrichten nicht ohne Weiteres ohne Einwilligung der Kommunikationsbeteiligten weitergegeben werden.[1222] Spätestens mit Entgegennahme der Daten durch den Arbeitgeber liegt eine rechtfertigungsbedürftige Verarbeitung vor.[1223] In der Regel ist allerdings die Kenntnisnahme privater Unterhaltungen selbst in Kommunikationsforen im Kollegenkreis und damit im betrieblichen Kontext nicht für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich.[1224] Zu beachten gilt, dass neben datenschutzrechtlichen Ansprüchen auch zivilrechtliche Ansprüche auf ein angemessenes Schmerzensgeld aus der Verletzung des Persönlichkeitsrechts erwachsen können, wenn es sich um einen schwerwiegenden Eingriff handelt.[1225]

Daher ist zu empfehlen, dass bei der Einrichtung einer Kommunikationsinfrastruktur eine klare und transparente Trennung zwischen innerbetrieblichen beruflichen Kontakten, externen beruflichen Kontakten und Räumen für den privaten, vertraulichen Austausch zwischen Beschäftigten implementiert wird.

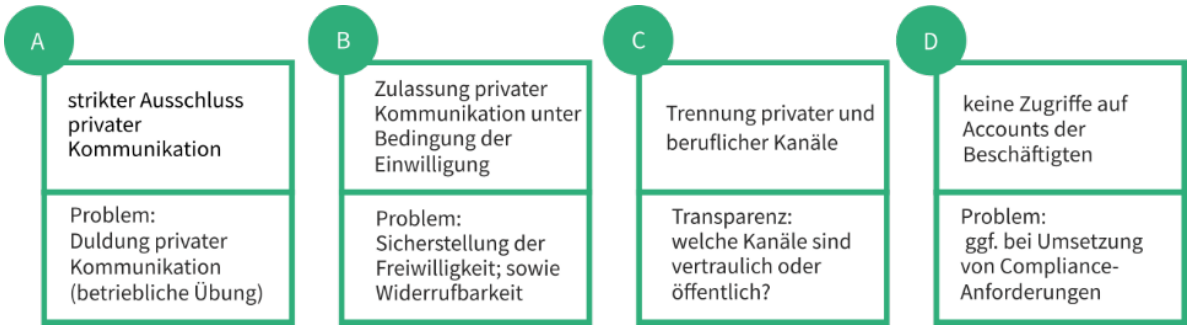
5.2.2.4.2 Einsicht in Nutzeraccounts der Beschäftigten

Es sind Fallkonstellationen denkbar, in welchen Arbeitgeber ein Interesse haben können, Zugriff auf den persönlich und eigenverantwortlichen geführten Account einer Beschäftigten zu nehmen, bspw. um im Falle langer Krankheit nachvollziehen zu können, inwiefern Kommunikationskontakte informiert und Gesprächskanäle auf andere Beschäftigte umgeleitet werden müssen. Insofern stellt sich im Rahmen der Erforderlichkeitsprüfung die Frage, ob das Schutzinteresse der Beschäftigten das Kontrollinteresse der Arbeitgeber über-

[1220] Vgl. ArbG Mainz, Urteil vom 15.11.2017 – 4 Ca 1240/17, Rn. 17 ff. unter Verweis auf: BAG, Urteil vom 10. 12. 2009 - 2 AZR 534/08, Rn. 23 ff.
[1221] ArbG Mainz, Urteil vom 15.11.2017 – 4 Ca 1240/17, Rn. 19.
[1222] Vgl. BAG, Urteil vom 10. 12. 2009 - 2 AZR 534/08, Rn. 23 ff.
[1223] Für die Beschäftigten könnte zuvor die Haushaltausnahme greifen, bei „gemischten" Kontexten allerdings zweifelhaft, vgl. Abschnitte 2.3.1.5 und 4.1.1.
[1224] Nur in seltenen Fällen wird man hiervon ausgehen können: die Beschäftigten im öffentlichen Dienst haben eine sog. außerdienstliche Wohlverhaltenspflicht, vgl. LfDI Rheinland-Pfalz, https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/weitergabe-von-chatnachrichten-aus-whatsapp-gruppen-an-den-arbeitgeber/ [letzter Abruf 11.08.2021].
[1225] Vgl. AG Berlin-Charlottenburg, Urteil vom 15.01.2015, Az. 239 C 225/14. Bei intimen Bildern kann bei der unberechtigten Weitergabe von Sprachnachrichten der Straftatbestand des § 201 Abs. 1 Nr. 1 StGB erfüllt sein.

wiegt. In der Vergangenheit wurde durchaus in Zweifel gezogen, ob es sich um eine Persönlichkeitsrechtsverletzung handelt, oder Beschäftigten bei auf Arbeitsmitteln der Arbeitgeber gespeicherten Daten stets mit Kenntnisnahme durch die Arbeitgeber rechnen müssen und daher nicht schutzbedürftig sind.[1226] Allerdings rechtfertigt nicht allein der Umstand, dass ein dienstlich bereitgestelltes Kommunikationsgerät genutzt wird, eine inhaltliche Kontrolle durch die Arbeitgeber.[1227] Insofern werden datenschutzrechtliche Bedenken geäußert unabhängig davon, ob Kontrollen offen angekündigt oder heimlich erfolgen oder ob private Unterhaltungen erlaubt oder nicht erlaubt stattfanden.[1228] Als Argument kann angeführt werden, dass wenn ein gesicherter Bereich (bspw. mit persönlichen Anmeldedaten und Kennwortschutz) bereitgestellt wird, automatisch eine geschützte „Persönlichkeitsenklave" entstehe. [1229] Zudem könnte die Verwirklichung eines Straftatbestands vorliegen (§ 202a StGB), wenn die Arbeitgeber mittels Überwindung einer Zugangssicherung Zugang zu den von der Arbeitnehmer*in gespeicherten Daten erhält, ohne dass eine Einwilligung oder mutmaßliche Einwilligung vorliegt oder sich das Vorgehen im Rahmen der Sozialüblichkeit (Sozialadäquanz) bewegt. [1230] Andere Autoren erkennen datenschutzkompatible Kontrollrechte an und empfehlen bei der Gestattung privater Nutzung diese von einer Einwilligung in die Kontrolle abhängig zu machen.[1231] Da es genug alternative Kommunikationsmöglichkeiten gibt, ist die Privatnutzung dienstlicher IT nur eine Vergünstigung bzw. Erweiterung des Handlungsspielraums, sodass keine Bedenken hinsichtlich der Freiwilligkeit bestünden. [1232] Selbst unter Annahme der Anwendbarkeit der strengeren Vorgaben des TTDSG sollen Zugriffe auf Nachrichten über eine Einwilligung legitimierbar sein, wenn die Kontrollmaßnahmen klar beschrieben werden.[1233]

Um zu vermeiden, dass es bei Zugriffen auf Postfächer oder Accounts der Beschäftigten zu Persönlichkeitsrechtsverletzungen kommt, wären die folgenden Alternativen möglich:



In jedem Fall sollten Arbeitgeber klar und transparent definieren, welche Bereiche von regelmäßigen Kontrollen (im Rahmen zulässiger Kontrollrechte), wann ausnahmsweise Zugriffe vorgesehen sind in ansons-

[1226] ArbG Frankfurt a.M., Urteil vom 2. 1. 2002 - 2 Ca 5340/01, NZA 2002, 1093 (1096).
[1227] BVerfG, Beschluss vom 19.12.1991 - 1 BvR 382/85.
[1228] *Weißberger*, NZA 2003, 1005 (1006).
[1229] *Weißberger*, NZA 2003, 1005 (1006).
[1230] *Weißberger*, NZA 2003, 1005 (1007). Zur Problematik wer berechtigt ist, auf Daten zuzugreifen (sog. Datenverfügungsberechtigung anhand des sog. Skripturakts): BGH, Urteil vom 10. Mai 2005 – 3 StR 425/04; OLG Naumburg, Urteil vom 27. August 2014 – 6 U 3/14; OLG München, Urteil vom 24. Juni 1993 – 5St RR 5/93; Eisele, Computer- und Medienstrafrecht, S. 36.
[1231] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 BDSG Rn. 171.
[1232] *Riesenhuber,* in: BeckOK DatenschutzR, § 26 BDSG Rn. 171; *Brink/Schwab*, ArbRAktuell 2018, 111 (113).
[1233] Noch zur alten Rechtslage der §§ 88 ff. TKG: *Brink/Schwab*, ArbRAktuell 2018, 111 (114); *Wybitul/Böhm*, CCZ 2015, 133 (134); *Schrey u. a.*, MMR 2017, 656 (660).

ten eigenverantwortlich organisierten Bereichen (bspw. bei langer Krankheit) und wo tatsächlich Vertraulichkeit angenommen werden kann. Somit sollte klargestellt werden, wo „Persönlichkeitsenklaven“ bestehen und wo nicht.

Praxistipp:

(1) Bei der Auswahl geeigneter Kommunikationswerkzeuge sollte darauf geachtet werden, ob unterschiedliche Vertraulichkeitslevel umsetzbar sind.
(2) Unternehmen sollten frühzeitig transparent darstellen, welche Kontrollmaßnahmen bei der Nutzung von Messengerlösungen geplant sind bzw. möglich sein sollen. Wichtig ist, dass keine Fehlvorstellungen über persönliche „Enklaven“ entstehen.
(3) Die Gestattung der Privatnutzung kann mit einer Einwilligung in klar umschriebene Datenzugriffe bzw. Zugriffsmöglichkeiten durch Arbeitgeber verbunden werden. Dabei ist sicherzustellen, dass die Beschäftigten hinreichend informiert sind.

5.2.2.5 Geltung des KUG bei Personenbildnissen

Bei den meisten Messengern als auch sonstigen Kollaborationslösungen werden die Beteiligten mit Namen und Profilbild angezeigt. Zumeist besteht die Möglichkeit das Bild frei zu wählen, wobei sich überwiegend die Nutzung eines Portraitbildes eingebürgert haben dürfte. Liegt bei der Verwendung dieses Bildes eine „Verbreitung“ oder ein „öffentlich zur Schau stellen“ vor, könnte neben der DSGVO das Kunsturhebergesetz (KUG) anwendbar sein. Auch dieses schützt die Persönlichkeitsrechte bildlich abgebildeter natürlicher Personen. Höchst umstritten ist die Frage, ob das KUG vom Anwendungsvorrang der DSGVO verdrängt wird.[1234] Die Gerichte haben dies zumindest im journalistischen Bereich verneint.[1235] Inwiefern das KUG auch außerhalb des journalistischen Bereichs weiter Geltung beanspruchen kann, ist noch nicht geklärt.[1236] § 22 KUG macht die Veröffentlichung von einer Einwilligung abhängig.[1237] Ausnahmen gelten gemäß § 23 KUG bspw. bei Bildnissen im Bereich der Zeitgeschichte oder im Rahmen der sog. „Panoramafreiheit“, wenn die Person nur Beiwerk auf einem Bild ist.

Verantwortliche können sich dieser Problematik wie folgt stellen: die Verwendung eines Profilbildes sollte als optional eingestellt sein. Die Beschäftigten sollten zudem frei wählen, ob sie ein Portraitbild, einen Avatar, einen Ersatz (bspw. das Firmenlogo, Abteilungskennzeichen, etc.) oder gar kein Bild verwenden wollen. Zudem sollte die Möglichkeit bestehen, dass Bild jederzeit ändern zu können. Somit sollte sichergestellt werden, dass eine Einwilligung freiwillig erfolgt und jederzeit widerrufbar ist. Die Einwilligung in die Nutzung des Bildes sollte nachweisbar dokumentiert sein.

[1234] *Benedikt/Kranig*, ZD 2019, 4; *Hansen/Brechtel*, GRUR-Prax 2018, 369; *Hoeren*, ZD 2018, 435; *Krüger/Wiencke*, MMR 2019, 76; *Lauber-Rönsberg/Hartlaub*, NJW 2017, 1057; *Ziebarth/Elsaß*, ZUM 2018, 578.
[1235] BGH, Urteil vom 7.7.2020 – VI ZR 250/19, Rn. 10 ff.; OLG Köln, Beschl. v. 18.6.2018 – 15 W 27/18; zustimmend *Hansen/Brechtel*, GRUR-Prax 2018, 369 (370); *Krüger/Wiencke*, MMR 2019, 76 (77); a.A. *Benedikt/Kranig*, ZD 2019, 4 (5).
[1236] *Rohrlich*, ZAP 2020, 1265 (1270).; *Hoeren*, ZD 2018, 435 (436); *Krüger/Wiencke*, MMR 2019, 76 (78).
[1237] Für das Erfordernis der Einwilligung bspw. bei Beschäftigtenbildern auf Homepages: *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 99.

5.2.3 Pflichten des Verantwortlichen

Im Hinblick auf eine Detailprüfung der datenschutzrechtlichen Eignung des Einsatzes von Apps mit besonderem Augenmerk auf die technische Gestaltung, hatte das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) bereits 2016 einen Prüfkatalog für technischen Datenschutz bei Apps herausgebracht.[1238] Dieser bezieht sich also noch auf die Rechtslage vor Inkrafttreten der DSGVO. Speziell für den Einsatz von Messengerdiensten verfasste die DSK Ende 2019 ein Whitepaper zu technischen Datenschutzanforderungen, allerdings bezogen auf den Einsatz im Krankenhausbereich.[1239] Diese Empfehlungen können zu Hilfe genommen werden, wenn es um den Schutz besonderer Kategorien personenbezogener Daten wie Gesundheitsdaten geht.

Im Übrigen werden im folgenden Abschnitt einige wesentliche Pflichten herausgegriffen und erläutert. Diese gelten grundsätzlich für alle hier betrachteten Fallkonstellationen – Besonderheiten werden erläutert, wenn Pflichten im Rahmen der Auftragsverarbeitung oder gemeinsamen Verantwortung durch mehrere Beteiligte umzusetzen sind.

5.2.3.1 Transparenz- und Informationspflichten

Den Verantwortlichen treffen die in Abschnitt 2.4.2.2 dargestellten Informationspflichten. Betreibt das Unternehmen den Messengerdienst On Premise hat es selbst in der Hand die entsprechenden Informationen in klarer und einfacher Sprache aufzubereiten. Dies dürfte aus Unternehmenssicht der einfachste Fall sein, wenn die Datenflüsse für das allein verantwortliche Unternehmen selbst ebenfalls nachvollziehbar sind. Komplexer wird die Situation bei der Nutzung von Drittdiensten.

Wissenschaftliche Untersuchungen deuten zudem in die Richtung, dass gerade im Beschäftigungskontext teilweise noch kein ausreichendes Bewusstsein darüber herrscht, welche „privaten Daten“ auch zu den personenbezogenen Daten zählen sowie, dass neben einer aktiven Bereitstellung von Daten an den Arbeitgeber zumeist auch zahlreiche Datenerhebungen im Hintergrund erfolgen.[1240] Bemängelt wurde von den Forschenden zudem das vorgefundene Risikobewusstsein, sodass der Schluss nahe liegt, bessere und effektivere Kommunikationsmaßnahmen zu fordern.[1241]

Informationspflichten nach Art. 12 ff. DSGVO: Das Unternehmen sollte darauf achten, dass es (bzw. der Messengerdienst) die relevanten Informationen entsprechend der Vorgaben in Art. 12 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache bereitstellt. Dabei sollten die Informationen weder zu viele technische oder juristische Fachbegriffe beinhalten oder insgesamt übermäßig komplex ausfallen.[1242] Hierbei sollten folgende Aspekte bedacht werden:

- Werden die **Zwecke der Verarbeitung** der personenbezogenen Daten hinreichend klar? Die Zwecke der Datenverarbeitung gehören zu den wichtigsten Informationen (vgl. Abschnitt 2.4.3).[1243]
  - Werden die Daten auch zu anderen Zwecken als den vorrangigen Zweck der Kommunikationsüber-

[1238] *BayLDA*, Prüfkatalog für den technischen Datenschutz bei Apps mit normalem Schutzbedarf, S. 2 ff. abrufbar unter https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf [letzter Abruf 05.07.2021].
[1239] *DSK - Datenschutzkonferenz,* Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, 2019.
[1240] *Polst u. a.*, DuD 2021, 19 (21).
[1241] *Polst u. a.*, DuD 2021, 19 (21).
[1242] Bzgl. Videokonferenzsysteme: *Bühr*, K&R 2021, 221 (223).
[1243] *Bühr*, K&R 2021, 221 (223).

mittlung verarbeitet? Wird aus Vorbehalten, die Daten zu anderen Zwecken zu nutzen, ausreichend klar, welche Zwecke dies umfasst? Stehen diese Zwecke in angemessenem Verhältnis zum Primärzweck?

  - Sofern sich der Verantwortliche auf die Interessenabwägung beruft: werden die berechtigten Interessen verständlich beschrieben?
- Wird die **Rechtsgrundlage** korrekt und hinreichend klar angegeben?
  - Insofern richtet sich die Rechtsgrundlage bei der Einbindung eines Messengerdienstes als Auftragsverarbeiter nach der des Unternehmens. Diese sollten daher in jedem Fall eine eigene Datenschutzerklärung abfassen, selbst wenn der Messengerdienst bereits eine Erklärung bereitstellt.
  - Soll die Datenverarbeitung bzw. ein Bestandteil der Datenverarbeitung auf einer Einwilligung beruhen, muss diese hinreichend eindeutig den davon betroffenen Datenverarbeitungsvorgängen zuordenbar sein. Auf das Widerrufsrecht ist hinzuweisen.
- Welche Angaben werden zur **Speicherdauer** gemacht?
  - Verarbeitet der Messengerdienst personenbezogenen Daten nur temporär bzw. flüchtig, richtet sich die Speicherdauer vor allem nach den internen Speicherrichtlinien im Unternehmen. Auf beides sollte hingewiesen werden.
- Ist der obligatorische Hinweis auf die **Betroffenenrechte** enthalten? Wird eine Kontaktmöglichkeit zur Geltendmachung dieser Rechte benannt (Kontakt Verantwortlicher, ggf. Datenschutzbeauftragte*r)
  - Erfolgt eine automatisierte Entscheidung im Einzelfall, ist auf die involvierte Logik und die angestrebten Auswirkungen aufzuklären.
- Werden Daten in einem **Drittland** verarbeitet? Wird darüber ausreichend aufgeklärt? Besteht ein Angemessenheitsbeschluss?

Bezüglich der Video-Call und Voice-Call-Funktionen ist die Orientierungshilfe der DSK zu Videokonferenzsystemen durchaus auch auf Messengerdienste übertragbar. Insofern hielten es die Datenschutzaufsichten für notwendig, dass der Veranstalter der Videokonferenz (in diesem Kontext das anordnende Unternehmen) zusätzlich auf mögliche Privatsphäreneinstellungsmöglichkeiten, die Nutzung von Pseudonymen sowie das Setzen eines künstlichen Hintergrundbilds hinweisen.[1244]

Auftragsverarbeitung: Unterstützt der Anbieter eines Messengerdienstes bei der Umsetzung und Verarbeitet dabei personenbezogene Daten ohne selbst Verantwortlicher zu sein, muss ein Auftragsverarbeitungsvertrag geschlossen werden. Bei der Auswahl der Anbieter dürfen nur solche berücksichtigt werden, die Garantien dafür bieten, dass die Vorgaben der DSGVO umgesetzt werden können. Da sich der Anspruch auf Auskunft auch auf die Kommunikation per Messenger bezieht,[1245] sollten organisatorische Vorkehrungen getroffen werden, um diesen umsetzen zu können.[1246]

Gemeinsame Verantwortlichkeit: Sollte – anders als hier vertreten – eine gemeinsame Verantwortlichkeit zwischen Unternehmen und Messengerdienstanbieter datenschutzrechtlich zulässig sein, haben die Beteiligten zwei Komplexe besonders zu beachten:

(1) die Parteien müssen festlegen, wer welchen Pflichten nachkommt und dies entsprechend den betroffenen Personen kommunizieren und

---

[1244] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 13 ff.; *Bühr*, K&R 2021, 221 (223).
[1245] Vgl. LG Bonn, Urteil vom 01.07.2021 – 15 O 372/20, Rn. 22.
[1246] vgl. *Bergt,* in: Koreng/Lachenmann - Formularhandbuch Datenschutzrecht, Kap. D. III. 2. Rn. 3.

(2) der Dienst muss in transparenter Weise Aufklärungsinformationen über Funktionen zur Datenverarbeitung bereitstellen (s.o.).

5.2.3.2 Datenschutz-Folgenabschätzung

In Abschnitt 2.4.4.5 wurde dargestellt, wann die Pflicht zur Durchführung einer DSFA gegeben ist. Hierfür wurden Kriterien der Artikel-29-Datenschutzgruppe[1247] sowie die Positiv-/Negativliste der DSK genannt. Im Beschäftigten- bzw. Unternehmenskontext sind folgende Punkte dieser Liste besonders hervorzuheben:

Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden	— Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen — Geolokalisierung von Beschäftigten	— Zentrale Aufzeichnung der Aktivitäten (z.B. Internetverkehr, Mailverkehr […]) am Arbeitsplatz mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen. — Ein Unternehmen lässt Bewegungsprofile von Beschäftigen erstellen […].
Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen […] sofern: — Verarbeitung in großem Umfang — für Zwecke, für welche nicht alle Daten direkt bei Betroffenen erhoben — Anwendung von Algorithmen, die für Betroffenen nicht nachvollziehbar — der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen	— Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden	— Ein Unternehmen mit umfangreichem Stamm an natürlichen Personen als Kunden, analysiert Daten über das Kaufverhalten der Kunden und die Nutzung der eigenen Webangebote einschließlich des eigenen Webshops, verknüpft mit Bonitätsdaten von dritter Seite und Daten aus der Werbeansprache über soziale Medien einschließlich der vom Betreiber des sozialen Medium bereitgestellten Daten über die angesprochenen Mitglieder, um Informationen zu gewinnen, die zur Steigerung des Umsatzes eingesetzt werden können.
Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person	— Kundensupport mittels künstlicher Intelligenz	— Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus — Ein Unternehmen setzt ein System zur Konversation mit Kunden ein, welches für deren Beratung personenbezogene Daten mittels KI verarbeitet

Tabelle 14 Auszug aus Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist der Datenschutzkonferenz (DSK)[1248]

Beim Einsatz von Messengerdiensten im Unternehmen liegen bezüglich der Kriterien der Artikel-29-Datenschutzgruppe der Faktor Machtungleichgewicht und innovative Anwendung neuer Lösungen (zumindest für

[1247] *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" - WP248 Rev.01, S. 12.

1248 DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, abrufbar unter: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf [letzter Abruf 21.07.2021].

den Unternehmenskontext) vor. Oftmals wird übersehen, dass über anfallende Metadaten mit Bezug zu Beschäftigten eine Leistungskontrolle möglich ist.[1249] Zudem bieten einige Lösungen die Erhebung von Standortdaten. Ob hiermit bereits die Schwellen der DSK-Liste erreichen, bedarf einer Betrachtung im Einzelfall. Unternehmen können sich dabei auch einer Einteilung der betroffenen Daten in Schutzklassen bedienen (vgl. Abschnitt 2.4.4.2.5.2). Es ist daher nicht ausgeschlossen, dass eine DSFA erforderlich werden könnte. Besteht hingegen durch die bereits implementierte technische Gestaltung ein geringes Risiko, bedarf es keiner DSFA.

Im Hinblick auf die in Kapitel 4 beschriebenen, am Markt verfügbaren Messengerdienste, bestehen einige Lösungen, welche kein signifikant gesteigertes Risikopotential im Vergleich zu herkömmlichen Kommunikationsformen im Unternehmen (bspw. Telefon, E-Mail-Kommunikation, etc.) aufweisen. Elementar für die Entscheidung über die Notwendigkeit der DSFA ist die Beschreibung der technischen Gestaltung. Liegen insofern ausreichend Informationen vor, um in dokumentierbarer und nachvollziehbarerweise Belegen zu können, dass nur ein geringes oder „normales“ Risiko besteht, kann dieser Dienst unbedenklich ohne Durchführung einer DSFA eingesetzt werden (vgl. zur Empfehlung die Entscheidung zu dokumentieren: Abschnitt 2.4.4.6).

Bestehen hingegen Bedenken, dass mit der Datenverarbeitung ein hohes Risiko verbunden ist, können durch die Dienstanbieter bereitgestellte Muster-DSFA Unternehmen in ihrer Rolle als datenschutzrechtlich Verantwortliche unterstützen. Allerdings ist derzeit kein Dienst bekannt, der eine solche Muster-DSFA zur Verfügung stellt.

5.2.3.3 Technische und organisatorische Maßnahmen

Im Rahmen der technischen und organisatorischen Maßnahmen sollten Unternehmen neben der Sichtung vorhandener datenschutzgerechter Technologien eruieren, ob im Unternehmenskontext sämtliche Funktionen, die ein Dienst bereitstellt, genutzt werden können, oder ob ggf. einzelne, mit besonderem Eingriffspotential behaftete Funktionen von vorneherein deaktiviert werden sollten. So werden bspw. im Rahmen von Videokonferenzsystemen Bedenken bezüglich der Aufnahmefunktion geäußert.[1250] Entsprechend des risikobasierten Ansatzes gilt zwar keine Pflicht das maximal mögliche Schutzniveau umzusetzen, allerdings ist bei Unterschreiten möglicher Standards – bspw. aufgrund wirtschaftlicher Erwägungen – eine besonders sorgfältige Risikoeinschätzung geboten, welche umfassend dokumentiert werden sollte.[1251]

5.2.3.3.1 Authentifikation

Um nur Personen zuzulassen, die zum Unternehmen gehören oder zur Interaktion eingeladen wurden, sollten Personen sich zunächst authentisieren. Welche Anforderungen gestellt werden, hängt entscheidend davon ab, welche Risiken mit unautorisierten Zugriffen verbunden wären. [1252] Insofern sollte ein Messengerdienst über Möglichkeiten zur Verifikation von Kontakten verfügen. Biometrische Features sollten dagegen deaktiviert werden.[1253]

[1249] *Schiering u. a.*, DuD 2020, 161 (162).
[1250] *Bühr*, K&R 2021, 221 (224).
[1251] *Suwelack*, ZD 2020, 561 (565).
[1252] *Bühr*, K&R 2021, 221 (224); *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 20.
[1253] *Bertram/Falder*, ArbRAktuell 2021, 95 (98).

Ein-Faktor-Authentifizierung: Bei geringen Risiken wird ein einfacher Nutzername nebst Passwort ausreichend sein.[1254] Hierbei ist entscheidend für das Sicherheitsniveau wo und wie das Passwort gespeichert ist, inwiefern Daten übertragbar sind und dass diese Daten nicht für weitere Authentifizierungsversuche genutzt werden können.[1255]

Zwei-Faktor-Authentifizierung: Bei höheren Risiken sollte die Zwei-Faktor-Authentifizierung eingesetzt werden.[1256] Diese wird empfohlen, wenn gerade durch mobiles Arbeiten / Home Office die typischerweise im Büroalltag anzutreffende Grundsicherung durch örtliche Begebenheiten unterschritten wird und so Sicherheitsbedenken kompensiert werden müssen.[1257]

Ein höheres Schutzniveau wird erreicht, wenn sich die Authentifizierungsfunktion des Messengerdienstes vom Schutz zur Entsperrung des Mobilgerätes unterscheidet.[1258]

5.2.3.3.2 Verschlüsselung

Als Stand der Technik muss eine sichere Ende-zu-Ende-Verschlüsselung gewährleistet sein und sollte als Voreinstellung aktiviert sein. Vertrauliche Daten dürfen nicht unverschlüsselt übertragen werden. Verantwortliche sollten die aktuellen Entwicklungen stets beobachten. Derzeit wird der Einsatz von Perfect-Forward-Secrecy-fähige Algorithmen für die Übertragung personenbezogener Daten empfohlen.[1259]

Besondere Bedenken werden geäußert, wenn ihm Rahmen der Verarbeitung sensibler bzw. besonders schützenswerter Daten private Endgeräte zum Einsatz kommen (Bring your own Device – BYOD).[1260] Insbesondere wird ein Kontrollverlust des Arbeitgebers im Hinblick auf die Möglichkeiten unkontrollierter Speicherung und Vervielfältigung vertraulicher Daten bemängelt.[1261] Empfohlen wird auch hier die technisch vermittelte Trennung von privaten und dienstlichen Daten (z.B. mit Hilfe von Container-Apps).[1262]

5.2.3.3.3 Löschfunktionen

Bei der Löschung von Daten gilt zu bedenken, dass aus Perspektive des Messengerdienstes eine Vorhaltung von Daten über kurz begrenzte Zeiträume regelmäßig nicht erforderlich sein wird. Das Unternehmen kann hingegen Dokumentationspflichten treffen (vgl. Abschnitt 2.4.1.3.1), wobei diese zumeist eher bei externer Kommunikation (Abschnitt 5.3) einschlägig sein dürften, wenn bspw. die Kommunikation per Messenger als Geschäftsbrief zu qualifizieren ist. Deshalb sollte es möglich sein, lokale Backups zu erstellen und so Nachrichten für die entsprechenden Fristen unternehmensseitig vorzuhalten.

[1254] Für Videokonferenzsysteme: *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 20; *Bühr*, K&R 2021, 221 (224).
[1255] Für Videokonferenzsysteme: *Bühr*, K&R 2021, 221 (224).
[1256] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 20.
[1257] *Bergt,* in: Koreng/Lachenmann - Formularhandbuch Datenschutzrecht, Kap. D. III. 2. Rn. 3; vgl. auch *Suwelack*, ZD 2020, 561 (564); *Gilga*, ZD-Aktuell 2020, 07113; *Stoklas*, ZD-Aktuell 2020, 07093.
[1258] *DSK - Datenschutzkonferenz*, Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, S. 3.
[1259] *Bergt,* in: Koreng/Lachenmann - Formularhandbuch Datenschutzrecht, Kap. D. III. 2. Rn. 14.
[1260] Pressemitteilung der LfD Niedersachsen: LfD Niedersachsen beanstandet Polizei-Messenger NIMes wegen Einsatz auf privaten Geräten, vom 17.03.2021 (Stand: 18.03.2021), abrufbar unter: https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-beanstandet-polizei-messenger-nimes-wegen-einsatz-auf-privaten-geraten-197397.html [letzter Abruf: 13.08.2021]; *Bertram/Falder*, ArbRAktuell 2021, 95 (98); *Bergt,* in: Koreng/Lachenmann - Formularhandbuch Datenschutzrecht, Kap. D. III. 2 Rn. 1; *Suwelack*, ZD 2020, 561 (563); *Schrey u. a.*, MMR 2017, 656 (660).
[1261] *Suwelack*, ZD 2020, 561 (564).
[1262] *Suwelack*, ZD 2020, 561 (564).

Im Rahmen einer BYOD-Umsetzung müssen Arbeitgeber sicherstellen, dass lokal gespeicherte Daten nach Beendigung des Beschäftigungsverhältnisses restlos gelöscht werden. Kommt es zu einem Verlust der Daten, kann dies einen meldepflichtigen Datenschutzverstoß (Data Breach Notification) darstellen.[1263]

Gerade im Hinblick auf die praktische Umsetzung (spezial-)gesetzlicher Aufbewahrungspflichten einerseits sowie dem Grundsatz der Speicherbegrenzung entsprechender Löschfristen andererseits bestehen bei klassischen Kommunikationsformaten im Unternehmenskontext durchaus noch Herausforderungen. Denn für eine Löschung nach Erreichung des jeweils konkreten Verarbeitungszwecks, müssten anhand der verschiedenen Kommunikationsthemen und -formate (inkl. Backups) zwischen aufbewahrungspflichtigen bzw. aufbewahrungswürdigen und löschpflichtigen Nachrichten differenziert werden. Aufgrund der schieren Masse wird dies im betrieblichen Alltag kaum möglich sein.[1264] Daher werden folgende Löschlösungen diskutiert:

Individuelles Sichten und Löschen: Grundsätzlich erwartet die DSGVO dem Risiko angemessene und damit verhältnismäßige technische und organisatorische Maßnahmen vom Verantwortlichen, um die Datenschutzpflichten differenziert umzusetzen und so ein „vernünftiges Aufwand-Nutzen-Verhältnis“ zu erreichen (vgl. Art. 24 DSGVO).[1265] Sofern keine Sonderkonstellationen wie Verarbeitung besonderer Kategorien personenbezogener Daten oder Profiling eingreifen, dürfte daher ein einzelfallabhängiges Sichten und Löschen bei hohem organisatorischen und zeitlichen Aufwand unverhältnismäßig sein.[1266]

Pauschales Löschen nach der längsten Frist: Ein Vorgehen, bei dem die längste, für das Unternehmen anwendbare Aufbewahrungsfrist ermittelt und pauschal auf alle Nachrichten angewandt wird, lässt dagegen eine Ausdifferenzierung der Risiken für die betroffenen Personen vermissen und erfüllt nicht die Löschpflichten.[1267]

Einordnung in Löschstufen: Einen Mittelweg zwischen individuellem und pauschalem Ansatz könnte die Einteilung der Nachrichten in verschiedene Löschklassen, die unterschiedlichen Löschfristen unterliegen, sein:[1268] So wird bspw. für den E-Mail-Verkehr im Unternehmen vorgeschlagen drei Löschregime zu definieren: (1) kurzfristig zu löschende Nachrichten, (2) Nachrichten mit längeren Aufbewahrungszeiträumen und (3) alle übrigen ein- und ausgehenden Nachrichten.[1269] Für die erste Kategorie können als Beispiel persönliche Informationen im Rahmen eines Bewerbungsverfahrens gezählt werden, welche i.d.R. sechs Monate nach Ende des Bewerbungsverfahrens gelöscht werden könnten.[1270] In die zweite Kategorie fallen Nachrichten, die den handels- und steuerrechtlichen Aufbewahrungspflichten unterfallen (6-10 Jahre) oder sonstige, schutzwürdige Nachweisbelange betreffen (z.B. bei patentrechtlicher Relevanz[1271]).[1272] Bei sonstiger Kommunikation kann bspw. der Kontext wie der Bezug zu einem bestimmten Projekt oder Vorgang eine Rolle spielen: oftmals werden Kommunikationsdaten noch für eine gewisse Zeit nach Projektabschluss benötigt, bspw. um Informationen für einen Projektabschluss zu extrahieren oder Abläufe zu rekonstruieren. Disku-

[1263] *Bertram/Falder*, ArbRAktuell 2021, 95 (97).
[1264] *Durmus/Selzer/Pordesch,* DuD 2019, 786 (787); *Wagner,* White Paper E-Mail-Archivierung und DSGVO 2019, 4 ff.
[1265] *Durmus/Selzer/Pordesch,* DuD 2019, 786 (787).
[1266] *Durmus/Selzer/Pordesch,* DuD 2019, 786 (788); so auch *Wagner,* White Paper E-Mail-Archivierung und DSGVO 2019, 4 ff.
[1267] *Durmus/Selzer/Pordesch,* DuD 2019, 786 (789).
[1268] *Wagner,* White Paper E-Mail-Archivierung und DSGVO 2019, 10.
[1269] *Durmus/Selzer/Pordesch,* DuD 2019, 786 (789).
[1270] *Durmus/Selzer/Pordesch,* DuD 2019, 786 (789).
[1271] Da Patente gemäß § 16 PatG eine Gültigkeit von 20 Jahren ab dem Anmeldetag haben wird eine Löscherinnerung nach 20 Jahren vorgeschlagen: *Durmus/Selzer/Pordesch,* DuD 2019, 786 (789).
[1272] *Durmus/Selzer/Pordesch,* DuD 2019, 786 (789).

tiert wird zudem, sich an Verjährungsfristen zu orientieren, nach deren Ablauf keinen Be- oder Entlastungsbeweis mehr erbringen können und damit zu löschen sind.[1273]

Da Messengerdienste oftmals auch eingesetzt werden, um einen informellen Austausch zu ermöglichen, wäre eine vierte Kategorie zu erwägen: Eine längerzeitige Aufbewahrung informellen Ausauschs der Beschäftigten, insbesondere wenn dies eher auf einer presönlichen Ebene geschieht, entfaltet eine stärkere persönlichkeitsrechtliche Relevanz, weshalb diese Daten in kürzeren Zylklen gelöscht werden sollten. Hier wird kaum jemand davon ausgehen, dass diese Kommunikation längerfristig aufbewahrt wird.

Archivierung als Vorstufe zur Löschung: Sofern Aufbewahrungspflichten eingreifen, beschränkt sich der Verarbeitungszweck auf die Speicherung bzw. Archivierung.[1274] Auch für sonstige Nachrichten wird die Möglichkeit diskutiert, Datenschutzbelange nach Abschluss einer aktuellen Kommunikationsbeziehung zu berücksichtigen, indem die Verarbeitung der personenbezogenen Daten dieser Nachrichten derart eingeschränkt wird, dass diese aus dem Wirkbereich in ein Archiv verschoben werden, auf welches die Zugriffsrechte beschränkt sind.[1275] Die damit verbundene Minimierung der Risiken unberechtigten Zugriffs könnte – je nach konkreter Interessenlage – eine längere Aufbewahrung bis hin zur längsten Aufbewahrungspflicht legitimieren und so die unternehmerischen Interessen befriedigen, Fehler im Hinblick auf vorschnelle Löschungen zu vermeiden.[1276]

5.2.3.3.4 Datentrennung

Zu einer Vermischung des beruflichen und privaten Kontextes kann es kommen, wenn vom Unternehmen Firmengeräte herausgegeben werden, wobei eine private Nutzung gestattet ist, oder im Unternehmen das BYOD-Konzept umgesetzt wird. Hier kann sich das Problem stellen, dass die Beschäftigten im privaten Kontext einen unsicheren Messenger nutzen möchten, welcher bspw. eine Übermittlung des gesamten Kontaktverzeichnisses vorsieht. Um diesem Problem zu begegnen, können Vorinstallationen vorgenommen werden, welche es Beschäftigten vereinfachen trotz privater Nutzung unsicherer Messengerdienste eine Trennung zum beruflichen Kontext zu vollziehen:

- Installation einer Softwarelösung, welche Container-Lösungen anbietet[1277]
- Ggf. Schulungen / Informationsangebote / Richtlinien zu datenschutzrechtlich konformen Arbeiten[1278]
- Implementierung eines Datenschutzmanagementsystems[1279]

Alternativ kann die private Nutzung und damit die Vermischung beruflicher und privater Daten untersagt werden. Einige Dienste bieten neben Smartphone-Anwendungen (Apps) zudem Desktop-Lösungen, sodass eine Nutzung auch ohne zusätzliche, dienstliche Endgeräte möglich wäre.

Beim arbeitgeberseitigen Verbot privater Kommunikation im Rahmen von Unternehmenslösungen gilt allerdings zu bedenken, wenn diese ohne Kontrollen nicht durchgesetzt und langfristig geduldet werden, kann

---

[1273] Bloß abstrakte Gefahr von rechtlichen Auseinandersetzungen aber keine Rechtsgrundlage für „anlasslose“ Speicherung: *Wagner,* White Paper E-Mail-Archivierung und DSGVO 2019, 7.
[1274] *Wagner,* White Paper E-Mail-Archivierung und DSGVO 2019, 10.
[1275] *Durmus/Selzer/Pordesch,* DuD 2019, 786 (790).
[1276] *Durmus/Selzer/Pordesch,* DuD 2019, 786 (790).
[1277] So auch: *Jung/Hansch*, ZD 2019, 143 (146); *Faas*, ArbRAktuell 2018, 594 (596); *Schrey u. a.*, MMR 2017, 736 (737); *Bertram/Falder*, ArbRAktuell 2021, 95 (97); *Suwelack*, ZD 2020, 561 (564); *Dury*, ZD-Aktuell 2020, 04405.
[1278] *Jung/Hansch*, ZD 2019, 143 (146); vgl. zum Home-Office: *Gilga*, ZD-Aktuell 2020, 07113; *Dury*, ZD-Aktuell 2020, 04405; *Suwelack*, ZD 2020, 561 (566).
[1279] *Jung/Hansch*, ZD 2019, 143 (146).

eine betriebliche Übung entstehen.[1280] Beschäftigte könnten sich dann darauf berufen, dass sie davon ausgehen durften, die eingesetzte Kommunikationslösung auch privat nutzen zu dürfen. In diesem Fall kommt es zum Streit, ob der Arbeitgeber ggü. seinen Beschäftigten als TK-Anbieter zu bewerten ist (vgl. Abschnitt 3.2.1.4). Abseits davon, könnten sich vergleichbare Pflichten aus einer grundrechtskonformen Auslegung der allgemeinen datenschutzrechtlichen Pflichten ergeben, sodass Arbeitgeber die Vertraulichkeit der privaten Kommunikation ihrer Beschäftigten zu wahren haben. Auch insoweit sollte daher eine Trennung zwischen privaten und beruflichen Sachverhalten durch die gewählte Kommunikationslösung unterstütz werden. Kommunikationsräume, welche als privat eingestuft sind, sollten durch den Arbeitgeber nicht einsehbar sein.

Ein weiteres BYOD-Problem ist die IT-Sicherheit privat verantworteter Endgeräte. Hier wird ein „Mobile Device Management“ empfohlen.[1281] Hierbei handelt es sich um eine zentralisierte Verwaltung von Mobilgeräten durch einen Administrator, um Sicherheitseigenschaften sicherzustellen. Dabei gilt allerdings zu bedenken, dass Zugriffe der Arbeitgeber auf private Endgeräte nicht mit einer Aufzeichnung der Daten im Bereich der privaten Nutzung einhergehen dürfen.[1282] Die Konfiguration muss sicherstellen, dass der privat genutzte Bereich nicht vom Arbeitgeber eingesehen werden kann.

5.2.3.3.5 Aktualisierungen

Arbeitgeber sollten ihre Beschäftigten dazu verpflichten ihre App-Versionen auf dem neuesten Stand zu halten, und Hinweise zu den Sicherheitsrisiken dokumentieren.[1283] So sollte sichergestellt werden, dass keine Datensicherheitsrisiken zur Nutzungszeit entstehen.

5.2.3.4 Umsetzung der Betroffenenrechte

Im Hinblick auf die Rechte der betroffenen Person gilt folgendes zu beachten:

Recht auf Auskunft: Machen Beschäftigte als datenschutzrechtlich betroffene Personen ihr Auskunftsrecht geltend, gilt dies grundsätzlich auch für via Messengerdienste ausgetauschte Nachrichten (vgl. Abschnitt 2.4.2.3). Im Hinblick auf das Recht eine Kopie zu erhalten, müssen allerdings auch die Persönlichkeits- und Urheberrechte der Kommunikationskontakte berücksichtigt werden. Ggf. sind Passagen zu schwärzen.

Recht auf Berichtigung: Da es sich bei der ausgetauschten Kommunikation um historische Daten handelt, dürfte sich das Berichtigungsrecht vornehmlich auf die Profildaten beziehen. Können diese durch die betroffenen Personen als Nutzende des Messengerdienstes unmittelbar geändert werden, wäre das Recht auf Berichtigung erfüllt.

Recht auf Löschung: Nicht trivial ist die Umsetzung des Rechts auf Löschung, da ausgetauschte Dokumente mit Unternehmensrelevanz handels- und steuerrechtlichen Aufbewahrungspflichten unterliegen können. Auch insofern bietet sich eine klare Trennung zwischen offizieller, zu dokumentierender Kommunikationsinhalte und informellem, ggf. privaten Austausch zwischen Beschäftigten an, um ein Löschkonzept umsetzen zu können.

[1280] Kritisch: *Riesenhuber,* in: BeckOK DatenschutzR, § 26 BDSG, Rn. 170 m.w.N.
[1281] Pressemitteilung der LfD Niedersachsen: LfD Niedersachsen beanstandet Polizei-Messenger NIMes wegen Einsatz auf privaten Geräten, vom 17.03.2021 (Stand: 18.03.2021), abrufbar unter: https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-beanstandet-polizei-messenger-nimes-wegen-einsatz-auf-privaten-geraten-197397.html [letzter Abruf: 13.08.2021].
[1282] *Bertram/Falder*, ArbRAktuell 2021, 95 (96).
[1283] *Schrey u. a.*, MMR 2017, 736 (737); *Suwelack*, ZD 2020, 561 (564).

Recht auf Einschränkung der Verarbeitung: Muss über ein Löschgesuch entschieden werden, muss eruiert werden, ob Daten quasi mit „einem Sperrvermerk“ versehen werden können (vgl. Abschnitt 2.4.6).

Recht auf Datenübertragbarkeit: Dieses Recht dürfte im Beschäftigtenkontext kaum eine Rolle spielen. Aufgrund der wettbewerbsrechtlichen Grundintention (vgl. Abschnitt 2.5.1.1) besteht kein Anlass für eine extensive Auslegung.

Recht auf Widerspruch: Dieses Recht besteht, sofern die Datenverarbeitung auf einer Interessenabwägung beruht. Legt die betroffene Person Widerspruch ein, so führt dies gemäß Art. 21 Abs.1 DSGVO nicht per se zur Pflicht weitere Datenverarbeitungen zu unterlassen, da der Verantwortliche zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

Widerrufsrecht: Betroffene Personen können ihre Einwilligung widerrufen, sofern (Bestandteile der) Datenverarbeitung auf einer Einwilligung beruhten. In praktischer Hinsicht sollten Verantwortliche bedenken, dass der Widerruf für die betroffene Person genauso einfach sein muss, wie die Erteilung der Einwilligung. Ggf. sind entsprechende Kommunikationskanäle vorzusehen.

5.2.4 Umsetzung innerbetrieblicher Kommunikation bei Einsatz von am Markt verfügbaren Messengerdiensten

Die dargestellten Pflichten treffen das Unternehmen als datenschutzrechtlich Verantwortlichen: bei Umsetzung von On-Premise-Lösungen hat es zwar sämtliche Pflichten in Eigenregie zu erfüllen, dabei aber auch die vollständige Kontrolle. Nutzt das Unternehmen dagegen einen am Markt angebotenen Messengerdienst, ist es regelmäßig auf die Mitwirkung des Messengerdienstanbieters angewiesen.

5.2.4.1.1 Gemeinsame Verantwortlichkeit

Im Fall von gemeinsamer Verantwortung richtet sich die Aufgabenverteilung nach der Vereinbarung i.S.d. Art. 26 Abs. 1 DSGVO. Als nicht ausreichend wird es erachtet, wenn der Messengerdienstanbieter pauschal sämtliche Pflichten übernimmt, um das (mit-)verantwortliche Unternehmen insofern von Pflichten freizustellen (vgl. die Kritik zur Reaktion auf das Urteil zu Facebook-Fanpages unter Abschnitt 2.5.2.1). Nichtsdestotrotz können die Beteiligten Beträge von sehr unterschiedlichem Gewicht verantworten.

Bei Messengerdiensten, die selbst keinen Zugriff auf Daten in personenbezogener Form haben, ist eine eigene Verantwortung mit der Verfolgung eigener Zwecke eher fernliegend. Daher dürfte diese Konstellation vielmehr Fälle betreffen, in der der Dienst personenbezogene Daten bei der Diensterbringung erfasst und für eigene Zwecke (weiter-)verarbeitet. Allerdings bestehen berechtigte Zweifel, ob insbesondere vor dem Hintergrund eines innerbetrieblichen Einsatzes die Verfolgung eigener Verarbeitungszwecke des Messengerdienstes auf eine rechtlich fundierte Basis gestellt werden kann. Insofern wird es auf eine Betrachtung des Einzelfalls ankommen, ob eine entsprechende Konstellation in der Praxis überhaupt umsetzbar ist.

5.2.4.1.2 Auftragsverarbeitung

Die DSGVO gibt konkrete Pflichten auf, in denen der Auftragsverarbeiter den Verantwortlichen und Auftraggeber bei der Umsetzung der Vorgaben der DSGVO unterstützen muss (vgl. Abschnitt 2.5.2.2). Im Folgenden sollen zwei Szenarien betrachtet werden: die durch den Messengerdienstanbieter eröffnete Möglichkeit den

Dienst auf eine Art und Weise zu nutzen, bei der der Anbieter selbst keinen Zugriff auf Inhalte der Kommunikation sowie Metadaten hat (Fall A: anonymisiert/pseudonymisierte Nutzungsmöglichkeit) und als Gegenpol den Fall der Übertragung zahlreicher Klardaten (Fall B: datenintensive Nutzungsmöglichkeit).

Mithilfe eines „Zero-Knowledge"-Ansatzes funktionieren Messenger auf eine Art und Weise, ohne dass der Anbieter selbst Einblicke in die Daten erhält. Über eine Ende-zu-Ende-Verschlüsselung können nur Sender und Empfänger die Nachrichten entschlüsseln. Werden zusätzlich Metadaten konsequent minimiert oder zusätzlich über eine Verschlüsselung geschützt und nur temporär zwischengespeichert, kann selbst der Anbieter keine oder nur kaum Rückschlüsse auf die Messengernutzung und –nutzenden ziehen.

Anonymisiert-/pseudonymisierte Nutzungsmöglichkeiten (Fall A):

Rechtliche Anforderungen		Anmerkungen zur Umsetzung
Anforderung an Verantwortlichen:	Auswahl Auftragsverarbeiter mit hinreichenden Garantien	Mit der konsequenten Umsetzung des Datenminimierungsgrundsatzes state-of-the-art wären hinreichende Garantien gegeben.
	Abschluss AV-Vertrag	Verarbeitet der Messengerdienst Daten in anonymisierter Form, läge zwar keine Verarbeitung personenbezogener Daten vor und die DSGVO wäre nicht anwendbar, sodass ein AV-Vertrag nicht zwingend wäre. Wie in Abschnitt 4.1.3.3 beschrieben, sollte allerdings trotz Verschlüsselung, Hashen und schnellstmöglicher Löschung vorsorglich von einer Identifizierbarkeit und damit vom Vorliegen eines Personenbezugs ausgegangen werden, sodass ein AV-Vertrag zu empfehlen ist, um Haftungsrisiken zu vermeiden.
Anforderungen an Auftragsverarbeiter:	Dokumentation	Sofern der Auftraggeber Weisungen erteilt, sind diese zu Dokumentieren
	Verschwiegenheitsklausel	Hat der Messenger keinen Einblick auf den Inhalt der Daten, sollte die Verpflichtung auf Verschwiegenheit kein Problem darstellen.
	Datensicherheit	Entsprechend der Apps nach dem Stand der Technik sollte der Messenger Transport- sowie Ende-zu-Ende-Verschlüsselung standardmäßig voreingestellt haben.
	Subbeauftragung	Setzt der Auftragsverarbeiter weitere Sub-Auftragsverarbeiter ein, sind die Anforderungen an die Genehmigungspflichtigkeit zu erfüllen.
	Unterstützung Umsetzung Betroffenenrechte[1284]	**Auskunft:** Sofern der Messenger selbst durch Verschlüsselung, Hashen und frühestmögliche Löschung keine Auskunft erteilen kann und für das Unternehmen weder über Backups oder andere Wege eine Zuordnung / Vorhaltung von Daten zu/von auskunftsersuchenden Personen möglich ist, könnte Art. 11 DSGVO einschlägig sein (vgl. Abschnitt 2.4.2.3.2). *Messengersicht:* Der Messenger würde seiner Unterstützungspflicht nachkommen mit dem Nachweis fehlender Identifizierbarkeit. *Unternehmenssicht:* Sind Leitungsorgane selbst an der Kommunikation beteiligt, dürfte eine Identifizierbarkeit regelmäßig gegeben sein, sodass über diese Daten Auskunft zu erteilen wäre.[1285] Eine Ausnahme von der

[1284] Das Recht auf Datenübertragbarkeit dürfte in der vorliegenden Konstellation keine Rolle spielen, da dieses sich gegen den Verantwortlichen richtet und die Rechtsgrundlage des Unternehmens für die Verarbeitung personenbezogener Daten seiner Beschäftigten auf § 26 BDSG beruht.

[1285] Hierbei wird zu beurteilen sein, ob diese als Beschäftigte i.S.d. § 26 Abs. 8 BDSG und betroffene Person i.S.d. Art. 4 Nr. 1 DSGVO einzustufen sind, oder als Repräsentant des Unternehmens und damit der Seite des Verantwortlichen.

		Auskunftspflicht wäre gegeben, wenn das Unternehmen (ebenfalls) keinen Einblick weder im Hinblick auf Metadaten noch Inhaltsdaten hat. **Berichtigung** Da es sich bei den Kommunikations(inhalts)daten ohnehin um historische Daten handelt, dürften vornehmlich die Profildaten für Korrekturwünsche in Betracht kommen. Insofern sollte es den Betroffenen ermöglicht werden, diese über ihre Accounts selbst aktuell zu halten. **Löschen:** Für die Umsetzung des Datensparsamkeitskonzepts sollte das Löschkonzept des Messengers ohnehin eine automatisierte Löschung vorsehen, sobald die Daten für die Diensterbringung nicht mehr erforderlich sind, sodass keine weiteren Unterstützungsmaßnahmen erforderlich wären.[1286]
	Unterstützung bzgl. Pflichten aus Artt. 32-36 DSGVO	Im Hinblick auf die Melde- und Benachrichtigungspflichten wäre zu erwägen, ob die Art der Datenverarbeitung zu einem geringen Risiko führt und damit bestimmte Ausnahmen greifen (siehe Abschnitt 2.4.7.3). In diesem Fall wäre auch eine DSFA entbehrlich.
	Lösch- bzw. Rückgabepflicht	Der Messenger kann die zentrale Möglichkeit der Löschung aller Unternehmensaccounts aber auch Löschung der Einzelaccounts vorsehen.
	Nachweis der Einhaltung des Art. 28 DSGVO	Auch insofern dürften die Datenminimierungsmaßnahmen den Nachweis erheblich erleichtern.

Datenintensive Nutzungsmöglichkeiten (Fall B):

Rechtliche Anforderungen		Anmerkungen zur Umsetzung
Anforderung an Verantwortlichen:	Auswahl Auftragsverarbeiter mit hinreichenden Garantien	Weicht der Messengerdienst vom in Abschnitt 2.4.4.2.2.4 beschriebenen Stand der Technik ab, besteht ein hoher Begründungsaufwand, warum die Wahl auf diesen Dienst gefallen ist. Bei ausschließlich interner innerbetrieblicher Kommunikation erscheint angesichts am Markt verfügbarer Lösungen kein Grund greifbar, weshalb bereits hierin ein Verstoß gegen Art. 28 DSGVO vorliegen dürfte.
	Abschluss AV-Vertrag	Ein AV-Vertrag ist verpflichtend. Die Regelungstiefe muss dabei für die Bedeutung der Auftragsverarbeitung und dem damit verbundenen Schutzbedarf angemessen sein.[1287] Dabei müssen alle relevanten Tätigkeiten erfasst werden, hierbei können sich die Beteiligten am Verarbeitungsverzeichnis nach Art. 30 DSGVO orientieren.[1288] Eine gesonderte Nennung bedürfen Daten i.S.d. Art. 9 Abs. 1 (besondere Kategorien) und Art. 10 DSGVO (Straftaten)[1289]

[1286] Vgl. auch *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 15.
[1287] *Borges,* in: BeckOK IT-Recht Art. 28 Rn. 46.
[1288] *Hartung,* in: Kühling/Buchner - DS-GVO/BDSG Art. 28 Rn. 65.
[1289] *Borges,* in: BeckOK IT-Recht Art. 28 Rn. 52.

Anforderungen an Auftragsverarbeiter:	Dokumentation	Sofern der Auftraggeber Weisungen erteilt, sind diese zu dokumentieren.
	Verschwiegenheitsklausel	Der Messengeranbieter muss sich sowie die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichten. Lediglich befugte Personen dürfen Zugriff auf die Daten haben. Verschwiegenheitserklärungen sollten dokumentiert sein.
	Datensicherheit	Entsprechend der Apps nach dem Stand der Technik sollte der Messenger Transport- sowie Ende-zu-Ende-Verschlüsselung standardmäßig voreingestellt haben.
	Subbeauftragung	Setzt der Auftragsverarbeiter weitere Sub-Auftragsverarbeiter ein, sind die Anforderungen an die Genehmigungspflichtigkeit zu erfüllen. Dabei sollte darauf geachtet werden, ob Unterauftragnehmer ein Drittlandbezug in ein unsicheres *Drittland ohne Angemessenheitsbeschluss* aufweisen. Eine derartige Einbindung erfordert zusätzliche rechtliche und technische Instrumente (vgl. Abschnitt 4.2).
	Unterstützung Umsetzung Betroffenenrechte	**Auskunft:** Sofern sich die relevanten Daten in der Sphäre des Messengers befinden, muss dieser dem Verantwortlichen die Möglichkeit einräumen, die nach Art. 15 Abs. 1 DSGVO geforderte Übersicht sowie die nach Art. 15 Abs. 3 DSGVO vorgesehene Kopie der personenbezogenen Daten an die betroffene Person innerhalb der vorgesehenen Frist zu übermitteln. Zum Schutz der Daten Dritter kann zudem eine Schwärzung relevanter Stellen erforderlich sein (vgl. Abschnitt 2.4.2.3.2). Probleme können sich ergeben, wenn das Auskunftsersuchen private Chats umfasst, auf welche der Arbeitgeber nicht zugreifen darf. Dies könnte über eine technische Option gelöst werden, welche die erforderlichen Informationen für die betroffene Person unmittelbar, leicht und einfach selbstständig auffindbar gestaltet und ihr ermöglicht eine Kopie zu erstellen. **Berichtigung:** Sind Profildaten unrichtig geworden, sollte es einfache Möglichkeiten geben, diese zu korrigieren. **Löschen:** Der Auftragnehmer muss den Verantwortlichen technisch-organisatorisch unterstützen Löschrechte umzusetzen, hierfür kann dem Verantwortlichen oder den betroffenen Personen selbst die unmittelbare Möglichkeit eingerichtet werden, ihre Rechte selbst wahrzunehmen.
	Unterstützung bzgl. Pflichten aus Artt. 32-36 DSGVO	**Melde- und Benachrichtigung:** Insbesondere, wenn personenbezogene Daten in Klartext vorliegen und/oder länger gespeichert, kann es zu Datenschutzverletzungen kommen, welche eine Data-Breach-Notification erforderlich machen können. **DSFA:** Dem Verantwortlichen obliegt eine Risikobeurteilung, inwiefern ein hohes Risiko vorliegt. Dieses dürfte sich vornehmlich aus der Sphäre des Unternehmens ergeben, allerdings bedarf es zur Evaluation und Umsetzung von TOMs entsprechender Kenntnis über die technischen Abläufe. Der Auftragsverarbeiter hat bei der Durchführung der DSFA und ggf. erforderlichen Konsultation der Aufsichtsbehörde zu unterstützen. Empfohlen wird, die notwendigen Angaben zu Wirkungsweise, Risiken und Schutzmaßnahmen ihrer Dienstleistung bzw. ihres Produktes in einer

		standardmäßigen Aufstellung bereitzuhalten bzw. sogar selbst eine DSFA vorzuhalten.[1290]
	Lösch- bzw. Rückgabepflicht	Die Rückgabe der überlassenen bzw. die Löschung der beim Auftragsverarbeiter gespeicherten Daten nach Beendigung des Auftrags muss geregelt sein. Der Verantwortliche hat ein Wahlrecht.
	Nachweis der Einhaltung des Art. 28 DSGVO	Verantwortliche sollten sich um auch faktisch in der Lage zu sein die Einhaltung der DSGVO nachweisen zu können entsprechende *Informationsrechte* und *Kontrollbefugnisse* einräumen lassen. Neben Vor-Ort-Kontrollen werden die Vorlage eines schlüssigen Datensicherheitskonzepts, Informationseinholung mittels Fragebögen, die Anforderung von Prüfergebnissen oder die Einschaltung von sachverständigen Dritten vorgeschlagen.[1291] Die Einhaltung genehmigter Verhaltensregeln oder einer Zertifizierung (sofern vorhanden) kann zudem als Nachweis herangezogen werden.

Im Hinblick auf die Intensität der Pflichten sowohl seitens des Verantwortlichen als auch des Auftragsverarbeiters fallen diese regelmäßig stärker ins Gewicht, je datenintensiver die umgesetzte Lösung ist.

In Bezug auf die während der Pandemie immer bedeutsamer gewordenen Videokonferenzsystem hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) die Auftragsverarbeitungsvertragsmuster verschiedener Anbieter geprüft und einer Gesamtnote nach einem Ampel-Schema unterworfen (Rot/Gelb/Grün).[1292] Einige dieser Systeme bieten auch Messengerfunktionen, daher soll zur Veranschaulichung typischer Probleme eine kleine Auswahl vorgestellt werden:

[1290] *Kühling/Buchner,* in: Kühling/Buchner - DS-GVO/BDSG Art. 28 Rn. 76.
[1291] *Klug,* in: Gola DS-GVO, Art. 28 Rn. 11.
[1292] *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten., abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf [letzter Abruf 12.08.2021].

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Hinweise für Berliner Verantwortliche zu Anbieter von Videokonferenzsystemen

[Version 2.0 vom 18. Februar 2021]

- **Rote Zone:** Es liegen Mängel vor, die eine rechtskonforme Nutzung des Dienstes ausschließen und deren Beseitigung vermutlich wesentliche Anpassungen der Geschäftsabläufe erfordert:
  - **Cisco Webex Meetings:** AVV lässt weisungswidrige Verarbeitungen zu (insbes. Zugriffsrechte ausländischer Behörden), Fehlen ergänzender Schutzmaßnahmen, Einschaltung nicht genehmigter Subauftragnehmer
  - **Microsoft Teams / Skype for Business:** Vorbehalt der Verarbeitung zu eigenen Zwecken, unzulässige Datenexporte, unzulässige Einschränkung des Weisungsrechts, Widersprüche (unterschiedliche Versionen)
- **Grüne Zone:** es wurden bei der Kurzprüfung keine Mängel gefunden:
  - **Wire Pro:** bietet Ende-zu-Ende-Verschlüsselung, Authentifizierung der teilnehmenden Geräte erfolgt über einen Abgleich ihrer digitalen Fingerabdrücke.

Die vollständige Liste kann in der Veröffentlichung der BlnBDI eingesehen werden. Klassische Messenger wurden nicht betrachtet. Es ist nicht ausgeschlossen, dass die jeweiligen Anbieter auf die festgestellten Mängel reagiert haben.[1293] Insofern sollten Unternehmen die AVV-Unterlagen stets nach dem aktuellen Stand prüfen, ob eines der Probleme vorliegt, welches eine rechtskonforme Nutzung ausschließt:[1294]

- Hat sich der Auftragsverarbeiter die Verarbeitung personenbezogener Daten aus dem Nutzungsverhältnis zu **eigenen Zwecken** oder **Zwecken Dritter** vorbehalten?
- Wie ist die Einbindung von **Subunternehmen** vorgesehen?
- Sieht der Vertrag **unzulässige Datenexporte** vor?
- Gibt es Indizien dafür, dass sich der Auftragsverarbeiter nicht an die Festlegungen im AV-Vertrag hält?
  - Nimmt der Auftragsverarbeiter ein **Nutzer-Tracking** vor, das für den Betrieb der Lösung nicht erforderlich ist?
  - Finden sich in den Datenschutzerklärungen, die den betroffenen Personen im Zuge der Dienstnutzung durch den Auftragsverarbeiter präsentiert oder zugänglich gemacht werden, Hinweise auf Datenverarbeitungen, die mit dem AV-Vertrag nicht in Einklang zu bringen sind?
- Ist die **Sicherheit** der verarbeiteten Daten und die Einhaltung des **Privacy by Design & by Default** auch unter den konkreten geplanten Einsatzumständen gegeben?
  - Hat der Auftragsverarbeiter ausreichende **Garantien** für die Vornahme angemessener technischer und organisatorischer Maßnahmen bei dem Betrieb des Dienstes vorgelegt?
  - Erfolgen **Datenlöschungen** nur verspätet oder eingeschränkt?

[1293] Vgl. bspw. die Reaktion von Microsoft, abrufbar unter https://news.microsoft.com/de-de/stellungnahme-zum-vermerk-berliner-datenschutzbeauftragte-zur-durchfuehrung-von-videokonferenzen-waehrend-der-kontaktbeschraenkungen/ [letzter Abruf 12.08.2021].

[1294] Vgl. *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten, S. 3, 36; vgl. auch *Suwelack*, ZD 2020, 561 (564).

Da es zu den Pflichten des Verantwortlichen zählt, bei der Auswahl eines AV-Anbieters sicherzustellen, dass die Vorgaben der DSGVO eingehalten werden sowie dies auch im zumutbaren Rahmen zu kontrollieren, ist eine ordnungsgemäße Beauftragung eines Dienstes in der Regel kaum begründbar, wenn Hinweise auf eine datenschutzwidrige Verarbeitung personenbezogener Daten bekannt sind.[1295]

5.2.5 Zwischenergebnis zur innerbetrieblichen Kommunikation

Festzuhalten sind die wesentlichsten Punkte:

- **Verantwortung:** Stellt ein Unternehmen einen Messenger-Dienst On-Premise bereit oder ordnet die Nutzung eines spezifischen Dienstes an, ist es datenschutzrechtlich Verantwortlicher. Bei der Duldung ist zu differenzieren, ob ein Mitarbeiterexzess vorliegt, eine betriebliche Übung oder einem dem Unternehmen zurechenbare Praxis. Das Unternehmen sollte im Zweifelsfall von einer Verantwortung ausgehen, und den Prozess der Auswahl und Umsetzung von Kommunikationslösungen aktiv zu gestalten.
- **Verantwortungssphären:** Wird die Lösung nicht On-Premise betrieben, muss das Unternehmen das Verhältnis zum Messengerdienstanbieter klären.
  - Bei einer Auftragsverarbeitung trifft das Unternehmen eine eigene Pflicht einen Dienst mit geeigneten Garantien zu wählen. Es kann auch für Datenschutzverstöße des Auftragsverarbeiters haften. Für den Auftragsverarbeiter bestehen gesetzliche Pflichten zur Unterstützung des Verantwortlichen bei der Umsetzung der Datenschutzpflichten.
  - Bei der gemeinsamen Verantwortung kann ebenfalls keine Verantwortung auf den Messenger „abgewälzt“ werden, vielmehr besteht gesamtschuldnerische Haftung. Besteht keine Möglichkeit zu prüfen, inwiefern der Messenger die Datenschutzvorgaben einhält, sollte vom Einsatz abgesehen werden. Ferner bestehen Unsicherheiten, da OTT-Dienste mit der neuen Rechtslage generell als Telekommunikationsdienste eingeordnet werden, selbst wenn das Zusammenspiel aus DSGVO und TTDSG komplex ist. Angesichts zahlreicher Angebote bedarf es einer eingehenden Prüfung, warum ein Dienst zum Einsatz kommen soll, welcher eigene Verarbeitungszwecke verfolgt.

▷ Rechtlich unzulässig ist der betriebliche Einsatz eines Messengerdienstes unter Verletzung einer Einschränkung auf Privatnutzung in den Nutzungsbedingungen, ohne Abschluss eines AV-Vertrags oder einer Vereinbarung über die gemeinsame Verantwortlichkeit.

- **Rechtsgrundlagen:** Nach der hier vertretenen Ansicht richten sich die Rechtsgrundlagen für das Unternehmen nach der DSGVO sowie im Rahmen der Öffnungsklausel zum Beschäftigtendatenschutz nach § 26 BDSG. Insofern ist eine Abwägung zwischen den Zielen zur Kommunikationsgestaltung und den Persönlichkeitsrechten der Beschäftigten vorzunehmen. Je weniger Datenschutzrisiken ein Kommunikationsformat bedingt, desto eindeutiger fällt diese Abwägung aus.
  - Liegt eine gemeinsame Verantwortung vor, muss der Messenger zusätzlich die Regelungen für TK-Dienste im Blick haben. Angesichts der gesamtschuldnerischen Haftung kann das Unternehmen Haftungsrisiken minimieren, indem entweder ein Dienst gewählt wird, der sämtliche Datenschutzanforderungen bestmöglich erfüllt, oder ein geschlossenes System On-Premise oder als Auftragsverarbeitung umgesetzt wird.

[1295] *Suwelack*, ZD 2020, 561 (564 f.).

  - Basieren wesentliche Funktionalitäten des Dienstes auf einer Einwilligung oder wird diese zur Nutzung des Dienstes gefordert, ist dieser Dienst im Beschäftigtenkontext nicht geeignet. Einwilligungen können nur dort freiwillig erteilt werden, wo Funktionen oder Daten optional sind.
  - Für geschlossene Nutzergruppen in einem Betrieb On Premise liegt nach hier vertretender Ansicht kein öffentlich zugänglicher oder geschäftsmäßig betriebener Telekommunikationsdienst vor, sodass §§ 3 ff. TTDSG nicht einschlägig sind – dies ist allerdings umstritten bei der Zulassung privater Kommunikation. Arbeitgeber können sich auf arbeitsgerichtliche Präzedenzfälle berufen, nicht als TK-Dienst eingeordnet zu werden.
- **Betriebsrat:** Der Betriebsrat sollte frühzeitig eingebunden werden. Eine Betriebsvereinbarung kann Rechtssicherheit schaffen.

▷ Bestmöglichen Schutz vor Haftungsrisiken bieten Dienste die – unabhängig von der Anwendbarkeit – sowohl die Anforderungen der DSGVO und des TTDSG erfüllen können. Je strenger das Datenschutzkonzept des Dienstes ausfällt, desto leichter können Verantwortliche ihren Rechenschafts- und Nachweispflichten nachkommen.

- **Transparenz:** Die Beschäftigten sind klar und verständlich über die Verarbeitung der sie betreffenden personenbezogenen Daten zu informieren. Bei der gemeinsamen Verantwortung kommt die Information über die Vereinbarung der Pflichtenverteilung hinzu.
- **Technische und Organisatorische Maßnahmen:** Bei der Auswahl von Lösungen muss berücksichtigt werden, welche datenschutzfreundliche Systeme am Markt verfügbar sind (Stand der Technik). Grundsätzlich dürfen auch Kosten und Arbeitsaufwand bei der Auswahl ebenfalls in die Rechnung einbezogen werden – diese müssen allerdings in Verhältnis mit den konkreten Risiken zu Schwere und Eintrittswahrscheinlichkeit von möglichen Schäden gesetzt werden: je höher die Risiken ausfallen, desto eher müssen auch kostenintensive Schutzmaßnahmen umgesetzt werden.
  - **Schutz der Kommunikationsinhalte:** Etabliert ist eine Kombination aus Transport- und Ende-zu-Ende-Verschlüsselung.
  - **Schutz der Metadaten:** Die Übermittlung des gesamten Adressverzeichnisses an den Messengerdienst stellt regelmäßig einen Datenschutzverstoß gegenüber denjenigen Kontakten dar, die diesen Dienst nicht nutzen. Solche Dienste können ohne zusätzliche Schutzmaßnahmen nicht im betrieblichen Kontext eingesetzt werden.
  - **Datenspeichermanagement:** Da Unternehmen neben der Pflicht zur Datensparsamkeit und Speicherbegrenzung auch Aufbewahrungs- und Dokumentationspflichten unterliegen können, ist es wesentlich, sich rechtzeitig einen Überblick über die betroffenen Kommunikationsarten, dabei ggf. anfallenden, geschäftlichen Dokumenten und die damit verbundenen Pflichten zu verschaffen. Hierbei sollten Kommunikationsräume nach Vertraulichkeitslevel getrennt werden und Transparenz im Hinblick auf die Ausübung von Kontrollmaßnahmen und Datenarchivierung geschaffen werden.
  - **Risikobewertung:** Das Unternehmen ist grundsätzlich verpflichtet eine Risikobewertung durchzuführen. Liegt ein hohes Risiko vor, schließt sich eine Datenschutzfolgenabschätzung (DSFA) an. Bleibt das Risiko hoch trotz Abhilfemaßnahmen ist die Aufsichtsbehörde zu konsultieren. Ist das Risiko hingegen gering, entfallen diese Pflichten. Zudem können Ausnahmen bei den Melde- und Benachrichtigungspflichten im Rahmen eines Datenschutzverstoßes greifen.
  - **Fristen und Organisation:** Sowohl im Hinblick auf die Umsetzung der Melde- und Benachrichtigungspflichten als auch der Betroffenenrechte sind Fristen einzuhalten: Abläufe sollten daher vorab bekannt und Ansprechpersonen benannt sein.

▷ Unternehmen sollten sich frühzeitig einen Überblick über das Risikolevel verschaffen, um ihre Pflichten abzustecken und entsprechende Verfahren im Unternehmen zu etablieren, Aufgaben und Verantwortlichkeiten unter den Beschäftigten zu definieren. Bieten Anbieter eine gute Dokumentation ihrer Schutzmaßnahmen oder bereits eine Muster-DSFA, fällt diese Aufgabe leichter.

- **Drittstaatentransfers:** Für eine rein innerbetriebliche Kommunikation erscheinen keine überzeugenden Gründe für eine Datenübermittlung in ein Drittland, welches über kein durch einen Angemessenheitsbeschluss der EU-Kommission belegtes angemessenes Schutzniveau verfügt, ersichtlich. Auch bei international verteilten Konzernstrukturen kann sich die Übermittlung personenbezogener Daten nicht auf inländische Sachverhalte erstrecken.

▷ Bei Auswahl eines Auftragsverarbeiters sollten Unternehmen darauf achten, dass keine Sub-Auftragnehmer aus unsicheren Drittländern eingebunden werden.

- **Trennung privater und beruflicher Inhalte:** Da umstritten ist, ob die Regelungen zum Fernmeldegeheimnis auf Arbeitgeber ggü. ihren Beschäftigten anwendbar sind – oder eine vergleichbare Pflicht aus der DSGVO i.V.m. BDSG ohnehin im Hinblick auf den Zugriff auf persönliche Nachrichten besteht, sollten Unternehmen entweder private Kommunikation gänzlich ausschließen oder sicherstellen, dass private von beruflicher Kommunikation getrennt wird. Um einer betrieblichen Übung der Duldung privater Kommunikation vorzubeugen, könnten unterschiedliche Kommunikationsräume geschaffen werden, für die unterschiedliche Vertraulichkeitslevel gelten.

▷ Beschäftigten sollte stets bewusst sein, wann es sich um vertrauliche Privatkommunikation im Kollegenkreis handelt, und wann Kontrollrechte und Speicherpflichten des Unternehmens eingreifen.

Merksatz: Auch aufgrund der Fürsorgepflicht des Arbeitgebers gegenüber seinen Beschäftigten ist ein Dienst auszuwählen, der die Rechte der Beschäftigten unter Berücksichtigung der Kommunikationsziele bestmöglich wahrt. Damit kommen Messengerdienste kaum in Betracht, die ihren Sitz außerhalb der EU bzw. Ländern mit Angemessenheitsbeschluss haben, eigene Verarbeitungszwecke verfolgen und dabei Methoden des Profilings oder Nutzertrackings einsetzen, die Erbringung wesentlicher Dienste an eine Einwilligung koppeln und/oder Daten Dritter ohne deren Kenntnis/Einverständnis vom Endgerät auslesen.

5.3 Externe Kommunikation des Unternehmens

Die Umsetzung neuer Kommunikationslösungen im Unternehmen dürften selten allein durch einen rein innerbetrieblichen Austausch motiviert sein oder auf diesen beschränkt werden. Oftmals wird es praktisch sein, wenn die gewählte Kommunikationsform auch Interaktionen mit Geschäftskontakten oder der Unternehmenskundschaft ermöglicht. Insofern treten die Beschäftigten in Vertretung des Unternehmens extern auf. Interessenkonstellationen können anders gelagert sein, als im Rahmen rein innerbetrieblicher, geschlossener Kommunikation. Zudem muss sich der datenschutzrechtlich Verantwortliche versichern, dass die Verarbeitung der personenbezogenen Daten der externen Kommunikationskontakte ebenfalls datenschutzkonform erfolgt.

5.3.1 Verantwortlichkeit des Unternehmens

Wie bereits zur internen Kommunikation festgestellt, ist für Unternehmen die Einhaltung der DSGVO von Bedeutung, wenn sie sich dafür entscheiden, dass Messengerdienste bei der Kommunikation im Unternehmenskontext verwendet werden sollen. An dieser Stelle soll ausschließlich auf Besonderheiten der Interaktion mit Kommunikationsteilnehmenden außerhalb des Unternehmens eingegangen werden. Im Übrigen gelten die gleichen Erwägungen wie unter Abschnitt 5.2.

5.3.1.1 Externe Vorgabe eines Kommunikationskanals

In diesem Szenario erfolgt die Nutzung eines Kommunikationssystems wie bspw. eines Messengerdienstes durch Beschäftigte auf Einladung Dritter wie bspw. Geschäftskontakte. Da Personen, die an einem Kommunikationsvorgang lediglich teilnehmen, grundsätzlich selbst nicht Verantwortliche sind, kann argumentiert werden, dass in diesem Szenario auch die Arbeitgeber keine Verantwortung trifft.[1296] Denn insofern besteht kein wirklicher Entscheidungsspielraum über das „Warum“ oder „Wie“ der Kommunikation, wenn diese Parameter extern vorgegeben werden.

Andererseits kann ein Eingriff in die Persönlichkeits- und Datenschutzrechte gegeben sein, wenn die Arbeitgeber im Rahmen ihrer Weisungsrechte die Teilnahme an extern vorgegebenen Kommunikationskanälen ohne angemessenes Datenschutzniveau verpflichtend machen. Auf einfachrechtlicher Ebene läge dann mangels Verantwortlichkeit i.S.d. Art. 4 Nr. 7 DSGVO zwar kein Datenschutzverstoß vor, aber eine Verletzung arbeitsvertraglicher Pflichten auf Rücksichtnahme.[1297]

5.3.1.2 Bereitstellung eines Messengerdienstes On Premise

Der Unterschied zum Szenario unter Abschnitt 5.2 liegt hier darin, dass das Unternehmen (zusätzlich) personenbezogene Daten von Kundschaft und Geschäftskontakten verarbeitet. Das berufliche Adressbuch unterfällt hierbei den Regelungen der DSGVO.[1298] Das Unternehmen ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO, unabhängig davon ob die Messengernutzung freiwillig erfolgt oder angeordnet wird.

5.3.1.3 Nutzung von am Markt verfügbaren Messengerdiensten

Zur Kontaktpflege kann es praktisch sein, bestehende Lösungen am Markt zu nutzen. Dabei gilt wiederum zu bedenken, dass einige Anbieter ihre Standard-Apps auf private Nutzung einschränken.

Messenger Marketing: „Messenger Marketing“ bezeichnet den Einsatz von Messengern im Rahmen des Kundenkontakts, bspw. zur Beantwortung von Kundenanfragen oder zur gezielten Werbung.[1299] Wählt das Unternehmen einen Messenger zu Marketingzwecken oder Kundenansprache bspw. im Rahmen des Kundensupport wird das Unternehmen nach Art. 4 Nr. 7 DSGVO verantwortlich für Verarbeitung personenbezogener Daten.[1300] Wann Unternehmen andere Unternehmen und/oder Privatkunden auf welche Form ansprechen

---

[1296] *Bühr*, K&R 2021, 221 (221).
[1297] Vgl. zur vergleichbaren Konstellation: BAG, Urteil vom 11.12.2014 – 8 AZR 1010/13, Rn. 32.
[1298] Vgl. zu den Grenzen der Haushaltsausnahme: *Gola/Lepperhoff*, ZD 2016, 9 (10); *Piltz*, K&R 2016, 557 (558).
[1299] Siehe ausführlich zur Nutzung von Messengerdiensten zum Kundenkontakt/Marketing: *Mehner*, Messenger Marketing.
[1300] *Ulbricht,* in: *Mehner*, Messenger Marketing, S. 70.

dürfen, ist parallel zum Datenschutzrecht auch eine Frage des unlauteren Wettbewerbs nach UWG. Diese Fragestellungen sollen in der vorliegenden Studie allerdings nicht betrachtet werden.

Fraglich ist, welche Rolle der Messengerdienst einnimmt: im Hinblick auf die Rechtsbeziehung zu den Privatkundinnen ist der Messengerdienst selbst Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO. Gegenüber dem Unternehmen könnte hingegen eine Auftragsverarbeitung vereinbart sein. Da es aber nicht darauf ankommt, welche Vereinbarung die Beteiligten getroffen haben, sondern welche Beziehung tatsächlich besteht, ist diese Frage nicht trivial. Die korrekte Einordnung hat entscheidende Bedeutung darüber, ob eine eigene Rechtsgrundlage für die Datenverarbeitung durch den Messengerdienst erforderlich ist und ob die Informationspflichten im Hinblick auf die Darstellung der gemeinsamen Verantwortlichkeit gegenüber den betroffenen Personen erfüllt wurde. Daher soll diese Problematik im folgenden Abschnitt zu den einschlägigen Rechtsgrundlagen weiter erörtert werden.

5.3.2 Einschlägige Rechtsgrundlagen

5.3.2.1 On-Premise-Lösungen: Unternehmen als allein Verantwortlicher

Verarbeitet das Unternehmen personenbezogene Daten, so betrifft dies regelmäßig zwei Gruppen: die externen Kommunikationskontakte einerseits und die Beschäftigten andererseits.

Verhältnis zu externen Kommunikationskontakten: Stellt das Unternehmen selbst einen Messengerdienst bereit und verantwortet diesen in alleiniger Verantwortung dürfte der aus datenschutzrechtlicher Perspektive im Hinblick auf die Pflichten der DSGVO vergleichbar einfachste Fall vorliegen. Je nachdem zu welchem Zweck die Kontaktaufnahme erfolgt, sind verschiedene Rechtsgrundlagen denkbar, bspw.:

Vertrag / vorvertraglicher Kontakt mit der betroffenen Person:

- Die Verarbeitung ist im Rahmen einer Kontaktaufnahme an das Unternehmen erforderlich zur Durchführung vorvertraglicher Maßnahmen (bspw. im Rahmen der Vertragsanbahnung), die auf Anfrage der betroffenen Person erfolgt (vgl. Art. 6 Abs. 1 Buchst. b DSGVO). Fraglich wäre, ob die Erforderlichkeit auch die Wahl des Kommunikationskanals umfasst: hier kann das Unternehmen verschiedene Wege bereitstellen. So wäre sichergestellt, dass die Messengernutzung auf einer selbstbestimmten Entscheidung der betroffenen Person beruht. Ferner kann die Einrichtung datenverarbeitungsarmer Gastzugänge, welche ohne App nutzbar sind, Datenschutzbedenken ausräumen.[1301]
- Die Verarbeitung ist erforderlich im Hinblick auf die Erfüllung des Vertrags bzw. Umsetzung flankierender rechtlicher Verpflichtungen, wie bspw. Benachrichtigungen nach § 312f Abs. 2 BGB bei Fernabsatzverträgen. Besteht keine andere Kontaktmöglichkeit zur betroffenen Person, bestehen kaum Zweifel an der Erforderlichkeit.

Geschäftsbeziehungen zu juristischen Personen / Personengesellschaften:

- Erfolgt der Austausch im Rahmen gemeinsamer Geschäftsbeziehungen im beruflichen Kontext ohne einen konkreten Vertrag könnte dies ebenfalls als Fall des Art. 6 Abs. 1 Buchst. b DSGVO, unter dem Aspekt der vorvertraglichen Maßnahmen argumentiert werden. Allerdings sind Beschäftigte, die im Na-

[1301] *Brüggemann/Hötzel,* in: Kipker/Voskamp - Sozialdatenschutz, Kap. 4 Rn. 127.

men einer juristischen Person oder Personengesellschaft handeln, regelmäßig nicht selbst Vertragspartei. In Teilen der Literatur wird daher ein weites Verständnis der „Vertragspartei“ präferiert.[1302] Die überwiegende Ansicht in Literatur und Rechtsprechung scheint dieser Interpretation allerdings bisher nicht zugetan und verweist auf den eindeutigen Wortlaut.[1303] Die Norm macht hingegen keine Angaben, wer auf Seiten des Verantwortlichen Vertragspartei sein muss: grundsätzlich kann auch die Verarbeitung durch einen Dritten legitimiert werden, wenn dies zur Vertragserfüllung erforderlich ist. [1304] Im Beschäftigungskontext liegt ein Vertrag der Beschäftigten mit ihren Arbeitgebern in Form des Arbeitsvertrags vor – dabei kommt es aber wiederum zu einer lex specialis-Anwendung des § 26 BDSG: für eine Rechtfertigung müssten auch die Datenverarbeitungen durch Geschäftskontakte zur Durchführung des Beschäftigungsverhältnisses erforderlich sein.[1305] Dies betrifft die Offenlegung durch das Vertragspartnerunternehmen in seiner Funktion als Verantwortlicher gegenüber dem den Messengerdienst bereitstellenden Unternehmen – ob es auch den gesamten Kommunikationsprozess als einheitlichen Lebenssachverhalt erfasst, ist allerdings mit einigen Unsicherheiten behaftet. [1306] Im Endeffekt verbleibt es bei einem Rekurs auf die Interessenabwägung.[1307] Zu erwähnen gilt, dass sich diese Problematik auch bei anderen Kommunikationsmedien wie E-Mail, Telefon, Postbrief, etc. stellt und keine Besonderheit der Messengerkommunikation ist. Bei Videokonferenzen können laut DSK berechtigte Interessen die Datenverarbeitung legitimieren, wenn grundsätzlich Alternativen zur Videokonferenz verbleiben und die Beschäftigten anderer Unternehmen teilnehmen.[1308] Organisatorisch müssen Verantwortliche beachten, dass betroffenen Personen ein Widerspruchsrecht nach Art. 21 DSGVO zusteht, wenn die Verarbeitung auf der Interessenabwägung beruht.

[1302] Für die Einbeziehung Daten Dritter: *Taeger,* in: Taeger/Gabel - DSGVO/BDSG Art. 6 Rn. 61.
[1303] *Wolff/Kosmider*, ZD 2021, 13 (14); *Heberlein,* in: Ehmann/Selmayr - DSGVO Art. 6 Rn. 13; *Albers/Veit,* in: BeckOK DatenschutzR Art. 6 Rn. 30; *Schulz,* in: Gola DS-GVO, Art. 6 Rn. 28; *Reimer,* in: Sydow, Europäische Datenschutzgrundverordnung Art. 6 Rn. 18.; vgl. auch OLG München, Urteil vom 16.1.2019 – 7 U 342/18, Rn. 30; VG Mainz, Urteil vom 20.2.2020 – 1 K 467/19.MZ, Rn. 29.
[1304] *Albers/Veit,* in: BeckOK DatenschutzR Art. 6 Rn. 30.
[1305] *Wolff/Kosmider*, ZD 2021, 13 (14 f.); vgl. auch *Gola,* in: Gola/Heckmann - BDSG, § 26 Rn. 91 ff.; *Zöll,* in: Taeger/Gabel - DSGVO/BDSG, § 26 Rn. 39.
[1306] *Wolff/Kosmider*, ZD 2021, 13 (14 f.).
[1307] *Wolff/Kosmider*, ZD 2021, 13 (16).
[1308] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 10.

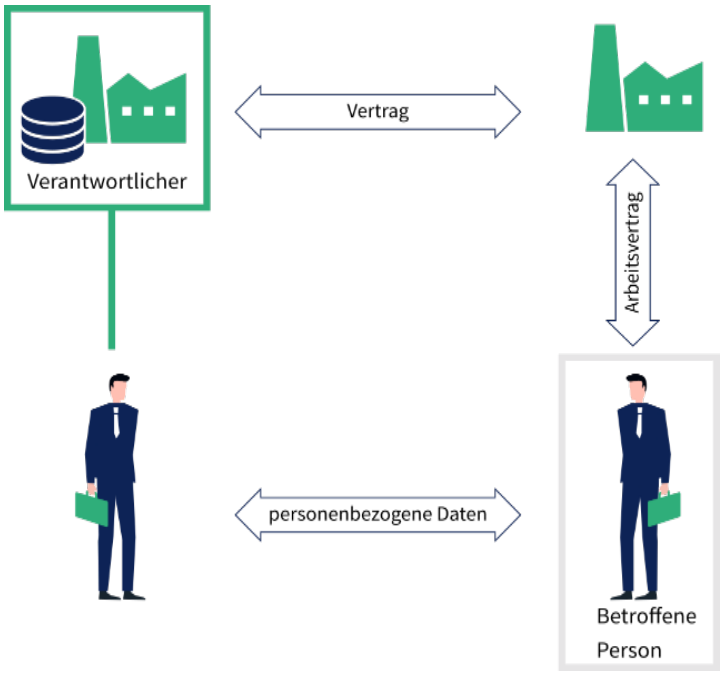


Abbildung 13 Dreickskonstellation bei unternehmerischen Geschäftsbeziehungen

- Der bloße Bezug zu einem Vertragsverhältnis reicht allerdings nicht aus, sodass Marketing und Marktforschungsmaßnahmen nicht mehr unter den Rechtfertigungstatbestand fallen[1309] – hier gelten keine Besonderheiten bezüglich der Wahl des Messengerdienstes als Kommunikationsmittel.

Einwilligung:

- Erfolgt die Kontaktaufnahme aktiv durch die Gegenseite vergleichbar mit der Übergabe einer Visitenkarte, kann eine Einwilligung in Betracht kommen.[1310] Der Verantwortliche muss allerdings die Nachweispflicht erfüllen und bei einem Widerruf der Einwilligung die Daten entsprechend löschen, sofern keine weitere Rechtsgrundlage eingreift.
- Sofern die Verarbeitungszwecke unter keine der vorgenannten Rechtsgrundlagen fällt und eine Einwilligung eingeholt werden soll, gilt zu bedenken, dass in diesem Fall auch andere Kontaktaufnahmemöglichkeiten bereitgestellt werden sollten, welche keine Einwilligung erfordern, um die Freiwilligkeit der Einwilligung sicherzustellen (vgl. Abschnitt 2.4.1.2.1.3).

Gesetzliche Verarbeitungspflichten:

- Eine sich an den Kommunikationsvorgang anschließende Speicherung/Archivierung der Daten kann aufgrund von gesetzlichen Aufbewahrungspflichten erforderlich sein (vgl. Abschnitt 2.4.1.3.1), insbesondere bei als Handelsbriefe einzuordnender Kommunikation oder steuerrechtlich relevanter Sachverhalte: § 257 HGB, § 147 AO.

[1309] *Wolff/Kosmider*, ZD 2021, 13 (13).; vgl. Abschnitt 2.4.1.2.2.1.
[1310] *DSK - Datenschutzkonferenz*, Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO), S. 9; *Wolff/Kosmider*, ZD 2021, 13 (15).

- Für den Fall, dass die Kontaktaufnahme Jedermann möglich ist und damit anzunehmen wäre, dass auch ein „öffentlich zugänglicher“ oder „geschäftsmäßig“ betriebener elektronischer Kommunikationsweg nach § 3 Abs. 2 TTDSG eröffnet würde, stellt sich die Frage, ob das Unternehmen auch als elektronischer Telekommunikationsdienst einzustufen wäre (vgl. Abschnitt 3.2.1 zum Streit um den Anwendungsbereich). Zwar tritt das Unternehmen auch als Anbieter um Hinblick auf die Kommunikationsübermittlung gegenüber Dritten auf, allerdings erfolgt die Kommunikation ja gerade *mit* dem Unternehmen. Das mit dem TTDSG spezifisch geschützte Fernmeldegeheimnis greift nur im Hinblick auf die Übermittlung und solange die Informationen noch nicht in den alleinigen Herrschaftsbereich der jeweiligen Kommunikationsbeteiligten gelangt sind.[1311] Sobald der Übermittlungsvorgang vollständig abgeschlossen ist, greift wieder die DSGVO. Erhöhte Anforderungen stellen sich aus dem TTDSG daher allenfalls nur für die Phase der Übermittlung: diese sollte ausreichend abgesichert erfolgen.
- **Folgen für Beschäftigte**: Im Hinblick auf die personenbezogenen Daten der Beschäftigten, welche im Rahmen betrieblich motivierter Kommunikation verarbeitet werden, folgt die Rechtsgrundlage ebenfalls aus § 26 Abs. 1 BDSG (vgl. Abschnitte 2.4.1.3.3 und 5.2.2). Insoweit könnte das Unternehmen als Arbeitgeber ggf. aufgrund von Compliance-Anforderungen verpflichtet sein, Arbeitsergebnisse zu kontrollieren.[1312] Zudem betreffen die Aufbewahrungspflichten bspw. nach §§ 257 HGB, 147 AO auch die Archivierung der personenbezogenen Daten der Beschäftigten. Die Mitbestimmungsrechte des Betriebsrats sind zu wahren. Im Rahmen der Gestaltung der Kommunikationskanäle sollte frühzeitig eruiert werden, welche Rollen im Unternehmen Zugriff auf Kommunikationsvorgänge haben müssen und wie diese auch nach außen transparent gestaltet werden können.

5.3.2.2 Nutzung von am Markt verfügbaren Messengerdiensten

Bei der Nutzung von bestehenden am Markt angebotenen Messengerdiensten entstehen mehrere Datenverarbeitungsbeziehungen. Im Hinblick auf die Rechtsgrundlage ist wiederum von Bedeutung, ob es sich um eine Auftragsverarbeitung oder gemeinsame Verantwortlichkeit handelt, da die Datenübermittlung an den Messengerdienst nur bei Letzterer einer eigenen Rechtsgrundlage bedarf.

Einbindung des Messengerdienstes auf Seiten eines Unternehmens: Schließt das die Kommunikation verantwortende Unternehmen einen AV-Vertrag mit einem Messengerdienst richtet sich die Rechtsgrundlage nach der Rechtsbeziehung des Unternehmens zu seinen Kommunikationskontakten. Es gelten vergleichbare Erwägungen wie im Abschnitt zuvor (5.3.2.1). Den Auftragsverarbeiter treffen die bereits dargestellten Unterstützungspflichten. Das Unternehmen ist verpflichtet nur Auftragsverarbeiter mit geeigneten Garantien zu verwenden. Kommunikationskontakte können sowohl Privatpersonen (bspw. Kundschaft eines Unternehmens) oder Geschäftspersonen (bspw. die Beschäftigten anderer Unternehmen) sein. In jedem Fall kommt es zur Verarbeitung personenbezogener Daten, für die das Unternehmen eine Rechtsgrundlage braucht.

[1311] Statt vieler: *Brink/Schwab*, ArbRAktuell 2018, 111 (112).
[1312] *Dietrich u. a.*, DuD 2021, 5 (7); *Riesenhuber,* in: BeckOK DatenschutzR, § 26 BDSG, Rn. 171; *Brink/Schwab*, ArbRAktuell 2018, 111 (111). *Wybitul/Böhm*, CCZ 2015, 133 (133 f.); *Schrey u. a.*, MMR 2017, 656 (660).

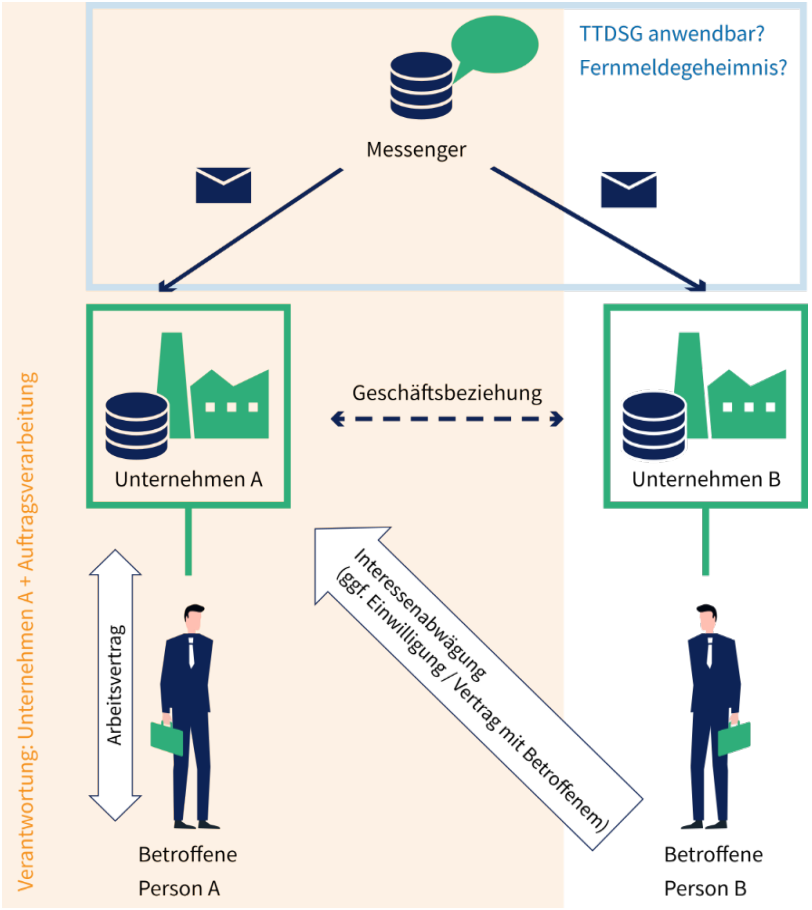


Abbildung 14 Einbindung eines Messengerdienstes auf Seiten eines Unternehmens

Trotz der Zweifel im Hinblick auf die Rechtslage zum TTDSG sollte der Messenger als Auftragsverarbeiter auch geeignete Garantien im Hinblick auf die telekommunikations- und telemedienrechtlichen Anforderungen des TTDSG bezüglich des Übermittlungsvorgangs bereitstellen. Denn sofern diese als ohnehin miterfüllt gelten können, entstehen keine Haftungsrisiken, selbst wenn das Unternehmen als TK-Dienstanbieter eingeordnet werden sollte (vgl. Abschnitt 3.3):

- eine enge Zweckbindung ergibt sich bereits aus der Natur der Auftragsverarbeitung: dieser darf ohnehin keine eigenen Zwecke verfolgen
- Datensicherheitsanforderungen ergeben sich gleichermaßen aus Art. 32 DSGVO als auch TTDSG
- Der gewählte Dienst sollte nicht mehr personenbezogene Daten verarbeiten, als dies zur Diensterbringung zwingend erforderlich ist, die Dienstgestaltung sollte sich am Grundsatz der Datenminimierung orientieren

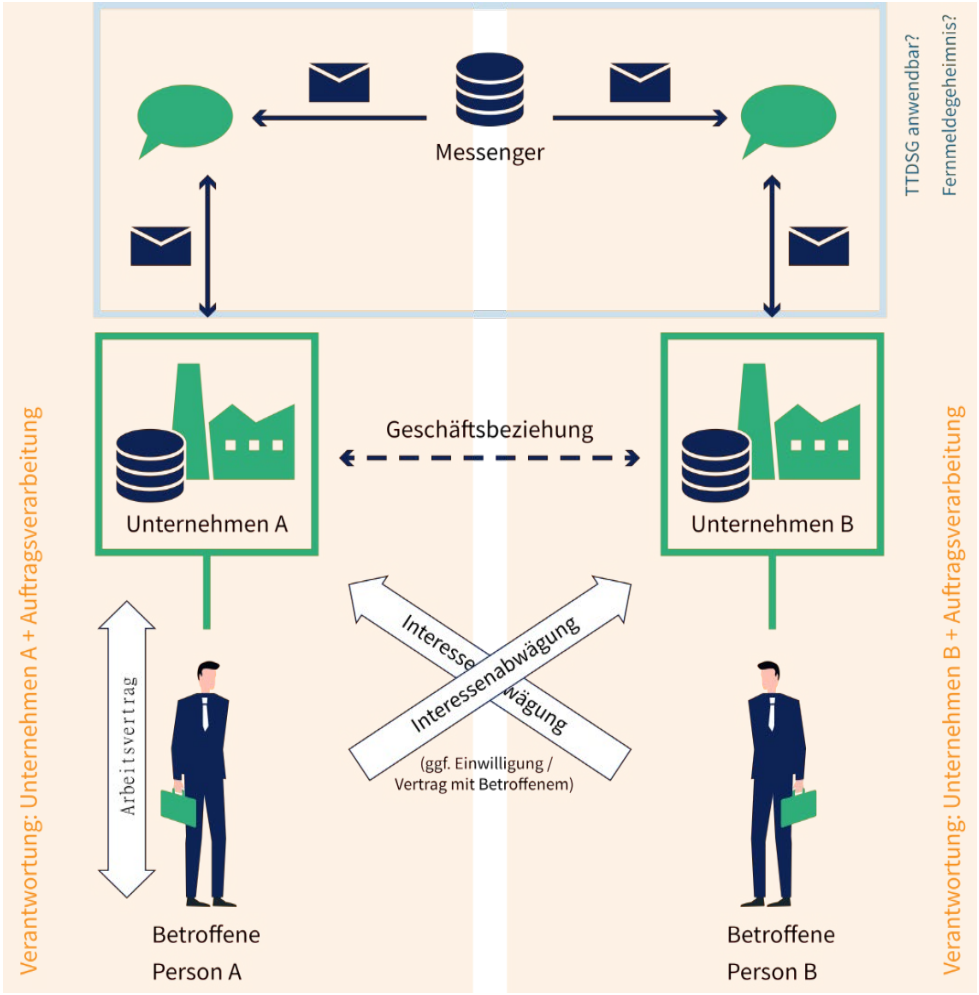


Abbildung 15 Einsatz eines unternehmensübergreifend gemeinsam genutzten Messengerdienstes als Auftragsverarbeitung (Software-as-a-Sevice)

Verantwortungsketten oder Vereinbarung zwischen Unternehmen als gemeinsam Verantwortliche? In Geschäftsbeziehungen stehende Unternehmen könnten sich darauf verständigen, eine bestimmte Kommunikationslösung zu verwenden. Ob eine Vereinbarung nach Art. 26 DSGVO erforderlich ist, hängt davon ab, ob die Kommunikation über einen Messenger als einheitlicher Vorgang oder Einzelverantwortlichkeit in unterschiedlichen Phasen einer Datenverarbeitung zu bewerten ist. Insofern könnten beide Unternehmen jeweils mit einem Messengerdienst eine entsprechenden AV-Vertrag abgeschlossen haben (vgl. Abbildung 15). In jedem Fall bedarf jedes an der Kommunikation als Verantwortlicher beteiligtes Unternehmen eine entsprechende Rechtsgrundlage für die Datenverarbeitung. Auch hier kann auf die oben genannten Erwägungen zurückgegriffen werden (5.3.2.1).

Gemeinsame Verantwortung in Dreiecksbeziehungen? Die komplexeste Konstellation dürfte sich ergeben, wenn der Messengerdienstanbieter eigene Zwecke verfolgt. Aus Sicht des Messengerdienstes könnte zwar eine Verarbeitung von Verkehrsdaten (§ 9 TTDSG) oder Verarbeitung zur Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DSGVO) die Datenverarbeitung legitimieren. Im ersteren Fall wäre eine Verarbeitung zu anderen Zwecken nach TTDSG ohnehin nur eingeschränkt möglich, im zweiten Fall wäre ein Rückgriff auf die Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DSGVO dagegen nicht von vorneherein ausgeschlossen. Eine Einwilligung müsste verweigert bzw. widerrufen werden können, ohne dass dies die Diensterbringung hindert.

Da mehrere an der Kommunikation beteiligte Unternehmen jeweils die Rechte ihrer Beschäftigten wahrnehmen müssen, erscheinen kaum Fallgestaltungen denkbar, in denen eine Auswahl eines Messengerdienstes sachgerecht erscheint, welcher über die zur Kommunikationsdiensterfüllung hinausgehende Datenverarbeitungen zu weiteren Zwecken vornimmt. Denn im Rahmen der Interessenabwägung ggü. der Verarbeitung personenbezogener Daten fremder Beschäftigter sowie im Rahmen der Abwägung nach § 26 Abs. 1 BDSG ggü. den eigenen Beschäftigten ist stets zu berücksichtigen, dass eine datenschutzfreundliche Gestaltung vorliegt. Je nachdem wie intensiv oder risikobehaftet die vom Messengerdienst in eigener Verantwortung anvisierten Datenverarbeitungsvorgänge im Einzelfall ausfallen, kann sich dies negativ auf die Legitimierbarkeit der Datenverarbeitung der Unternehmen auswirken. Diese Wechselwirkung gilt es in derartigen Dreieckkonstellationen zu bedenken. Es besteht daher ein erhöhter Begründungsaufwand, je mehr personenbezogene Daten über die bloßen Kommunikationszwecke und damit in direktem Zusammenhang stehenden Aspekten wie Sicherstellung der IT-Sicherheit, Ausfallsicherheit, etc. hinaus verarbeitet werden. Bisher sind keine Fälle bekannt, in der ein solches Szenario beabsichtigt ist.

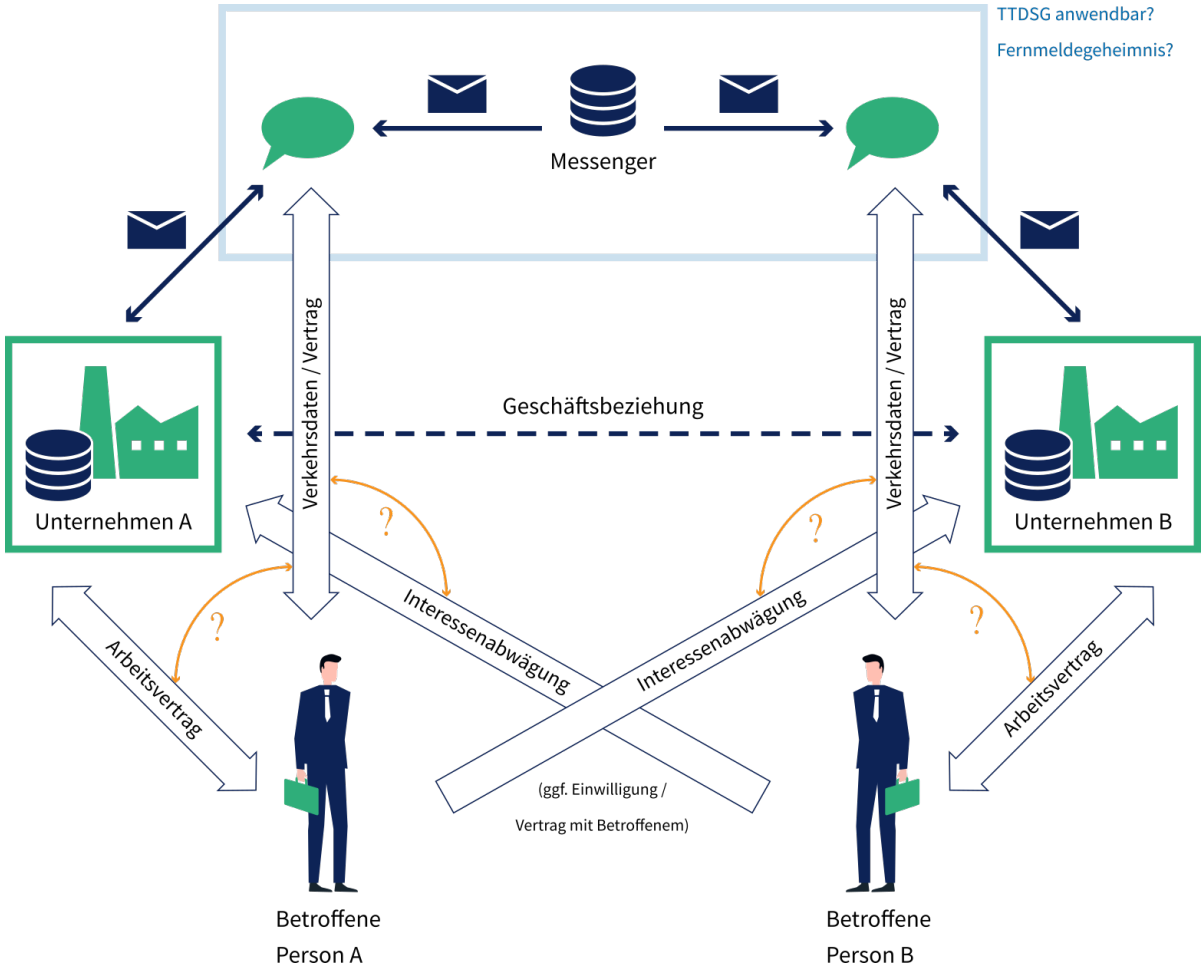


Abbildung 16 Einsatz eines Messengerdienstes in gemeinsamer Verantwortung

Als Fazit kann auch hier wiederum festgehalten werden, dass in der Kommunikation mit dem Unternehmen auch Messengerdienste als Software-as-a-Service im Wege der Auftragsverarbeitung eingebunden werden können. Dabei gilt allerdings zu bedenken, dass für die Kommunikation zwischen Unternehmen nur Messengerdienste ausgewählt werden sollten, welche keine eigenen, über die Bereitstellung des Dienstes sowie die

Erfüllung eines AV-Vertrages hinausgehenden Verarbeitungszwecke verfolgen. Wann eine Auftragsverarbeitung ausgeschlossen ist und welche Aspekte bei der Auswahl eines geeigneten Dienstes zu beachten sind, wurde in Abschnitt 5.2.4.1.2 vorgestellt.

5.3.2.3 Messenger Marketing und die Problematik der Joint Controller

Die Besonderheit des Marketings via Messengerdienste dürfte in der Zielsetzung liegen, möglichst die beliebtesten Messenger zu adressieren, um den erreichbaren Kundenkreis zu optimieren. Insofern kann diese Zielsetzung im Konflikt mit der Auswahl eines datenschutzkonformen Messengerdienstes stehen. Ist dies der Fall, sind damit die weitreichsten, rechtlichen Implikationen für die Beschäftigten verbunden, die im Rahmen ihrer Aufgabenstellung Messengerdienste nutzen sollen, und dabei auch personenbezogene Daten preisgeben müssen.

Bei der Nutzung von Drittangeboten entstehen mehrere Datenverarbeitungsbeziehungen. Die Besonderheit liegt hier auch darin, dass Privatpersonen einen Messenger zu privaten Zwecken als auch zur Kommunikation mit Unternehmen nutzen. Eine Rechtsbeziehung besteht bereits zum Messenger, dieser verfolgt regelmäßig den eigenen Zweck der Bereitstellung eines Messengerdienstes gegenüber der Allgemeinheit sowie ggf. weiterer Zwecke, sodass fraglich erscheint, ob eine Auftragsverarbeitung in Betracht kommt. Nach der Ratio der Fanpage-Entscheidung des EuGH[1313] dürfte das per Messengerdienst mit Privatpersonen kommunizierende Unternehmen jedenfalls als Verantwortlich einzustufen sein. Im Hinblick auf die Rechtsgrundlagen müssen unterschiedliche Perspektiven und Rechtsbeziehungen unterschieden werden:

Privatperson – Messengerdienst: Die Verarbeitung von Daten der betroffenen Personen im Rahmen der gewöhnlichen Nutzung des Messengerdienstes erfolgt zur Erbringung des Messengerdienstes und damit gewöhnlich zu eigenen Zwecken unter den Vorgaben zu Verkehrsdaten (§ 9 TTDSG) oder der Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DSGVO) – je nachdem welches Regime einschlägig ist, ggf. zusätzlich über eine Einwilligung je nach Dienstgestaltung. Für die Wirksamkeit der Einwilligung ist relevant, ob die Freiwilligkeit einschränkende Konstellationen wie Monopolstellungen und Netzwerkeffekte und/oder eine Kopplung vorliegt. Zudem sollten differenzierte Einwilligungsmöglichkeiten bereitgestellt sein.

Unternehmen – Privatperson: Das Unternehmen steht zumindest in der (Mit-)Verantwortung für zwei wesentliche Phasen der Datenverarbeitung: die Nutzung des Messengerdienstes als Kommunikationskanal und der Datenverarbeitung im Unternehmen selbst. Für Letzteres kommt es auf den Kommunikationszweck an: Vertragserfüllung, vorvertragliche Maßnahmen, Einwilligung in Kontaktaufnahme, rechtliche Verpflichtung oder berechtigte Interessen kommen grundsätzlich in Betracht – hier gilt nichts anderes, als bei anderen Kommunikationsmitteln. Für die Phase der Kommunikation stellen sich folgende Fragen: Kommt es zur Anwendung des TTDSG? Liegt bei der Nutzung eines Messengerdienstes eine Mitwirkung des Unternehmens vor? Als Praxistipp wird empfohlen vorab eine Einwilligung im Hinblick auf die Wahl des Kommunikationskanals einzuholen.[1314] Diese kann insbesondere dann erforderlich sein, wenn es zu Datentransfers in ein unsicheres Drittland kommt und andere rechtliche Instrumente sowie technische Schutzmaßnahmen nicht greifen. Dabei sollte stets bedacht werden, dass das Unternehmen unterschiedliche Möglichkeiten zur Kontaktaufnahme bereitstellen sollte, um sicherzugehen, dass es auch einer bewussten und selbstbestimmten Entscheidung der betroffenen Person beruht, einen bestimmten Messenger zu nutzen.

[1313] EuGH, Urteil vom 05-06-2018 – C-210/16 – Wirtschaftsakademie.
[1314] *Ulbricht,* in: *Mehner*, Messenger Marketing, S. 72 ff.

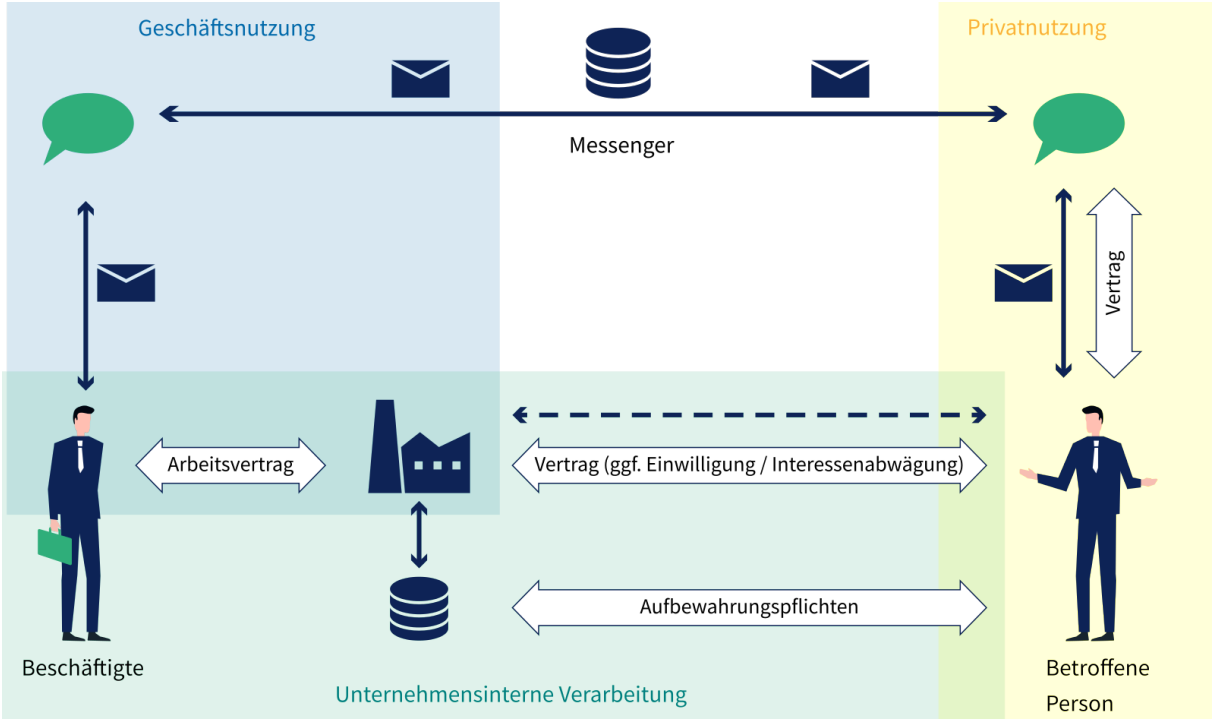


Abbildung 17 Rechtsbeziehungen beim Messenger Marketing

Unternehmen – Beschäftigte: Im Hinblick auf den Einsatz der Beschäftigten zur Betreuung von Messengerdiensten, welche über kein angemessenes Datenschutzniveau verfügen bzw. hohe Datenschutzrisiken in sich bergen, kann auf die Erwägungen zu Schutzmaßnahmen im Hinblick auf Drittstaatentransfers zurückgegriffen werden (siehe Abschnitt 4.2.1.1). Das Unternehmen sollte eigene Schutzmaßnahmen ergreifen, um die personenbezogenen Daten der Beschäftigten sowie sonstiger vertraulicher Daten auf den Endgeräten vor dem Messengerdienst abzuschirmen.

Gemeinsame Verantwortlichkeit oder Auftragsverarbeitung: Grundsätzlich können zwei Datenverarbeitungscluster differenziert werden: die Kommunikation mittels Messengerdienst und die anschließende Datenverarbeitung im Unternehmen. Für letztere zeichnet sich der Messengerdienst nicht verantwortlich, diese liegt allein im Unternehmensbereich. Ausschließlich für den Kommunikationsprozess stellt sich die Frage des Verhältnisses zwischen Messengerdienst und Unternehmen. Einerseits könnte der Messengerdienst als Verantwortlicher gelten anderseits in einer Doppelrolle auftreten: Verantwortlicher für die gewöhnliche Messengerkommunikation zwischen Privatpersonen (Abbildung 17 – gelber Bereich) und Auftragsverarbeiter bei der Kommunikation mit dem Unternehmen (Abbildung 17 – blauer Bereich). Dann müsste der Messengerdienst zumindest in dieser Beziehung den Weisungen des Unternehmens als Auftraggeber unterliegen. Messengerdienste, die sich hingegen weite Spielräume bei der Umsetzung ihres Kommunikationsangebots einräumen, dürften auch insofern in der Rolle des Verantwortlichen verbleiben.

Beschäftigte – Messengerdienst: Kommt man zum Ergebnis, dass der Messengerdienst im Hinblick auf die für das Unternehmen geführte Kommunikation kein Auftragsverarbeiter des Unternehmens, sondern selbst Verantwortlicher ist, benötigt dieser auch in Beziehung zur Verarbeitung der Daten der im Unternehmen Beschäftigten einer Rechtsgrundlage (Abbildung 18). Insofern könnten auch hier die Verarbeitung von Verkehrsdaten (§ 9 TTDSG) oder der Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DSGVO) eingreifen.

Aufklärung über gemeinsame Verantwortung: Zunächst einmal muss zwischen dem Unternehmen und dem Messengerdienstanbieter eine Vereinbarung abgeschlossen werden, in der festgelegt wird, wer welche Rechte erfüllt. Die wesentlichen Inhalte der Vereinbarung müssen den betroffenen Personen zur Verfügung gestellt werden. Diese müssen wissen, wer in welcher Rolle welche Daten verarbeitet.[1315] Dabei sollen die folgenden drei Punkte hervorgehoben werden:

- Wird ausreichend klar, zu welchen Zwecken Daten vom Messengerdienst einerseits und vom Unternehmen andererseits verarbeitet werden sollen?
- Wird die Rechtsgrundlage korrekt und hinreichend klar angegeben? Insofern könnten die Rechtsgrundlagen im Hinblick auf eine private Messengerdienstnutzung gegenüber einer beruflich motivierten divergieren. Von daher kann es im Einzelfall nicht ausreichen, einfach auf die übliche Datenschutzerklärung des Messengerdienstes zu verweisen.
- Werden Daten in einem Drittland verarbeitet? Wird ausreichend darüber aufgeklärt, welche Folgen diese Datenverarbeitung in einem Drittland für die Rechte der betroffenen Person hat?

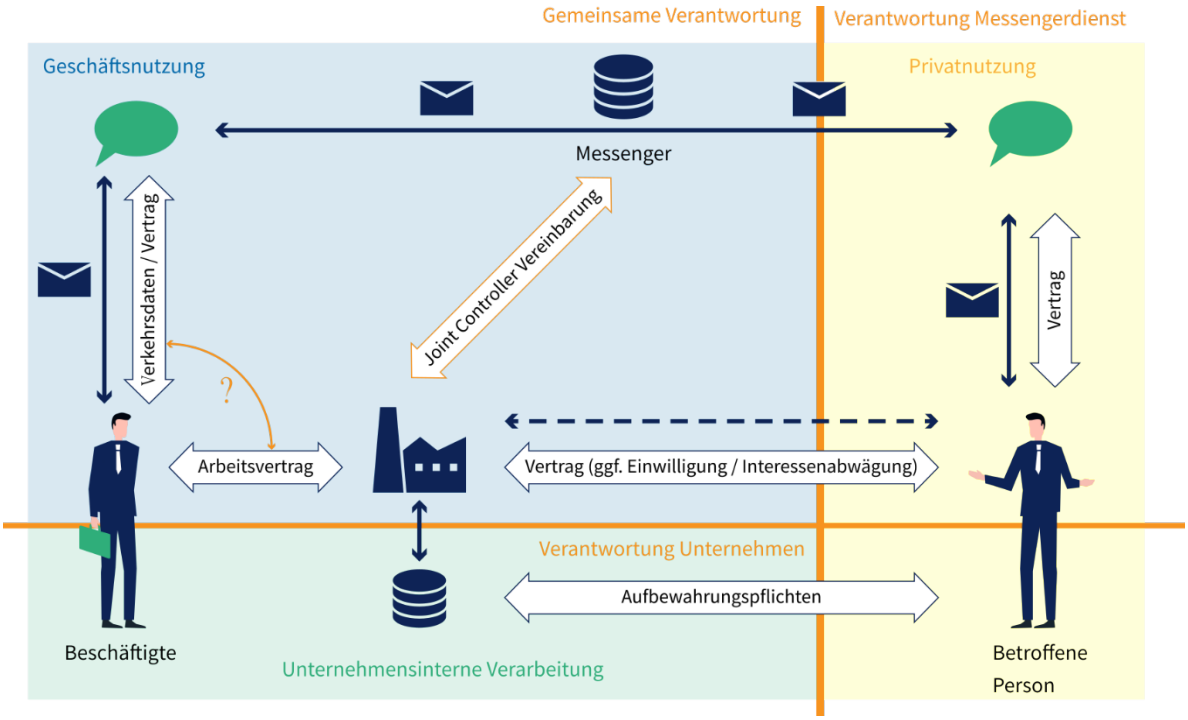


Abbildung 18 Unternehmen und Messengerdienst als gemeinsam Verantwortliche (Joint Controller)

5.3.3 Pflichten des Verantwortlichen

In diesem Abschnitt sollen ausschließlich Abweichungen bezüglich der dargestellten Pflichten in Abschnitt 5.2.3 hervorgehoben werden. Insgesamt gelten die bereits dargestellten Anforderungen gleichermaßen. Zusätzlich wäre zu bedenken:

[1315] *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 9.

Einsatzszenarien:

- Sowohl im Hinblick auf die Rechtsgrundlage als auch die Risikobewertung können Unterschiede daraus resultieren, dass die *Zwecksetzung* eines Messengerdienstes bzw. einer Kommunikationslösung abweichen können, je nachdem ob eine rein interne oder (auch) externe Kommunikation intendiert ist:
  - Sollen im Rahmen von Geschäftsbeziehungen Beschäftigte unterschiedlicher Unternehmen, Behörden oder sonstigen Institutionen miteinander kommunizieren gelten ähnliche Erwägungen, wie der innerbetrieblichen Kommunikation: Die Arbeitgeber haben jeweils im Verhältnis zu ihren Beschäftigten auf die Umsetzung eines angemessenen Datenschutzniveaus hinzuwirken. Insofern dürfte es regelmäßig schwer zu begründen sein, Dienste einzusetzen, die nicht dem Stand der Technik entsprechen, Drittstaatentransfers ohne Angemessenheitsbeschluss und/oder technische Schutzmaßnahmen vorsehen und/oder personenbezogene Daten zu kommunikationsfremden, eigenen Zwecken nutzen (bzw. sich eine solche Nutzung vorbehalten).
  - Für den Fall der Zielsetzung über die international verbreiteten Messengerdienste für Kundenanfragen erreichbar zu sein, könnte ein legitimes Interesse daran bestehen, Dienstangebote mit geringeren oder gar fehlenden Datenschutzgarantien zu verwenden. Hier muss allerdings das Unternehmen selbst kompensierende Schutzmaßnahmen – regelmäßig technischer Natur und ggf. unterstützt durch organisatorische und rechtliche Maßnahmen – ergreifen.

Risikobewertung:

- Im Hinblick auf die einzunehmenden Perspektiven gilt zu bedenken, dass sich die Schutzanforderungen sowohl auf die Persönlichkeitsrechte der Beschäftigten als auch die der Kommunikationskontakte erstreckt. Sowohl bei der Kommunikation mit Privatpersonen als auch mit Beschäftigten anderer Unternehmen, Behörden und sonstigen Stellen fallen personenbezogene Daten an.

Transparenz:

- Informationen zu Dokumentationserfordernissen und Datenaufzeichnungen, welche nicht bereits durch die Datenschutzerklärungen der Messengerdienste abgedeckt sind, müssen den betroffenen Personen gesondert bereitgestellt werden.
- Da sich Auskunftsersuchen der betroffenen Personen sowie die Rechenschaftspflicht des datenschutzrechtlich verantwortlichen Unternehmens auch auf die Kommunikation via Messenger bezieht, muss die Datenspeicherung so organisiert werden, dass Auskunft im Rahmen der gesetzlichen Fristen erteilt werden können und die Konversationen in das Verarbeitungsverzeichnis nach Art. 30 DSGVO aufgenommen werden.[1316] Dies kann herausfordernd sein, wenn Daten nur lokal bei den jeweiligen Beschäftigten gespeichert sind.

Mindestinhalte bei Geschäftsbriefen:

- Sofern keine Ausnahmen von den gesetzlichen Pflichtangaben greifen, müssen auf Geschäftsbriefen bestimmte Mindestangaben bspw. zur Rechtsform, Sitz der Gesellschaft, Registergericht, etc. nach § 35 Abs. 1 S.1 GmbHG bzw. § 80 Abs. 1 AktG sowie § 37a HGB oder § 125a HGB gemacht werden. Verstöße können mit Ordnungsgeldern geahndet werden.[1317]

[1316] vgl. *Bergt,* in: Koreng/Lachenmann - Formularhandbuch Datenschutzrecht, Kap. D. III. 2. Rn. 3.
[1317] Ausführlich: *Schrey u. a.*, MMR 2017, 656 (659).

Datenspeicherung und Datenzugriffe:

- Im Hinblick auf das Datenmanagementsystem gilt zu bedenken, dass § 147 AO auch Prüf- und Einsichtsrechte der Finanzbehörden vorsieht, weshalb eine strukturierte Ablage empfohlen wird.[1318] Die Umsetzung von Compliance-Anforderungen kann es erforderlich machen, die gesamte im Rahmen der Geschäftsbeziehung gewechselte Kommunikation nachvollziehbar zu dokumentieren und daher auch Chatverläufe zentral zu speichern und nicht nur auf den Endgeräten der Beschäftigten.[1319]
- Verfügt der Dienst über eine Ende-zu-Ende-Verschlüsselung, welche auch einen unternehmensseitigen Zugriff auf Chat-Verläufe vollständig ausschließt, liegt dies zwar im Interesse eines umfassenden Datenschutzes, steht aber im Widerspruch zur Umsetzung der Einsichts- und Prüfpflichten. Insofern sollte bei der technischen Gestaltung darauf geachtet werden, dass Unternehmen auch beim Einsatz sicherer Messengerdienste weiterhin Zugriffsmöglichkeiten auf Geschäftskommunikation der Beschäftigten haben können.
- Dabei sollte transparent dokumentiert sein, auf welche Kommunikationsinhalte und Metadaten Unternehmen Zugriffsmöglichkeiten haben. Dies hat wiederum erheblichen Einfluss auf die datenschutzrechtliche Risikobeurteilung im Hinblick auf den Schutz der Rechte und Freiheiten der Beschäftigten.

5.4 Sonderkonstellation: Verarbeitung besonderer Kategorien personenbezogener Daten mittels Messengerdiensten

Sollte es im Rahmen der internen oder externen Kommunikation im bzw. mit dem Unternehmen zur Verarbeitung besonderer Kategorien personenbezogener Daten kommen, kann als Hilfestellung die Orientierungshilfe der DSK zu den technischen Datenschutzanforderungen an Messengerdienste im Krankenhausbereich herangezogen werden, da die Gesundheitsdaten einen Unterfall der besonderen Kategorien bilden. Die DSK hat zur Messenger-Applikation, der Kommunikation, der Sicherheit der Endgeräte sowie zu Plattform/Betrieb konkrete Anforderungen definiert, die sich als Muss-Anforderung entweder zwingend aus Datenschutzvorschriften in Verbindung mit der besonderen Schutzbedürftigkeit dieser Datenkategorien ergeben oder als Soll-Vorgabe mittels unterschiedlich ausgeprägter Handlungsalternativen realisierbar sind.[1320] Bei diesen Anforderungen gilt allerdings zu bedenken, dass im Arzt-Patienten-Verhältnis neben den Datenschutzpflichten noch weitere Pflichten als Berufsgeheimnisträger (§ 203 StGB) sowie ärztliche Berufsregeln (vgl. §§ 7 ff. MBO-Ä, Krankenhausgesetze) treten.

Diese anspruchsvollen Anforderungen der DSK sind dem hohen Schutzbedürfnis besonderer Kategorien personenbezogener Daten insbesondere im Patienten-Arzt-Verhältnis im Krankenhauskontext geschuldet. Es handelt sich somit nicht um einen Minimalstandard für eine gewöhnliche App-Nutzung im Betrieb. Ähnliche Schutzbedürftigkeit könnten aber in Konstellationen, wie der Kommunikation mit Betriebsärzt*innen, auftreten. Andererseits verfügen Messengerdienstangebote, die viele oder gar alle dieser Kriterien erfüllen, über ein sehr hohes Schutzniveau, was im Rahmen der Erforderlichkeitsprüfung einer Datenverarbeitung sowie der Berücksichtigung technischer Schutzmaßnahmen positiv ins Gewicht fällt. Sind entsprechende Angebote zu zumutbaren Kosten wirtschaftlich wie technische realisierbar, kann die Entscheidung für ein weniger Schutz bietendes System datenschutzwidrig ausfallen – jedenfalls wäre es gut zu begründen.

[1318] *Schrey u. a.*, MMR 2017, 656 (659).
[1319] *Schrey u. a.*, MMR 2017, 656 (660).
[1320] *DSK - Datenschutzkonferenz*, Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, S. 3 ff.

5.5 Fazit zu Chancen und Risiken des Einsatzes von Messengern im Unternehmenskontext

In der Praxis dürften sich für Unternehmen auf der Suche nach einer Business-Lösungen regelmäßig zwei Optionen bieten: Software-Lizenzen für einen On-Premise-Betrieb erwerben (ggf. mit Support-/Wartungsvertrag) oder einen Vertrag zur Auftragsverarbeitung (AVV) abschließen. Nach einer groben Durchsicht bieten die meisten Lösungen dies an. Allerdings gilt zu bedenken: wenn ein Messengerdienstbetreiber einen AVV anbietet, welcher die Verarbeitung personenbezogener Daten aus dem Nutzungsverhältnis zu *eigenen Zwecken* vorsieht, liegt keine Auftragsverarbeitung, sondern eine gemeinsame Verantwortung vor. Der Datenschutzverstoß besteht hier dann bereits darin, dass eine Vereinbarung über die gemeinsame Verantwortung nach Art. 26 DSGVO fehlt.

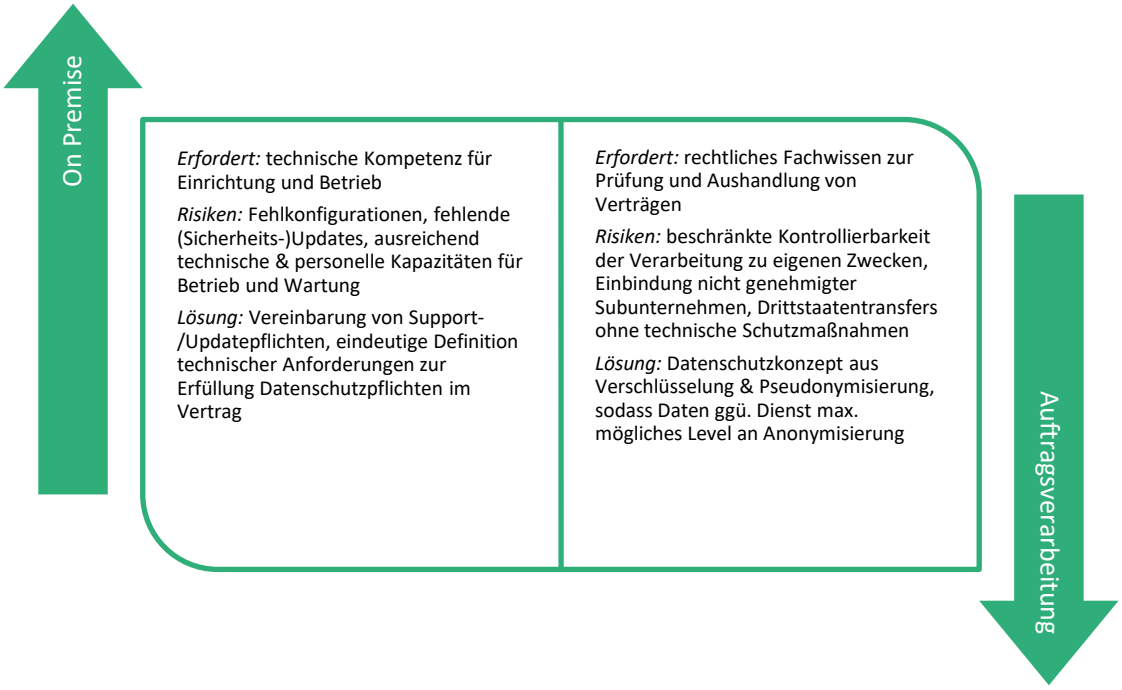


Abbildung 19 Typische Risiken und potentielle Lösungen je nach Betriebsform

Hervorzuheben ist, dass gerade viele „Big Player“ auch für Business-Lösungen im Hinblick auf die Rechtskonformität ihrer AVV bei deutschen Aufsichtsbehörden in der Kritik stehen,[1321] und der Verantwortliche zunächst primärer Adressat für Schadensersatz- oder Bußgeldforderungen ist. Können Messengerlösungen gerade aus dem US-amerikanischen Raum einen nach EU-Recht als unzulässig zu bewertenden Zugriff amerikanischer Behörden nicht (technisch) ausschließen (oder behalten sie sich die Erfüllung der US-amerikanischen Mitwirkungspflichten ggü. Behörden im AVV vor), so können diese Lösungen nicht als Software-as-a-Service, sondern allenfalls als On-Premise-Lösung eingesetzt werden. Wird ein zusätzlicher Wartungsvertrag geschlossen, bei dem die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, muss allerdings

[1321] *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten.

ebenfalls ein AV-Vertrag vereinbart werden.[1322] Die Risiken im Hinblick auf EU-rechtsverletzende Datenherausgabepflichten an Institutionen aus Drittländern ohne angemessenes Datenschutzniveau fallen allerdings geringer aus, wenn die betroffenen Daten nicht standardmäßig in den Herrschaftsbereich des Auftragsverarbeiters fallen.

In Tabelle 15 wird in verkürzter Form ein Überblick über unterschiedliche Rechtsaspekte zum Datenschutz je nach Betriebsform und damit verbundenem Verantwortungsmodell zusammengestellt.

	On-Premise-Betrieb in alleiniger Verantwortung	Messengerdienst als Auftragsverarbeiter	Messengerdienst als gemeinsam Verantwortlicher
Anwendbares Recht	Sitzlandprinzip bei Unternehmenssitz in EU	Sitzland- und/oder Marktortprinzip: auch bei Sitz außerhalb EU ist DSGVO / BDSG / TTDSG bei Angebot ggü. Personen in EU / BRD anwendbar	
Bestimmung der Verantwortlichkeit	Alleinige Verantwortung	Abgrenzung zur gemeinsamen Verantwortung, Verfolgung keiner eigenen Zwecke	Abgrenzung zur Auftragsverarbeitung, Verfolgung eigener Zwecke
Bestimmung der Rechtsgrundlage: Welche Rechtsgrundlagen kommen in Frage und sollten geprüft werden?	Innerbetrieblich: — § 26 Abs. 1 BDSG bei Anordnung (Erforderlichkeit) — Einwilligung bei freiwilliger Nutzung — Betriebsvereinbarung mit Betriebsrat — Fraglich: TTDSG einschlägig bzgl. privater Kommunikation?		Innerbetrieblich: Problematisch, wenn Messenger eigene Zwecke verfolgt
	Extern: — Vertrag/Vertragsanbahnung — Einwilligung — Aufbewahrungspflichten (rechtliche Pflichten) — Fraglich: Einhaltung TTDSG bzgl. Kommunikationsvorgang / privater Kommunikation?		Extern: — Fraglich: TTDSG — Vertrag (mit betroffener Person) — Einwilligung
Transparenz: Informationspflichten	Datenschutzerklärung durch Unternehmen	Unterstützung durch Messenger; bieten oftmals eigene Erklärungen	Vereinbarung über Pflichtenerfüllung, Information über Vereinbarung an Betroffene
Zweckbindung: Festlegung von Zwecken und Bindung an diese	Zwecke werden durch das Unternehmen festgelegt und umgesetzt, Zweckänderung nach Kompatibilitätstest grundsätzlich möglich	Keine Verfolgung eigener Zwecke erlaubt	Zwecke des Messengers sollten nicht im Widerspruch mit Zielen / Pflichten des Unternehmens stehen, Zweckänderung nach Kompatibilitätstest

[1322] Vgl. *DSK - Datenschutzkonferenz*, Orientierungshilfe Videokonferenzsysteme, S. 17.

TOMs: Datenminimierung (Privacy by Design / Default), Datensicherheit	Auswahl geeigneter Softwarelösung, Risikobewertung, Umsetzung geeigneter Schutzmaßnahmen	Auswahlverschulden, wenn Messenger keine geeigneten Garantien bietet, Unterstützung durch Messenger bei Umsetzung	Vereinbarung über Pflichtenerfüllung, keine pauschale Übernahme durch eine Seite
Umsetzung Betroffenenrechte im Hinblick auf Transparenz, Richtigkeit, Speicherbegrenzung, Datenübertragbarkeit	Umsetzung durch Unternehmen, Software sollte Pflichtenerfüllung ermöglichen (insbes. Speicher-/Löschkonzept, Berichtigungsoptionen, Auskunft (mit Kopie der Daten))	Umsetzung durch Unternehmen erfordert i.d.R. Mitwirkung durch Auftragsverarbeiter (insbes. bei Löschung, Datenherausgabe für Auskunft, Berichtigungsoptionen)	Vereinbarung über Pflichtenerfüllung muss Aufgaben klar verteilen; Unternehmen trotzdem Adressat ggü. Rechtewahrnehmung durch betroffene Person
Rechenschaftspflicht	Dokumentation & Kontrolle „inhouse“	Unternehmen muss erforderliche Nachweise von Auftragsverarbeiter anfordern	Unternehmen muss in der Lage sein, die Einhaltung der Datenschutzpflichten durch Messenger bewerten zu können, ggf. Nachweise anfordern
Drittstaatentransfers	Unproblematisch bei innerhalb EU/EWR gehosteten Servern; ggf. im Rahmen internationaler Konzernstrukturen relevant	Anbieter (inkl. Subunternehmer) sollten innerhalb EU/EWR/Land mit Angemessenheitsbeschluss operieren; ansonsten zusätzlich zu rechtlichen Instrumenten wie SCC technische Maßnahmen, die illegale Datenzugriffe ausschließen (+ ggf. organisatorische & vertragliche Maßnahmen)	Verantwortliche sollten innerhalb EU/EWR/Land mit Angemessenheitsbeschluss operieren; ansonsten zusätzlich zu rechtlichen Instrumenten wie SCC technische Maßnahmen, die illegale Datenzugriffe ausschließen (+ ggf. organisatorische & vertragliche Maßnahmen)
Bei Verarbeitung **besonderer Kategorien** personenbezogener Daten	Umsetzung eines hohen Schutzniveaus	Umsetzung eines hohen Schutzniveaus, erhöhte Geheimhaltungspflichten	Problematisch, wenn Messenger eigene Zwecke verfolgt, die mit Schutzniveau inkompatibel
Haftung: Schadensersatz und Sanktionen (Bußgelder)	Alleinige Haftung (ggf. Mängel-gewährleistungsansprüche ggü. Software-Anbieter)	Gesamtschuldnerische Haftung, Haftung für Verstöße des Auftragsverarbeiters nach außen nicht ausschließbar	Gesamtschuldnerische Haftung, Haftung für Verstöße des (Mit-) Verantwortlichen nach außen nicht ausschließbar

Tabelle 15 Vergleich der Betriebsformen und Verantwortungsmodelle

– Abschnitt C: Geschäftsgeheimnisse

6 Der Schutz von Geschäftsgeheimnissen bei Unternehmenskommunikation und -kollaboration

Im Hinblick auf die Auswahl und technische Umsetzung eines Kommunikations- und/oder Kollaborationswerkzeugs wie bspw. eines Messengerdienstes dürfte für viele Unternehmen nicht nur der Datenschutz einen maßgeblichen Faktor darstellen. Im ureigenen Interesse liegt zumeist auch der Know-How-Schutz. Zum Teil kann dieser aber auch in der Kommunikation mit anderen Unternehmen eine limitierende Größe darstellen, wenn Kommunikationskontakte die Wahl des Kommunikationskanals von einem angemessenen Schutzniveau abhängig machen. Denn praktisch jedes Unternehmen verfügt über nicht allgemein zugängliches Unternehmens-Know-How, von dessen Vertraulichkeit zum Teil auch der wirtschaftliche Erfolg abhängen kann, sodass der rechtliche Schutz von Geschäftsgeheimnissen ein zentrales Element des Unternehmensschutzes darstellen kann.[1323] Über die Auswertung von Kommunikations- und Metadaten könnten Rückschlüsse bspw. auf Produktionsprozesse, Lieferketten oder Kundenkontakte im Betrieb gezogen werden. Somit könnten Betriebs- und Geschäftsgeheimnisse hergeleitet werden und damit unternehmensbezogenes Wissen abfließen. Daher soll im Folgenden die aktuelle Rechtslage zum Schutz von Geschäftsgeheimnissen aufbereitet und dabei Parallelen zum Datenschutzrecht aufgezeigt werden.

6.1 Reform des Know-How-Schutzes in der EU

Bisher war der Schutz von Betriebs- und Geschäftsgeheimnissen in den §§ 17, 18 UWG dergestalt geregelt, dass Ansprüche auf Unterlassung und Schadensersatz nur dann bestanden, wenn auf ein Unternehmen bezogene Tatsachen, Umstände oder Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat, unbefugt offengelegt werden.[1324] Eine Neuregelung machte die Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung notwendig. Diese Richtlinie enthält sowohl mindest- als auch vollharmonisierende Regelungsaufträge an die mitgliedstaatlichen Gesetzgeber sowohl auf materiell-rechtlicher Ebene als auch im Hinblick auf verfahrensrechtliche Vorschriften.[1325] Das Begriffspaar „Betriebs- und Geschäftsgeheimnis“ wurde nun durch den Terminus „Geschäftsgeheimnis“ ersetzt, welcher grundsätzlich sowohl kaufmännisches als auch technisches Wissen sowie den in der Richtlinie verwendeten Begriff des Know-Hows erfasst.[1326]

[1323] *Alexander*, AfP 2019, 1 (1).
[1324] vgl. BVerfG, Beschluss vom 14.03.2006 – 1 BvR 2087/03, 1 BvR 2111/03 –, BVerfGE 115, 205-259; *Maaßen*, GRUR 2019, 352 (352); *Kalbfus*, GRUR-Prax 2017, 391 (391).
[1325] *Alexander*, AfP 2019, 1 (1).
[1326] BT-Drs. 19/4724, S. 24; *Hiéramente,* in: BeckOK GeschGehG, § 2 Rn. 1.

6.2 Qualifikation von Informationen als Geschäftsgeheimnis

Möchten nach der künftigen Rechtslage Beteiligte in den Genuss des rechtlichen Schutzes von Daten als Geschäftsgeheimnisse kommen, müssen sie die neue Definition des Geschäftsgeheimnisses bedenken.

6.2.1 Definition auf EU-Ebene

Art. 2 Nr. 1 (a)-(c) der Richtlinie (EU) 2016/943 definieren Geschäftsgeheimnisse als Information, die

- geheim (nicht allgemein bekannt oder nicht ohne weiteres zugänglich),
- von kommerziellem Wert, weil sie geheim ist, und
- Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen ist.
- Folglich wird – anders als die bisherige Rechtslage in Deutschland – ein Geheimhaltungsinteresse nicht bereits vermutet, sondern es müssen aktiv „angemessene" Geheimhaltungsmaßnahmen ergriffen werden.[1327] Eine homogene Definition des Geschäftsgeheimnisses soll alle Informationen erfassen, „bei denen sowohl ein legitimes Interesse an ihrer Geheimhaltung besteht als auch die legitime Erwartung, dass diese Vertraulichkeit gewahrt wird" (Erwägungsgrund 14 RL (EU) 2016/943). Wird der Zugriff auf die Daten nicht durch technische Mittel oder organisatorische Maßnahmen derart erschwert, dass ein Datenzugriff unverhältnismäßigen Aufwand erfordern würde, dürfte aber auch kein rechtlicher Schutz bestehen.[1328] Nicht ausreichen werden bloß vertragliche Vereinbarungen zur pauschalen Geheimhaltung.[1329] Um zu verhindern, dass Wettbewerber Kenntnis unternehmensbezogener Daten erhalten, könnten sich gegebenenfalls bekannte Mechanismen aus dem Datenschutzrecht anbieten, wie beispielsweise Datentrennung, Zugriffskontrolle und Anonymisierung (im Sinne einer Entfernung des Unternehmensbezugs).

6.2.2 Definition im GeschGehG

Die Trade-Secrets-Richtlinie war zunächst in deutsches Recht umzusetzen. Nach § 2 Nr. 1 GeschGehG ist ein Geschäftsgeheimnis im Sinne dieses Gesetzes:

> eine Information
>
> a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist

[1327] Zur Notwendigkeit *aktiven* Handelns: LAG Düsseldorf, Urteil vom 03.06.2020 – 12 SaGa 4/20, Rn. 80; *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 Rn. 49; *Fuhlrott,* in: BeckOK GeschGehG, § 21.
[1328] Vgl. *Maaßen*, GRUR 2019, 352 (353); *Kalbfus*, GRUR-Prax 2017, 391 (392); *Fuhlrott,* in: BeckOK GeschGehG, § 2 Rn. 20 ff.: keine Verpflichtung zu „Perfektem Geheimnisschutz". Aber eigene Obliegenheit des Geheimnisinhabenden Schutzvorkehrungen zu treffen; vgl. auch: *Dann/Markgraf*, NJW 2019, 1774 (1775).
[1329] LAG Düsseldorf, Urteil vom 03.06.2020 – 12 SaGa 4/20, Rn. 79 ff.

und daher von wirtschaftlichem Wert ist und

b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht;

Die Anforderungen müssen kumulativ vorliegen, um als Geschäftsgeheimnis qualifiziert werden zu können, und so in den Anwendungsbereich dieses Gesetzes zu gelangen.[1330] Die Begrifflichkeiten „Daten“, „Information“ und „Wissen“ werden in diesem Zusammenhang synonym verwendet.[1331] Auf der inhaltlichen Ebene gibt es grundsätzlich keine Einschränkung: so können Tatsachen, Geschehnisse, Zustände, subjektive Wertungen und Meinungen, Kommunikationsakte, die Nichtexistenz einer Begebenheit sowie maschinengenerierte Daten unter die geschützten Informationen fallen.[1332] Dies gilt auch unabhängig von der Struktur, Beschaffenheit, Verkörperung, Darstellung, Verständlichkeit oder der Tatsache, ob es sich um ein einzelnes Datum, Datensätze, Datenpools oder Datenbanken handelt.[1333] Insofern bestehen grundsätzlich weder qualitative noch quantitative Anforderungen. [1334] Auch wenn der Schutzzweck in der Förderung der Innovation im Wettbewerb verortet wird, muss die Information keine innovative Note (wie bspw. Individualität, Neuheit, Eigenart, Eigentümlichkeit, Kreativität, Originalität, Schöpfungshöhe oder ähnliches) aufweisen.[1335]

6.2.2.1 Geheimhaltung

Wesentlich für die Frage der Geheimhaltung ist die praktische Zugänglichkeit einer Information für einen bestimmten Personenkreis.[1336] Bei Datensätzen können zwar die einzelnen Daten öffentlich verfügbar sein, aber gleichzeitig in ihrer konkreten Anordnung und Zusammensetzung nicht bekannt und damit geheim sein.[1337]

Eine im Beschäftigtenkontext aus rechtsvergleichender Sicht interessante Entscheidung fällte der Österreichische Oberste Gerichtshof.[1338] Dieser hatte einen Fall zu entscheiden, bei dem ein Mitarbeiter im Rahmen seiner Funktion freien Zugang zu allen Laufwerken und damit zu allen Daten der hauseigenen EDV-Plattform seines Arbeitgebers hatte und diese für die Gründung eines Konkurrenzunternehmens nutzte. Fraglich war, ob es sich um Geschäftsgeheimnisse nach der Definition entsprechend der Trade-Secrets-Richtlinie handelte. In seiner Entscheidung hat der ÖOGH klargestellt, dass eine Information u. a. nur dann ein Geschäftsgeheimnis ist, wenn sie nicht allgemein bekannt oder ohne Weiteres zugänglich ist.

[1330] *Hiéramente,* in: BeckOK GeschGehG, § 2 Rn. 1.
[1331] *Wagner*, Datenökonomie und Selbstdatenschutz, S. 59.
[1332] *Hiéramente,* in: BeckOK GeschGehG, § 2 Rn. 2; *Alexander*, AfP 2019, 1 (4).
[1333] *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 25.
[1334] *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 27; *Alexander*, AfP 2019, 1 (4).
[1335] *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 27.
[1336] *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 31; *Ohly*, GRUR 2019, 441 (443); *Alexander*, AfP 2019, 1 (4).
[1337] *Ohly*, GRUR 2019, 441 (443); *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 32; *Hiéramente,* in: BeckOK GeschGehG, § 2 Rn. 2.
[1338] ÖOGH, Entscheidung vom 26.01.2021 – 4Ob188/20f.

ÖOGH zum Geschäftsgeheimnis, Urteil vom 26.01.2021 – 4Ob188/20f

- „Eine Information ist nicht nur dann geheim (§ 26 b Abs. 1 S. 1 öUWG), wenn sie absolut neu ist; maßgeblich ist vielmehr die *praktische Zugänglichkeit* der Information für einen bestimmten Personenkreis."
- „Der maßgebliche Personenkreis ist nach einem objektiven und normativen Maßstab *informationsspezifisch* zu bestimmen. Bei Informationen technischer Art ist auf die durchschnittlichen Fachkreise abzustellen."
- „Ohne Weiteres zugänglich ist eine Information, […] die eine Person des maßgeblichen Verkehrskreises *ohne erheblichen Aufwand und Einsatz an Zeit, Mühe, Kosten und/oder Geschick* mit ansonsten lauteren Mitteln verschaffen kann."

Nur ein Teil der betroffenen Informationen wurde vom Gericht als geheim eingestuft, da insoweit nicht *alle Details* öffentlich zugänglich oder bekannt waren.[1339] Nach der bisherigen Rechtsprechung in Deutschland (vor Einführung des GeschGehG) wird der Geheimnischarakter im Allgemeinen nicht dadurch aufgehoben, dass Vorgänge in einem Produktionsbetrieb den dort beschäftigten Personen bekannt werden.[1340] Es kann wohl davon ausgegangen werden, dass an dieser Rechtsprechung auch im geltenden Recht festgehalten werden kann.[1341]

Auch durch die Möglichkeit, die Information mittels Reverse Engineerings zu ermitteln, verliert die Information grundsätzlich nicht bereits ihren Geheimnischarakter.[1342] Relevant ist hier, ob mit dem Reverse Engineering ein hoher Aufwand verbunden wäre.[1343]

6.2.2.2 Wirtschaftlicher Wert

Gerade aufgrund dieser „Nicht-Offenkundigkeit" muss die Information über einen wirtschaftlichen Wert verfügen.[1344] Ein wirtschaftlicher Wert einer Information ist dann gegeben, wenn sie aus Sicht eines objektiven und verständigen Betrachters über einen tatsächlichen oder künftigen Handelswert verfügt oder ihr Bekanntwerden für die Inhaber*in des Geschäftsgeheimnisses wirtschaftliche Nachteile bedeutet.[1345] Nach Erwägungsgrund 14 RL (EU) 2016/943 ist das Kriterium des wirtschaftlichen Werts weit zu verstehen. [1346] Ausgenommen sind lediglich „belanglose Informationen", denen unter wirtschaftlicher Betrachtung unter keinem Gesichtspunkt ein Wert zukommt. [1347] Ein potenzieller Wert kann hingegen dann nicht festgestellt werden,

[1339] ÖOGH, Entscheidung vom 26.01.2021 – 4Ob188/20f Rn. 41 ff.
[1340] BGH, Urteil vom 7. 11. 2002 - I ZR 64/00 – Präzisionsmessgeräte; BGH, Urteil vom 22.3.2018 – I ZR 118/16 Rn. 38 – Hohlfasermembranspinnanlage II.
[1341] *Ohly*, GRUR 2019, 441 (443); *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 34.
[1342] *Ohly*, GRUR 2019, 441 (443).
[1343] ÖOGH, Entscheidung vom 26.01.2021 – 4Ob188/20f, Rn. 33.
[1344] *Ohly*, GRUR 2019, 441 (443); *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 39; *Hauck*, WRP 2018, 1032 (1033); *Dann/Markgraf*, NJW 2019, 1774 (1775).
[1345] *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 40.
[1346] *Ohly*, GRUR 2019, 441 (443); *Alexander*, AfP 2019, 1 (4). So auch: ÖOGH, Entscheidung vom 26.01.2021 – 4Ob188/20f, Rn. 37.
[1347] BT-Drs. 19/4724, S. 24; *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 41.

wenn auch eine zukünftige wirtschaftliche Verwertung nach dem gewöhnlichen Verlauf der Dinge unwahrscheinlich ist oder von vornherein ausgeschlossen erscheint. [1348] Rein ideelle Werte sind ebenfalls nicht erfasst.[1349]

Bezüglich des kommerziellen Werts unterstreicht der ÖOGH für die Rechtslage in Österreich – welche aber auch auf einer umfassenden Analyse des Schrifttums in Deutschland zum GeschGehG beruht – dass der Schutz von Geschäftsgeheimnissen keine besonderen Auswirkungen auf den Wettbewerb voraussetzt, etwa im Sinne eines Spürbarkeitserfordernisses.[1350] Es sei nur danach zu fragen, ob die Kenntniserlangung bzw. Verwertung oder Offenlegung durch Mitbewerber oder Dritte kommerzielle Interessen des Inhabers beeinträchtigen würde.[1351]

Umstrittene Fälle sind:

- Informationen über ein rechtswidriges Verhalten[1352]
- Information über private Umstände mit Unternehmensbezug[1353]

6.2.2.3 Angemessene Geheimhaltungsmaßnahmen

Bezüglich der „angemessenen" Geheimhaltungsmaßnahmen gilt ein relativer Maßstab.[1354] Zunächst sind die Umstände des Einzelfalls zu berücksichtigen, wobei diese stets Veränderungen bzw. Anpassungen unterliegen können. [1355] Der Maßstab ist objektiv, die Angemessenheit ist nach den konkreten Kontexten im Sinne einer Verhältnismäßigkeitsprüfung zu würdigen, wobei folgende Aspekte berücksichtigt werden können: „Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten; Natur der Information, Bedeutung für das Unternehmen; Größe des Unternehmens; die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen, die Art der Kennzeichnung der Informationen, vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern."[1356]

Hervorzuheben ist, dass rechtlichen Schutz nur genießt, wer sein Geheimhaltungsinteresse nicht nur erklärt, sondern aktiv wird und darlegbare Bestrebungen zum Schutz der Information unternimmt.[1357] Den Schutzmaßnahmen kommt eine gewisse Doppelrolle zu: sie sind nicht nur deshalb zu ergreifen, um das Geheimnis vor unbefugten Zugriffen zu schützen, sondern müssen bereits deshalb eingerichtet werden, dass die Information überhaupt als Geschäftsgeheimnis angesehen wird und damit vom rechtlichen Schutz dieses Gesetzes profitieren kann.[1358] Zumeist werden folgende Geheimhaltungsmaßnahmen als Möglichkeiten genannt:[1359]

[1348] *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 43.
[1349] *Alexander,* in: Köhler/Bornkamm/Feddersen, UWG, § 2 GeschGehG Rn. 44.; vgl. BT-Drs. 19/4724, S. 24.
[1350] ÖOGH, Entscheidung vom 26.01.2021 – 4Ob188/20f, Rn. 38.
[1351] ÖOGH, Entscheidung vom 26.01.2021 – 4Ob188/20f, Rn. 39.
[1352] *Alexander*, AfP 2019, 1 (4 f.); *Hauck*, WRP 2018, 1032 (1033); *Dann/Markgraf*, NJW 2019, 1774 (1776).
[1353] *Alexander*, AfP 2019, 1 (5).
[1354] *Alexander*, AfP 2019, 1 (4); *Leister*, GRUR-Prax 2020, 579 (579); *Maaßen*, GRUR 2019, 352 (353 f.).
[1355] BT-Drs. 19/4724, S. 24; *Alexander*, AfP 2019, 1 (4).
[1356] LAG Düsseldorf, Urteil vom 03.06.2020 – 12 SaGa 4/20, Rn. 81; BT-Drs. 19/4724, S. 24.
[1357] LAG Düsseldorf, Urteil vom 03.06.2020 – 12 SaGa 4/20, Rn. 80; *Gola*, DuD 2019, 569 (570). Der Geheimnisinhaber ist im Streitfall beweisbelastet: BT-Drs. 19/4724, S. 24.
[1358] *Gola*, DuD 2019, 569 (570).
[1359] *Alexander*, AfP 2019, 1 (4); *Maaßen*, GRUR 2019, 352 (357 ff.).

- **Tatsächliche Zugangsbeschränkungen:**[1360]
  - Zugangssperren (Schließsysteme, Alarmanlagen, etc.)
  - räumliche Zugangssicherungen (bauliche und technische Maßnahmen)
  - Zugangskonzepte für interne Beschäftigte und Externe bzw. Besucher*innen
  - Reglementierung der Nutzung externer Speichermedien
- **Technische und organisatorische Schutzvorkehrungen**
  - IT-Sicherheitsmaßnahmen (CIA-Prinzipen), Sicherheitsüberprüfungen
  - Zugriffsbeschränkungen, Beschränkung des Zugangs zum Internet und Netzwerkschutz
  - Einsatz von Authentifizierungsverfahren, Passwortschutz und Verschlüsselungstechnik
  - Protokollierungen und Datensicherheit
  - Interne Richtlinien und Anweisungen (z.B. Wissensaufsplittung nach dem Need-to-Know-Prinzip, Schulungen und Sensibilisierungsmaßnahmen, etc.)[1361]
  - Benennung von Sicherheitsverantwortlichen
  - Verbot der Nutzung bestimmter Medien „(wie z. B. WhatsApp) zur betrieblichen Kommunikation“[1362]
- **Rechtliche Geheimhaltungsverpflichtungen:** Auch vertragliche Vereinbarungen können ein Mittel der Geheimhaltung sein.[1363] Diese dürfen allerdings nicht pauschal auf sämtliche Informationen bezogen werden, denen jeder Bezug zum Begriff des Geschäftsgeheimnisses fehlt.[1364]

Die Speicherung einer Information auf privaten Endgeräten der Beschäftigten nach dem BYOD-Prinzip könnte in Konflikt mit dem Erfordernis angemessener Geheimhaltungsmaßnahmen geraten.[1365] Nicht abschließend geklärt ist, inwieweit unbeabsichtigte Sicherheitslücken das Vorliegen von Geschäftsgeheimnissen künftig ausschließen werden.[1366]

6.2.2.4 Berechtigte Interessen an der Geheimhaltung

Anders als die Trade-Secret-Richtlinie enthält § 2 GeschGehG mit den berechtigten Interessen an der Geheimhaltung ein weiteres Merkmal. Diesem dürfte aber ohnehin keine große Bedeutung zukommen, da es stets erfüllt sein dürfte, wenn der Information ein Vermögenswert zukommt.[1367] Der Begriff soll auf diese Weise aus objektiven und subjektiven Kriterien bestimmt werden, denn trotz objektiv vorliegenden Schutzkriterien, kann der/die Inhaber*in jederzeit auf Schutzmaßnahmen verzichten.[1368]

Zur Bestimmung der Angemessenheit von Schutzmaßnahmen ist es auf Unternehmensseite ohnehin im Rahmen eines strukturierten Vorgehens erforderlich Schutzbedarfe und Schutzmaßnahmen zu analysieren:

[1360] Beispiele bei: *Fuhlrott,* in: BeckOK GeschGehG, § 2 R. 35; *Dann/Markgraf*, NJW 2019, 1774 (1776).
[1361] *Fuhlrott,* in: BeckOK GeschGehG, § 2 Rn. 37.
[1362] *Fuhlrott,* in: BeckOK GeschGehG, § 2 Rn. 37.
[1363] LAG Düsseldorf, Urteil vom 03.06.2020 – 12 SaGa 4/20, Rn. 80.
[1364] LAG Düsseldorf, Urteil vom 03.06.2020 – 12 SaGa 4/20, Rn. 80.
[1365] *Maaßen*, GRUR 2019, 352 (354).
[1366] *Maaßen*, GRUR 2019, 352 (355).
[1367] *Gola*, DuD 2019, 569 (569).
[1368] *Gola*, DuD 2019, 569 (569).

- Schritt 1: **Identifizierung** aller relevanten Informationen, die schützenswert sind[1369]
- Schritt 2: Unterteilung in „**Schutzstufen**“
  - Klassisch werden hier drei Stufen vorgeschlagen:[1370]
  - *(1) „Kronjuwelen“* (= existenzbedrohende Folgen für das Unternehmen bei Offenlegung),
  - *(2) strategisch wichtige Information* (= dauerhafter wirtschaftlicher Nachteil bei Offenlegung) und
  - *(3) sonstige schützenswerte, sensible Information* (= kurzfristiger wirtschaftlicher Nachteil bei Offenlegung)
- Schritt 3: Festlegung konkreter **Schutzmaßnahmen** für jede Schutzstufe[1371]
- Schritt 4: Periodische **Überprüfung** und ggf. Aktualisierung des Schutzkonzepts[1372]

Sowohl im Hinblick auf das Kosten-Nutzen-Verhältnis, die Möglichkeit differenzierte Geheimhaltungsmaßnahmen darlegen zu können und Gefahren einer „Verwässerung“ des Geheimnisschutzes sowie nachlassender Sorgfalt bei mangelnder Akzeptanz auf Seiten der Beschäftigten begegnen zu können, wird die Kategorisierung empfohlen, auch wenn eine eindeutige Abgrenzung oft schwierig ausfällt.[1373] Eine pauschale Klassifizierung von Unternehmens-Know-How als Geschäftsgeheimnis ist hingegen nicht geeignet, das den „Umständen entsprechende“ und „angemessene“ Geheimhaltungsniveau zu identifizieren, um konkrete Schutzmaßnahmen festzulegen.[1374] Bei der Einteilung in Schutzklassen und Auswahl entsprechender Schutzmaßnahmen sollten auch die möglichen Angriffswege untersucht und ein Zugriffsrisiko ermittelt werden.[1375]

[1369] Hierbei können bspw. entlang des Wertschöpfungsprozesses von Forschung und Entwicklung, über Konstruktion, Fertigung, Marketing, Vertrieb bis hin zu Kundenbetreuung Informationen sondiert und bewertet werden: *Kalbfus*, GRUR-Prax 2017, 391 (393).
[1370] *Fuhlrott,* in: BeckOK GeschGehG, § 2 Rn. 23; *Dann/Markgraf*, NJW 2019, 1774 (1776); *Maaßen*, GRUR 2019, 352 (356); *Kalbfus*, GRUR-Prax 2017, 391 (393).
[1371] *Fuhlrott,* in: BeckOK GeschGehG, § 2 Rn. 23.
[1372] *Leister*, GRUR-Prax 2020, 579 (579). Als dynamische Aufgabe wird es zumeist erforderlich sein, dem neuesten Stand der Technik zu entsprechen: *Dann/Markgraf*, NJW 2019, 1774 (1776).
[1373] *Maaßen*, GRUR 2019, 352 (356); ähnlich *Kalbfus*, GRUR-Prax 2017, 391 (393).
[1374] *Kalbfus*, GRUR-Prax 2017, 391 (393).
[1375] *Maaßen*, GRUR 2019, 352 (357).

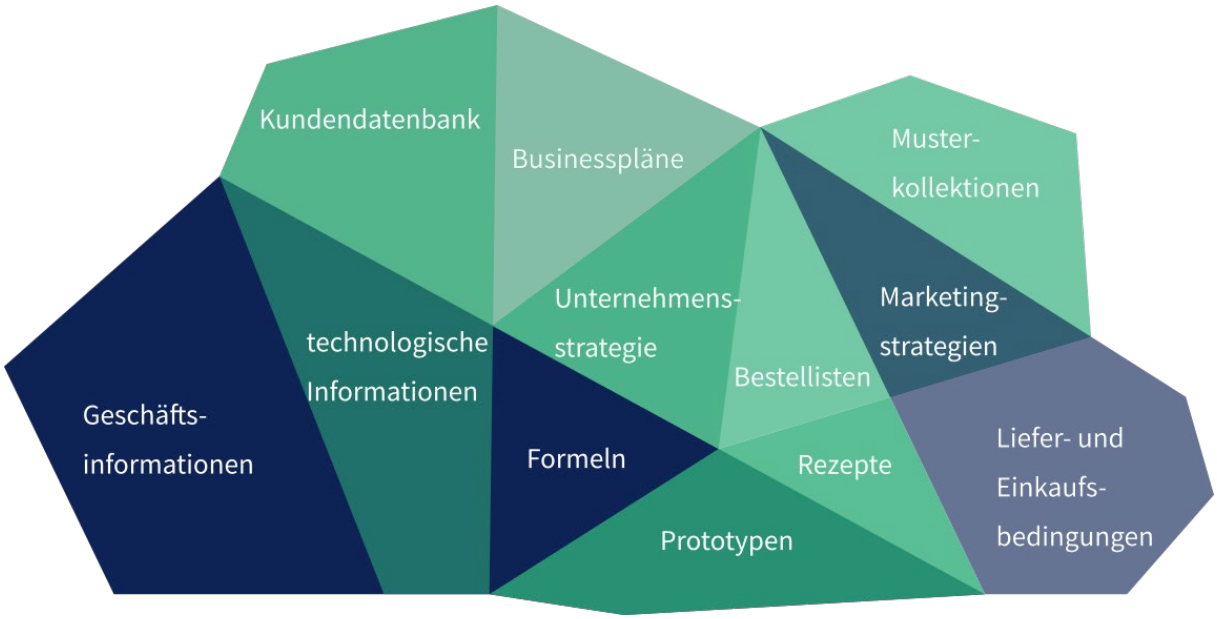


Abbildung 20 Beispiele für typische Geschäftsgeheimnisse

6.2.2.5 Zwischenergebnis: Vorliegen eines Geschäftsgeheimnisses

Bei der betrieblichen Kommunikation gilt stets zu bedenken, dass schützenswertes Unternehmens-Know-How tangiert sein könnte. Da der rechtliche Schutz des neuen GeschGehG auf solche Informationen beschränkt, die aktiv geschützt werden, kann dies zum Ausschluss bestimmter, unsicherer Kommunikationsformen und Messengerdienste führen. Auf der anderen Seite kann die Wahl besonders sicherer Kommunikationswege auch als Geheimhaltungsmaßnahme i.S.d. § 2 GeschGehG honoriert werden.

Praxistipp:

(1) Systematische Identifizierung der im Unternehmen vorhandenen Informationen, die geheim gehalten werden sollten
(2) Ordnung dieser Informationen in Geheimhaltungsstufen im Hinblick auf die Angemessenheit der Sicherungsmaßnahmen

6.3 Reichweite des rechtlichen Schutzes von Geschäftsgeheimnissen

Das GeschGehG regelt den Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung. geschützt wird der „Inhaber eines Geschäftsgeheimnisses“. Hierbei handelt es sich nach § 2 Nr. 2 GeschGehG um:

> jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis hat;

Diese Person ist abzugrenzen zum Rechtsverletzer i.S.d. § 2 Nr. 3 GeschGehG:

> jede natürliche oder juristische Person, die entgegen § 4 ein Geschäftsgeheimnis rechtswidrig erlangt, nutzt oder offenlegt; Rechtsverletzer ist nicht, wer sich auf eine Ausnahme nach § 5 berufen kann;

Die Handlungsverbote werden in § 4 GeschGehG gelistet. Dabei werden die Erlangung, Nutzung und Offenlegung gesondert adressiert:

- § 4 Abs. 1 GeschGehG: Unerlaubte **Erlangung** des Geschäftsgeheimnisses durch:
  - unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder
  - jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht
- § 4 Abs. 2 GeschGehG: Unerlaubte **Offenlegung** des Geschäftsgeheimnisses, wenn:
  - dieses unerlaubt erlangt wurde,
  - gegen eine Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt oder
  - gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen
- Die Erlangung, Nutzung und Offenlegung ist auch dann verboten, wenn das Geheimnis illegal über eine Dritte Person bezogen wird (§ 4 Abs. 3 GeschGehG).

6.3.1 Verhältnis zu den Rechten und Pflichten im Arbeitsverhältnis

§ 1 Abs. 3 Nr. 4 legt fest, dass durch die Regelungen im GeschGehG sowohl die „Rechte und Pflichten aus dem Arbeitsverhältnis“ als auch die „Rechte der Arbeitnehmervertretungen“ unberührt bleiben.[1376]

6.3.2 Erlaubte Handlungen und Ausnahmen

Das Gesetz unterscheidet in „erlaubte Handlungen“ und „Ausnahmen“. § 3 GeschGehG definiert die erlaubten Handlungen, wozu zählen:

- Eigenständige Entdeckung oder Schöpfung
- Erlaubtes Reverse Engineering
- Ausüben von Informations- und Anhörungsrechten der Arbeitnehmer oder Mitwirkungs- und Mitbestimmungsrechte der Arbeitnehmervertretung
- Gestattung durch Gesetz, aufgrund eines Gesetzes oder durch Rechtsgeschäft

[1376] *Fuhlrott,* in: BeckOK GeschGehG, § 1 Rn. 30.

Ausnahmen nach § 5 GeschGehG betreffen:

- Journalismus, Medien- und Meinungsfreiheit
- Whistleblower
- im Rahmen der Offenlegung durch Arbeitnehmer gegenüber der Arbeitnehmervertretung, wenn dies erforderlich ist, damit die Arbeitnehmervertretung ihre Aufgaben erfüllen kann.

6.4 Folgen für den Einsatz von Messengerdiensten im Unternehmenskontext

Mit der Änderung der Rechtslage zu „angemessenen Geheimhaltungsmaßnahmen“ als Schutzvoraussetzung eröffnen sich auch neue Haftungsfragen für im Unternehmen in verantwortlicher Position Beschäftigte.[1377] Zudem regelt das neue Gesetz ausdrücklich die Rechte der/des Inhaber*in von Geschäftsgeheimnissen gegenüber der/dem Rechtsverletzer*in.

6.4.1 Haftungsrisiken bei fehlenden Geheimhaltungsmaßnahmen

Fehlende Geheimhaltungsmaßnahmen können für die Geschäftsführung Haftungsrisiken bergen.[1378] Denn ohne den rechtlichen Schutz als Geschäftsgeheimnis können keine Unterlassungs- und Schadensersatzansprüche durch das Unternehmen nach dem GeschGehG gegenüber den Rechtsverletzenden geltend gemacht werden.[1379] Das Unternehmen könnte für so entstehende Schäden die verantwortlich Handelnden in Regress nehmen wollen (interne Haftung). Zwar dürften Fehlende Geheimhaltungsmaßnahmen der Information nicht bereits ihren wirtschaftlichen Wert rauben, sodass noch kein unmittelbarer Vermögensnachteil eintritt.[1380] Dieser entsteht erst, wenn der fehlende Schutz durch Dritte ausgenutzt wurde. So ist umstritten, ob bei dieser späteren Erlangung / Offenbarung eine Unmittelbarkeit zwischen Pflichtverletzung und Vermögensnachteil bestehen müsste.[1381] Es wird allerdings wohl im Rahmen der „Sorgfalt eines ordentlichen Kaufmanns“ verlangt werden können, nach der neuen Rechtslage erforderliche Sicherungsmaßnahmen entsprechend zu kennen und umzusetzen.[1382] Des Weiteren wird eine Haftungsmöglichkeit und § 130 OWiG diskutiert.[1383]

Schäden können aber auch „versteckter“ Natur sein: basiert der Wert eines Unternehmens stark auf seinem Know-How oder wurden bestimmte Geschäftsgeheimnisse als vorhanden definiert und unterliegt dieses keinem angemessenem Schutz, könnte dies den Unternehmenswert schmälern und bei Unternehmenstransaktionen Kaufpreisminderung, Garantiefall oder Rückabwicklung und Schadensersatzansprüche auslösen.[1384]

Zudem könnte ein Unternehmen sich gegenüber Dritten verpflichtet haben Drittgeheimnisse vertraulich zu behandeln. Die Nichteinhaltung der Anforderungen sowie auferlegter Schutzmaßnahmen könnte auch in dieser Konstellation zu Haftungsrisiken führen.

[1377] Ausführlich zu Haftungsrisiken: *Leister*, GRUR-Prax 2020, 579.
[1378] *Fuhlrott,* in: BeckOK GeschGehG, § 2 Rn. 21a; *Dann/Markgraf*, NJW 2019, 1774 (1775).
[1379] *Leister*, GRUR-Prax 2020, 579 (579).
[1380] *Fuhlrott,* in: BeckOK GeschGehG, § 2 Rn. 21a. *Dann/Markgraf*, NJW 2019, 1774 (1775) lehnen daher auch eine Untreuestrafbarkeit nach § 266 StGB ab.
[1381] *Dann/Markgraf*, NJW 2019, 1774 (1775).
[1382] *Leister*, GRUR-Prax 2020, 579 (580).
[1383] *Fuhlrott,* in: BeckOK GeschGehG, § 2 Rn. 21b; *Dann/Markgraf*, NJW 2019, 1774 (1775).
[1384] *Fuhlrott,* in: BeckOK GeschGehG, § 2 Rn. 21b; *Leister*, GRUR-Prax 2020, 579 (580).

6.4.2 Regressmöglichkeiten

Liegen hingegen angemessene Geheimhaltungsmaßnahmen sowie die übrigen Kriterien für die Annahme von Geschäftsgeheimnissen vor, gewährt das GeschGehG dem Inhaber des Geschäftsgeheimnisses unterschiedliche Rechtsinstrumente zur Durchsetzung seiner Interessen:

- § 6 GeschGehG: Beseitigung und Unterlassung (bei Wiederholungsgefahr bzw. erstmalig drohender Rechtsverletzung),
- § 7 GeschGehG: Vernichtung oder Herausgabe von Dokumenten u.ä., Rückruf bzw. Entfernung und Vernichtung rechtsverletzender Produkte oder Rücknahme vom Markt,
- § 8 GeschGehG: Auskunft über rechtsverletzende Produkte, Schadensersatz bei Verletzung dieser Auskunftspflicht,
- § 10 GeschGehG: Anspruch auf Schadensersatz (Gewinnabschöpfung, fiktive Lizenz oder tatsächlicher Schaden),
- § 12 GeschGehG: Ansprüche nach §§ 6-8 GeschGehG auch gegen Unternehmen, bei dem Rechtsverletzer beschäftigt ist (bzw. für das er/sie Beauftragte/r ist),
- § 13 geschGehG: Herausgabeanspruch nach Eintritt der Verjährung

Diese Ansprüche werden flankiert durch einen Anspruchsausschluss bei Unverhältnismäßigkeit (§ 9 GeschGehG), eine Abwendungsmöglichkeit durch Abfindung in Geld (§ 11 GeschGehG) sowie ein Missbrauchsverbot (§ 14 GeschGehG).

6.5 Parallelen zum Datenschutzrecht

6.5.1 Schutzgegenstand

Das Datenschutzrecht fokussiert auf den Schutz personenbezogener Daten. Der dabei verwendete Begriff der „Daten“ ist dabei grundsätzlich ebenso weit gefasst, wie die zum Geschäftsgeheimnisschutz gebräuchlichen Begrifflichkeiten der „Information“ oder des „Wissens“.[1385] Folglich kann es zu Überlappungen kommen: verfügen Geschäftsgeheimnisse gleichzeitig über einen Personenbezug, ist auch das Datenschutzrecht parallel anwendbar. Dagegen unterfallen personenbezogene Daten nur dann dem Geschäftsgeheimnisschutz, wenn diese entsprechend geheim gehalten, von wirtschaftlichem Wert und Gegenstand angemessener Geheimhaltungsmaßnahmen sind.

[1385] Zum Datenbegriff ausführlich: *Wagner*, Datenökonomie und Selbstdatenschutz, S. 35 ff.

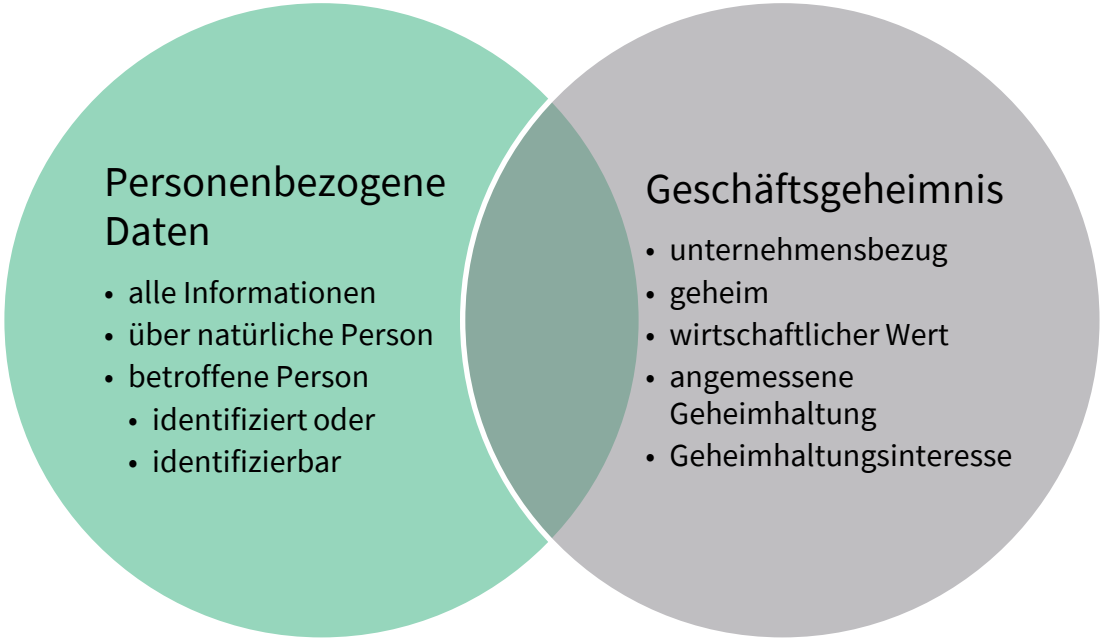


Abbildung 21 Überschneidungen und Unterschiede zwischen personenbezogenen Daten und Geschäftsgeheimnissen

6.5.2 Schutzziele

Das Geheimnisschutzrecht adressiert die Frage, wer über den Zugang zu den Informationen entscheiden darf, sodass es sich im Ergebnis um einen Zugangsschutz handele.[1386] Damit sollen keine Immaterialgüterrechte generiert werden.[1387] Im Prinzip fokussiert der Schutz auf das Datum bzw. die Daten und die darin verkörperten immateriellen Werte. Das Datenschutzrecht hingegen darf nicht auf den Schutz der Daten selbst beschränkt werden – sondern hat den Schutz des Menschen „hinter" den Daten im Fokus.[1388] Hierbei handelt es sich um eine Art Vorfeldschutz, da potentielle Schäden für die Persönlichkeitsentfaltung ab Preisgabe der Daten nicht mehr kontrollierbar sind.[1389] Bereits die Unkenntnis darüber, wer über welche Informationen über die eigene Person verfügt, kann die freie Entfaltung hemmen.[1390] Daher zielt das Danteschutzrecht nicht allein auf Geheimhaltung, sondern forciert auch die Transparenz der Datenverarbeitungsvorgänge.

[1386] *Hauck*, WRP 2018, 1032 (1033).
[1387] Vgl. BT-Drs. 19/4724, S. 26.
[1388] BT-Drs 7/1027, S. 14; *von Lewinski*, Die Matrix des Datenschutzes, S. 4; ähnlich *Sahl*, RDV 2015, 236 (239); *Grimm*, JZ 2013, 585 (585); *Schnabel*, ZUM 2008, 657 (657); a.A. wohl *Specht*, CR 2016, 288 (290).
[1389] BVerfGE 120, 274-350 – Online-Durchsuchung, Rn. 198; BVerfGE 120, 378-433 – automatisierte Kennzeichenerfassung, Rn. 64; BVerfGE 120, 351-377 – Rasterfahndung, Rn. 57; BVerfGE 118, 168-211 – Kontenabfrage, Rn. 87; BVerfGE 113, 29 – Beschlagnahme von Datenträgern, Rn. 82.
[1390] Wegweisend: BVerfGE 65, 1-71 – Volkszählungsurteil.

6.5.3 Schutzwirkung von Sicherungsmaßnahmen

Während aus Art. 24, 25, 32 sowie 35 DSGVO dem Risiko angemessene Handlungs*pflichten* (zum Schutz fremder Rechte) entspringen, handelt es sich bei § 2 Nr. 1 Buchst. b GeschGehG lediglich um eine Handlungs*obliegenheit* (zum Schutz eigener Rechte). Die Parallelität der zu erbringenden Nachweise zu technischen und organisatorischen Maßnahmen ist hingegen offensichtlich. [1391] Erst mit der Sicherstellung des faktischen (Zugangs-)Schutzes erhält der Inhaber ein zivilrechtliches Instrumentarium an die Hand, um weit effektiver als bisher den Geheimnisschutz auch zivilrechtlich durchsetzen zu können. [1392] In beiden Konstellationen lassen sich Schutzmaßnahmen auf den drei Stufen technisch / organisatorisch / rechtlich verorten:[1393]

Organisatorisch	– Zugangsbeschränkungen, Need-to-Know-Prinzip, – Dokumentation, – Training, Schulungen, – Audits
Technisch	– Verschlüsselung, – Anonymisierungsmaßnahmen (Entfernung des Unternehmensbezugs, Entfernung des Personenbezugs), – Datentrennung,
Rechtlich	– Geheimhaltungsvereinbarung, – Vereinbarung von Meldeobliegenheiten

Tabelle 16 Beispiele von Sicherungsmaßnahmen

Im Zusammenhang mit der Organisation der betrieblichen Kommunikation ergriffene Schutzmaßnahmen können folglich eine Doppelfunktion erfüllen: als geeignete TOMs im Rahmen der datenschutzrechtlichen Pflichten (insbesondere Art. 24, 25, 32 DSGVO) sowie als angemessene Geheimhaltungsmaßnahmen i.S.d. § 2 Nr. 1 Buchst. b GeschGehG. Im ersten Fall ist allerdings bei der der Schutzrichtung zu beachten, dass Risiken im Datenschutzrecht nicht nur durch Zugriffe von *außen* entstehen, sondern durchaus auch durch die Verarbeitung beim Verantwortlichen *selbst* (vgl. Abschnitt 2.4.4.2.1), während der Schutz der Geschäftsgeheimnisse eher die klassische IT-sicherheitstechnische Perspektive des Angreifers von außen unter Einbezug der Innentäter einnehmen dürfte. Dies bedeutet, dass auch wenn sich die Maßnahmen stark überschneiden, sollten stets die Perspektiven anhand der schutzbedürftigen Subjekte / Objekte eingenommen werden.

Während der Verantwortliche datenschutzrechtlich zum Nachweis der Einhaltung der Vorgaben der DSGVO verpflichtet ist (Rechenschaftspflicht), liegt es im eigenen Interesse des Geheimnisinhabers nachweisen zu können, angemessene Schutzmaßnahmen ergriffen zu haben. Denn wer sich auf Ansprüche aus der Verlet-

[1391] *Gola*, DuD 2019, 569 (570); vgl. auch zur Notwendigkeit der Ende-zu-Ende-Verschlüsselung aus zwei Perspektiven: *Schrey u. a.*, MMR 2017, 736 (737).
[1392] *Hauck*, WRP 2018, 1032 (1033).
[1393] Vgl. *Leister*, GRUR-Prax 2020, 579 (579); *Balaban/Wagner*, Minimizing the Risks of Data Protection Infringement - Data Lifecycle Risk Assessment, S. 359.

zung von Geschäftsgeheimnissen beruft, dem obliegt die Beweislast, dass die Schutzvoraussetzungen vorlagen.[1394] Insofern bietet sich auch hier eine lückenlose Dokumentation an.[1395]

	Datenschutz	Geschäftsgeheimnisse
Sensitivitäts- und Vertraulichkeitslevel	— besondere Kategorien personenbezogener Daten — gewöhnliche personenbezogene Daten — pseudonymisierte Daten — anonymisierte Daten	— "Kronjuwelen" — strategisch wichtige Informationen — sonstige schützenswerte Informationen
Risiken (Angreiferperspektive)	— Risiken durch Datenverarbeitung — Risiken durch unautorisierte Datenzugriffe — Dritte (Hacker) — Innentäter	— Risiken durch unautorisierte Datenzugriffe — Dritte (Hacker) — Innentäter
Organisation: Einzubeziehende Rollen	— Verantwortliche Leitungsebene — ggf. Durchführungsverantwortliche / IT-Verantwortliche — Datenschutzbeauftragte(r) — Betriebsrat	— Verantwortliche Leitungsebene — ggf. Durchführungsverantwortliche / IT-Verantwortliche — empfohlen: Person als „Geheimnisschutzbeauftragten“ zu ernennen[1396]

Tabelle 17 Vergleich zur Umsetzung von Schutzkonzepten zwischen Datenschutz und dem Schutz von Geschäftsgeheimnissen

6.5.4 Zusätzliche Auswirkungen von Schutzmaßnahmen als Zugangssicherung für den strafrechtlichen Schutz vor Hackerangriffen

Liegen Daten verschlüsselt gespeichert auf Servern und/oder Endgeräten und erhalten Dritte nichtsdestotrotz über eine Sicherheitslücke Zugriff auf diese vertraulichen Daten, kann das Unternehmen bzw. seine Beschäftigten als „Datenverfügungsberechtigte“ im strafrechtlichen Sinne Strafantrag nach §§ 202a, 205 StGB stellen.[1397] Das strafrechtliche Unrecht manifestiert sich hier in der Überwindung der Zugangssicherung.[1398] Werden die Daten hingegen auf dem Kommunikationsweg abgefangen oder sich über die elektromagnetische Abstrahlung einer Datenverarbeitungsanlage verschafft, kommt es für eine Strafbarkeit nach § 202a

[1394] *Maaßen*, GRUR 2019, 352 (360).
[1395] *Maaßen*, GRUR 2019, 352 (360).
[1396] *Maaßen*, GRUR 2019, 352 (359); *Kalbfus*, GRUR-Prax 2017, 391 (392). Allerdings handelt es sich auch um eine Querschnittsaufgabe sodass die fachabteilungsübergreifende Zusammenarbeit sicherzustellen ist.
[1397] Zur „Datenverfügungsberechtigung“: BGH, Beschluss vom 27.7.2017 – 1 StR 412/16 Rn. 32; BGH, Urteil vom 10. 05. 2005 – 3 StR 425/04 –, Rn. 12; Bayerisches Oberstes Landesgericht, Urteil vom 24. 06. 1993 – 5St RR 5/93 –, Rn. 24; OLG Naumburg, Urt. v. 27.8.2014 – 6 U 3/14.
[1398] BT-Drs. 16/3656, S. 10.

StGB hingegen nicht auf eine Verschlüsselung an.[1399] Der Versuch ist zwar nicht strafbar, allerdings erfasst § 202c STGB (auch „Hackerparagraph“ genannt) bestimmte Vorbereitungshandlungen.[1400] Eine Strafbarkeit kann sich zudem aus der Verletzung der Geschäftsgeheimnisse nach § 23 GeschGehG ergeben.

6.6 Fazit zum Schutz von Geschäftsgeheimnissen

In der Praxis besteht die Gefahr, dass gerade mit der Verschiebung der Arbeitsschwerpunkte ins Home-Office Beschäftigte auf andere, private Kommunikationswege zurückgreifen und dabei auch vertrauliche Daten übermitteln könnten.[1401] Arbeitgeber sind somit gut beraten, aktiv Kommunikationskanäle zu organisieren. Anders als beim Datenschutzrecht ist die Implementierung angemessener Geheimhaltungsmaßnahmen im Hinblick auf den Schutz von Geschäftsgeheimnissen keine gesetzliche Pflicht, sondern erfolgt im Interesse des Unternehmens. Werden bei der Auswahl und beim Einsatz einer Kommunikations- bzw. Kollaborationslösung wie bspw. Messengerdiensten der Schutz von Geschäftsgeheimnissen nicht bedacht, kann das Unternehmen allerdings einen Schaden erleiden, da in diesem Fall auch der rechtliche Schutz versagt bleibt. Können keine Rechtsansprüche gegenüber Rechtsverletzern geltend gemacht werden oder verliert das Unternehmen insgesamt an Wert, da der Bestand des als Geschäftsgeheimnis im rechtlichen Sinne zu qualifizierenden Know-Hows kleiner ausfällt als angegeben, können daraus Haftungsrisiken gegenüber den Entscheidungspersonen im Unternehmen erwachsen. Insofern sollten stets auch zur Wahrung von Geschäftsgeheimnissen ausschließlich Lösungen in die engere Auswahl genommen werden, welche über ausreichend technische und organisatorische Schutzmaßnahmen verfügen. Der Blickwinkel ist insofern der der klassischen IT: Schutz vor Angriffen „von außen“ sowie von Innentätern. Bei der konkreten Umsetzung von Maßnahmen als „angemessen“ muss ein relativer Maßstab eingenommen werden. Empfohlen wird hierbei die Definition von Schutzklassen. Diese können bspw. eingeteilt werden in Informationen, die den Wert des Unternehmens ausmachen („Kronjuwelen“), strategisch wichtige Informationen und sonstige schützenswerte Informationen.

Konkret umsetzbar im Rahmen der Nutzung von Messengerdiensten sind diese Geheimhaltungsinteressen u.a. durch eine sichere Verschlüsselung, die Definition von Nutzergruppen und geschlossener Nutzerkreise zur Umsetzung des Need-to-Know-Prinzips, Container-Lösungen zur Datentrennung sowie einem Datenmanagement im Hinblick auf Löschung und Archivierung.

[1399] BT-Drs. 16/3656, S. 11.
[1400] Zur Reichweite siehe: BVerfG, Nichtannahmebeschluss vom 18. 05. 2009 –2 BvR 2233/07, Rn. 59 ff.; BT-Drs. 16/3656, S. 19.
[1401] *Suwelack*, ZD 2020, 561 (563).

– Abschnitt D: Ergebnisse

7 Fazit zum Einsatz von Messengerdiensten im Unternehmenskontext mit normalem Schutzbedarf (Checkliste)

Der Einsatz von digitalen Lösungen ist stets mit Risiken und Chancen verbunden. Gerade in Zeiten des Home-Office wird geraten, gänzlich auf die Verwendung von Papier zu verzichten, um Datenschutzrisiken im Hinblick auf sichere Aufbewahrung und Vernichtung zu minimieren.[1402] Die Tendenz geht somit zu digitalen Kommunikationslösungen.

Plant ein Unternehmen den Einsatz von Kommunikations- bzw. Kollaborationslösungen, welche heutzutage von vielen Messengerdiensten bereitgestellt werden, sollte es systematisch folgende Fragen als Leitfaden ggf. bereits gemeinsam mit der betrieblichen Datenschutzbeauftragten und dem Betriebsrat sowie IT-Verantwortlichen durchgehen:[1403]

Handelt es sich im Folgenden um Ja-Nein-Fragen, sind diese zumeist so konzipiert, dass in der Regel ein „Ja“ als Antwort positiv zu bewerten ist. Bei einer Abweichung muss bzw. sollte eine Begründung vorgelegt werden, anhand derer geprüft werden kann, ob Abweichungen im Einzelfall zulässig sind. Sofern in den Tabellen „Daten“ genannt werden, sind für gewöhnlich personenbezogene Daten gemeint. „Normaler Schutzbedarf“ bezieht sich darauf, dass keine spezifischen Sonderkonstellationen vorliegen, welche ein erhöhtes Schutzbedürfnis auslösen (wie bspw. Verarbeitung medizinischer Daten im Gesundheitssektor, vgl. hierzu die Empfehlungen der DSK[1404]). Grundlage ist u.a. der Prüfkatalog des LDA Bayern, allerdings angepasst an die aktuelle Rechtslage. Der Prüfkatalog kann als Checkliste dienen und gleichzeitig bei der Umsetzung der Dokumentationspflichten unterstützen.

[1402] *Bertram/Falder*, ArbRAktuell 2021, 95 (96); *Suwelack*, ZD 2020, 561 (563).
[1403] In Anlehnung an: *BayLDA*, Prüfkatalog für den technischen Datenschutz bei Apps mit normalem Schutzbedarf, abrufbar unter: https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf 2016 [letzter Abruf 18.08.2021]; siehe auch: *Rohrlich*, ZAP 2020, 1265 (1265 f.).
[1404] *DSK – Datenschutzkonferenz,* Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, 2019.

Einsatzzweck

<table>
<tr><th colspan="3">Wofür soll der Dienst eingesetzt werden?</th></tr>
<tr><td>Kommunikation</td><td>Rein innerbetriebliche Kommunikation</td><td>Externe Kommunikation mit Geschäftskontakten und/oder Kundschaft</td></tr>
<tr><td>Betroffene Daten / Personen</td><td>Schutz der Beschäftigtendaten</td><td>Schutz der Beschäftigtendaten
Schutz der Daten von Privatpersonen und / oder Beschäftigten anderer Unternehmen</td></tr>
<tr><td>Datenzugriffe</td><td>Welche Einsatzszenarien sollen adressiert werden?
Einsatz zur rein beruflichen oder auch privaten Kommunikation?
— Regelung zum unter-neh-mensseitigen Zugriff auf Nut-zeraccount / Einzelchats</td><td>Unternehmen sollte vorab prüfen:
Welche Datenzugriffe sind erforderlich zur Umsetzung von Compliance-Anforderungen?
Welche Form der Datenarchivierung ist wegen handels- / steuerrechtlicher Pflichten erforderlich?</td></tr>
<tr><td>BYOD / COPE</td><td colspan="2">Welche Vorkehrungen müssen getroffen werden, um Anwendungen auf privaten Endgeräten bzw. privat genutzten Firmengeräten zu betreiben?
— Welche Lösungen bietet das System, um Kontaktverzeichnisse zu trennen, Richtlinien umzusetzen, Funktionen vorzudefinieren?
— Welche Lösungen bietet das System, um private und berufliche Kommunikation zu trennen (z. B. Container)?</td></tr>
<tr><td>Vertraulichkeit</td><td colspan="2">Sollen Informationen ausgetauscht werden, die als Geschäftsgeheimnis geschützt werden sollen?
— Bietet die Lösung sowohl unterschiedliche Vertraulichkeitslevel für geschlossene Nutzerkreise als auch Möglichkeiten zur Einbindung Externer an?</td></tr>
<tr><td>Sonstige Randbedingungen</td><td colspan="2">Was deckt das finanzielle und zeitliche Budget ab?
Wie muss die Leistungsfähigkeit ausgelegt sein?
Ist ein temporärer oder dauerhafter Einsatz geplant?</td></tr>
</table>

Im Rahmen des risikobasierten Ansatzes dürften auch Implementierungskosten bei der Auswahl einer technischen Lösung berücksichtigt werden, es ist allerdings nicht zu erwarten, dass Aufsichtsbehörden allein den Verweis auf erhöhte Kosten einer datenschutzfreundlichen Lösung bei einem Datenschutzverstoß gelten lassen. Insbesondere sollte auch das Geschäftsmodell eines Dienstanbieters in den Blick genommen werden: Kostenlose Angebote sind zwar attraktiv, im Hinblick auf Datenschutz, Zuverlässigkeit und Ausfallsicherheit kommen allerdings nur kostenpflichtige Lösungen für unternehmerische Zwecke realistisch in Betracht.

Praxistipp:

Unternehmen sollten eine Liste der in Frage kommenden Angebote nebst verfügbaren Informationen zu den Datenschutzeigenschaften erstellen und anhand des Einsatzzweckes nachvollziehbar dokumentieren, welche Angebote ausgeschlossen und welche in die engere Wahl aufgenommen wurden. Diese Dokumentation kann bei Bedarf Aufsichtsbehörden vorgelegt werden.

Betriebsform

Wer soll den Dienst betreiben?			
Betriebsform	in **Eigenregie On Premise**	mit Hilfe eines **Dienstleisters (SaaS)**	Joint Controller
Interne Kommunikation	Diensterbringung unterliegt alleiniger Kontrolle des Unternehmens	☐AV-Vertrag	Kaum begründbar: Zulässigkeit beschränkt auf erforderliche Daten für Kommunikationsleistung
Externe Kommunikation		ggf. Doppelrolle des Messengerdienstes in Dreiecksbeziehungen zwischen Unternehmen und Kommunikationskontakten (Einzelfallprüfung)	Der Anbieter verfolgt mit der Verarbeitung der Nutzungsdaten eigene Zwecke, die über die bloße Erbringung der Kommunikationsleistung hinausgehen (z.B. Profilbildung, Werbezwecke/Marketing, Ver-besserung des eigenen Angebots, etc.)
Welche **Garantien** und **Serviceleistungen** bieten Angebote?	Sind Funktionen zur Erfüllung der Datenschutzvorgaben im (Lizenz-) Vertrag geregelt?	Werden TOMs bereitgestellt und dokumentiert (siehe auch Transparenz)? ☐Ja ☐Nein, Begründung: _____	Werden TOMs bereitgestellt und dokumentiert (siehe auch Transparenz)? ☐Ja ☐Nein, Begründung: _____
Umsetzung	Existieren geeignete Kompetenzen im Betrieb zur Einführung und Betreuung erforderlicher Soft- und Hardware?	Werden Mindestanforderungen der Auftragsverarbeitung erfüllt: ☐Dienst verfolgt **keine eigenen Verarbeitungszwecke** / Zwecke Dritter? ☐Dienst unterwirft sich **Weisungen** des Auftraggebers? ☐Keine nichtabgesprochene Einbindung von **Subunternehmen**? ☐Verschwiegenheitsvereinbarung liegt vor? ☐Dienst bietet **Garantien** für technische und organisatorische Schutzmaßnahmen?	Aufgrund von Rechtsunsicherheiten für solche Fälle ist besonders zu prüfen, ob die Nutzung dieses Diensts tatsächlich geboten ist. ☐Bietet der Dienst eine Vereinbarung über die gemeinsame Verantwortung, welche **nicht pauschal** alle Pflichten einseitig verteilt? ☐Sind die Rechtsgrundlagen zur Datenverarbeitung sowie Einhaltung aller Datenschutz-bestimmungen durch den Dienst **plausibel** genug beschrieben?
Folgen	Softwarelieferanten, die nicht als Auftragsverarbeiter zu qualifizieren sind, unterliegen nicht den Datenschutzvorgaben: Hier können Pflichten aber über den Nutzungs-/Lizenzvertrag vereinbart werden.	Der Dienst wird **„als verlängerter Arm“** des Unternehmens tätig, benötigt keine Rechtsgrundlage. Dienst ist gesetzlich verpflichtet, Unternehmen bei Erfüllung des Datenschutzes zu **unterstützen.** Chancen und Risiken zwischen Betrieb in Eigenregie und durch Dienstleister hängen entscheidend vom Datenschutzniveau des Systems ab.	Datenübermittlung an Dienst erfordert Rechtsgrundlage. Dienst dürfte als OTT-Dienst dem TTDSG / künftig der ePrivacy-VO unterfallen. — Einhaltung des Fernmeldegeheimnisses — Verarbeitung von Verkehrsdaten soweit erforderlich — Einschränkung bei Standortdaten — ggf. Einwilligungen

Rechtsgrundlagen des Unternehmens (Betriebsform On Premise / SaaS)

Auf welche Rechtsgrundlagen soll der Dienst gestützt werden?		
Betroffene Person	Perspektive Beschäftigte	Perspektive Externe
(Arbeits-)Vertrag	Anforderungen erfüllt, wenn der Messengerdiensteinsatz **erforderlich** ist: ☐die Funktionen des Dienstes erfüllen die beschriebenen Zwecke (**Geeignetheit**)? ☐der Dienst bietet die geringsten Datenschutzrisiken bei gleichzeitiger Erfüllung des Einsatzzwecks (**relativ mildeste Mittel**)? ☐die Risiken sind **angemessen** im Hinblick auf die verfolgten Zwecke?	Anforderung erfüllt, wenn: ☐Vetrag mit der betroffenen Person selbst ☐Datenverarbeitung **erforderlich** zur Vertragserfüllung oder: ☐erforderlich für Vertragsanbahnung / vorvertragliche Maßnahmen auf Anfrage der betroffenen Person
Einwilligung	Anforderungen erfüllt, wenn Erteilung: ☐**informiert** (vgl. Transparenz) ☐**freiwillig**, d.h. nur für optionale Daten ☐jederzeit **widerrufbar** ohne Nachteile ☐durch **aktive** Handlung ☐elektronisch oder schriftlich	Anforderungen erfüllt, wenn Erteilung: ☐**informiert** (vgl. Transparenz) ☐**freiwillig**, d.h. nur für optionale Daten ☐jederzeit **widerrufbar** ohne Nachteile ☐durch aktive Handlung
Kollektiv-vereinbarung	**Betriebsvereinbarung**: wirksam sofern Datenverarbeitung ☐Geeignet, erforderlich, angemessen	
Gesetzliche Pflichten	Erstrecken sich handels- / steuerrechtliche Pflichten auch auf interne Kommunikation (z. B. Handels- & Geschäftsbriefe)? Betrifft die Messengerdienstnutzung Daten, für die im Unternehmen gesetzliche Verarbeitungs- bzw. Vorhaltungspflichten bestehen? — Einzelfallprüfung (abhängig vom Einsatzzweck)	ggf. relevant: — **Aufbewahrungspflichten** für handelsrechtlich relevante Unterlagen — Steuerrechtliche Aufbewahrungs-pflichten (z. B. für Handels-/ Geschäftsbriefe) — Daten müssen für bestimmte Zeiträume archiviert werden — Ggf. Einsichtsnahmerechte der Finanzbehörden — Einzelfallprüfung
Berechtigte Interessen	Relevant ggü. Kontakten im Adressbuch (Dritte) bei: — Adressbuchabgleich – erfüllt, wenn: ☐optional, nicht automatisch ☐nicht im Klartext, mind. gehasht ☐Speicherung nur flüchtig	Relevant für: — Adressbuchabgleich, Anforderungen siehe links — Verarbeitung von **Beschäftigtendaten anderer Unternehmen**, bei Geschäftsbeziehungen zum Unternehmen

Für jede Datenverarbeitung muss eine Rechtsgrundlage erfüllt sein. Dabei können unterschiedliche Datenverarbeitungsvorgänge unter mehrere Rechtsgrundlagen fallen.

Transparenz

<table>
<tr><th colspan="3">Wie transparent ist das Angebot?</th></tr>
<tr><td>Datenschutzerklärung</td><td>Mindestanforderung:
☐Liegt vor
☐in deutscher Sprache
☐getrennt von anderen Erklärungen, jederzeit innerhalb App einsehbar
☐präzise, verständlich und vollständig
☐Liegt nicht vor, Begründung:
_____</td><td>Transparenzsteigernd:
☐Datenschutzbestimmungen speziell für die App (nicht gleichzeitig Webseite, andere Angebote, etc.)?
☐Übersichtliche Gliederung (z.B. multi-layered)?
☐Kurz und prägnant?
☐Nein, Begründung: _____</td></tr>
<tr><td>Dokumentation der TOMs</td><td colspan="2">☐Sicherheitsaudits wurden durchgeführt und veröffentlicht?
☐Der Quellcode wurde offengelegt (Open Source) und
☐ist aktuell und
☐für Dritte reproduzierbar?
☐Die verwendeten Algorithmen für die Verschlüsselung und den Metadatenschutz sind ausführlich dokumentiert?
☐Die Software kann von dritter Seite geprüft werden, Sicherheitsmeldungen werden entgegengenommen und veröffentlicht?
☐Nein, Begründung: _____</td></tr>
<tr><td>Zusätzliche Informationen</td><td colspan="2">Werden sonstige Informationen für die Risikobewertung bereitgestellt?
Liegt eine Muster-Datenschutz-Folgenabschätzung vor?
☐Ja ☐Nein, Begründung: _____ ☐Nicht anwendbar
Verfügt das Angebot über Zertifikate (sofern vorhanden), um zugesicherte Eigenschaften zu belegen? Derzeit sind keine einschlägigen Zertifizierungen bekannt.
☐Ja ☐Nein, Begründung: _____ ☐Nicht anwendbar</td></tr>
<tr><td colspan="3">Die Funktionen, Sicherheitseigenschaften und Datenschutzmaßnahmen müssen ausreichend transparent beschrieben sein. Liegt eine den DSGVO-Anforderungen entsprechende Datenschutzerklärung vor oder werden ausreichend Informationen bereitgestellt, um eine eigene Erklärung erstellen zu können?
☐Ja ☐Nein, Begründung: _____</td></tr>
</table>

Datensicherheit

Wie sicher ist die Technik gestaltet?		
Verschlüsselung	Entspricht die Verschlüsselung dem Stand der Technik? — Ende-zu-Ende-Verschlüsselung — **Transportverschlüsselung:** Wird TLS1.2 oder TLS 1.3 eingesetzt? — Werden gespeicherte Daten verschlüsselt? — Ist die Schlüssellänge bei asymmetrischen Verfahren ausreichend lang (z.B. 4096-Bit bei RSA)? — Wird Perfect Forward Secrecy eingesetzt? — Sind sslv2 und sslv3 sowie TLS 1.0 und 1.1 deaktiviert?	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar
Datenübertragung	An welche Server werden Daten abgehend vom Gerät übertragen? IP-Adresse/Domainname: Empfänger: Innerhalb EU/EWR? _____ _____ ☐ Ja ☐ Nein _____ _____ ☐ Ja ☐ Nein _____ _____ ☐ Ja ☐ Nein Welche Daten werden dabei an welchen Empfänger zu welchen Zweck übertragen? Daten: Verantwortlicher: Personenbezogen? Zweck: _____ _____ ☐ Ja ☐ Nein _____ _____ _____ ☐ Ja ☐ Nein _____ _____ _____ ☐ Ja ☐ Nein _____ — Werden vertrauenswürdige SSL-Zertifikate verwendet und diese auch zur Verhinderung von Man-In-The-Middle Angriffen überprüft? — Wird SSL-Pinning (feste "Verdrahtung" des SSL-Zertifikats in der App) eingesetzt? — Werden Token-Werte statt Account-Daten für einen Session-Bezug zum Backend verwendet?	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar
Authentisierung, Identifizierung der Kommunikationsbeteiligten	— Besteht die Möglichkeit einer Registrierung und Anmeldung mit eigenen Zugangsdaten (Benutzername und Passwort)? — Ist die Verifikation von Kontakten möglich?	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar
Zugangsdaten: Welche Daten werden für die Registrierung und Anmeldung genutzt?	— Werden die Zugangsdaten lokal im geschützten App-Bereich gespeichert? — Werden die Zugangsdaten in einem für die Passwortspeicherung geeignetem kryptographischen Verfahren transformiert, bevor diese lokal gespeichert werden (d.h. nicht im Klartext)? — Werden in der App lokale Session-Timeouts in Abhängigkeit des jeweiligen Schutzbedarfs eingesetzt, die ein erneutes Einloggen nach einer gewissen inaktiven Zeit erzwingen? — Werden Passwörter bei der Eingabe in der App maskiert (evtl. auswählbar), um ein „Shoulder-Surfing“ zu verhindern? — Werden Passwörter bei einer „Passwort vergessen“-Funktion über einen zeitlich begrenzen Weblink zurückgesetzt?	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar

Datenminimierung

Wie datenschutzfreundlich ist die Technik gestaltet?		
Erforderliche Angaben zur Registrierung	Welche personenbezogene Daten über Nutzung und Identifikation werden automatisch verarbeitet (Metadaten)? _____ _____ _____ — Wird eine eigene ID erstellt? — Sind Mobilfunknummer / E-Mail-Adresse optional? — Ist die Nutzung von Pseudonymen statt Klardaten möglich? — Sind Profilbilder optional? — Werden keine anderen gerätebezogenen Daten (z.B. IMEI-Nummer) als Identifizierungswerte im Rahmen der Authentifizierung verwendet? Welche Kommunikationsinhalte werden verarbeitet? _____ _____ _____ Sofern es sich dabei im besondere Kategorien personenbezogener Daten handelt, siehe: DSK, Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar / nicht sinnvoll
Erforderliche Daten während Nutzung	— Sind Aktivitäts-/Anwesenheitsanzeigen („Statusanzeigen“) optional oder deaktivierbar? — Sind Videobilder optional bei (Video-)Konferenzen? — Funktionen zum Verrauschen des Hintergrunds?	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar
Privatsphären-einstellungen	— Stellt die Software datenschutzfreundliche Einstellungsmöglichkeiten bereit? — Ist eine einfache Bedienbarkeit gegeben? — Welche zentralen Zugriffsmöglichkeiten sind gegeben / voreingestellt? Sind diese an Vertraulichkeitslevel und Unternehmensrollen geknüpft?	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar
Berechtigungen	Welche Berechtigungen erhält die App auf dem Gerät und ist damit ein Zugriff auf personenbezogene Daten möglich? Berechtigungen: Zugriff auf personenbezogene Daten: _____ ☐ nicht möglich ☐ möglich, Begründung: _____ _____ ☐ nicht möglich ☐ möglich, Begründung: _____ _____ ☐ nicht möglich ☐ möglich, Begründung: _____ _____ ☐ nicht möglich ☐ möglich, Begründung: _____	

	— Werden nur Berechtigungen eingefordert, die für die Funktion der App **zwingend benötigt** werden? — Erfüllt die Einforderung von nicht zwingend benötigten Berechtigungen die Anforderung an eine wirksame Einwilligung?	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar
Speicherung	Welche Daten werden lokal auf dem Endgerät gespeichert? Daten: Personenbezogen: _____ ☐ Personenbezug ☐ Kein Personenbezug _____ ☐ Personenbezug ☐ Kein Personenbezug _____ ☐ Personenbezug ☐ Kein Personenbezug Welche Daten werden auf externen Servern gespeichert? _____ ☐ Personenbezug ☐ Kein Personenbezug _____ ☐ Personenbezug ☐ Kein Personenbezug _____ ☐ Personenbezug ☐ Kein Personenbezug — Werden personenbezogene Daten nur gespeichert, soweit und solange sie für den Betrieb der App notwendig sind? — Werden die gespeicherten Daten nach Deinstallation der App gelöscht?	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar
	Werden Trackingverfahren (z.B. Reichweitenmessung) eingesetzt? ☐ Werden nicht eingesetzt ☐ Werden eingesetzt, Begründung: _____ Falls Tracking erfolgt: — Wird die IP-Adresse vor der systematischen Verarbeitung (z.B. Geolokalisierung) ausreichend anonymisiert? — Wird in der Datenschutzerklärung ausreichend darüber informiert? — Existiert für Nutzende eine jederzeit leicht auffindbare Widerspruchsmöglichkeit innerhalb der App? — Existiert ein Vertrag zur Auftragsdatenverarbeitung mit dem Dienstleister (falls Reichweitenmessung nicht selbst betrieben)? — Werden eindeutige (Geräte-) IDs vergeben/verwendet? — ☐ IMEI ☐ IMSI ☐ MAC-Adresse ☐ Unique-IDs ☐ Andere: ___ — Welche Tracking-Cookies werden eingesetzt? Cookie-Name: Zweck: _____ _____ _____ _____ _____ _____	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar
	Wird in der App auf Standortdaten des Geräts zugegriffen? ☐ Keine Geolokalisierung ☐ Zugriff auf Standorte, Begründung: _____ Bei Zugriff auf Standorte: — Werden Standortdaten nur in der unbedingt nötigen Auflösung („Verwaschung“) erfasst? — Sind die Abtastintervalle der Standortdaten so groß wie möglich?	☐ Ja ☐ Nein, Begründung: _____ ☐ Nicht anwendbar

	— Werden genaue Standortdaten nur lokal verarbeitet („Rasterbereich“) und gespeichert? (bei Übertragung an Backend: Wieso erfolgt keine lokale Standortverarbeitung?) — Besteht die Möglichkeit, die Lokalisierung auszuschalten?	

Sollen Datenschutzeinstellungen durch die Beschäftigten und/oder das Unternehmen umgesetzt werden, sollte diese leicht auffindbar und verständlich gestaltet werden, um die Gefahr von Fehlkonfigurationen zu vermeiden. Je mehr Voreinstellungen bereits der Datenminimierung und Datensicherheit entsprechen, desto weniger Datenschutzrisiken sind zu befürchten.

Datenmanagement

Welche Optionen des Datenmanagements bietet die Lösung?		
Management auf Endgeräten	— Kann die Nutzung auf Endgeräten zentral gesteuert, eingeschränkt oder beendet werden, z. B. über ein Mobile-Device-Management-System (MDM)? — Stehen den Beschäftigten jeweils eigene Endgeräte zur Verfügung?	☐ Ja ☐ Nein, Begründung: _____ ☐ *Nicht anwendbar*
Vertraulichkeit	Sind unterschiedliche Vertraulichkeitslevel umsetzbar? — Können Kommunikationskanäle nach dem Need-to-Know-Prinzip gestaltet werden? — Sind Zugangsbeschränkungen einstellbar? — Zugangsschutz zu Gruppen-Chats/Konferenzräumen über Passwörter/individuelle Einladungslinks — Wird sichergestellt, dass Personen (insbes. Admins) nicht auf Informationen außerhalb ihrer Befugnisse zugreifen können? — Erfolgen keine automatischen Aufzeichnungen bei Videokonferenzen (mind. deaktivierbar)?	☐ Ja ☐ Nein, Begründung: _____ ☐ *Nicht anwendbar*
Speicherung	Für den Fall gesetzlicher Aufbewahrungspflichten / Compliance-Anforderungen im Unternehmen, die Zugriffsrechte erfordern: — Können Speicher- und Löschroutinen erstellt werden? — Backups erfolgen zentral beim Unternehmen? Für den Fall sensibler / vertraulicher Kommunikation: — Können Speicher- und Löschroutinen erstellt werden? — Backups dezentral auf Endgeräten?	☐ Ja ☐ Nein, Begründung: _____ ☐ *Nicht anwendbar*

Erläuterung: Erwägungen zu unmittelbaren Zugriffsmöglichkeiten des Unternehmens auf Kommunikationsinhalte sowie die Kommunikationsumstände stehen teils in direktem Konflikt zur Umsetzung eines hohen Datenschutzniveaus. Denn eine zentrale Datensicherung sowie Umsetzung von Compliance-Anforderungen ist mit echter Ende-zu-Ende-Verschlüsselung nicht vereinbar. Insofern müssen Unternehmen entscheiden, welche Zielsetzungen höher zu priorisieren sind bzw. wie kollidierenden Pflichten nachgegangen werden kann (bspw. über interne Regeln, Definition zusätzlicher Datenablageorte, Dokumentationspflichten). Dies steht wiederum in engem Zusammenhang mit dem Einsatzzweck.

Umsetzung Betroffenenrechte

Wie unterstützt die Lösung bei der Umsetzung der Bertoffenenrechte?		
Auskunft	Ist es möglich, fristgerecht Auskunft zu erteilen über: — die verarbeiteten personenbezogenen Daten und — die Kontextinformationen (Zweck, Kategorien, Empfänger, etc.) sowie eine **Kopie** bereitzustellen, ohne Rechte Dritter zu verletzen (personenbezogene Daten Dritter, Urheberrechte, Geschäftsgeheimnisse, etc.)?	☐ Ja ☐ Nein, Begründung: _____ ☐ *Nicht erforderlich, da Identifizierung ausgeschlossen*
Berichtigung	— Ist sichergestellt, dass **unrichtige** Daten berichtigt werden? — Kann die betroffene Person selbstständig unrichtige / unvollständige Daten berichtigen oder besteht die Möglichkeit, Berichtigungsersuchen fristgerecht umzusetzen?	☐ Ja ☐ Nein, Begründung: _____
Löschung / Sperrung (Einschränkung der Verarbeitung)	— Werden Daten automatisch nach Ablauf von Speicherfristen gelöscht? — Ist sichergestellt, dass individuelle **Löschanfragen** fristgerecht beantwortet werden können? — Ist sichergestellt, dass eine Sperrung der Daten erfolgen kann, sofern bspw. über ein Lösch- / Berichtigungsersuchen entschieden werden muss oder die betroffene Person die Sperrung beantragt?	☐ Ja ☐ *Nein, Begründung:* _____
Widerruf	Falls Daten auf Grundlage einer Einwilligung verarbeitet werden: — Wurde die betroffene Person darüber informiert, dass die Einwilligung jederzeit widerrufbar ist? — Ist der Widerruf genauso leicht erteilbar wie die Einwilligung? — Ist sichergestellt, dass eine Datenverarbeitung nach Widerruf beendet wird?	☐ Ja ☐ *Nein, Begründung:* _____ ☐ *Nicht anwendbar*
Widerspruch	Falls Daten auf Grundlage einer Interessenabwägung verarbeitet werden: — Wurde die betroffene Person darüber informiert, dass sie ein Recht auf Widerspruch hat? — Im Fall von Direktwerbung: Ist sichergestellt, dass die Datenverarbeitung zum Zweck der Direktwerbung nach Widerspruch eingestellt wird?	☐ Ja ☐ *Nein, Begründung:* _____ ☐ *Nicht anwendbar*
Datenübertragbarkeit	Falls Daten auf Grundlage einer Einwilligung oder eines Vertrags verarbeitet werden und von der betroffenen Person bereitgestellt wurden: — Können die Daten auf Anfrage in einem strukturierten, gängigen und maschinenlesbaren Format herausgegeben werden, ohne dass dadurch Rechte Dritter beeinträchtigt werden?	☐ Ja ☐ *Nein, Begründung:* _____ ☐ *Nicht anwendbar*
Kontaktmöglichkeit	Ist den betroffenen Personen bekannt, welcher Stelle gegenüber sie ihre Rechte geltend machen können?	☐ *Ja* ☐ *Nein, Nennung eines Kontakts*

Dokumentation

Wie unterstützt die Lösung bei der Umsetzung und Erfüllung von Nachweispflichten?		
Verzeichnisse	Aufnahme ins Verzeichnis von Verarbeitungstätigkeiten: — Zwecke der Verarbeitung, Kategorien betroffener Personen und Daten, Kategorien von Empfängern von Daten, Datenübermittlungen in Drittländer, vorgesehene Fristen für die Löschung verschiedener Datenkategorien sowie eine Beschreibung der TOMs liegen vor, um ein Verarbeitungsverzeichnis zu erstellen — Dienste als Auftragsverarbeiter führen ein eigenes Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten	☐ Ja ☐ Nein, Begründung: _____ ☐ *Nicht anwendbar:* Unternehmen hat weniger als 250 Beschäftigte und Verarbeitung birgt kein Risiko für Betroffene
Risikobewertung	Sind ausreichend Informationen vorhanden, zur Dokumentation der Auswahlentscheidung und durchgeführten Risikobewertung? Falls ein hohes Risiko für die Grundrechte der betroffenen Personen festgestellt wird: — Ausreichend Information vorhanden zur Durchführung der DSFA oder Muster-DSFA liegt vor — Risikominimierungsmaßnahmen, die hohes Risiko absenken oder Datenschutzaufsichtsbehörde bestätigt Verarbeitung nach Konsultation	☐ Ja ☐ Nein, Begründung: _____ ☐ *Nicht anwendbar*
Im Fall von Einwilligungen	— Einwilligungserklärungen sind nachweisbar? — Bei Beschäftigten: Erklärungen liegen in schriftlicher oder elektronischer Form vor?	☐ Ja ☐ Nein: Nachweisbarkeit herstellen

Wurde nach Risikobewertung ein normales oder geringes Risiko festgestellt, sollte dies ebenfalls dokumentiert werden. Die Risikobewertung sollte regelmäßig wiederholt werden, um zu evaluieren, ob die zuvor angenommene Risikoeinstufung aktuell ist oder ob Änderungen eine Neubewertung erforderlich machen. Mussten hohe Risiken durch gesteigerte Sicherheits-/Schutzmaßnahmen mitigiert werden, sollte regelmäßige überprüft werden, ob diese weiterhin ein angemessenes Schutzniveau sicherstellen

Datentransfers in Drittstaaten

<table>
<tr><th colspan="3">Stellt sich bei einem internationalen Anbieter eine Drittstaatproblematik (z.B. USA[1405])?</th></tr>
<tr><th>Keine Drittstaatentransfers</th><th>Drittstaat mit angemessenem Datenschutzniveau</th><th>Drittstaat ohne angemessenes Datenschutzniveau</th></tr>
<tr><td>☐Sitz des Anbieters in EU/EWR
☐Serverstandorte, Ort der Datenverarbeitung sind in EU/EWR
☐Anbieter bindet keine Sub-Dienstleister aus Drittstaat ein
☐Anbieter und Dienstleister unterliegen keinen drittstaatlichen Regeln, die Datentransfer in Drittstaat erfordern (z. B. Cloud Act)</td><td>Es ligt ein Angemessenheitsbeschluss der EU-Kommission vor für:
☐Sitz des Anbieters
☐Serverstandort, Ort der Datenverarbeitung
☐Standorte Sub-Dienstleister
☐Anbieter und Dienstleister unterliegen keinen drittstaatlichen Regeln, die Datentransfer in Drittstaat erfordern (z. B. Cloud Act)</td><td>☐Transfergarantien, wie Standardvertragsklauseln, Binding Corporate Rules, etc. sofern im Drittland durchsetzbar (erfordert Analyse Drittstaatenrecht)
☐Transfergarantien mit technischen Zusatzmaßnahmen, z. B.:
☐Datenzugriffe ausschließende Verschlüsselung (robust gegen Brute-Force-Angriffe)
☐Pseudonymisierung (ohne Möglichkeit Person aus Gruppe herauszugreifen)
☐Split / multi-party processing
☐Ausnahmen, die Transfer rechtfertigen, z. B. ausdrückliche Einwilligung</td></tr>
<tr><td colspan="2">— Keine zusätzlichen Schutzmaßnahmen erforderlich</td><td>— Regelmäßige Re-Evaluation
— Information ggü. betroffener Person
— ggf. Einholung erforderlicher Erklärungen/Genehmigungen/ Einwilligungen</td></tr>
</table>

Nutzungsbedingungen

Welche Betriebsformen werden von den Nutzungsbedingungen unterstützt?
☐Kein Ausschluss geschäftlicher Nutzung
☐Kein Ausschluss innerbetrieblicher Nutzung (bei interner Kommunikation)

Unternehmensinterne Organisation

Dieser Punkt betrifft nicht mehr die Auswahl eines Messengerdienstes selbst, steht aber in enger Wechselwirkung zur Auswahlentscheidung, da unternehmensinterne Pflichten umfangreicher ausfallen können, sofern mehr Datenschutzrisiken mit der Kommunikationsform verbunden sind. Bietet der Messengerdienst hingegen bereits ein sehr hohes Datenschutzniveau, können einzelne Pflichten im Einzelfall entbehrlich sein.

[1405] Der Einsatz von US-Dienstleistern ist nach dem Schrems-II-Urteil nur noch mit sehr hohem Aufwand möglich – zum Teil wird die Einbindung gänzlich abgelehnt, siehe Abschnitt 4.2.1.2.

Welche zusätzlichen Maßnahmen sollte das Unternehmen ergreifen?		
Einbindung interner und externer Stellen	Wurde die Zustimmung des **Betriebsrats** eingeholt? — Ist die Zustimmung entbehrlich, weil keine Überwachungsmöglichkeit besteht und keine Verhaltensregel aufgestellt wird? Wurde der/die **Datenschutzbeauftragte** eingebunden (z. B. spätestens bei Notwendigkeit, eine DSFA durchzuführen)? Wurden Personen / Stellen eingebunden, welche für den Schutz der **Geschäftsgeheimnisse** zuständig sind? — Liegen Verschwiegenheitsvereinbarungen mit Kommunikationskontakten vor, welche diesen angemessene Geheimhaltungsmaßnahmen auferlegen?	☐ Ja ☐ Nein, Begründung: _____ ☐ *Nicht erforderlich* ☐ *Nicht vorhanden*
Richtlinien	Hat das Unternehmen **interne Richtlinien** zur Nutzung des Messengerdienstes durch die Beschäftigten aufgestellt? — Wird transparent klargestellt, welche Daten **vertraulich** zu behandeln sind (insbes. als Geschäftsgeheimnisse geschützt werden sollen) und welche Daten wie mit wem ausgetauscht werden dürfen? — Wird eine Regelung zum **Zugang** des Arbeitgebers zu Accounts der Beschäftigten getroffen, die Compliance-Interessen und Persönlichkeitsrechte in angemessenen Ausgleich bringt? — Wird die **private** Nutzung gestattet und wurden entsprechende Regelungen getroffen, sofern Zugriffsmöglichkeiten des Arbeitgebers erforderlich sind (z.B. Einwilligung oder Datentrennung)?	☐ Ja ☐ Nein, Begründung: _____ ☐ *Nicht erforderlich*
Training und Schulungen	Sind alle Beschäftigten zu Datenschutzbestimmungen ausreichend geschult und **sensibilisiert**? Unterliegen die Beschäftigten internen **Meldepflichten**, sofern ein Datenschutzverstoß bzw. eine Offenlegung von Geschäftsgeheimnissen zu befürchten ist?	☐ Ja ☐ Nein, Begründung: _____ ☐ *Nicht erforderlich*

8 Danksagung

Diese Studie wurde von der Threema GmbH finanziell unterstützt. Wir bedanken uns für die impulsgebenden Gespräche und wertvollen Einblicke in die Welt der Messengerdienste. Sie gibt die Sichtweise der Autor*innen wieder; eine Einflussnahme auf die Ergebnisse durch den Auftraggeber erfolgte nicht.

9 Glossar und Abkürzungsverzeichnis

9.1 Abkürzungen

a. A.	Andere Ansicht
a. F.	Alte Fassung
AAKD	Anbieter abgeleiteter Kommunikationsdienste (nach schweizer Recht)
Abs.	Absatz
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
ArbG	Arbeitsgericht
Art.	Artikel
AV	Auftragsverarbeitung
AV-Vertrag	Auftragsverarbeitungsvertrag
BAG	Bundesarbeitsgericht
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (Schweiz)
BVerfG	Bundesverfassungsgericht
BYOD	Bring your own Device (dienstliche Nutzung privater Endgeräte)

COPE	Corporate-Owned, Personally Enabled devices (Privatnutzung von Dienstgeräten)
DSFA	Datenschutz-Folgenabschätzung
DSG	Datenschutzgesetz (Schweiz)
DSGVO	Datenschutz-Grundverordnung VO (EU) 2016/679
DSK	Datenschutzkonferenz (Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder)
E2EE	Ende-zu-Ende-Verschlüsselung
EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
EDSA / EDPB	Europäischer Datenschutzausschuss / European Data Protection Board (vormals Art-29-Datenschutzgruppe)
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EWR	Europäischer Wirtschaftsraum
ePrivacy-RL	Datenschutzrichtlinie für elektronische Kommunikation, Richtlinie 2002/58/EG
ePrivacy-VO	Geplante Verordnung zur Ablösung der ePrivacy-RL
EuGH	Europäischer Gerichtshof
EU-GrCh	EU-Grundrechtecharta
f.	folgende (die folgende Seite/der folgende Paragraph/Artikel/etc.)
ff.	fortfolgende (mehrere folgende Seiten/Paragraphen/Artikel/etc.)
FMG	Fernmeldedienst (nach schweizer Recht)
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GG	Grundgesetz
HGB	Handelsgesetzbuch
iOS	von Apple entwickeltes mobiles Betriebssystem
KG	Kammergericht
LAG	Landesarbeitsgericht
LDSG	Landesdatenschutzgesetz
LfDI	Landesbeauftragte für den Datenschutz und die Informationsfreiheit
LG	Landgericht
m. w. N.	Mit weiteren Nachweisen
MDM	Mobile Device Management
n. F.	Neue Fassung
OLG	Oberlandesgericht
öOGH	Oberste Gerichtshof Österreich
OTT	Over the Top (Übermittlung von Daten über Internetzugänge)

PFS	Perfect Forward Secrecy
RL	Richtlinie
Rn.	Randnummer
SaaS	Software as a Service
SCC	Standard Contractual Clauses / Standardvertragsklauseln
Sog.	sogenannt
TK-Dienst	Telekommunikationsdienst
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
TOM	Technische und organisatorische Maßnahmen
TTDSG	Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien
UWG	Gesetz gegen den unlauteren Wettbewerb
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
Vgl.	Vergleiche
VO	Verordnung
XMPP	Extensible Messaging and Presence Protocol

9.2 Glossar zu verwendeten Begriffen

Auftragsverarbeiter	Im Auftrag eines Verantwortlichen tätige Stelle definiert in Art. 4 Nr. 8 DSGVO, die keine eigenen Verarbeitungszwecke verfolgt
Beschäftigte	Arbeitnehmer*innen / Mitarbeiter*innen eines Unternehmens / Organisation, definiert in § 26 Abs. 8 BDSG
Besondere Kategorien personenbezogener Daten	Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person i.S.d. Art. 9 Abs. 1 DSGVO
Betroffene Person	Identifizierte oder identifizierbare natürliche Person, auf die sich Daten beziehen i.S.d. Art. 4 Nr. 1 DSGVO
Betroffenenrechte	Rechte der betroffenen Person auf Auskunft, Berichtigung, Löschung bzw. Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch und Ausschluss automatisierter Entscheidungen im Einzelfall (Kapitel 3 DSGVO)
Daten	Informationen (hier Synonym verwendet)

Datenschutzgrundrechte	Bezieht sich auf die datenschutzrechtlich relevanten Grundrechte wie Recht auf informationelle Selbstbestimmung, Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme, Achtung des Privat und Familienlebens, Recht auf Schutz personenbezogener Daten
Drittstaat / Drittland	Staat bzw. Land außerhalb der EU und des EWR
Geschäftsgeheimnis	Eine Information, die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und bei der ein berechtigtes Interesse an der Geheimhaltung besteht, § 2 Nr. 1 GeschGehG
Joint Controller	Englisch für gemeinsame Verantwortlichkeit. Wird ein Messengerdienst eigenverantwortlich betrieben, ist der Dienstanbieter Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO. Ist das dienstnutzende Unternehmen ebenfalls als Verantwortlicher zu qualifizieren, müssen die Anforderungen gemeinsamer Verantwortlichkeit erfüllt werden.
Know-How-Schutz	Schutz von Geschäftsgeheimnissen
Kommunikationsinhalte	Nachrichten, Texte, Voice-Calls, Video-Calls, Mediendateien, etc.
Metadaten	Informationen zu den Umständen der Kommunikation, wie z. B. Telefonnummern, Kontaktdetails, Zeitpunkte und Dauer einer Kommunikation sowie ggf. Standort der kommunizierenden Parteien
On Premise	Bezieht sich im vorliegenden Kontext auf den Betrieb eines Messengerdienstes „vor Ort“ durch das Unternehmen selbst, d.h. lokale, serverbasierte Nutzung von Software: Das Unternehmen erwirbt Lizenzen zur Nutzung von Software und betreibt diese in eigener Verantwortung
Privacy by Default	Datenschutzfreundliche Voreinstellungen (vgl. Art. 25 Abs. 2 DSGVO)
Privacy by Design	Datenschutzfreundliche Technikgestaltung (vgl. Art. 25 Abs. 1 DSGVO)
Software as a Service	Software und IT-Infrastruktur werden bei/von einem externen IT-Dienstleister betrieben. Im vorliegenden Kontext wird der Begriff genutzt, um den Fall der Auftragsverarbeitung zu beschreiben.
Unternehmen	Wirtschaftlich selbstständige Organisationseinheit, wobei im vorliegenden Kontext privatrechtlich organisierte Unternehmen im Fokus stehen. Hierbei handelt es sich regelmäßig um juristische Personen oder Personengesellschaften (z.B. GmbH, AG, SE etc.)
Verantwortlicher	Für die Verarbeitung personenbezogener Daten verantwortliche Stelle definiert in Art. 4 Nr. 7 DSGVO

10 Literatur

Acquisti, Alessandro/ Grossklags, Jens, Privacy and rationality in individual decision making, IEEE Security and Privacy Magazine 2005, 26–33.

Albrecht, Jan Philipp, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, 88–98.

Albrecht, Jan Philipp/ Jotzo, Florian, Das neue Datenschutzrecht der EU: Grundlagen, Gesetzgebungsverfahren, Synopse, 1. Auflage, Baden-Baden 2017.

Alexander, Christian, Geheimnisschutz nach dem GeschGehGE und investigativer Journalismus, AfP 2019, 1–11.

Ambrock, Jens, Mitarbeiterexzess im Datenschutzrecht, ZD 2020, 492–497.

Ambrock, Jens/ Karg, Moritz, Ausnahmetatbestände der DS-GVO als Rettungsanker des internationalen Datenverkehrs?, ZD 2017, 154–161.

Apel, Simon, Anmerkung zu BGH: Übergang eines Facebook-Nutzungsvertrags beim Tod des Kontoinhabers, ZD 2018, 486.

Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ - WP 136, 2007.

Artikel-29-Datenschutzgruppe, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten - WP 202, 2013.

Artikel-29-Datenschutzgruppe, Opinion 03/2013 on Purpose Limitation - WP 203, 2013.

Artikel-29-Datenschutzgruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG - WP 217, 2014.

Artikel-29-Datenschutzgruppe, Leitlinien zum Recht auf Datenübertragbarkeit - WP 242 rev.01, 2016.

Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" - WP248 Rev.01, 2017.

Artikel-29-Datenschutzgruppe, Opinion 2/2017 on data processing at work - WP 249, 2017.

Artikel-29-Datenschutzgruppe, Guidelines on consent under Regulation 2016/679 - WP 259, 2017.

Artikel-29-Datenschutzgruppe, Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01, 2018.

Auer-Reinsdorff, Astrid/ Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage, München 2019.

Bäcker, Matthias, Grundrechtlicher Informationsschutz gegen Private, Der Staat 51 (2012), 91 -116.

Balaban, Silvia/ Wagner, Manuela, Minimizing the Risks of Data Protection Infringement - Data Lifecycle Risk Assessment, Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security 2017, 356–362.

Baumgartner, Ulrich/ Ewald, Konstantin, Apps und Recht, 2. Auflage, München 2016.

Baumgartner, Ulrich/ Gausling, Tina, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, ZD 2017, 308–313.

BayLDA, Prüfkatalog für den technischen Datenschutz bei Apps mit normalem Schutzbedarf, 2016.

Becker, Maximilian, Ein Recht auf datenerhebungsfreie Produkte, JZ 2017, 170–181.

Beißwenger, Michael/ Pappert, Steffen, Small Talk mit Bildzeichen, Zeitschrift für Literaturwissenschaft und Linguistik 2020, 89–114.

Benedikt, Kristin/ Kranig, Thomas, DS-GVO und KUG – ein gespanntes Verhältnis - Ende des KUG nach 111 Jahren?, ZD 2019, 4–7.

Bergt, Matthias, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts - Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, 365-371.

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten, 2021.

Bertram, Axel/ Falder, Roland, Datenschutz im Home Office - Quadratur des Kreises oder Frage des guten Willens?, ArbRAktuell 2021, 95–98.

BfDI, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 2020.

BfDI, Tätigkeitsbericht 2020, Bonn 2021.

Bieker, Felix, Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, DuD 2018, 27–31.

Bieker, Felix/ Bremert, Benjamin/ Hansen, Marit, Die Risikobeurteilung nach der DSGVO, DuD 2018, 492–496.

Blasek, Katrin, Anmerkung zu VG Mainz: Datenübermittlung an Inkassounternehmen durch Tierarzt, ZD 2020, 376–380.

Bodungen, Benjamin von/ Hoffmann, Martin, Hoch- und vollautomatisiertes Fahren ante portas – Auswirkungen des 8. StVG-Änderungsgesetzes auf die Herstellerhaftung, NZV 2018, 97–102.

Boehm, Franziska/ Andrees, Markus, Zur Vereinbarkeit der Vorratsdatenspeicherung mit europäischem Recht, CR 2016, 146–154.

Boehm, Franziska/ Cole, Mark D., Studie zu den Folgen des EuGH-Urteils zur Vorratsdatenspeicherung - Auswirkungen auf Mitgliedstaaten, EU-Rechtsakte und internationale Abkommen, ZD 2014, 553-557.

Boehme-Neßler, Volker, Privacy: a matter of democracy. Why democracy needs privacy and data protection, International Data Privacy Law 2016, 222-229.

Boehme-Neßler, Volker, Das Ende der Anonymität: Wie Big Data das Datenschutzrecht verändert, DuD 2016, 419–423.

Borges, Georg/ Hilber, Marc (Hrsg.), BeckOK IT-Recht, 1. Edition, München 2021.

Bräutigam, Peter/ Klindt, Thomas, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, 1137–1142.

Brecht, Corinna/ Steinbrück, Anne/ Wagner, Manuela, Der Arbeitnehmer 4.0? - Automatisierte Arbeitgeberentscheidungen durch Sensorik am smarten Arbeitsplatz, PinG 2018, 10–15.

Breyer, Patrick, Datenschutz im Internet: Zwangsidentifizierung und Surfprotokollierung bleiben verboten - Warum Internetnutzer auch in Zukunft einen besonderen Datenschutz brauchen, ZD 2018, 302-303.

Brink, Stefan, Datenschutzrechtliche Konsequenzen der Gestattung privater Nutzung des dienstlichen E-Mail-Accounts, jurisPR-ArbR 2011, Anm. 5.

Brink, Stefan/ Schwab, Sabrina, Die private E-Mail-Nutzung am Arbeitsplatz, ArbRAktuell 2018, 111–114.

Britz, Gabriele, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, 1–11.

Brockmeyer, Henning, Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge?, ZD 2018, 258-263.

Brüggemann, Sebastian, Das Recht auf Datenportabilität, K&R 2018, 1–5.

Brummund, Anke, Smartphones und Apps: Datenschutzrechtliche Risiken und deren Begrenzung., GI-Jahrestagung 2014, 539–550.

BSI, Die Lage der IT-Sicherheit in Deutschland 2017, 2017.

BSI, Die Lage der IT-Sicherheit in Deutschland 2020, 2020.

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006.

Buchner, Benedikt, Die Einwilligung im Datenschutzrecht: — vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument, DuD 2010, 39–43.

Buchner, Benedikt/ Kühling, Jürgen, Die Einwilligung in der Datenschutzordnung 2018, DuD 2017, 544–548.

Bühlmann, Lukas/ Metin, Hatun, Totalrevision des Schweizer Datenschutzgesetzes vor dem Hintergrund der DS-GVO, ZD 2019, 356–362.

Bühr, Oliver M., Videokonferenzen und Datenschutz, K&R 2021, 221–225.

Bundesverband IT-Sicherheit e.V. (TeleTrusT), IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen, Berlin 2020.

Busche, Axel Frhr. von dem/ Voigt, Paul (Hrsg.), Konzerndatenschutz: Rechtshandbuch, 2. Auflage, München 2019.

Calliess, Christian/ Ruffert, Matthias (Hrsg.), EUV/AEUV: das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta: Kommentar, 5 Auflage, München 2016.

Caspar, Johannes, Klarnamenpflicht versus Recht auf pseudonyme Nutzung, ZRP 2015, 233-236.

Cohn-Gordon, Katriel/ Cremers, Cas/ Dowling, Benjamin/ Garratt, Luke/ Stebila, Douglas, A formal security analysis of the signal messaging protocol, Journal of Cryptology 2020, 1914–1983.

Culik, Nicolai/ Döpke, Christian, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226–230.

Dammann, Ulrich, Erfolge und Defizite der EU-Datenschutzgrundverordnung - Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307–314.

Dann, Matthias/ Markgraf, Jochen, Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, NJW 2019, 1774–1779.

Datta, Amit/ Klein, Urs Albrecht, Kostenlose Apps – eine vertragsrechtliche Analyse, CR 2017, 174–181.

Dietrich, Aljoscha/ Bosse, Christian K./ Schmitt, Hartmut, Kontrolle und Überwachung von Beschäftigten, DuD 2021, 5–10.

DSK - Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, 2016.

DSK - Datenschutzkonferenz, Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen, 2018.

DSK - Datenschutzkonferenz, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018 - Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 2018.

DSK - Datenschutzkonferenz, Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO), 2018.

DSK - Datenschutzkonferenz, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit, 2019.

DSK - Datenschutzkonferenz, Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, 2019.

DSK - Datenschutzkonferenz, Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich, 2019.

DSK - Datenschutzkonferenz, Orientierungshilfe Videokonferenzsysteme, 2020.

DSK - Datenschutzkonferenz, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, 2021.

Dümeland, Malte, Sachmangelhaftigkeit von Software bei nicht DSGVO-konformer Entwicklung, K&R 2019, 22-25.

Durmus, Erdem/ Selzer, Annika/ Pordesch, Ulrich, Das Löschen nach der DSGVO, DuD 2019, 786-791.

Dury, Marcus, „Home-Office“ und Datenschutz, ZD-Aktuell 2020, 04405.

Düwell, Franz Josef/ Brink, Stefan, Die EU-Datenschutz-Grundverordnung und der Beschäftigtendatenschutz, NZA 2016, 665–668.

Ehmann, Eugen/ Selmayr, Martin (Hrsg.), DS-GVO: Datenschutz-Grundverordnung: Kommentar, 2. Auflage, München 2018.

Engeler, Malte, Das überschätzte Kopplungsverbot, ZD 2018, 55-62.

Engeler, Malte/ Felber, Wolfram, Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis, ZD 2017, 251–257.

Engeler, Malte/ Quiel, Philipp, Recht auf Kopie und Auskunftsanspruch im Datenschutzrecht, NJW 2019, 2201–2206.

Engels, Barbara, Datenschutzpräferenzen von Jugendlichen in Deutschland, 2018.

Ernst, Stefan, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110-114.

European Data Protection Board, Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01, 2017.

European Data Protection Board, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, Brüssel 2018.

European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, 2019.

European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 2019.

European Data Protection Board, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, Angenommen am 29. Januar 2020, 2020.

European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679 (Version 1.1), 2020.

European Data Protection Board, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems, 2020.

European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, 2020.

European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, 2020.

European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, 2021.

European Data Protection Board/ European Data Protection Supervisor, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex), 2019.

European Data Protection Supervisor (EDPS), A Preliminary Opinion on data protection and scientific research, 2020.

European Network and Information Security Agency (ENISA), Good practice guide on vulnerability disclosure: from challenges to recommendations., LU 2015.

Faas, Thomas, WhatsApp & Outlook auf dem beruflichen Smartphone: Haftungsrisiken und Auswege, ArbRAktuell 2018, 594–596.

Felber, Wolfram, Anmerkung zu VG Bayreuth: Datenschutzrechtliche Anordnung zur Löschung von Kundenlisten beim Einsatz von Facebook Custom Audience, ZD 2018, 382–387.

Feldmann, Thorsten, Mobile Apps: Zivilrecht - Telemedienrecht - Datenschutz, DSRITB 2011, 47–65.

Fitting, Karl/ Engels, Gerd/ Schmidt, Ingrid/ Trebinger, Yvonne/ Linsenmaier, Wolfgang (Hrsg.), Betriebsverfassungsgesetz: Handkommentar, 28. Auflage, München 2016.

Fokken, Martin, Telekommunikationsrechtliche Pflichten des Arbeitgebers bei privater E-Mail-Nutzung der Mitarbeiter, NZA 2020, 629–633.

Forgó, Nikolaus/ Helfrich, Marcus/ Schneider, Jochen (Hrsg.), Betrieblicher Datenschutz: Rechtshandbuch, 3. Auflage, München 2019.

Franzen, Martin/ Gallner, Inken/ Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 2. Auflage, München 2018.

Fritsch, Lothar/ Roßnagel, Heiko/ Schwenke, Matthias/ Stadler, Tobias, Die Pflicht zum Angebot anonym nutzbarer Dienste, DuD 2005, 592-596.

Fuhlrott, Michael/ Hiéramente, Mayeul, BeckOK GeschGehG, 7. Edition, München 2021.

Gausling, Tina, Offenlegung von Daten auf Basis des CLOUD Act, MMR 2018, 578–582.

Geminn, Christian/ Roßnagel, Alexander, „Privatheit“ und „Privatsphäre“ aus der Perspektive des Rechts – ein Überblick, JZ 2015, 703–708.

Geppert, Martin/ Schütz, Raimund (Hrsg.), Beck'scher TKG-Kommentar, 4. Auflage, München 2013.

Gersdorf, Hubertus/ Paal, Boris P. (Hrsg.), Beck'scher Online-Kommentar zum Informations- und Medienrecht, 27. Edition, München 2020.

Gierschmann, Sybille, Was „bringt" deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD 2016, 51-55.

Gierschmann, Sybille, Positionsbestimmung der DSK zur Anwendbarkeit des TMG, ZD 2018, 297-301.

Gilga, Carolin, Beschäftigtendatenschutz und Covid-19: Daten sicher im Homeoffice?, ZD-Aktuell 2020, 07113.

Gola, Peter, Neues Recht – neue Fragen: Einige aktuelle Interpretationsfragen zur DSGVO, K&R 2017, 145-149.

Gola, Peter (Hrsg.), Datenschutz-Grundverordnung VO (EU) 2016/679: Kommentar, 1. Auflage München 2017.

Gola, Peter (Hrsg.), Datenschutz-Grundverordnung VO (EU) 2016/679: Kommentar, 2. Aufage, München 2018.

Gola, Peter, Das Geschäftsgeheimnisgesetz und die Datenschutz-Grundverordnung: Parallele Regelungen mit neuen Verpflichtungen und Aufgaben für Datenschutzbeauftragte?, DuD 2019, 569–574.

Gola, Peter/ Heckmann, Dirk (Hrsg.), Bundesdatenschutzgesetz: Kommentar, 13. Auflage, München 2019.

Gola, Peter/ Lepperhoff, Niels, Reichweite des Haushalts- und Familienprivilegs bei der Datenverarbeitung, ZD 2016, 9–12.

Golembiewski, Claudia, Anonymität im Recht der Multimediadienste, in: *Bäumler, Helmut/Mutius, Albert von (Hrsg.)*, Anonymität im Internet, 1. Aufl, Braunschweig, Wiesbaden 2003, 107-116.

Golland, Alexander, Das Kopplungsverbot in der Datenschutz-Grundverordnung, MMR 2018, 130–135.

Gomille, Christian, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76–82.

Graf von Westphalen, Friedrich/ Wendehorst, Christiane, Hergabe personenbezogener Daten für digitale Inhalte - Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenmarkt?, BB 2016, 2179–2187.

Grafenstein, Maximilian von, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit: Zur mangelnden Differenzierung der Rechtsgüterbetroffenheit in der Datenschutzgrund-VO, DuD 2015, 789–795.

Grages, Jan-Michael/ Plath, Kai-Uwe, Black Box statt Big Brother: Datenschutzkonforme Videoüberwachung unter BDSG und DSGVO, CR 2017, 791–797.

Grimm, Dieter, Der Datenschutz vor einer Neuorientierung, JZ 2013, 585–592.

Gsell, Beate/ Krüger, Wolfgang/ Lorenz, Stephan/ Reymann, Christoph (Hrsg.), GROSSKOMMENTAR zum Zivilrecht, München 2019.

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035-1041.

Hagen, Christoph/ Weinert, Christian/ Sendner, Christoph/ Dmitrienko, Alexandra/ Schneider, Thomas, All the Numbers are US: Large-scale Abuse of Contact Discovery in Mobile Messengers, Proceedings 2021 Network and Distributed System Security Symposium 2021.

Hammer, Volker/ Knopp, Michael, Datenschutzinstrumente Anonymisierung, Pseudonyme und Verschlüsselung, DuD 2015, 503–509.

Hansen, Hauke/ Brechtel, Sandra, KUG vs. DS-GVO: Kann das KUG anwendbar bleiben?, GRUR-Prax 2018, 369–370.

Hansen, Marit, Auf dem Weg zum Identitätsmanagement - von der rechtlichen Basis bis zur Realisierung, in: *Bäumler, Helmut/Mutius, Albert von (Hrsg.)*, Anonymität im Internet, 1. Auflage, Braunschweig, Wiesbaden 2003, 198.

Härting, Niko, Datenschutz-Grundverordnung, ZD-Aktuell 2016, 04215.

Härting, Niko, Digital Goods und Datenschutz – Daten sparen oder monetarisieren?, CR 2016, 735–740.

Hassemer, Winfried, Gesetzesbindung und Methodenlehre, ZRP 2007, 213–219.

Hauck, Ronny, Grenzen des Geheimnisschutzes, WRP 2018, 1032–1037.

Heckmann, Dirk, Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen, MMR 2006, 280–285.

Hermstrüwer, Yoan, Informationelle Selbstgefährdung, Tübingen 2016.

Hoeren, Thomas, Herbeiführung praktischer Konkordanz zwischen Datenschutz und KUG, Anmerkung zu OLG Köln, Beschluss vom 18.6.2018 – 15 W 27/18, ZD 2018, 435–436.

Hoeren, Thomas/ Sieber, Ulrich/ Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, 42. Auflage, München 2015.

Horner, Susanne/ Kaulartz, Markus, Haftung 4.0 Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7–19.

Hornung, Gerrit/ Herfurth, Constantin, Datenschutz bei Big Data Rechtliche und politische Implikationen, in: *König, Christian/Schröder, Jette/Wiegand, Erich (Hrsg.)*, Big Data, Wiesbaden 2018, 149–183.

Jandt, Silke, Spezifischer Datenschutz für Telemedien und die DS-GVO - Zwischen Rechtssetzung und Rechtsanwendung, ZD 2018, 405-408.

Jandt, Silke/ Steidle, Roland (Hrsg.), Datenschutz im Internet: Rechtshandbuch zu DSGVO und BDSG, 1. Auflage, Baden-Baden 2018.

Jansen, Marek, Microsofts „Search Warrant“ Case – oder die Zukunft der europäischen Datensouveränität, ZD 2018, 149–150.

Jarass, Hans D, Charta der Grundrechte der Europäischen Union, 3. Auflage, München 2016.

Jaspers, Andreas, Die EU-Datenschutz-Grundverordnung: Auswirkungen der EU-Datenschutz-Grundverordnung auf die Datenschutzorganisation des Unternehmens, DuD 2012, 571–575.

Jensen, Sarah/ Knoke, Friederike, EuGH-Urteil zur Personenbezogenheit dynamischer IP-Adressen: Quo vadis, deutsches Datenschutzrecht?, ZD-Aktuell 2016, 05416.

Johannes, Paul C./ Richter, Philipp, Privilegierte Verarbeitung im BDSG-E: Regeln für Archivierung, Forschung und Statistik, DuD 2017, 300–305.

Jülicher, Tim/ Röttgen, Charlotte/ Schönfeld, Max von, Das Recht auf Datenübertragbarkeit, ZD 2016, 358–362.

Jung, Alexander, Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, ZD 2018, 208–213.

Jung, Alexander/ Hansch, Guido, Die Verantwortlichkeit in der DS-GVO und ihre praktischen Auswirkungen, ZD 2019, 143–148.

Kalbfus, Björn, Angemessene Geheimhaltungsmaßnahmen nach der Geschäftsgeheimnis-Richtlinie, GRUR-Prax 2017, 391–393.

Kamp, Meike/ Rost, Martin, Kritik an der Einwilligung: Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen, DuD 2013, 80–84.

Karg, Moritz, Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, 520–526.

Kersten, Jens, Anonymität in der liberalen Demokratie, JuS 2017, 193-203.

Kingreen, Thorsten/ Poscher, Ralf, Grundrechte, 32. Auflage, Heidelberg Hamburg 2016.

Kipker, Dennis-Kenji/ Voskamp, Friederike (Hrsg.), Sozialdatenschutz in der Praxis, 1. Auflage, Baden-Baden 2021.

Kirchhof, Ferdinand, Grundrechtsschutz durch europäische und nationale Gerichte, NJW 2011, 3681–3686.

Klein, Urs Albrecht/ Datta, Amit, Vertragsstrukturen beim Erwerb kostenloser Apps, CR 2016, 587–590.

Klink-Straub, Judith/ Straub, Tobias, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201–3206.

Kluge, Steffen, Klarnamenspflicht bei Facebook – Rechtliche Grenzen und Möglichkeiten, K&R 2017, 230-236.

Knauer, Christoph/ Kudlich, Hans/ Schneider, Hartmut (Hrsg.), Münchener Kommentar zur Strafprozessordnung, 1. Auflage, München 2018.

Kobeissi, Nadim/ Bhargavan, Karthikeyan/ Blanchet, Bruno, Automated Verification for Secure Messaging Protocols and Their Implementations: A Symbolic and Computational Approach, 2017 IEEE European Symposium on Security and Privacy (EuroS&P) 2017, 435–450.

Köhler, Helmut/ Bornkamm, Joachim/ Feddersen, Jörn (Hrsg.), Gesetz gegen den unlauteren Wettbewerb, 39. Auflage, München 2021.

Köllmann, Thomas, Die Corona-Warn-App, NZA 2020, 831–836.

Konferenz der Justizministerinnen und Justizminister der Länder, Arbeitsgruppe „Digitaler Neustart“, Bericht vom 15. Mai 2017 unter Mitwirkung der Länder Baden-Württemberg, Bayern, Berlin, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen (Federführung), Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein, 2017.

Koreng, Ansgar/ Lachenmann, Matthias (Hrsg.), Formularhandbuch Datenschutzrecht., 2. Auflage, München 2018.

Krauß, Christoph/ Pape, Thilo von/ Robrahn, Rasmus/ Zelle, Daniel, Selbstdatenschutz im vernetzten Fahrzeug: Eine Datenschutzlösung unter Berücksichtigung der technischen, rechtlichen und Nutzeranforderungen, DuD 2017, 217–222.

Kremer, Sascha, Vertragsgestaltung bei Entwicklung und Vertrieb von Apps für mobile Endgeräte, CR 2011, 769–776.

Kring, Markus/ Marosi, Johannes, Ein Elefant im Porzellanladen-Der EuGH zu Personenbezug und berechtigtem Interesse, K&R 2016, 773–776.

Krohm, Niclas, Abschied vom Schriftformgebot der Einwilligung - Lösungsvorschläge und künftige Anforderungen, ZD 2016, 368-373.

Krohm, Niclas/ Müller-Peltzer, Philipp, Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung - Das Aus für das Modell „Service gegen Daten“?, ZD 2017, 551-556.

Krönke, Christoph, Datenpaternalismus, Der Staat 2016, 319–351.

Krüger, Jochen/ Möllers, Frederik, Metadaten in Justiz und Verwaltung, MMR 2016, 728–731.

Krüger, Stefan/ Wiencke, Julia, Bitte recht freundlich – Verhältnis zwischen KUG und DS-GVO, MMR 2019, 76–80.

Kugelmann, Dieter, Datenfinanzierte Internetangebote: Regelungs- und Schutzmechanismen der DSGVO, DuD 2016, 566–570.

Kühling, Jürgen/ Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung: Kommentar, 2. Auflage, München 2018.

Kühling, Jürgen/ Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung, BDSG Kommentar, 3. Auflage, München 2020.

Kühling, Jürgen/ Klar, Manuel, Anmerkung zu EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite, ZD 2017, 27-29.

Kühling, Jürgen/ Martini, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448-454.

Kühling, Jürgen/ Martini, Mario/ Johanna, Heberlein/ Benjamin, Kühl/ Nink, David/ Weinzierl, Quirin/ Wenzel, Michael, Die Datenschutz-Grundverordnung und das nationale Recht: erste Überlegungen zum innerstaatlichen Regelungsbedarf, 1. Auflage, Münster 2016.

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Unsere Daten: Daten nützen – Daten schützen, Tätigkeitsbericht 2020, 2020.

Langhanke, Carmen/ Schmidt-Kessel, Martin, Consumer Data as Consideration, EuCML 2015, 218-223.

Lauber-Rönsberg, Anne/ Hartlaub, Anneliese, Personenbildnisse im Spannungsfeld zwischen Äußerungs- und Datenschutzrecht, NJW 2017, 1057–1062.

Laue, Philip/ Nink, Judith/ Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Auflage, Baden-Baden 2016.

Leister, Alexander, Haftungsgefahren beim neuen Geheimnisschutz, GRUR-Prax 2020, 579–581.

Leupold, Andreas/ Wiebe, Andreas/ Glossner, Silke (Hrsg.), IT-Recht: Recht, Wirtschaft und Technik der digitalen Transformation, 4. Auflage, München 2021.

Lewinski, Kai von, Die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes, Tübingen 2014.

Luch, Anika D./ Schulz, Sönke E., eDaseinsvorsorge - Neuorientierung des überkommenen (Rechts-)Begriffs „Daseinsvorsorge" im Zuge technischer Entwicklungen?, MMR 2009, 19-24.

Lurtz, Helmut, Betriebliches Datenschutz-Paradox oder betrieblicher Datenschutz-Calculus?, ZD-Aktuell 2021, 05269.

Maaßen, Stefan, „Angemessene Geheimhaltungsmaßnahmen" für Geschäftsgeheimnisse, GRUR 2019, 352–360.

Magiera, Siegfried, Die Grundrechtecharta der Europäischen Union, DÖV 2000, 1017–1026.

Maier, Dominik/ Franzen, Fabian/ Wagner, Manuela, Mehr schlecht als Recht: Grauzone Sicherheitsforschung: Reverse Engineering vor Gericht, DuD 2020, 511–517.

Malgieri, Gianclaudio, 'User-provided personal content' in the EU: digital currency between data protection and intellectual property, International Review of Law, Computers & Technology 2018, 118–140.

Marnau, Ninja, Anonymisierung, Pseudonymisierung und Transparenz für Big Data: Technische Herausforderungen und Regelungen in der Datenschutz-Grundverordnung, DuD 2016, 428–433.

Marsch, Nikolaus, Das europäische Datenschutzgrundrecht: Grundlagen, Dimensionen, Verflechtungen, Tübingen 2018.

Martin, Nicholas/ Mester, Britta Alexandra/ Schiering, Ina/ Friedewald, Michael/ Hallinan, Dara, Datenschutz-Folgenabschätzung: Ein notwendiges „Übel" des Datenschutzes?, DuD 2020, 149–153.

Marx, Matthias/ Zimmer, Ephraim/ Mueller, Tobias/ Blochberger, Maximilian/ Federrath, Hannes, Hashing of personally identifiable information is not sufficient, Sicherheit 2018 2018, 55–68.

Masing, Johannes, Datenschutz - ein unterentwickeltes oder überzogenes Grundrecht?, RDV 2014, 3–9.

Mausbach, Julian, Europäischer Datenschutz und medizinische Forschung in der Schweiz, ZD 2019, 450–454.

McDonald, Aleecia/ Cranor, Lorrie Faith, The cost of reading privacy policies, ISJLP 2008, 543-568.

Mehner, Matthias, Messenger Marketing: Wie Unternehmen WhatsApp & Co erfolgreich für Kommunikation und Kundenservice nutzen, Wiesbaden 2019.

Metzger, Axel, Dienst gegen Daten: Ein synallagmatischer Vertrag, AcP 2016, 817–865.

Meyer, Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage, Baden-Baden 2014.

Meyer-Ladewig, Jens/ Nettesheim, Martin/ Raumer, Stefan von/ Albrecht, Frauke, EMRK: Europäische Menschenrechtskonvention: Handkommentar, 4. Auflage, Baden-Baden 2017.

Michl, Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh — zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, DuD 2017, 349–353.

Molnár-Gábor, Fruzsina, Die Regelung der wissenschaftlichen Forschung in der DSGVO, DSRITB 2018, 159–173.

Monopolkommission, Sondergutachten 68: Wettbewerbspolitik: Herausforderung digitale Märkte - Sondergutachten der Monopolkommission gemäß § 44 Abs. 1 Satz 4 GWB, 2015.

Monopolkommission, Wettbewerb 2018, XXII. Hauptgutachten der Monopolkommission gemäß § 44 Abs. 1 Satz 1 GWB, Stand: 2018.

Monreal, Manfred, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO, ZD 2016, 507–512.

Müller-Broich, Jan D., Telemediengesetz, 1. Auflage, 2012.

National Cyber Security Centre, Coordinated Vulnerability Disclosure: the Guideline, The Hague 2018.

Nebel, Maxi, Die Zulässigkeit der Erhebung des Klarnamens nach den Vorgaben der Datenschutz-Grundverordnung, K&R 2019, 148-152.

Nettesheim, Martin, Grundrechtsschutz der Privatheit, VVDStRL 2011, 7–49.

Ohly, Ansgar, Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, 441–451.

Oppermann, Bernd H./ Stender-Vorwachs, Jutta (Hrsg.), Autonomes Fahren: Rechtsprobleme, Rechtsfolgen, technische Grundlagen, 2. Auflage, München 2020.

Paal, Boris P./ Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, 2. Auflage, München 2018.

Paal, Boris P/ Pauly, Daniel A, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Auflage, München 2021.

Picot, Arnold/ Aaken, Dominik van/ Ostermaier, Andreas, Privatheit als Freiheit, in: *Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander (Hrsg.)*, Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden 2017, 169–180.

Piltz, Carlo, Die Datenschutz-Grundverordnung, K&R 2016, 557-567.

Plath, Kai-Uwe (Hrsg.), Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG, 1. Auflage, Köln 2013.

Plath, Kai-Uwe (Hrsg.), DSGVO/BDSG Kommentar, 2. Auflage, Köln 2018.

Polst, Svenja/ Tolsdorf, Jan/ Dehling, Florian/ Feth, Denis, Verarbeitung von Beschäftigtendaten: – Sichtweisen und Wünsche von Beschäftigten, DuD 2021, 19–22.

Probst, Thomas, Anonymität und Pseudonymität bei biometrischen Identifikationsverfahren, in: *Bäumler, Helmut/Mutius, Albert von (Hrsg.)*, Anonymität im Internet, 1. Auflage, Braunschweig, Wiesbaden 2003, 179.

Pupillo, Lorenzo Maria/ Ferreira, Afonso Henriques Borges/ Varisco, Gianluca, Software vulnerability disclosure in Europe: technology, policies and legal challenges : report of a CEPS Task Force, Brüssel 2018.

Purtova, Nadezhda, Property Rights in Personal Data: a European Perspective, Oisterwijk 2011.

Raabe, Oliver/ Wagner, Manuela, Verantwortlicher Einsatz von Big Data: Ein Zwischenfazit zur Entwicklung von Leitplanken für die digitale Gesellschaft, DuD 2016, 434–439.

Raabe, Oliver/ Wagner, Manuela, Die Zukunft des Datenschutzes im Kontext von Forschung und Smart Data, Stand: November 2016.

Radlanski, Philip, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, Tübingen 2016.

Rentrop, Christopher/ Zimmermann, Stephan/ Huber, Melanie, Schatten-IT ein unterschätztes Risiko, Proceedings of the D· A· CH Security Conference 2015, 291–300.

Richter, Frederick, Die Einwilligung, immer noch Zukunftsmodell?, PinG 2018, 6.

Richter, Philipp, Big Data, Statistik und die Datenschutz-Grundverordnung, DuD 2016, 581–586.

Rihaczek, Karl, Freiheit zu, DuD 2003, 667.

Rockstroh, Sebastian/ Kunkel, Hanno, IT-Sicherheit in Produktionsumgebungen, MMR 2017, 77–82.

Roggan, Frederik, G-10-Gesetz, 2. Auflage, Baden-Baden 2018.

Rohrlich, Michael, Sichere Kommunikation in Krisenzeiten per App und in der Cloud, ZAP 2020, 1265–1274.

Roßnagel, Alexander, Big Data - Small Privacy?, ZD 2013, 562–567.

Roßnagel, Alexander, Pseudonymisierung personenbezogener Daten - Ein zentrales Instrument im Datenschutz nach der DS-GVO, ZD 2018, 243-247.

Roßnagel, Alexander, Kein „Verbotsprinzip“ und kein „Verbot mit Erlaubnisvorbehalt“ im Datenschutzrecht, NJW 2019, 1-5.

Roßnagel, Alexander, Datenschutz in der Forschung, ZD 2019, 157–164.

Roßnagel, Alexander/ Pfitzmann, Andreas/ Garstka, Hansjürgen, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Stand: September 2001.

Roßnagel, Alexander/ Scholz, Philip, Datenschutz durch Anonymität und Pseudonymität Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721-731.

Säcker, Franz Jürgen (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, 7. Auflage, München 2017.

Sahl, Jan Christian, Daten als Basis der digitalen Wirtschaft und Gesellschaft, RDV 2015, 236–242.

Samardzic, Darko/ Becker, Thomas, Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps, EuZW 2020, 646–654.

Sarunski, Maik, Big Data – Ende der Anonymität?: Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern, DuD 2016, 424–427.

Sattler, Dr. Andreas, Personenbezogene Daten als Leistungsgegenstand, JZ 2017, 1036–1046.

Schafft, Thomas/ Ruoff, Andreas, Nutzung personenbezogener Daten für Werbezwecke zwischen Einwilligung und Vertragserfüllung, CR 2006, 499–504.

Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841.

Schätzle, Daniel, Zum Kopplungsverbot der Datenschutz-Grundverordnung, PinG 2017, 203–208.

Scheurle, Klaus-Dieter/ Mayen, Thomas (Hrsg.), Telekommunikationsgesetz: Kommentar, 3. Auflage, München 2018.

Schiering, Ina/ Mester, Britta Alexandra/ Friedewald, Michael/ Martin, Nicholas/ Hallinan, Dara, Datenschutz-Risiken partizipativ identifizieren und analysieren: Datenschutz-Folgenabschätzung in Unternehmen und Behörden, DuD 2020, 161–165.

Schmidt-Kessel, Martin/ Grimm, Anna, Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten, ZfPW 2017, 84-108.

Schmitz, Barbara, Der Abschied vom Personenbezug, ZD 2018, 5-8.

Schmitz, Sandra, Facebook's Real Name Policy, JIPITEC 2013, 190-204.

Schnabel, Christoph, Das Recht am eigenen Bild und der Datenschutz - Die richterrechtliche Dogmatik zur Einwilligung vor dem Hintergrund europarechtlicher Einflüsse des Datenschutzes, ZUM 2008, 657–662.

Schnabel, Christoph/ Freund, Bernhard, „Ach wie gut, dass niemand weiß ..." – Selbstdatenschutz bei der Nutzung von Telemedienangeboten, CR 2010, 718–721.

Schneider, Jana/ Schindler, Stephan, Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten, ZD 2018, 463–469.

Schneider, Jochen, Datenschutz: nach der EU-Datenschutz-Grundverordnung, 2. Auflage, München 2019.

Schneider, Mathias, WhatsApp & Co. Dilemma um anwendbare Datenschutzregeln – Problemstellung und Regelungsbedarf bei Smartphone-Messengern, ZD 2014, 231-237.

Schrader, Paul T., Haftungsfragen für Schäden beim Einsatz automatisierter Fahrzeuge im Straßenverkehr, DAR 2016, 242–246.

Schrey, Joachim/ Kielkowski, Jacek/ Gola, Patricia, Chatten für den Arbeitgeber, MMR 2017, 656-661.

Schrey, Joachim/ Kielkowski, Jacek/ Gola, Patricia, Betriebliche Nutzung von Messenger-Diensten aus datenschutz- und arbeitsrechtlicher Sicht, MMR 2017, 736–740.

Schröder, Markus, Der risikobasierte Ansatz in der DS-GVO, ZD 2019, 503–506.

Schuster, Fabian/ Hunzinger, Sven, Pflichten zur Datenschutzeignung von Software, CR 2017, 141–148.

Schwartmann, Rolf, Die Verantwortlichkeit für die Verarbeitung von Forschungsdaten an Hochschulen, Ordnung der Wissenschaft 2020, 77–84.

Schwartmann, Rolf/ Benedikt, Kristin/ Reif, Yvette, Entwurf zum TTDSG: Für einen zeitgemäßen Online-Datenschutz? Ein Zwischenruf, MMR 2021, 99–102.

Schwartmann, Rolf/ Burkhardt, Lucia, „Schrems II" als Sackgasse für die Datenwirtschaft?, ZD 2021, 235–241.

Schwartmann, Rolf/ Hentsch, Christian-Henner, Eigentum an Daten - Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV 2015, 221–230.

Seeger, Börge, Anmerkung zu E-Mail-Dienst-Anbieter muss IP-Adressen überwachter Accounts herausgeben, Newsdienst Compliance 2019, 23024.

Seidel, Ulrich, Das Grundrecht auf Datensouveränität, ZG 2014, 153–165.

Selk, Robert, EU-DS-GVO: Neue Anforderungen an die Einwilligung?, DANA 2016, 59.

Simitis, Spiros, Die informationelle Selbstbestimmung - Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398-404.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden 2014.

Simitis, Spiros/ Hornung, Gerrit/ Spiecker gen. Döhmann, Indra (Hrsg.), NomosKommentar Datenschutzrecht: DSGVO mit BDSG, 1. Auflage, Baden-Baden 2019.

Solmecke, Christian/ Taeger, Jürgen/ Feldmann, Thorsten (Hrsg.), Mobile Apps: Rechtsfragen und rechtliche Rahmenbedingungen, 1. Auflage, Berlin 2013.

Specht, Louisa, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 288–296.

Specht, Louisa/ Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht: bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, 1. Auflage, München 2019.

Spies, Axel, Anmerkung zu EuGH: Gmail ist kein TK-Dienst, MMR 2019, 516–517.

Spindler, Gerald, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?, JZ 2016, 805–816.

Spindler, Gerald/ Schmitz, Peter (Hrsg.), Telemediengesetz: mit Netzwerkdurchsetzungsgesetz: Kommentar, 2. Auflage, München 2018.

Spindler, Gerald/ Schuster, Fabian (Hrsg.), Recht der elektronischen Medien: Kommentar, 3. Auflage, München 2015.

Spindler, Gerald/ Schuster, Fabian (Hrsg.), Recht der elektronischen Medien: Kommentar, 4. Auflage, München 2019.

Stadler, Thomas, Verstoßen Facebook und Google Plus gegen deutsches Recht?, ZD 2011, 57-59.

statista, Instant Messenger, 2021.

Steege, Hans, Ist die DS-GVO zeitgemäß für das autonome Fahren?, MMR 2019, 509–513.

Stoklas, Jonathan, Datenschutz in Zeiten von Corona, ZD-Aktuell 2020, 07093.

Stroscher, Jan-Philipp, Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) – Was gibt es Neues?, ZD-Aktuell 2021, 05222.

Suwelack, Felix, Datenschutzrechtliche Vorgaben für Homeoffice und Remote Work, ZD 2020, 561–566.

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung: Handkommentar, 2. Auflage, Baden-Baden, Wien 2018.

Taeger, Jürgen/ Gabel, Detlev (Hrsg.), DSGVO - BDSG: Kommentar, 3. Auflage, Frankfurt am Main 2019.

Tiedemann, Jens, Anmerkung zu LAG Niedersachsen: Exzessiver privater E-Mail-Verkehr während der Arbeitszeit, MMR 2010, 639–642.

Veil, Winfried, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip - Eine erste Bestandsaufnahme, ZD 2015, 347–353.

Veil, Winfried, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686–696.

Voitel, Björn, Sind Hash-Werte personenbezogene Daten?: Auf Kollisionskurs mit der EU-DSGVO, DuD 2017, 686–687.

Wagner, Axel-Michael, White Paper E-Mail-Archivierung und DSGVO, 2019.

Wagner, Bernd/ Goeble, Thilo, Freie Fahrt für das Auto der Zukunft?, ZD 2017, 263–269.

Wagner, Manuela, Datenökonomie und Selbstdatenschutz - Grenzen der Kommerzialisierung personenbezogener Daten, 2020.

Wagner, Manuela, Hacken im Dienst der Wissenschaft: Proaktive IT-Sicherheitstests im Angesicht des Strafrechts, PinG 2020, 66–77.

Wagner, Manuela, IT-Sicherheitsforschung in rechtlicher Grauzone, DuD 2020, 111–120.

Wagner, Manuela, Das neue Mobilitätsrecht, 2021.

Weichert, Thilo, Der Personenbezug von Geodaten, DuD 2007, 113–119.

Weichert, Thilo, Die Forschungsprivilegierung in der DS-GVO, ZD 2020, 18–24.

Weinhold, Robert, EuGH: Dynamische IP-Adresse ist personenbezogenes Datum – Folgen der Entscheidung für die Rechtsanwendung, ZD-Aktuell 2016, 05366.

Weißberger, Michael, Das Einsehen kennwortgeschützter Privatdaten des Arbeitnehmers durch den Arbeitgeber, NZA 2003, 1005–1009.

Weisser, Ralf/ Färber, Claus, Rechtliche Rahmenbedingungen bei Connected Car - Überblick über die Rechtsprobleme der automobilen Zukunft, MMR 2015, 506–512.

Wendehorst, Christiane/ Graf von Westphalen, Friedrich, Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, 3745-3750.

Westphal, Miriam/ Wichtermann, Marco, Datenportierung nach Art. 20 DS-GVO, ZD 2019, 191–194.

Westphalen, Friedrich Graf von/ Thüsing, Gregor (Hrsg.), Vertragsrecht und AGB-Klauselwerke, 46. Auflage, München 2021.

Weth, Stephan/ Herberger, Maximilian/ Wächter, Michael/ Sorge, Christoph (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Auflage, München 2019.

Winter, Max, Demokratietheoretische Implikationen des Rechts auf informationelle Selbstbestimmung, in: *Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander (Hrsg.)*, Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden 2017, 37–48.

Wirth, Thomas, Die Pflicht zur Löschung von Forschungsdaten – Urheber- und Datenschutzrecht im Widerspruch zu den Erfordernissen guter wissenschaftlicher Praxis?, ZUM 2020, 585–592.

Wolf, Abraham de, Kollidierende Pflichten: zwischen Schutz von E-Mails und „Compliance" im Unternehmen, NZA 2010, 1206–1211.

Wolff, Heinrich Amadeus/ Brink, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht (BeckOK Datenschutzrech), 25. - 36. Edition, München 2018 - 2021.

Wolff, Heinrich Amadeus/ Kosmider, Thomas, Verarbeitung der E-Mail-Adressen von Mitarbeitern von Vertragspartnern, ZD 2021, 13–18.

Wybitul, Tim, Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte?, ZD 2016, 203-208.

Wybitul, Tim, EU-Datenschutz-Grundverordnung in der Praxis – Was ändert sich durch das neue Datenschutzrecht?, BB 2016, 1077.

Wybitul, Tim/ Böhm, Wolf-Tassilo, E-Mail-Kontrollen für Compliance-Zwecke und bei internen Ermittlungen, CCZ 2015, 133–138.

Wybitul, Tim/ Ströbel, Lukas/ Ruess, Marian, Übermittlung personenbezogener Daten in Drittländer, ZD 2017, 503-509.

Żdanowiecki, Konrad, Data is Cash - Daten als Entgelt, DSRITB 2018, 559–577.

Ziebarth, Lennart/ Elsaß, Lennart, Neue Maßstäbe für die Rechtmäßigkeit der Nutzung von Personenbildnissen in der Unternehmenskommunikation?, ZUM 2018, 578–585.

Ziegler, Stephanie, Typisierte Maßnahmenpläne für IT-Sicherheit im Mittelstand, DuD 2021, 330–335.