Auswahl & Nutzung datenschutzfreundlicher Messengerdienste im Unternehmen – ein Überblick

Angeheizt durch die Diskussionen in Bezug auf Kommunikations- und Kollaborationswerkzeuge der Unternehmen im Home-Office während der Corona-Pandemie, stehen viele Unternehmen vor der Frage, wie sie ihren Beschäftigten eine datenschutzkonforme Nutzung von Messengerdiensten im beruflichen Kontext ermöglichen können, ohne auf die Bedürfnisse zur Geheimhaltung von Geschäftsgeheimnissen zu verzichten.

Um Informationssuchende bei der strukturierten Entscheidungsfindung zu unterstützen, veröffentlichte das FZI die Studie: **Daten- und Geheimnisschutz bei der Kommunikation im Unternehmenskontext**. Die Ergebnisse der Studie fließen in diesen Leitfaden ein.

Für einen schnellen Einstieg bietet dieser Überblick Checklisten, Infografiken sowie ein Entscheidungsdiagramm. Hier wird gezeigt, worauf es im Wesentlichen bei der Auswahl eines geeigneten Messengerdienstes ankommt. Ausgangspunkt ist eine typische Situation im Unternehmen:

Antonia ist Managerin des mittelständischen Unternehmens für intelligente Telekommunikationstechnologie IKT GmbH und benötigt für das mobile Arbeiten eine einfach bedienbare Kommunikationslösung. Ihr ist jedoch aufgrund der Informationsfülle unklar, worauf sie hierbei achten muss und welche Punkte insbesondere bezüglich Daten- und Geheimnisschutz wichtig sind.

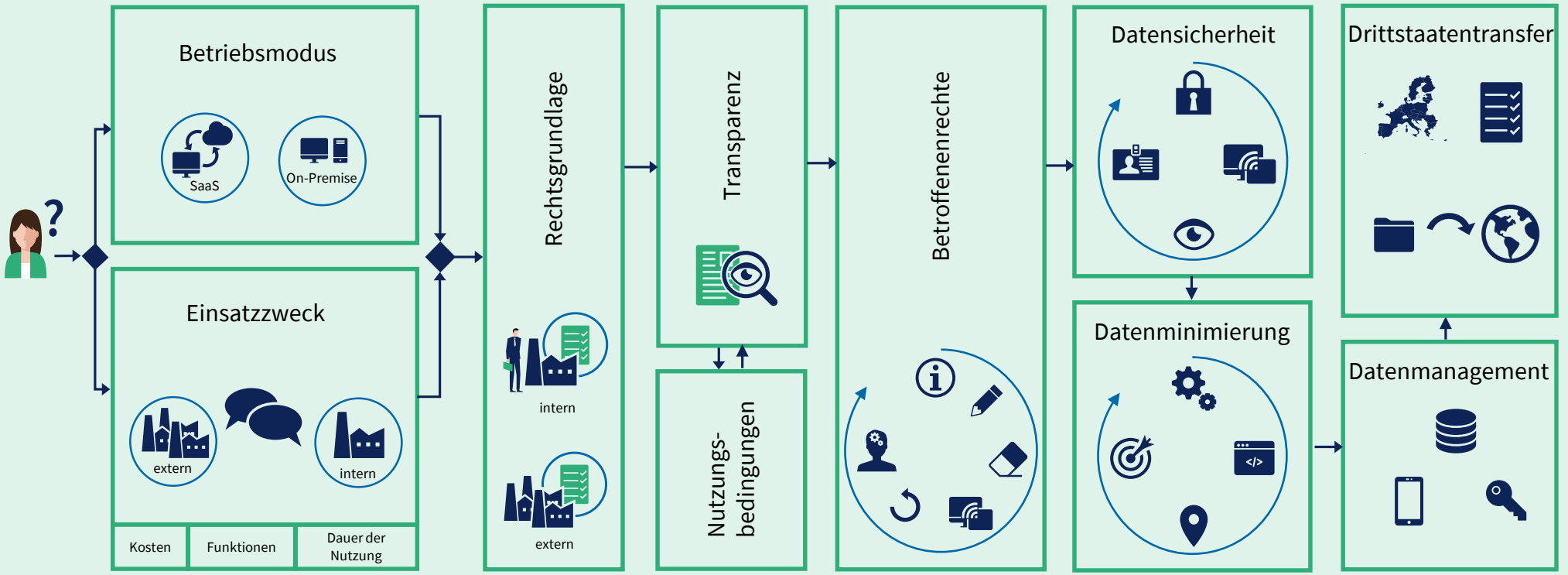
Von anderen Unternehmen weiß sie, dass Sanktionen wegen Datenschutzverstößen drohen, wenn die Beschäftigten eigenmächtig Dienste für Teamkommunikation nutzen, welche das EU-Datenschutzrecht nicht erfüllen. Antonia fragt sich deshalb, worauf beim Einsatz von Messengerdiensten geachtet werden muss, um keine rechtlichen Sanktionen zu riskieren.

Der Einsatz eines Messengers hinterlässt Datenspuren: Antonia muss darauf achten, dass sowohl die Kommunikationsinhalte (Chat-Nachrichten, Voice-Calls, Video-Calls, etc.) als auch die Metadaten über beteiligte Personen, Kontaktverzeichnisse, Zeitpunkte, Dauer und Häufigkeit der Kommunikation, Standorte etc. ausreichend geschützt sind.

Per Messenger werden die Beschäftigten auch Informationen austauschen, die nicht publik werden dürfen, da andernfalls dem Unternehmen Schaden droht – Informationen, die Antonia als Geschäftsgeheimnis vor der Konkurrenz bzw. vor der Öffentlichkeit schützen möchte.

	Datenschutz:	**Geschäftsgeheimnis:**
Worauf sich die Regeln beziehen:	Findet Anwendung, sofern **personenbezogene Daten** einer **betroffenen Person** von einem **Verantwortlichen** verarbeitet werden = alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen Gehen Sie davon aus, dass alle Daten bei der Kommunikation via Messengerdienst personenbezogen sind	Liegt vor, sofern es sich handelt um eine - **nicht ohne weiteres zugängliche** Information (geheim), - von **kommerziellem Wert**, weil sie geheim ist, - mit **berechtigtem Interesse** an der Geheimhaltung und - gesichert durch **angemessene Geheimhaltungsmaßnahmen**. (Diese können technischer, organisatorischer und / oder rechtlicher Natur sein.)
	Dient dem Schutz der Menschen. Rechte stehen der **betroffenen Person** zu: die natürliche Person, auf die sich die Daten beziehen. Personenbezogene Daten können sich auf mehrere betroffene Personen beziehen!	Dient dem Schutz der **Unternehmensinteressen**: Inhaber eines Geschäftsgeheimnisses ist die natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis hat
	Der Verantwortliche **muss** datenschutzrechtliche Vorgaben einhalten. **„Verantwortlicher“** ist die Stelle (natürlich oder juristische Person), die - über den **Zweck** der Datenverarbeitung und - die **Mittel** der Datenverarbeitung allein oder gemeinsam mit anderen entscheidet.	Das Unternehmen **entscheidet selbst**, dem Geheimhaltungsbedürfnis entsprechende Geheimhaltungsmaßnahmen zu treffen.
	Betroffene Personen können bei Verletzung ihrer Rechte Schadensersatz- und Unterlassungsansprüche geltend machen. **Aufsichtsbehörden** können bei Datenschutzverstößen Geldbußen verhängen.	**Rechtsinhaber** und Rechtsinhaberinnen können ggü. rechtswidriger Erlangung und Offenlegung Unterlassungs- und Schadensersatzansprüche geltend machen.
Folge	Das Unternehmen ist bei der Kommunikationsgestaltung rechtlich verpflichtet ein **angemessenes** Datenschutzniveau umzusetzen. „Angemessen“ bezieht sich stets auf die mit der Verarbeitung personenbezogener Daten verbundenen **Risiken** für die Rechte und Freiheiten der betroffenen Personen.	Bereits die Definition als Geschäftsgeheimnis setzt voraus, dass **angemessene** Geheimhaltungsmaßnahmen ergriffen wurden. Ein hohes Schutzniveau des Messengerdienstes wirkt sich somit nicht nur positiv im Hinblick auf die datenschutzrechtliche Bewertung aus, sondern sichert Antonia gleichzeitig die Möglichkeit, gegen Verletzungen ihrer Rechte als Inhaberin von Geschäftsgeheimnissen rechtlich vorzugehen.

Möglicher Entscheidungsweg (schematisch):



Antonia steht vor dem dargestellten Entscheidungsprozess, der ihr bei der Recherche und im Gespräch mit verschiedenen Anbietern als Gedächtnisstütze hilft. Die einzelnen Aspekte werden im folgenden erläutert.

Die Art der Bereitstellung sowie der Einsatzzweck (Kommunikationswege) haben dabei unmittelbar Einfluss auf die datenschutzrechtlichen Anforderungen, die die IKT GmbH als datenschutzrechtlich Verantwortlicher entsprechend berücksichtigen muss. Ihre Möglichkeit Datenschutzprinzipien effektiv umzusetzen, hängt entscheidend davon ab, welche Funktionen der gewählte Dienst bereitstellt.

Antonia ist vor allem wichtig, einen Messengerdienst zu verwenden, der ihr Risiko bzgl. Sanktionen minimiert. Denn sie weiß, dass Bußgelder bis zu 4 % des weltweiten Jahresumsatzes oder 20 Mio. € verhängt werden können und es in der Vergangenheit bereits zu Strafen in Millionenhöhe kam. Sie sorgt sich zudem, dass ihrem Unternehmen Datenschutzverstöße ihrer Beschäftigten zugerechnet werden, wenn sie die Nutzung datenschutzwidriger Dienste erlauben oder dulden würde.

1. Fragen im Vorfeld: Betriebsmodus

Fragen im Vorfeld

Kommunikation:	intern (nur innerbetrieblich)	intern & extern
Installationsumgebung:	Private Endgeräte (App)	Dienstgeräte (App) / Client für Browser
Betriebsart:	SaaS / Online-Dienst	On-Premise

Die einzelnen Bausteine sind unterschiedlich kombinierbar. Das kann die Komplexität erhöhen oder senken!

Es besteht die Pflicht einen geeigneten Dienstanbieter auszuwählen!

Was geregelt werden muss

		Betriebsintern:
AV-Vertrag:	Unterstützung bei Datenschutzpflichten, Datenverarbeitung nur zu Zwecken des Auftraggebers	ggf. individuelle oder kollektive Betriebsvereinbarung/ interne Richtlinien
oder		
Gemeinsame Verantwortlichkeit:	Dienst verfolgt eigene Zwecke; erfordert Zuständigkeits-regel, wer welche Datenschutzpflichten erfüllt	

Umsetzung	Bei Erwerb einer Softwarelizenz zum Eigenbetrieb trifft den Softwarehersteller keine Pflicht zur Einhaltung des Datenschutzrechts.	Bei der **Auftragsverarbeitung** (AV) wird der Dienst als „verlängerter Arm“ des für die Verarbeitung Verantwortlichen tätig.	Bei **gemeinsam Verantwortlichen** gestaltet der Dienstanbieter seine Leistung sehr eigenständig und/oder verfolgt eigene Verarbeitungszwecke.
Garantien	Funktionen zur Umsetzung der Datenschutzpflichten können aber in einem Lizenzvertrag vereinbart werden.	Der AV-Vertrag muss die Pflichten des Auftragnehmers zur Unterstützung bei der Umsetzung der Datenschutzpflichten sowie Kontroll- und Weisungsrechte des Auftraggebers regeln.	Vereinbarung muss umfassende und genaue Regelung der jeweiligen Verantwortlichkeiten beinhalten. Modell steht in Widerspruch zum Grundsatz der Datenminimierung.
Folgen	Das Unternehmen ist allein Verantwortlicher, sollte über ausreichend technische Expertise verfügen.	Das Unternehmen bleibt allein Verantwortlicher, benötigt aber keine eigene Rechtsgrundlage für die AV. Sollte AV-Vertrag rechtlich genau prüfen.	Datenübermittlungen an den Messenger-dienst bedürfen einer eigenen Rechts-grundlage, zusätzlich ist das Tele-kommunikationsrecht zu beachten.

SaaS

Antonia tendiert dazu, eine **SaaS-Lösung** zu verwenden, da ihr keine eigene Infrastruktur zur Verfügung steht und sie davon ausgeht, dass ihre Beschäftigten so eine niedrigere „Einstiegsschwelle“ haben, wenn keine aufwendige Implementierung und Wartung (abgesehen von Updates) für den Dienst nötig sind.

AV-Musterverträge sollten sorgfältig geprüft werden!

Mit Anbieter A müsste statt einem AV-Vertrag eine Vereinbarung über die gemeinsame Verantwortung getroffen werden, deren wesentlicher Inhalt den betroffenen Personen zur Verfügung zu stellen ist.

Für den Messengerdienst kann zusätzlich als **öffentlich zugänglicher elektronischer Kommunikationsdienst** das Telekommunikationsrecht gelten. Dann müssen zusätzliche Aspekte zum Schutz des **Fernmeldegeheimnisses**, der Verarbeitung zum Datenverkehr erforderlicher Daten (Verkehrsdaten) sowie der Verarbeitung von Standortdaten beachtet werden.

Anbieter A

- (!) Dienst behält sich vor das Angebot nach **eigenem Ermessen** zu erweitern / einzuschränken
- (!) Verarbeitung personenbezogener Daten erfolgt zu rechtmäßigen Geschäftsvorgängen im Zusammenhang mit der Bereitstellung der Dienste (z. B. zur Verbesserung des eigenen Angebots)
- (!) Dienst informiert nur, sofern weitere **Unterauftragnehmer** eingebunden werden (keine Zustimmungspflicht)
- (!) Der Anbieter weist auf potenzielle **Datenherausgabepflichten** ggü. Behörden eines Drittlands hin, welche im Widerspruch zu EU-Recht stehen könnten
- (!) Pflichten unter **Vorbehalten** z. B. anderer Sonderregelungen (mit intransparentem / widersprüchlichem Inhalt)

Keine Auftragsverarbeitung

Anbieter B

- ☐ Dienst verfolgt **keine eigenen Verarbeitungszwecke** / Zwecke Dritter
- ☐ Die Datenverarbeitung geht nicht über das zur Erfüllung der AV-Pflichten notwendige Maß hinaus
- ☐ Dienst unterwirft sich **Weisungen** des Auftraggebers
- ☐ Einbindung von **Subunternehmen** nur mit Zustimmung des Auftraggebers
- ☐ Keine ungenehmigte Offenlegung von personenbezogenen Daten ggü. Dritten
- ☐ **Verschwiegenheitsvereinbarung** liegt vor
- ☐ Dienst bietet **Garantien / Zusagen** für technische und organisatorische Schutzmaßnahmen

Auftragsverarbeitung

Wird im Fall einer gemeinsamen Verantwortlichkeit ein AV-Vertrag geschlossen, liegt hierin bereits der erste Datenschutzverstoß!

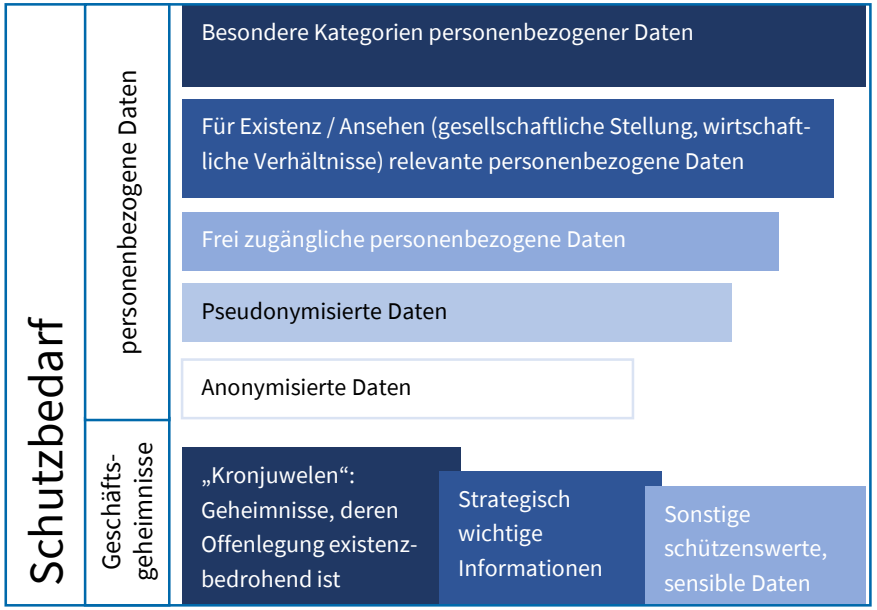
In jedem Fall muss der für die Verarbeitung Verantwortliche (das Unternehmen) für die Einhaltung der Datenschutzpflichten Sorge tragen!

Antonia möchte, dass ihre Beschäftigten den Messengerdienst sowohl **intern** als auch **extern** nutzen können. Eine Nutzung des Dienstes soll sowohl auf privaten Smartphones möglich sein, aber auch auf dem Dienstlaptop.

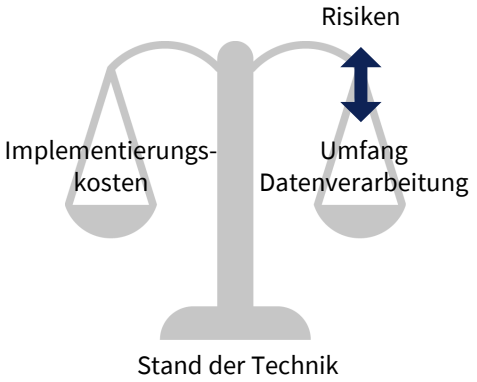
- Beschäftigtendaten
- Daten Dritter
- Geschäftsgeheimnisse?
- Besondere Kategorien?

	Dienstgeräte	Private Endgeräte
Anordnung der Messengerdienstnutzung	✓	✗
Bereitstellung für freiwillige Nutzung	✓	✓
Duldung Messengerdienst-Nutzung im Betrieb	✓	✓
Hoher Schutzbedarf	✓	✗

Um das erforderliche Datenschutz- und Geheimhaltungsniveau zu bestimmen, teilt sie alle potenziell betroffenen Daten in Schutzklassen ein. Sollen rechtsverbindliche Dokumente wie Geschäfts- und Handelsbriefe (z. B. Aufträge, Rechnungen etc.) mit externen Geschäftskontakten ausgetauscht werden? Dann könnte ein **professionelles Datenmanagement** erforderlich werden, was sich im Funktionsumfang widerspiegelt. Fokussiert sie hingegen auf den informellen und/oder privaten Austausch, steht eher die **Vertraulichkeit im Vordergrund**.



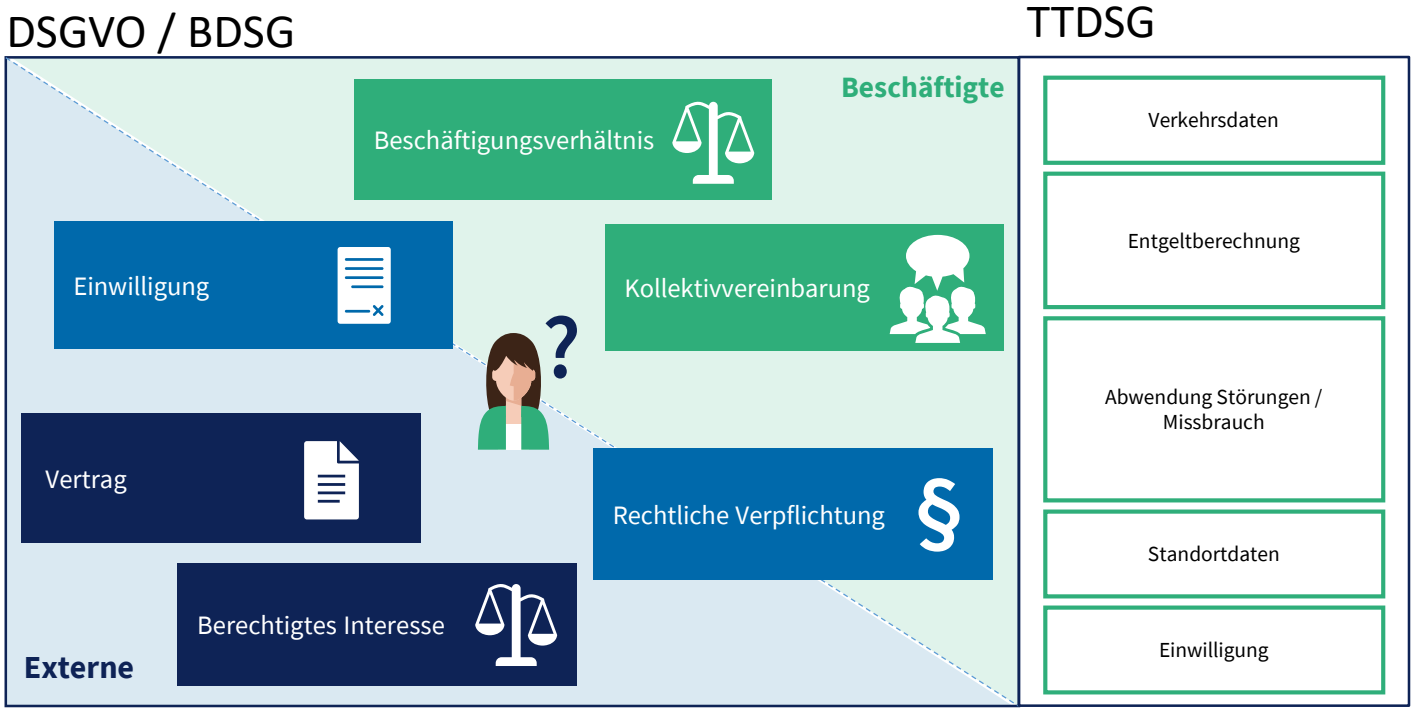
Bei den Kosten eines Diensts ist zu beachten: Maßgeblich ist der Stand der Technik, Unterschreitungen werden kaum allein mit dem Verweis auf höhere Kosten begründbar sein!



Nachdem sie sich entschieden hat, den Dienst sowohl für die interne als auch externe Kommunikation einzusetzen, braucht sie eine **Rechtsgrundlage** für die mit dem Dienst verbundene Verarbeitung personenbezogener Daten.

Antonia weiß, dass Einwilligungen im Beschäftigtenkontext kritisch sein können. Die wichtigsten Punkte, die sie beachten muss, sind Freiwilligkeit, Informiertheit, Bestimmtheit, Widerrufbarkeit sowie Nachweisbarkeit der Einwilligungserklärung.

Einwilligungen müssen **freiwillig** erfolgen, d. h. jederzeit ohne Nachteil verweigert oder widerrufen werden können. Werden Personen von Kommunikationsforen ausgeschlossen („Gruppenzwang“) oder besteht unmittelbarer **Druck** durch den Arbeitgeber (Weisungen), wäre eine Einwilligung kaum freiwillig. Zudem sollte die Nutzungsmöglichkeit eines Dienstes keinesfalls an die Erteilung einer Einwilligung geknüpft werden („Kopplungsverbot“). Daraus folgt, dass Einwilligungen im Messenger- und Unternehmenskontext zwar möglich sind, sich aber nur auf **optional** bereitzustellende Daten oder optionale Funktionen beziehen sollten.



DSGVO: Datenschutz-Grundverordnung
BDSG: Bundesdatenschutzgesetz (hier: § 26 BDSG zur Datenverarbeitung im Beschäftigungsverhältnis)
TTDSG: Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien

Beispiele für Sanktionen bei Verstößen:

- 10 Mio € Bußgeld für unzulässige Videoüberwachung von Beschäftigen [1]
- 35 Mio € Bußgeld für Ausspähen von Beschäftigten [2]

3. Rechtsgrundlage

Jede Verarbeitung personenbezogener Daten muss auf eine Rechtsgrundlage gestützt werden – wobei auch mehrere nebeneinander bestehen/verwendet werden können:

intern

Zu bedenken: Ist die Lösung geeignet, Beschäftigte zu überwachen, muss der Betriebsrat zustimmen!

extern

Beispiel-Sonderfälle: besondere Kategorien personenbezogener Daten, Telekommunikationsdaten nach TTDSG (bei öffentlich zugänglichen Telekommunikationsdiensten)

Zweck Beschäftigungsverhältnis

☐ Die Datenverarbeitung ist für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses **erforderlich**, wenn
- ☐ Funktionen **geeignet** sind, beschriebene Zwecke zu erfüllen,
- ☐ keine datenschutzfreundlicheren Alternativen bestehen,
- ☐ und Risiken in **angemessenem** Verhältnis zum verfolgten Zweck stehen.

Einwilligung

☐ Die Beschäftigten können in die Datenverarbeitung einwilligen, sofern die wie folgt geschieht:
- ☐ **informiert**, für einen oder mehrere Verarbeitungszwecke,
- ☐ **freiwillig** (praktisch nur bei optionalen Daten/Vorgängen),
- ☐ jederzeit ohne Nachteile **widerrufbar**,
- ☐ durch eine **aktive Handlung**, sowie
- ☐ **elektronisch** oder **schriftlich**.

Rechtliche Verpflichtung

☐ Eine rechtliche Verpflichtung im Unionsrecht oder deutschen Recht kann eine Datenverarbeitung zwingend erforderlich machen.
Im Unternehmenskontext sind oftmals einschlägig:
- ☐ **Aufbewahrungspflichten** von Handels- und Geschäftsbriefen (sowie vergleichbaren Dokumenten),
- ☐ **steuerrechtliche Nachweispflichten**.

Kollektivvereinbarung

☐ Es wurde eine Betriebsvereinbarung mit dem Betriebsrat geschlossen.

Vertrag

Bei externen Kommunikationskontakten kann es sich um Beschäftigte anderer Unternehmen oder Privatpersonen handeln. Ein Vertrag / vorvertragliche Maßnahmen legitimieren die Datenverarbeitung, sofern
- ☐ der Vertrag mit der **betroffenen Person** selbst geschlossen wird
- ☐ und die Verarbeitung personenbezogener Daten zur Vertragserfüllung **erforderlich** ist.

Einwilligung

☐ Es gelten die gleichen Wirksamkeitsvoraussetzungen (siehe Kasten links), aber betroffene Personen können in die Datenverarbeitung **formfrei** einwilligen. Der Verantwortliche muss die Einwilligung aber **nachweisen** können.

Rechtliche Verpflichtung

☐ Eine rechtliche Verpflichtung kann eine Datenverarbeitung zwingend erforderlich machen, siehe Kasten links.

Berechtigtes Interesse

☐ Gerade bei Beschäftigten anderer Unternehmen besteht keine direkte Vertragsbeziehung mit der betroffenen Person, sodass auf die Interessenabwägung zurückgegriffen werden muss:
- ☐ Es besteht ein **berechtigtes Interesse** des Verantwortlichen oder eines Dritten,
- ☐ die Datenverarbeitung ist **erforderlich** zur Umsetzung des Interesses und
- ☐ es **überwiegenden** keine schutzwürdigen Belange der betroffenen Person.

Die private Kommunikation soll zwar nicht über den Messengerdienst erfolgen, Antonia geht aber davon aus, dass die Beschäftigten sich trotzdem auch zu privaten Zwecken austauschen werden. Muss sie ein Verbot verhängen und dies auch kontrollieren?

Bisher wurde Unternehmen oft empfohlen, die private Kommunikation über Unternehmensinfrastruktur zu verbieten, da das Unternehmen sonst als **Telekommunikationsdienst** eingeordnet werden könnte, womit zusätzliche Pflichten verbunden wären*. Insbesondere wäre ein arbeitgeberseitiger Zugriff auf Kommunikationsinhalte der Beschäftigten ausgeschlossen.

Aus datenschutzrechtlicher Sicht hat die **DSGVO** Vorrang vor telekommunikationsrechtlichen Spezialregeln, sofern es sich nicht um **öffentlich zugängliche** elektronische Kommunikationsdienste handelt (worunter mittlerweile auch Messenger fallen sollen). Für innerbetriebliche, geschlossene Systeme gilt somit die DSGVO.

Sollte die private Nutzung vorsorglich ausgeschlossen werden?

Besteht Kenntnis über private Kommunikation und wird diese geduldet, kann eine **betriebliche Übung** entstehen, dann muss sich der Arbeitgeber so behandeln lassen, als wäre die Privatnutzung erlaubt worden.

Besser ist klar zu regeln, bezüglich welcher Kanäle Vertraulichkeit erwartet werden kann und auf welcher der Arbeitgeber bspw. aus Compliance-Gründen zugreifen muss. Die Gestattung privater Kommunikation kann hier ggf. an eine **Einwilligung in klar kommunizierte Zugriffsrechte geknüpft** werden.

Antonia entschließt sich, mehrere Kanäle (Gruppen) mit unterschiedlichen Vertraulichkeitsleveln einzurichten:

Privatkommunikation: Arbeitgeberseitige Datenzugriffe ausgeschlossen

Kommunikation mit externen Kunden: Kontrollmöglichkeiten durch leitende Angestellte

Informationsbereitstellung gegenüber Privatpersonen (ohne Antwortmöglichkeit und ohne Personenbezug)

*Ab dem 01.12.2021 gilt in Deutschland das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG).

4. Transparenz

Wer auf Transparenz nicht achtet, riskiert Sanktionen. Außerdem benötigt Antonia als Verantwortliche ausreichend Informationen über Dienste, um Risikobewertungen durchführen zu können. Hier sieht sie, welche Aspekte ihr behilflich sein können.

Datenschutzerklärung

Messenger-Apps sollten über **Datenschutzerklärungen** verfügen, die:
- ☐ vor Installation der App und innerhalb der App jederzeit einsehbar ist,
- ☐ verständlich, vollständig, in deutscher Sprache ist,
- ☐ idealerweise nur den Messenger betreffend (nicht gleichzeitig Webseite, Kontaktformulare etc.) und
- ☐ möglichst keine technischen Begriffe und rechtlichen Fachtermini verwendet sowie kurz und prägnant gehalten ist.

Dokumentation TOMs

Quellcode offen

Transparenzfördernd sind zudem:
- ☐ **Dokumentation** der Sicherheitseigenschaften und technischen Schutzmaßnahmen (TOM),
- ☐ **Sicherheitsaudits**, Prüfungen von dritter Seite (ggf. Zertifikate, Sicherheitsmeldungen wurden veröffentlicht),
- ☐ **Quellcode** ist öffentlich, aktuell und für Dritte reproduzierbar.

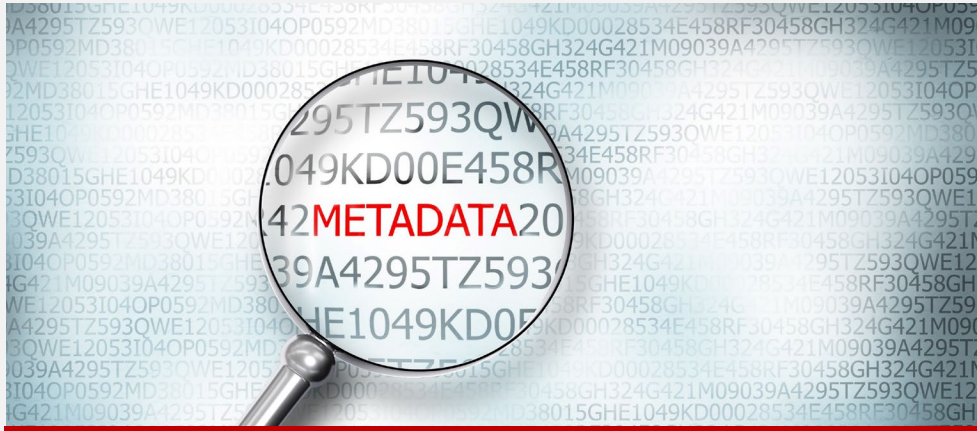
Risikobewertung (DSFA, Zertifikate)

Sofern ein **hohes Risiko** mit der Datenverarbeitung verbunden ist (z. B. bei Standorttracking, Verarbeitung von Gesundheitsdaten etc.) muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden, hier können Dienstanbieter mit Muster-DSFA unterstützen.

Bei normalem/geringen Risiko ist keine DSFA erforderlich → Folge: Pflicht zur regelmäßig wiederholten Einschätzung des Risikos.

Um das mit der Datenverarbeitung durch den Messengerdienst verbundene **Risiko** korrekt einschätzen zu können, muss der Verantwortliche zudem über so viel Informationen wie möglich zur **technischen Funktionsweise** und dabei den **technischen und organisatorischen Schutzmaßnahmen** (TOMs) verfügen. Einige Anbieter beschreiben diese ausführlich. Zudem geben **Sicherheitsaudits** und Prüfungen von dritter Seite Gewissheit, dass Werbeversprechen tatsächlich umgesetzt werden. Sofern Außenstehende ungehinderten Zugriff auf den **Quellcode** haben, wenn dieser Open Source und veröffentlicht ist, können diese jederzeit Sicherheitsüberprüfungen durchführen.

Neben der Datenschutzerklärung sollten Interessenten wie Antonia auch einen Blick in die **Nutzungsbedingungen** werfen. Diese machen meistens deutlich, ob eine berufliche Nutzung möglich ist, oder das Dienstdesign ausschließlich auf die **Privatnutzung** fokussiert. Bei Messengerdiensten für den Privatgebrauch wird eine Nutzung zu Geschäfts- und Berufszwecken oftmals sogar explizit ausgeschlossen. Wird ein Dienst trotzdem geschäftlich genutzt, kann hierin ein **Vertrags- und Urheberrechtsverstoß** liegen, da die Einräumung der Softwarenutzungslizenzen zumeist an die Erfüllung der Nutzungsbedingungen geknüpft ist.



Beispiele für Sanktionen bei Verstößen:

- 50 Mio € wegen Intransparenz bei personalisierter Werbung [3]
- 225 Mio € wegen Intransparenz zur Datenweitergabe an Konzernmutter [4]

5. Betroffenenrechte

Ausnahmen / Nicht anwendbar:

Auskunft	Betroffene Person ist tatsächlich nicht identifizierbar	Rechte Dritter (z. B. Persönlichkeits-, Urheberrechte, Geschäftsgeheimnisse)	
Berichtigung			
Vergessenwerden/ Löschung/Sperrung			Verarbeitung bleibt erforderlich bspw. für rechtliche Verpflichtung
Datenübertrag-barkeit			Keine Einwilligung / kein Vertrag
Widerruf / Widerspruch	Datenverarbeitung beruht nicht auf Einwilligung / Interessenabwägung		
Automatisierte Einzelfall-entscheidung	Entscheidung entfaltet gegenüber betroffener Person keine rechtliche Wirkung oder beeinträchtigt sie nicht in ähnlicher Weise erheblich		

Werden beim Dienstanbieter selbst Daten nur flüchtig verarbeitet und unmittelbar gelöscht, wird der Aufwand zur Umsetzung der Betroffenenrechte regelmäßig geringer ausfallen.

Im Hinblick auf die **lokal archivierten** Daten bzw. Daten auf eigenen Endgeräten (welche der Arbeitgeberseite zuzuordnen sind) muss Antonia allerdings ebenfalls die Rechte der Betroffenen berücksichtigen.

Ein Recht auf Datenübertragbarkeit dürfte ggü. dem Arbeitgeber nicht bestehen. Bei automatisierten Entscheidungen im Einzelfall hat die betroffene Person mindestens das Recht auf eine **menschliche Intervention**. Bei gewöhnlicher Kommunikation via Messenger dürfte dies nicht anwendbar sein.

Beispiel für Sanktionen bei Verstößen:

14.5 Mio € wegen unzureichender Löschmöglichkeiten [5]

Die DSGVO gewährt den betroffenen Personen bestimmte Rechte, über die diese zunächst in der Regel im Rahmen der Datenschutzerklärung aufzuklären ist.

☐ Es muss eine **Kontaktmöglichkeit** zur Wahrnehmung dieser Rechte bereitgestellt werden.

☐ Der Messengerdienstanbieter sollte dabei unterstützen.

Eine fehlende Unterstützung durch Dienstanbieter kann kritisch sein, wenn das Unternehmen selbst keinen Zugriff auf die Server hat. Daher sollte ein Dienstleister gewählt werden, der Serviceleistungen mit anbietet.

☐ Es ist 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 (ggf. mittels Schwärzungen).

Die Tatsache, dass die per Messengerdienst ausgetauschten Daten den Kommunikationsbeteiligten bekannt sind, beschränkt nicht deren Recht auf Auskunft, wozu grundsätzlich auch eine **Kopie der personenbezogenen Daten** zählt.

☐ Unrichtige Daten werden **berichtigt,** indem:
- ☐ die betroffene Person selbstständig unrichtige / unvollständige Daten berichtigen kann oder
- ☐ es ist sichergestellt, dass Berichtigungsersuchen **fristgerecht** umgesetzt werden.

Das Berichtigungsrecht dürfte sich vornehmlich auf die Profildaten beschränken, da es sich bei ausgetauschter Kommunikation regelmäßig um historische und damit nicht „unrichtige“ Daten handelt.

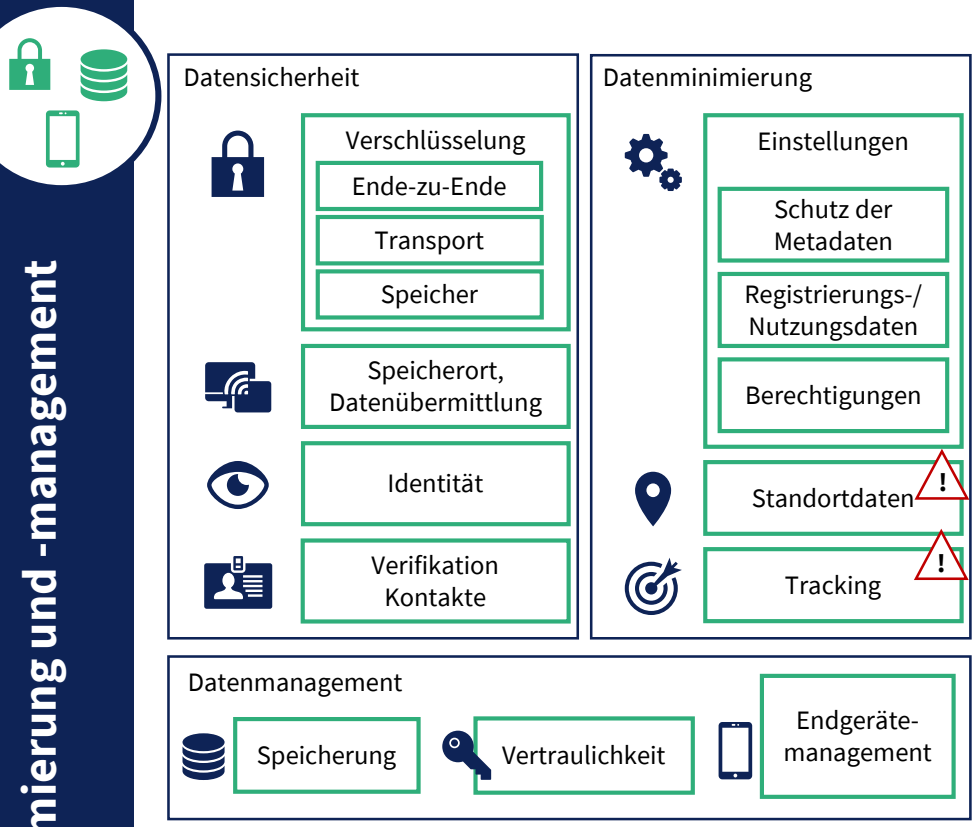
☐ Individuelle Löschanfragen werden fristgerecht beantwortet.

☐ Eine **Sperrung** der Daten erfolgt, sofern bspw. über ein Lösch- / Berichtigungsersuchen entschieden werden muss oder die betroffene Person die Sperrung beantragt.

☐ Sofern **Speicherfristen** definiert sind, können Daten (ggf. automatisch) nach Ablauf gelöscht werden

Ein wesentliches Augenmerk sollte auf die Frage der Datenspeicherung bzw. -löschung gelegt werden: diese ist von den **Einsatzkontexten** abhängig.

6. Datensicherheit, -minimierung und -management



☐ Speicherung verschlüsselt / getrennt von anderen Sachverhalten
☐ Verschlüsselte Backups auf internen Servern oder lokalen Endgeräten?

Zur Sicherheit ist die lokale Speicherung einer Cloud-Lösung vorzuziehen. Insgesamt sollten alle Datenübertragungsvorgänge **transparent** offengelegt und dem **Sicherheitsbedürfnis** entsprechend abgesichert sein.

☐ Identifikation Kontakte: Authentifizierung und Authentisierung

Für eine sichere Kommunikation relevant ist zudem: Welche Mechanismen bietet das System zum **Nachweisen einer Identität** ggü. Kommunikationskontakten? Erfolgt eine Prüfung dieses Identitätsnachweises auf seine Authentizität? Welche **Zugangsdaten** erfordert die App und wie werden diese abgesichert?

☐ Ende-zu-Ende-Verschlüsselung
☐ Transportverschlüsselung (TLS 1.2 / TLS 1.3)
☐ Verschlüsselung gespeicherter Daten

Standardeinstellung
Durchgängig ohne „Lücken“

Mit **durchgängiger Verschlüsselung** sind die Kommunikationsinhalte zumeist bereits gut geschützt, bei der Nutzung von Messengerdiensten fallen allerdings zahlreiche **Metadaten** an. Der beste Schutz der Metadaten besteht darin, diese erst gar nicht zu erheben. Je nach Einsatzzweck kann es im unternehmerischen Kontext allerdings notwendig sein bspw. unter Klarnamen aufzutreten.

☐ Nutzung von IDs, Pseudonyme möglich (soweit im Unternehmenskontext sinnvoll)? Klarname, E-Mail, Mobilnummer optional?
☐ Profilbilder optional, Blurring-Funktion
☐ Aktivitäts- / Anwesenheitsanzeigen, Tippstatus, Lesebestätigungen optional, mindestens deaktivierbar
☐ Kein Adressbuchabgleich oder nur optional als Hash mit unmittelbarer Löschung
☐ Keine Form des Nutzertrackings

Eine einfache, **nutzerfreundliche Bedienbarkeit** von Privatsphäreneinstellungen sichert zudem, dass diese auch von technischen Laien umgesetzt werden können. Insgesamt sollten alle relevanten Sicherheits- und Schutzmechanismen aber bereits **voreingestellt** sein.

Erfasst der Anbieter Standortdaten oder führt Nutzertracking durch, erhöht sich das Risiko der Datenverarbeitung!

☐ Datenzugriffsberechtigungen für Verarbeitungszwecke erforderlich?
☐ Ggf. Mobile-Device-Management

Werden App-Berechtigungen angefordert, sollte stets klar sein, **zu welchem Zweck** und auf **welche personenbezogene Daten** zugegriffen werden kann. Fordert eine App mehr Berechtigungen ein, als notwendig erscheinen, sollte dies stets hellhörig machen.

Beispiele für Sanktionen bei Verstößen:

- 100.000 € gegen KMU wegen unzureichendem Schutz vor unbefugtem Zugriff [6]
- 35 Mio € wegen unerlaubtem Tracking [7]

7. Datentransfer in Drittsaaten

Antonia hat eine Liste mit für sie in Frage kommenden Messengerdiensten erstellt. Hierbei fällt ihr auf, dass viele Anbieter aus den USA kommen oder mit US-amerikanischen Dienstleistern kooperieren. Teilweise wird auf die Einhaltung des **„Privacy Shield“** bzw. „Datenschutzschildes“ verwiesen. Dieser wurde allerdings vom EuGH für unwirksam erklärt, daher ist sie verunsichert, ob sie diese Dienste nun noch in ihrem Betrieb einsetzen darf.

Als Drittstaat / Drittland werden Länder bezeichnet, die **außerhalb der EU bzw. des EWR** liegen. Hierzu zählt bspw. auch die Schweiz, für diese – wie auch einige weitere Staaten – hat die EU-Kommission festgestellt, dass das Datenschutzniveau vergleichbar mit dem der EU ist. Somit bestehen hier derzeit keine Bedenken bei Datenübermittlungen in die Schweiz, und somit sind **keine zusätzlichen Bedingungen** zu erfüllen. Anders ist dies mit den USA: Da insofern gern genutzte, rein rechtlich wirkende **„Transfergarantien“** wie **Standardvertragsklauseln** nach US-amerikanischen Recht nicht durchsetzbar sind, bedarf es weiterer **technischer Schutzmechanismen**. Der Einsatz solcher Dienste ist daher durchaus komplex. Die Verlagerung des Standorts der Datenverarbeitung in die EU löst kaum das Problem, da US-Unternehmen nach amerikanischem Recht (vgl. Cloud Act) zu einem nach EU-Recht rechtswidrigen Datentransfer in die USA verpflichtet sein können.

EU / EWR	Angemessenheitsbeschluss

Soll ein Transfer in ein unsicheres Drittland vermieden werden, gilt Folgendes zu beachten:

- ☐ Sitz des Anbieters in **EU/EWR** oder Land mit **Angemessenheitsbeschluss** der EU-Kommission
- ☐ **Serverstandorte, Ort der Datenverarbeitung** sind in EU/EWR oder Land mit Angemessenheitsbeschluss
- ☐ Anbieter bindet keine **Sub-Dienstleister** aus Drittstaat ein
- ☐ Anbieter und Dienstleister unterliegen keinen **drittstaatlichen Regeln**, die Datentransfer in Drittstaat erfordern (z. B. Cloud Act)

Rechtliche und technische Transfergarantien	Ausnahmen?

Trifft einer der links aufgeführten Punkte nicht zu, so muss mindestens eines der folgenden Kriterien erfüllt sein:

- ☐ Transfergarantien, wie **Standardvertragsklauseln**, **Binding Corporate Rules**, etc. sofern im Drittland **durchsetzbar** (erfordert Analyse Drittstaatenrecht) oder
- ☐ Transfergarantien mit **technischen Zusatzmaßnahmen**, z. B.:
  - ☐ Datenzugriffe ausschließende Verschlüsselung
  - ☐ Pseudonymisierung (ohne singling-out-Möglichkeit)
  - ☐ Split / multi-party processing
- ☐ **Ausnahmen**, die Transfer rechtfertigen, z. B. **ausdrückliche Einwilligung** (enge Voraussetzungen, kaum in Beschäftigungskontext realisierbar).

Liste mit Angemessenheitsbeschlüssen unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

8. Dokumentation und unternehmensinterne Organisation

Antonia beschäftigt weniger als 250 Beschäftigte. Diese befassen sich nur sehr gelegentlich mit der Verarbeitung personenbezogener Daten. Jedoch sind die Mitarbeiter hochspezialisiert und ihr Wissen Teil des Wertes des Unternehmens.

Das Datenschutzniveau des Dienstes ist bereits sehr hoch, **Risiken** für Betroffene **gering**

☐ Antonia muss aufgrund der geringen Anzahl an Beschäftigten **kein** Verzeichnis von Verarbeitungstätigkeiten erstellen.

☐ Sie benötigt aber ausreichend Information zur Durchführung der **Risikobewertung**, diese sollte sie dokumentieren und regelmäßig wiederholen.

☐ Sofern sie Einwilligungen einholt, stellt sie sicher, dass sie die Erklärungen nachweisen kann.

Der Messenger ermöglicht keine Überwachung der Beschäftigten. Eine Verhaltensregelung ist nicht erforderlich.

Kein Mitbestimmungsrecht des Betriebsrats

Das Datenschutzniveau des Dienstes ist sehr gering, **Risiken** für Betroffene **hoch**

☐ Antonia benötigt ausreichend Information zur Erstellung eines **Verzeichnisses** von **Verarbeitungstätigkeiten.**
☐ Sie benötigt zudem ausreichend Information zur Durchführung einer **Risikobewertung,** diese sollte sie dokumentieren und regelmäßig wiederholen.
☐ Zudem muss sie eine **Datenschutz-Folgenabschätzung** durchführen.
☐ Sofern sie Einwilligungen einholt, stellt sie sicher, dass sie die Erklärungen nachweisen kann.

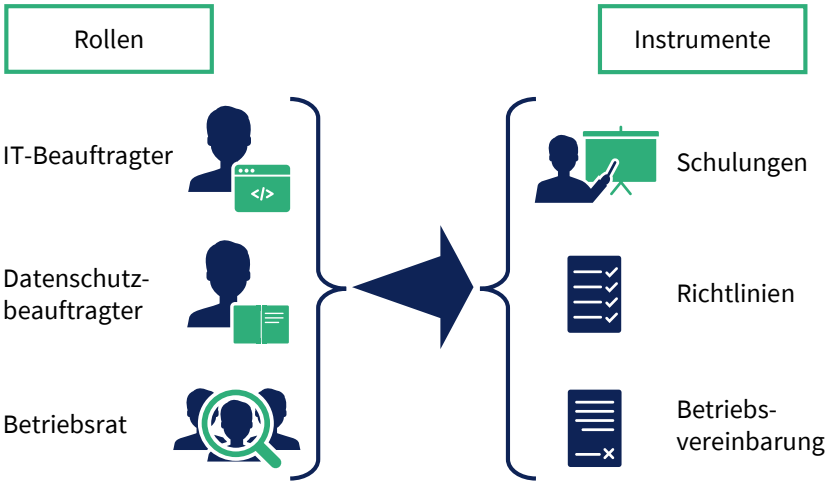
Der Messenger ermöglicht die Überwachung der Beschäftigten und / oder es muss eine Verhaltensregelung aufgestellt werden.

Mitbestimmungsrecht des Betriebsrats

Die gezeigten Transparenz sowie Datensicherheits- und Datenminimierungsmechanismen des gewählten Dienstes haben direkten Einfluss auf den Umfang der Pflichten, die das Unternehmen nun bei der praktischen Einführung des Messengerdienstes treffen. Je mehr Punkte erfüllt wurden, desto niedriger ist das Risiko und desto leichter fallen Dokumentations-, Kontroll- und Organisationsanforderungen.

Antonia hat einen betrieblichen Datenschutzbeauftragten, IT-Beauftragten und einen Betriebsrat in ihrem Unternehmen. Diese Rollen sind gegebenenfalls alle mit einzubeziehen!

Je mehr risikominimierende Aspekte bei der Entscheidungsfindung nicht berücksichtigt werden, umso aufwändiger wird die interne Organisation: Schulungen, Aufstellen interner Richtlinien zur Messengernutzung, ggfs. Betriebsvereinbarung und umso mehr Parteien müssen mit einbezogen werden. Zusätzlich müssen Aspekte bzgl. des Geheimnisschutzes berücksichtigt werden. Auch hierfür sind interne Regelungen notwendig.



Ob ein Messengerdienst zur Überwachung geeignet ist, hängt davon ab, welche Zugriffsmöglichkeiten der Arbeitgeber hat und ob diese eine Leistungs- und Verhaltenskontrolle ermöglichen. So können bspw. Aktivitäts-/Anwesenheitsanzeigen, Lesebestätigungen oder Tippstatus zeigen, wann jemand welcher Arbeit nachgeht und wie lange hierfür benötigt wird.

Um ihr Risiko zu minimieren, entscheidet sich Antonia für eine datenschutzfreundliche Alternative, die so wenig Daten verarbeitet wie möglich, um alle relevanten Funktionen für die Kommunikation im bzw. mit dem Unternehmen zu erfüllen, und zudem personenbezogene Daten auf Dienstservern nur für kurze Zeit zwischenspeichert.

Folgende wichtige Aspekte hat sie sich für die Umsetzung ihres Projekts gemerkt, welche sie auch beim Abschluss des AV-Vertrags bedenken sollte.

Checkliste: Achtung, wenn beim geplanten Einsatz eines Messengerdienstes einer der folgenden Punkte nicht erfüllt werden kann …

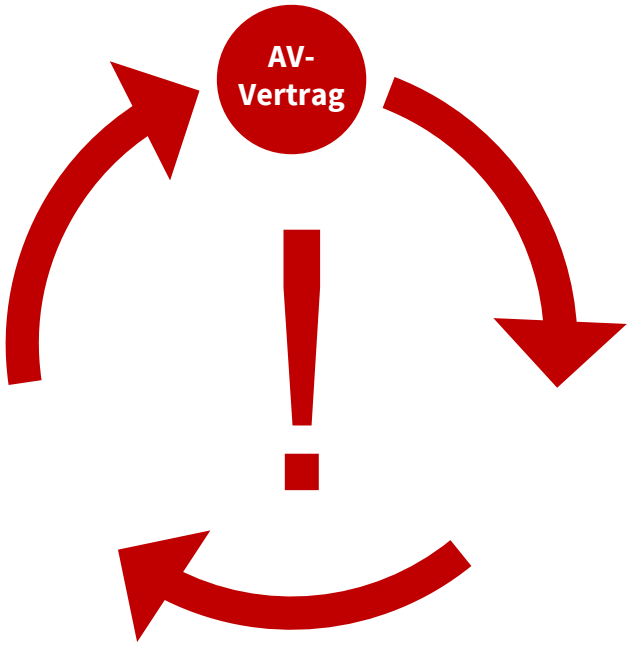
… es kann auf Sie als Verantwortlichen negativ zurückfallen!

Rechenschaftspflicht:
Keine Dokumentation zur Nachweiserbringung

Richtigkeit:
Keine Möglichkeit inkorrekte Daten zu berichtigen (Betroffenenrechte)

Integrität und Vertraulichkeit:
(Datensicherheit)
Keine lückenlose Verschlüsselung
Keine Möglichkeit zur Verifikation von Kontakten

Speicherbegrenzung:
Keine Löschung nach Nutzungsende
Löschregeln nicht umsetzbar (unter Berücksichtigung der geschäftlichen Aufbewahrungspflichten)



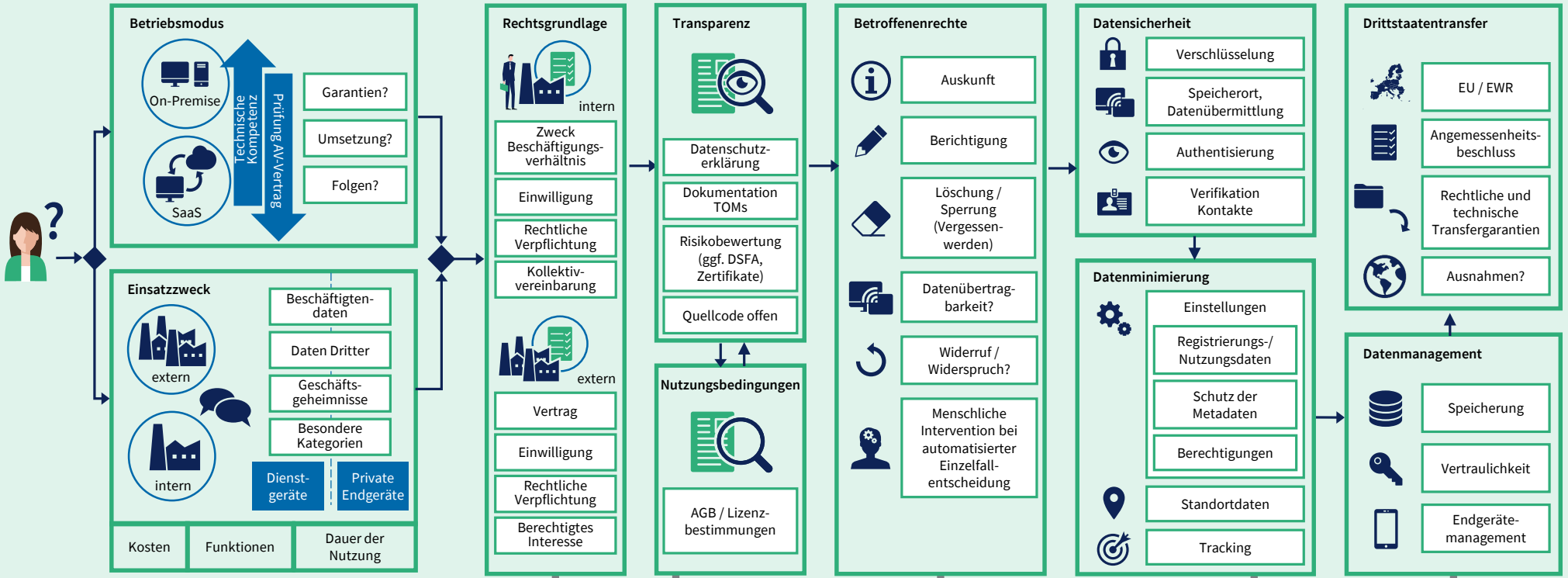
Rechtmäßigkeit:
Unklar, auf welcher Rechtsgrundlage Datenverarbeitung beruht, keine Unterscheidung erforderlicher und optionaler Daten (Einwilligung)

Transparenz:
fehlende oder unzureichende Datenschutzerklärung, fehlende Mitwirkung des Dienstanbieters bei Auskunftsersuchen

Zweckbindung:
Verfolgung eigener Zwecke durch Messengerdienstanbieter
Weiterverarbeitung zu anderen Zwecken

Datenminimierung:
Anfrage von nicht notwendigen Daten (z. B. Kontaktbuch), nicht notwendigen Datenzugriffsberechtigungen sowie fehlende Schutzmaßnahmen (z. B. Datenübermittlung von Adressdaten in Klartext, Speicherung länger als erforderlich)

Der Entscheidungsprozess (Zusammenfassung)



Für die zur Kommunikationsübermittlung erforderlichen Daten beruft sich Antonia v.a. auf die Arbeits-/Verträge; für das Zeigen eines Profilbilds ihrer Beschäftigten holt sie zusätzlich Einwilligungen ein.

Antonia muss als für die Verarbeitung Verantwortliche eine **eigene Datenschutzerklärung** mit den Kontaktdaten der IKT GmbH und ihrem Datenschutzbeauftragten erstellen und zugänglich machen. Inhaltlich freut sie sich darüber, dass sie weitgehend die Erklärung des von ihr gewählten Messengerdienstes übernehmen kann.

Da der von ihr gewählte Dienst personenbezogene Daten nur lokal speichert, muss Antonia Auskunfts- und Löschrechte im Hinblick auf die **in Endgeräten gespeicherten Daten** umsetzen. Die Definition bestimmter Gruppen unterstützt sie dabei.
Unrichtige Daten können die Dienstnutzenden selbständig berichtigen sowie ihr Profilbild löschen.

Der von Antonia gewählte Dienst übertrifft die Sicherheitsgarantien aller anderen Dienste. Damit ist Antonia auf der sicheren Seite und muss sich keine Gedanken über eigene Sicherheitsvorkehrungen machen. Das hilft ihr auch beim Schutz ihrer Geschäftsgeheimnisse.

Antonia wählt einen Dienst aus Europa, welcher auch keine **Subunternehmer** / Dienstleister aus Drittstaaten einsetzt.

Zum Datenmanagement hat sie **interne Richtlinien** erlassen, die sie mit Hilfe des Dienstes umsetzen kann.
Diese hat sie zuvor mit ihrem Betriebsrat abgestimmt.

Quellen

[1]
https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html

[2]
https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren

[3]
https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[4]
https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry

[5]
https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen

[6]
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf

[7]
https://www.dsgvo-portal.de/dsgvo-bussgeld-gegen-amazon-europe-core-2020-12-09-FR-772.php

Herausgeber
FZI Forschungszentrum Informatik
Stiftung des bürgerlichen Rechts

Themenfeld Recht

Haid-und-Neu-Str. 10−14
76131 Karlsruhe
Tel: +49 721 9654-0
Fax: +49 721 9654-909

www.fzi.de

Veröffentlichung: November 2021
Version 1.0

Bilder
Adobe Stock/ Jane Kelly (Titel)
Adobe Stock/ Imillian (Seite 10)

Diese Informationsbroschüre wurde von der Threema GmbH, Schweiz, finanziell unterstützt, wobei die Verantwortung über die Inhalte allein beim FZI lag. Sie gibt die Sichtweise der Autor*innen wieder; eine Einflussnahme auf die Ergebnisse durch den Auftraggeber erfolgte nicht.