Leitfaden Datenschutz und Datensicherheit

SVDGV e.V.

Version 1.2

Stand: 20.5.2021

Wichtige Hinweis:

1.) Dieses Dokument ist ausschließlich für den internen Gebrauch von Verbandsmitglieder des SVDGV e.V. vorgesehen. Eine Herausgabe an Dritte ist untersagt.

2.) Bitte beachten Sie, dass dieses Dokument nur die allgemeine Rechtslage wiedergibt und keine Rechtsberatung darstellt. Das Dokument wurde mit größter Sorgfalt erstellt, erhebt jedoch keinen Anspruch auf Vollständigkeit oder Richtigkeit. Änderungen und Updates sind in der Revisionstabelle nachvollziehbar.

Revisionsübersicht

Versionsnummer	**Beschreibung**	**Datum**	**Autor(en)**
1.3	● Aktualisierung Kapitel 8.2.3.2 bezüglich der neuen EU-Standardvertragsklauseln	22.11.2021	@Alexander Burnhauser
1.2	● Hinweis hinzugefügt, dass der Leitfaden nur für den internen Gebrauch von Verbandsmitgliedern vorgesehen ist	20.5.2021	@Alexander Burnhauser
1.1	● Aktualisierung Kapitel 8.4. (Cloud Anbieter) mit neuer Interpretation BfArm zu Sicherheitsmaßnahmen (Verschlüsselung **und** Zusicherung) ● Konsistente Verwendung des Begriffs “Standardvertragsklauseln” (statt “Standarddatenschutzklauseln”)	16.02.2021	@fmoser
1.0	● Initialer Dokument Launch	31.03.2021	#ak_datenschutz

Inhaltsverzeichnis

7. Technische und Organisatorische Maßnahmen

- **7.1** Definition
  - **7.1.1** Technische Maßnahmen
  - **7.1.2** Organisatorische Maßnahmen
  - **7.1.3** Auswahlkriterien
- **7.2** Beispiele wichtiger Maßnahmen
  - **7.2.1** Bewertung der Passwortstärke
  - **7.2.2** Beispiel Multifaktor Authentisierung
  - **7.2.3** Management mobiler Geräte
- **7.1** Beispiel/ Auszug einer Checkliste zur Überprüfung der TOMs

8. Umgang mit Auftragsverarbeitenden

- **8.1** Abgrenzung zu eigenständiger und gemeinsamer Verantwortlichkeit
- **8.2** Eignungsprüfung
  - **8.2.1** Vertragsprüfung
    - **8.2.1.1** AV-Vertrag (AVV)
    - **8.2.1.2** Hauptvertrag
  - **8.2.2** Technische und organisatorische Maßnahmen
    - **8.2.2.1** TOMs im Rahmen des AVV
    - **8.2.2.2** Zertifikate als Nachweise (ISO 27001, SOC I, SOC II, ISO 27017, ISO 27018)
  - **8.2.3** Auftragsverarbeitung in Drittländern
    - **8.2.3.1** Verbindliche interne Datenschutzklausel
    - **8.2.3.2** Standardvertragsklauseln
  - **8.2.4** Audit
- **8.3** Unterauftragsverarbeitung
- **8.4** Informationen zur Nutzung von Cloud-Infrastrukturen
  - **8.4.1** Hintergrund und bisherige Interpretation des BfArM
  - **8.4.2** Handreichung des BfArM am 28.01
  - **8.4.3** Mögliche Ansätze zur technischen Umsetzung
    - **8.4.3.1** Sonderthema “3rd Party Appstore” (d.h. Google Play, Apple Appstore)
    - **8.4.3.2** Welche Möglichkeit des eigenen Key Managements sollte ich verwenden?

1. Begriffsbestimmung

1.1. Verantwortlicher

Bei dem “Verantwortlichen” gemäß Art. 4 DSGVO handelt es sich um 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. (mehr zum Thema gemeinsame Verantwortlichkeit unter 9.)

1.2. Verarbeitung

Unter Verarbeitung versteht man jede 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;

1.3. Personenbezogene Daten

Personenbezogene Daten (pbDs) umfassen alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

1.4. Gesundheitsdaten

Gesundheitsdaten sind 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; Entsprechend sind alle Nutzerdaten die im Zusammenhang mit einer Gesundheitsdienstleistung verarbeitet werden, Gesundheitsdaten.

Gesundheitsdaten sind personenbezogene Daten besonderer Kategorien und unterliegen einem grundsätzlichen Verarbeitungsverbot. Zur Aufhebung dieses Verbots sieht das Gesetz jedoch eine Reihe von Ausnahmetatbeständen vor. (mehr zu diesem Thema unter 5.)

1.5. privacy by design

Bereits bei der Konzipierung von Anwendungen ist eine Umsetzung zu wählen, bei der die Daten der Nutzer bestmöglich geschützt werden und es müssen organisatorische sowie technische Sicherheitsmaßnahmen implementiert werden, um versehentliche oder unrechtmäßige Zerstörung, Verlust, Änderung, unbefugte Offenlegung oder Zugriff auf die

Daten des Nutzers zu vermeiden. Zur Ausübung der Rechte des Betroffenen sollen benutzerfreundliche Anwendungen bereitgestellt werden, mittels derer dem Nutzer eine Ausübung seiner Rechte leicht fällt.

1.6. privacy by default

Wird dem Nutzer eine Auswahl hinsichtlich des Schutzumfangs angeboten und dieser wählt keine Option aktiv aus, ist als Voreinstellungen standardmäßig die am wenigsten datenschutzinvasive Option festzulegen. Nutzer sollen möglichst einzelnen Anwendungen gesondert zustimmen könne, um nur für die von ihnen tatsächlich genutzten Teilanwendungen einer Datennutzung zustimmen zu müssen. Hierzu soll der Nutzer möglichst einfach seine Einstellungen einsehen und bearbeiten können.

2. Allgemeine Rechtliche Anforderungen

2.1. Notwendigkeit eines DSB

Pflicht zur Bestellung

Sowohl die DSGVO als auch das BDSG sehen für bestimmte Verarbeitungstätigkeiten eine Pflicht zur Bestellung eines Datenschutzbeauftragten (DSB) vor. Dieser soll den Verantwortlichen bezüglich der Einhaltung der datenschutzrechtlichen Vorgaben beraten und unterstützen. Art. 37 DSGVO sieht für nicht-öffentliche Stellen die Bestellung eines DSB vor, wenn deren Kerntätigkeit

- eine umfangreiche, regelmäßige und systematische Überwachung von Betroffenen erfordert oder
- in einer umfangreichen Verarbeitung von besonderen Kategorien von Daten (Art. 9 DSGVO) oder solcher über strafrechtliche Verurteilungen (Art. 10 DSGVO) besteht.

Die umfangreiche Verarbeitung von Gesundheitsdaten im Rahmen von Gesundheits-Apps dürfte in den meisten Fällen bereits nach dieser Regelung eine DSB-Pflicht begründen.

Zusätzlich dazu formuliert § 38 BDSG weitere Gründe einer Pflicht zur DSB-Bestellung, nämlich dann, wenn

- mindestens 20 Personen ständig mit der einer Verarbeitung von personenbezogenen Daten betraut sind,
- eine Datenschutz-Folgenabschätzung für die Verarbeitung durchgeführt werden muss, oder
- eine geschäftsmäßige Verarbeitung zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung vorliegt.

Die Bestellung des DSB und jede spätere Änderung auf dieser Position sind an die zuständige Datenschutzaufsichtsbehörde zu melden. Diese bieten hierfür auf ihren Websites meist ein eigenes Formular an.

Bei einem DiGa-Hersteller ist grundsätzlich immer davon auszugehen, dass ein DSB benannt werden muss.

Stellung und Funktion des DSB

Als DSB können sowohl eigene Mitarbeiter als auch Externe bestellt werden. Voraussetzung ist insofern nur, dass der Bestellte über ausreichende Sachkunde auf dem Gebiet des Datenschutzes verfügt (Art. 37 Abs. 5 DSGVO). Eine bestimmte Zertifizierung ist nicht vorgeschrieben. Die Sachkunde muss aber dargelegt werden können. Soll nicht auf externe Experten zurückgegriffen werden bietet sich eine Datenschutzschulung an, wie sie bspw. der TÜV anbietet. Bei der Bestellung eines Mitarbeiters als DSB ist zu beachten, dass für diesen dann Kündigungsschutz bis ein Jahr nach Abbestellung besteht. Der DSB muss in seiner Tätigkeit unabhängig und frei von Weisungen agieren können (Art. 38 Abs. 3 DSGVO) und direkt an die Geschäftsführung berichten.

2.2. Datenschutzvorfälle und Meldepflichten

Art. 33 und 34 DSGVO sehen Meldepflichten für Datenschutzvorfälle vor. Während Art. 33 DSGVO die Meldepflicht an die zuständige Aufsichtsbehörde regelt, sieht Art. 34 DSGVO erstmals eine Meldung direkt an die Betroffenen vor. Ausgangspunkt beider Meldepflichten ist die Verletzung des Schutzes personenbezogener Daten. Der Begriff ist in Art. 4 Nr. 12 DSGVO legal definiert als „*Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt*".

2.2.1. Meldepflicht nach Art. 33 DSGVO

Eine Verletzung des Schutzes der personenbezogenen Daten (Datenpanne) muss grundsätzlich immer an die zuständige Aufsichtsbehörde gemeldet werden, es sei denn, diese führt voraussichtlich nicht zu einem Datenschutz-Risiko für die betroffenen Personen. Das kann z. B. der Fall sein, wenn das entstandene Risiko durch Gegenmaßnahmen beseitigt wird oder Unbefugte mit den von der Panne betroffenen Daten nichts anfangen können. Einige Aufsichtsbehörden der Länder und die Artikel 29-Gruppe haben zur Frage, was eine meldepflichtige Panne darstellt, verschiedene Hinweise veröffentlicht[1], die eine sinnvolle Orientierung für die Beurteilung bieten können.

Die Meldung muss in der Regel innerhalb von 72 Stunden ab interner Kenntnisnahme der Panne erfolgen, eine Verzögerung muss der Verantwortliche rechtfertigen können. Die Meldefrist ist unabhängig von Wochenenden und Feiertagen. Die Datenschutzbehörden halten auf ihren Websites typischerweise Online-Formulare zur Meldung von Datenpannen bereit. Die Mindestinhalte einer Meldung sind in Art. 33 Abs. 3 geregelt:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (Datenpanne);
- 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.

---

[1] Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 (WP250rev.01), abrufbar unter https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html, konkrete Beispiele ab S. 36; Orientierungshilfe des LDA Bayern, abrufbar unter: https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf; FAQ des LDI Niedersachsen, abrufbar unter https://lfd.niedersachsen.de/startseite/infothek/faqs_zur_ds_gvo/meldung-von-datenschutzverstoeen-167312.html

Wenn nicht alle Informationen vorab verfügbar sind, können diese nach der initialen Meldung auch nachgereicht werden. Relevant ist insofern, dass eine Erstmeldung innerhalb der Frist erfolgt.

Wenn in die Verarbeitung Auftragsverarbeiter mit einbezogen werden, kann die Panne naturgemäß auch bei diesen auftreten. Der Auftragsverarbeiter ist dann selbst aus Art. 33 Abs. 2 DSGVO verpflichtet, die Panne unverzüglich an den Verantwortlichen, nicht direkt an die Aufsichtsbehörde zu melden. Der Auftragsverarbeiter muss jede Datenpanne an den Verantwortlichen melden, eine Ausnahme wegen eines fehlenden Risikos besteht nicht. Die Meldepflicht muss zusätzlich auch in der Vereinbarung zur Auftragsverarbeitung geregelt werden. Der Verantwortliche erhält Kenntnis von der Panne in der Regel erst mit der Mitteilung durch den Auftragsverarbeiter[2]. Da die 72-Stunden-Frist für den Auftragsverarbeiter nicht gilt, empfiehlt es sich, hier eine feste zeitliche Grenze für die Meldung zu verankern[3].

Meldepflicht nach Art. 34 DSGVO

Die Meldepflicht gegenüber dem Betroffenen nach Art. 34 DSGVO folgt den entgegengesetzten Voraussetzungen wie die Meldepflicht gegenüber der Aufsichtsbehörde. Eine Datenpanne muss nur dann gemeldet werden, wenn diese voraussichtlich zu einem hohen Risiko für den Betroffenen führt. Darüber hinaus regelt Art. 34 Abs. 3 DSGVO weitere Ausnahmen einer Meldepflicht, nämlich wenn:

- geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese auf die betroffenen personenbezogenen Daten angewendet wurden,
- durch nachfolgende Maßnahmen sichergestellt wurde, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht,
- die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre.

Der letzte Fall des unverhältnismäßigen Aufwandes ist insbesondere bei einer großen Anzahl von Betroffenen gegeben. Hier kann alternativ eine öffentliche Bekanntmachung erfolgen. In jedem Fall hat die Meldung in einer einfachen Sprache zu erfolgen.

---

[2] WP250rev.01., S. 15.

[3] Der Entwurf einer Vereinbarung zur Auftragsverarbeitung der EU-Kommission sieht eine 48 Stunden-Frist vor, abrufbar unter: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Data-protection-standard-contractual-clauses-between-controllers-processors-located-in-the-EU-implementing-act- (Sec. 7.3. lit a).

3. Rechtsgrundlage für die Verarbeitung personenbezogener Gesundheitsdaten

Innerhalb der DSGVO gibt es verschiedene Rechtsgrundlagen, auf denen eine Verarbeitung personenbezogener Daten verschiedener Kategorien legal erfolgen kann. Oftmals kommt es hier zu Überschneidungen der Anwendungsbereiche, so dass es vor allem darauf ankomme, die für Anwendungsfall geeignetste, nachhaltigste, und v.a. rechtssichere Grundlage zu finden.

3.1 Allgemeine Grundsätze (Artikel 5 DS-GVO)

Bei der Verarbeitung von personenbezogenen Daten muss im Allgemeinen immer auf folgende Punkte geachtet werden.

- auf rechtmäßige, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise (Rechtmäßigkeit)
- nur für festgelegte, eindeutige und legitime Zwecke (d.h. eine Weiterverarbeitung für andere Zwecke als ursprünglich “vereinbart” ist nicht zulässig)
- dem Zweck angemessen sowie auf das notwendige Maß beschränkt (“Datenminimierung”)
- sachlich richtig und auf dem neuesten Stand. Unrichtige Daten (im Hinblick auf den Zweck) müssen korrigiert oder gelöscht werden (“Richtigkeit”)
- nur für den erforderlichen Zeitraum des Zwecks (“Speicherbegrenzung”)
- angemessene Sicherheit der Daten vor unrechtmäßiger Verarbeitung, Verlust, Schädigung durch geeignete technische und organisatorische Maßnahmen

Als Hersteller (bzw. als Verantwortlicher i.S. der DS-GVO) ist man verpflichtet, diese Grundsätze einzuhalten und nachweisen zu können (“Rechenschaftspflicht”)

3.2 Relevante Rechtsgrundlagen für Hersteller

Die folgenden Tabellen geben eine Übersicht der gängigsten Rechtsgrundlagen für die Verarbeitung personenbezogener Daten in Abhängigkeit der Kategorie.

Wichtig: Es gibt bei den Rechtsgrundlagen keine Hierarchie oder Auswahlmöglichkeit. Die anwendbare Rechtsgrundlage muss auf Basis der vorliegenden Umstände richtig bestimmt werden.

Je nach Art der Daten, welche verarbeitet werden, sind insbesondere Artikel 6 (für personenbezogene Daten, die nicht zur Kategorie der besonderen Daten gehören) bzw. Artikel 9 (für personenbezogene Daten, die zur Kategorie der besonderen Daten (z.B. Gesundheitsdaten) gehören), relevant. Bei letzterer bedarf es i.d.R. einer Einwilligung. Soweit die Daten zur Durchführung eines Vertrags mit dem Betroffenen (z.B. einem Versicherten) erforderlich sind, kann die Einwilligung ausnahmsweise an den Vertragsschluss gekoppelt werden. Ist die Verarbeitung hingegen bereits aufgrund nationaler (z.B. arbeitsrechtlicher) Vorschriften gesetzlich vorgeschrieben, bedarf es keiner Einwilligung

mehr. Die Verarbeitung kann sich auch aus speziellen Gesetzen wie der DiGaV ergeben (siehe dazu 4.)

Rechtsgrundlage **(fett markiert sind die gängigsten für Hersteller von Gesundheitsanwendungen)**	**Beispiel/Kommentar**
Einwilligung **(Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a)**	**- Anmeldung Newsletter** **- Anmeldung DiGA** **- siehe Verarbeitungszwecke 5**
Zur Vertragserfüllung notwendig **(Art. 6 Abs. 1 lit. b)**	**- Identifikationsdaten für Anmeldung, (Selbstzahler: Bankverbindung; sonst KK-Code)**
Zur Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt, erforderlich **(Art. 6 Abs. 1 Lit c)**	**- Rechnung im Kontext des HGB**

3.3 DiGa relevante Rechtsgrundlagen und Bestimmungen

Für Hersteller von Anwendungen von digitalen Gesundheitsanwendungen i.S. des §139e Abs 7-9 SGB V ist zusätzlich die Digitale Gesundheitsanwendung-Verordnung (DiGaV) relevant und hier v.a. der Artikel 4 “Anforderungen an Datenschutz und Datensicherheit”. Neben der Anforderung, die gesetzlichen Vorgaben des Datenschutzes zu gewährleisten (siehe Rechtsgrundlagen oben) gilt hier:

- Eine Verarbeitung von personenbezogenen Daten nur aufgrund einer Einwilligung nach Artikel 9 Abs. 2 lit a der DS-GVO erfolgen. Damit entfallen andere Rechtsgrundlagen wie bspw. “Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen” als alleinige Rechtsgrundlage und es muss immer eine informierte und explizite Einwilligung erfolgen (“active opt-in”)
- Zudem gilt, dass nur für die folgenden Zwecke Daten verarbeitet werden dürfen
    - für den bestimmungsgemäßen Gebrauch
    - zum Nachweis positiver Versorgungseffekte im Rahmen der Aufnahme in das DiGa Verzeichnis auf Erprobung
    - Zur Nachweisführung bei Vereinbarungen nach §134 Abs 1 lit 3 SGB V (erfolgsabhängig Preisbestandteile bei Vereinbarungen mit dem GKV SV)
    - Für die dauerhafte Gewährleistung der technischen Funktionsfähigkeit, Nutzerfreundlichkeit und der Weiterentwicklung (hierfür ist allerdings eine getrennte Einwilligung erforderlich)

4. Verarbeitungszwecke bei DiGAs

- Die folgenden Hinweise gelten nur für DiGA-Hersteller -

4.1. DiGAV

Die Verarbeitung von personenbezogenen Daten die im Rahmen einer digitalen Gesundheitsanwendung erhoben werden sind ausschließlich auf folgende Zwecke beschränkt (§ 4 Abs. 2 S.1 DiGAV):

1. Dem bestimmungsgemäßen Gebrauch der digitalen Gesundheitsanwendung durch die Nutzer,
2. zu dem Nachweis positiver Versorgungseffekte im Rahmen einer Erprobung nach § 134 Abs. 1 S. 3 SGB V
3. zu der Nachweisführung bei Vereinbarungen nach § 134 Abs.1 S.3 SGB V
4. zu der dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der digitalen Gesundheitsanwendung

Die Punkte 1.-3. können in einer gemeinsamen Einwilligung zusammengefasst werden. Punkt 4. ist nur mit einer zusätzlichen, separaten Einwilligung möglich. Die Ablehnung von Punkt 4 darf keine Einschränkung der Funktionalität mit sich bringen. Der Umfang der damit erfassten informationen bezieht sich beispielsweise auf das Anzeigen von Nutzerfragebögen über die DiGA zur Erhebung und Verarbeitung von Rückmeldungen zur Nutzererfahrung oder zu technischen Problemen. Nicht zulässig ist hingegen ein umfassendes Tracking der Nutzeraktivitäten.

Datenverarbeitungsbefugnisse zu anderen Zwecken bleiben unberührt, siehe dazu 4.2.

Wie oben aufgeführt ist nach § 4 Abs. 2 S.1 Nr. 4 DiGAV für DiGAs ein separates Opt-in Verfahren für folgende Verarbeitungszwecke vorgesehen: “*zu der dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der digitalen Gesundheitsanwendung*”;

Hierunter fallen beispielsweise

- Informationen, die nur mittelbar auf den aktuellen Betrieb und die aktuelle Nutzung einwirken und zur Weiterentwicklung der DiGA dienen
- Anzeigen von Nutzerfragebögen über die DiGA zur Erfassung von Rückmeldungen für die Nachhaltigkeit und Weiterentwicklung
- Beispielsweise dürfte der Hersteller den Nutzer bitten, über die DiGA Produktdaten und weitere Betriebsdaten zu einem im Rahmen der DiGA genutzten Pulsmesser anzugeben, um die Unterstützung dieser Art von Pulsmesser zukünftig zu verbessern

4.1.1 Werbung

Werbung in der DiGA:

Gemäß § 5 Absatz 4 DiGAV darf eine DiGA nicht als Vehikel für Werbung verwendet werden, weder für Eigenwerbung noch für Angebote Dritter. Das eigene Logo darf in der DiGA verwendet werden. Auch die Kontaktaufnahme mit den Nutzern der DiGA per E-Mail zu Werbezwecken ist nicht erlaubt. Reine Newsletter, die keine Werbung enthalten, sind nicht untersagt.

Gemäß SGB V sind kostenpflichtige Erweiterungen einer DiGA zulässig. Der Hersteller darf laut § 5 Absatz 4 DiGAV auf diese Erweiterungen hinweisen, diese aber nicht anpreisen.

Werbung für die DiGA:

Werbung für DiGA ist, unter Beachtung der gesetzlichen Vorgaben für Medizinprodukte, grundsätzlich erlaubt. Hier greift insbesondere das Gesetz gegen den unlauteren Wettbewerb (UWG) und das Heilmittelwerbegesetz (HWG), welche nicht Gegenstand dieses Dokumentes sind:

Gesetz gegen den unlauteren Wettbewerb:
https://www.buzer.de/s1.htm?g=Gesetz+gegen+den+unlauteren+Wettbewerb&f=1

Heilmittelwerbegesetz:
https://www.buzer.de/gesetz/1998/index.htm

4.1.2 Cookies & Tracking

Eine Protokollierung von sicherheitsrelevanten Vorgängen (beispielsweise Authentisierungen) innerhalb der DiGA werden durch die Digitale Gesundheitsanwendungen-Verordnung (DiGAV), Anlage 1, Fragebogen gemäß § 4 Absatz 6, Abschnitt "Datensicherheit" gefordert.

Ein umfassendes Tracking der Nutzeraktivitäten innerhalb des Scopes der DiGA ist nicht erlaubt.

Vor dem Hintergrund des gekippten EU-US-Privacy-Shields durch das Schrems-II-Urteil (siehe auch 8.4 Informationen zur Nutzung von Cloud-Infrastrukturen) ist eine Erfassung von Benutzerdaten mit Services von beispielsweise Google nicht zulässig, da sich hier der Datenstandort und der Mutterkonzern in den USA befinden. Als Alternative für die Erfassung von Nutzerverhalten im erlaubten Rahmen gibt es beispielsweise die on-premise-Variante von Matomo (https://matomo.org/).

4.2. Sonstige Verarbeitungsbefugnisse

Nach § 4 Abs.2 Satz 3 DiGAV bleiben Datenverarbeitungsbefugnisse nach anderen Vorschriften unberührt. Da es sich bei allen DiGAs zwingend um Medizinprodukte handelt ist hier die EU-Medizinproduktverordnung (MDR) einschlägig. Da auch die Übergangsfrist für bereits zugelassene Medizinprodukte am 26.5.2021 abläuft lassen wir hier frühere Medizinproduktrichtlinen (93/42/EWG & 90/385/EWG) unerwähnt.

Darüber hinaus handelt es sich bei der MDR um Europarecht, welches grundsätzlich höherrangig als die DiGAV als eine deutsche Rechtsverordnung íst. Entsprechend würde die MDR bei Widersprüchen diese überlagern. Relevant sind hier die Überwachung nach dem Inverkehrbringen (Post-Market Surveillance, kurz PMS) nach Artikel 83-86 MDR sowie die Vigilanz nach Artikel 87-92 MDR. Die konkret zur Erfüllung dieser Verpflichtungen erforderlichen Daten unterscheiden sich von Medizinprodukt zu Medizinprodukt, können aber über die medizinproduktrechtliche Dokumentation nachgewiesen werden.

Zweites wichtiges sonstiges Verarbeitungsbefugnis ist die Abrechnung gegenüber den Krankenkassen nach § 302 SGB V. Entsprechend sind hier bezüglich zulässiger Zwecke und legitimerweise zu verarbeitenden Daten für die Abrechnung, nicht die DiGAV-Vorgaben sondern, die Vorgaben aus §302 SGB V zu betrachten.

5. Wahrung der Rechte Betroffener

Zur Umsetzung der Betroffenenrechte werden schriftlich Prozesse dokumentiert, welche jedem Mitarbeiter des Unternehmens bekannt sind. Es bestehen mindestens Prozesse zu den folgenden Rechten:

a. Das Recht auf Auskunft
b. Das Recht auf Datenportabilität
c. Das Recht auf Löschung
d. Das Recht auf Korrektur und Einschränkung
e. Das Widerspruchsrecht
f. Das Recht auf Widerruf

Bei der Erstellung der Prozesse wird auf die jeweilige Rolle des Unternehmens geachtet (beispielsweise müssen Auftragsverarbeiter in ihrem Auftragsverarbeitungsvertrag regeln, wer für die Beantwortung einer Auskunftsanfrage nach Art. 15 DSGVO zuständig ist).

Um eine Umsetzung der Betroffenenrechte sicherzustellen, werden allen Mitarbeiter des Unternehmens die Prozesse erläutert und schriftlich zur Verfügung gestellt. Neue Mitarbeitern werden diese während der Einarbeitung mitgeteilt.

Betroffene werden in der Datenschutzerklärung über ihre Rechte aufgeklärt. Das Unternehmen richtet für Anfragen eine E-Mailadresse für Fragen im Bereich Datenschutz ein und veröffentlicht diese ebenfalls in der Datenschutzerklärung.

Es wird darauf geachtet, dass die Umsetzung geltend gemachter Betroffenenrechte weitestgehend zu automatisieren und somit so einfach und personenunabhängig wie möglich durchführbar zu machen.

5.1. Informationspflicht

Zur Erfüllung der Informationspflichten gemäß Art. 12-14 DSGVO werden Datenschutzerklärungen für die Betroffenen vor dem Start der Datenverarbeitung zur Verfügung gestellt (z.B. wenn beim (erstmaligen) Öffnen einer App bereits personenbezogene Daten wie Tracking oder Device ID übermittelt werden). Die Formulierungen sollten einfach und leicht verständlich sein sowie das Prinzip nach Transparenz erfüllen.

Um mehr Transparenz zu schaffen, sollte je nach Verarbeitungstätigkeit statt einer umfassenden Datenschutzerklärung mehrere, klar benannte, zur Verfügung gestellt werden (beispielsweise „Datenschutzerklärung App“ und „Datenschutzerklärung Website“).

Die Datenschutzerklärung soll den Betroffenen unkompliziert und dauerhaft zur Verfügung stehen. Auf einer Website sollte die Erklärung als direkter Link sichtbar sein.

Bei jeder Änderung der Datenverarbeitung wird die betroffene Datenschutzerklärung überarbeitet. Um dies zu gewährleisten werden die Mitarbeiter regelmäßig geschult und daran erinnert, dass neue Datenverarbeitungen in der Datenschutzerklärung zu benennen sind. Dazu können unter anderem der Einsatz neuer Drittanbieter oder die Erweiterung der Nutzungsmöglichkeiten gehören.

Standard für DIGAs

Die Datenschutzerklärungen müssen auch nach Installation einfach auffindbar sein.

In der Datenschutzerklärung werden alle Informationspflichten nach Art. 13 und 14 DSGVO erfüllt, wobei bei der Nennung der Betroffenenrechte eine erweiterte Informationspflicht gilt. Die DIGAs müssen in einfacher Sprache erklären wie der Löschprozess bei einem Widerruf der Einwilligung oder bei der Löschung der App gewährleistet wird. Es wird darauf geachtet, dass die Daten nicht nur im eigenen Unternehmen, sondern auch bei allen Drittanbietern gelöscht werden.

Der Nutzer wird zudem in dem Prozess über sein Recht auf Datenübertragbarkeit aufgeklärt, damit er die Möglichkeit hat, seine Daten zu exportieren bevor diese gelöscht werden.

5.2. Auskunftsrecht

Nach Artikel 15 DSGVO haben die betroffenen Personen das Recht auf eine Bestätigung ob personenbezogene Daten verarbeitet wurden. Darauf aufbauend haben betroffene Personen das Recht auf Auskunft über diese personenbezogenen Daten. Das verarbeitende Unternehmen hat gemäß Artikel 15 DSGVO alle darin genannten Punkte umzusetzen und ein entsprechendes Konzept zu erarbeiten.

Unerlässlich für die Inhalte aus Artikel 15 DSGVO ist die Verifizierung der antragstellenden Person: die verarbeitende Firma muss vor der Auskunft an die betroffene Person sicherstellen, dass es sich wirklich um diese Person handelt. Hierfür sind unternehmensintern geeignete Prozesse zu entwickeln. Darüber hinaus müssen für die Bereitstellung der Auskunft sichere Transportwege (bspw. sicherer E-Mail Versand, passwortgeschützte PDF-Datei…) zur Verfügung gestellt werden.

Wenn eine betroffene Person von ihrem Auskunftsrecht Gebrauch macht, sind ihr die zu erteilenden Informationen gemäß Art. 12 Abs. 3 DSGVO unverzüglich, in jedem Fall **aber** innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen. Diese Frist kann in komplexen Fällen um zwei Monate verlängert werden.

Falls personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantie gemäß Artikel 46 Abs. 2 DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden.

5.3. Recht auf Berichtigung

Nach Artikel 16 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person

das Recht die Vervollständigung unvollständiger personenbezogener Daten - auch mittels einer ergänzenden Erklärung - zu verlangen.

Auch hier ist für das verarbeitende Unternehmen eine Verifizierung der antragstellenden Person unerlässlich. Entsprechende Konzepte und Prozesse sind zu entwickeln.

5.4. Recht auf Löschung

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden (Artikel 17 DSGVO), und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich - ohne schuldhaftes Zögern - zu löschen. Die Gründe für eine Löschung sind in Artikel 17 DSGVO zu lesen und anzuwenden. Auch hier gilt, wie in den vorher genannten Punkten, die Verifizierung der antragstellenden Person als unerlässlich.

Die Datenspeicherung ist gemäß Art. 5 DSGVO nur so lange zulässig, wie es für den vorher festgelegten, eindeutigen sowie legitimen Zweck erforderlich und angemessen ist. Grundsätzlich muss ein datenverarbeitendes Unternehmen aber nicht in jedem Fall Daten löschen. Es gibt einige gesetzliche Aufbewahrungsfristen und ggf. ein “berechtigtes Interesse” (Art. 6 Abs 1. lit. f DSGVO), die unternehmensintern mit einem Datenschutzbeauftragten oder unter Zuhilfenahme juristischer Fachexpertise individuell zu klären sind. Sollte dies der Fall sein tritt das Recht auf Einschränkung der Verarbeitung in Kraft, welches in 3.5 näher beschrieben wird.

Daten können als gelöscht angesehen werden, sobald keine Möglichkeit mehr besteht, die Daten ohne unverhältnismäßigen Aufwand wahrzunehmen. Dies beinhaltet auch pseudonymisierte Daten und die Löschung der Daten bei vom Unternehmen genutzten Auftragsdatenverarbeitern.

5.5. Recht auf Einschränkung der Verarbeitung

Nach Artikel 18 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen. Die Voraussetzungen hierfür sind im entsprechenden Artikel zu lesen und anzuwenden. Wiederum gilt hier, dass das Unternehmen die antragstellende Person ausreichend verifizieren muss, bevor eine solche Anfrage umgesetzt wird.

Das Recht auf Einschränkung tritt in den meisten Fällen dann in Kraft, wenn das Löschen der Daten mit entsprechender gesetzliche Grundlage nicht möglich ist. Die Daten sind serverseitig vorhanden, dürfen aber nicht mehr - ohne Zustimmung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen - eingesehen oder verarbeitet werden. Eine weitere Möglichkeit ist, dass die betroffene Person Widerspruch gegen die Verarbeitung einlegt, aber noch nicht festgelegt ist, wessen Gründe überwiegen - die der betroffenen Person oder die des datenverarbeitenden Unternehmens. Für datenverarbeitende Unternehmen bedeutet dieser Abschnitt, dass für die Einschränkung der Verarbeitung (“einfrieren”) ein individuelles Konzept erarbeitet werden muss, welches eine tatsächliche Einschränkung der Verarbeitung garantiert.

5.6. Datenportabilität

Nach Artikel 20 DSGVO hat die betroffene Person das Recht ihre personenbezogenen Daten vom Verantwortlichen der Verarbeitung in einer strukturierten, gängigen, maschienenlesbaren Form zur Verfügung gestellt zu bekommen, sowie diese in einer solchen Form an einen anderen Verantwortlichen übermitteln zu lassen.

Im Kontext von DiGAs erfolgt dies im Moment noch meist über ein PDF-Dokument. Aufgrund der Komplexität und noch unklaren Rahmenbedingungen in der Interaktion zwischen Patienten, deren Endgeräten, Arztpraxen und Krankenhäusern, Forschungseinrichtungen, den Krankenkassen sowie der elektronischen Patientenakte wird dieser Punkt erst in einer künftigen Version des Leitfadens genauer behandelt.

6. Datenschutz-Folgeabschätzung und Risikoanalysen

6.1. Datenschutz-Folgenabschätzung

6.1.1 Was ist das und wann brauche ich das?

Eine Datenschutzfolgeabschätzung (DSFA) nach Art. 35 Abs. 1 S. 2 DSGVO dient der Prävention und dem Schutz der erhobenen Daten und ist unter bestimmten Voraussetzungen sowohl sinnvoll oder auch verpflichtend.

> **Wichtig:** Gemäß der DiGaV **muss jeder Hersteller einer DiGa eine Datenschutzfolgeabschätzung vornehmen** und dokumentieren, da es sich i.d.R. bei DiGas immer um Gesundheitsdaten nach Artikel 9 DS-GVO handelt, welche eine solche notwendig machen.

Insbesondere bei der Verwendung neuer Technologien ist vorab zu prüfen, ob mit diesen voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen einhergeht. Eine solche Prüfung empfiehlt sich typischerweise in den folgenden Fällen:

- ein neues Produkt/Feature wird designed
- bestehende Daten werden zu neuen Zwecken verarbeitet
- ein Dienstleister zur Datenverarbeitung wird gewechselt
- …

Eine Übersicht darüber, unter welchen Voraussetzungen eine DSFA notwendig ist, kann man sich auf den Webseiten der Landesdatenschutzbehörden (z.B. hier beim bayerischen Landesamt für Datenschutz) oder vom vom BfDI Liste der Verarbeitungsvorgänge - BfDI) mittels vordefinierter Listen holen.

6.1.2 Wer macht das (für mich) und warum ist das wichtig?

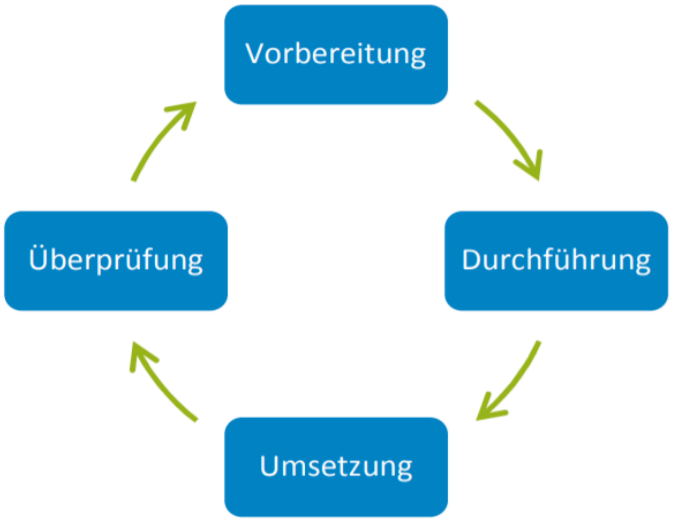
Die Verantwortlichkeit bei diesen Prozessen liegt bei der Geschäftsführung. Die Geschäftsführung zieht den Datenschutzbeauftragten hinzu und holt sich von diesem Rat ein.

Bei neuartigen Methoden zur Datenerhebung - beispielsweise bei Art, Umfang, Umständen oder Zweck der Erhebung - muss zum frühestmöglichen Zeitpunkt (vor Beginn der eigentlichen Verarbeitung) abgeschätzt werden, welche Folgen für die personenbezogenen Daten entstehen können. Da in der Entwicklungsphase meist noch nicht alle Verarbeitungsvorgänge bekannt sind, kann nur durch eine ständige Aktualisierung der DSFA gewährleistet werden, dass der Datenschutz gebührende Beachtung findet (ggf. müssen im Verlaufe des Produkt-Lebenszyklus einige Vorgänge der Datenschutz-Folgenabschätzung wiederholt werden). Der festzulegende Prozess bestimmt, dass eine DSFA keineswegs

einen statischen und einmaligen, sondern vielmehr einen kontinuierlichen und dynamischen Prozess mit ständigen Variationen und Veränderungen darstellt. Dieser Prozess wiederholt sich im Sinne des kontinuierlichen Verbesserungsprozess eines Qualitätsmanagements (z.B. “Plan, Decide, Check, Act, PDCA”) regelmäßig.

Falls mehrere Verarbeitungsvorgänge mit ähnlich hohen Risiken durchgeführt werden, kann eine einzige Abschätzung vorgenommen werden (vgl. Art. 35 Abs. 1 S. 2 DSGVO). Formelle Mindestanforderungen an Datenschutz-Folgenabschätzungen sind in Art. 35 Absatz 7 DSGVO beschrieben. Die zu bewertenden Verarbeitungsvorgänge und deren Zwecke müssen beschrieben und nachfolgend auf Notwendigkeit und Verhältnismäßigkeit bewertet werden. Daraus lassen sich dann mögliche Risiken für Rechte und Freiheiten der betroffenen Personen abschätzen, welche ebenfalls bewertet und durch entsprechende Maßnahmen soweit möglich eingegrenzt werden müssen. Insgesamt wird hiermit das Ziel verfolgt Risiken, die aufkommen können, zu minimieren.

Für geplante Prozesse, die so im Unternehmen erst zukünftig stattfinden werden, hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) beschreiben im Kurzpapier Nr. 5 ab Seite 2 eine Vorgehensweise für die Durchführung von Datenschutz-Folgenabschätzungen vorgeschlagen. Diese Vorgehensweise wird vom SVDGV e.V. unterstützt:



In der **Vorbereitungsphase** sollte ein Team zusammengestellt und der Beurteilungsumfang klar definiert werden. Darüber hinaus sollten alle Akteure und betroffenen Personen, sowie die Rechtsgrundlagen identifiziert werden. Zusätzlich sollte bereits hier geklärt werden, ob die Verarbeitungsvorgänge überhaupt notwendig sind oder ggf. durch bereits vorhandene Verarbeitungsvorgänge ersetzt werden können.
In der **Durchführungsphase** werden die Quellen der Risiken identifiziert, beurteilt und durch entsprechende Maßnahmen eingedämmt werden. Aufbauend auf diese Erkenntnisse wird dann der DSFA-Bericht erstellt, welcher die Inhalte gemäß Artikel 35 Abs. 7 DSGVO widerspiegeln muss.
In der **Umsetzungsphase** gilt es dann, die im DSFA-Bericht beschriebenen Maßnahmen auch tatsächlich in der Praxis umzusetzen und ggf. zu testen.
Die **Überprüfung** kann zum einen durch Auditierung des Berichts durch unabhängige Dritte erfolgen. Zum anderen gilt hier die Fortführung der DSGVO-konformen Überwachung entsprechender Prozesse. Spätestens bei Änderungen der entsprechenden Verarbeitungsvorgänge ist eine erneute DSFA von Nöten.

Dieser Prozess ist darauf aufgebaut, Prozesse zu überprüfen, bevor sie überhaupt entwickelt werden. In den meisten Fällen werden von den Unternehmen bereits bestehende Prozesse überprüft werden müssen. Hier kann der oben genannte DSFA-Prozess individuell angepasst werden.

Aufbauend darauf ist noch zu sagen, dass es sehr wichtig ist, nicht nur die Kernprozesse des Unternehmens über eine Datenschutz-Folgenabschätzung abzusichern. Auch viele Nebenprozesse, beispielsweise im CRM- oder HR-Bereich, können darunter fallen. Hier lohnt es eine differenzierte interne Begutachtung aller Prozesse durchzuführen. Auch der Blick eines externen Gutachters (Berater oder externer Datenschutzbeauftragter) kann lohnenswert sein.

Der SVDGV e.V. setzt für seine Mitglieder die Bestellung eines Datenschutzbeauftragten voraus. Für die Durchführung von Datenschutz-Folgenabschätzungen, gibt es beispielsweise vom TÜV Nord, selbstverständlich auch von vielen anderen Unternehmen Vorlagen. Weiterführende Informationen zu Datenschutz-Folgenabschätzungen finden sich unter anderem hier.

Die bayerischen Behörden stellen unter https://www.datenschutz-bayern.de/dsfa/ bzw. https://www.datenschutz-bayern.de/download/PIA.Setup.2.0.0.5.exe u.a. das PIA (Privacy Impact Assessment) Tool kostenlos zur Verfügung, welches welches sehr gut geeignet ist, selbst eine DSFA mit einem externen oder internen Datenschutzbeauftragten vorzunehmen.

6.2 Schutzbedarfsfeststellung

- Die folgenden Hinweise gelten nur für DiGA-Hersteller -

Die Schutzbedarfsfeststellung ist im BSI-Standard-200-2, IT Grundschutz Methodik, Kapitel 8.2, beschrieben.
Ziel der Schutzbedarfsfeststellung ist es, die Sicherheitsanforderungen bezüglich **Vertraulichkeit, Integrität und Verfügbarkeit** der einzelnen erfassten Schutzobjekte des Unternehmens einzuschätzen und festzulegen und die Auswahl angemessener Sicherheitsmaßnahmen für diese zu steuern.

Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen Anwendungen und damit der jeweiligen Geschäftsprozesse verbunden sind. Es handelt sich also um den potenziellen Schaden **für das Unternehmen selbst**.

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt sich BSI Standard auf eine qualitative Aussage, indem er den Schutzbedarf in drei Kategorien unterteilt:

Schutzbedarfskategorien	
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Ein Unternehmen kann auch nur ein bis zwei oder mehr als drei Schutzbedarfskategorien festlegen. Wichtig ist, dass die festgelegten **Schadensabstufungen abgrenzbar und nachvollziehbar** sind.

Um die Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ voneinander abgrenzen zu können, empfiehlt der Standard, die Grenzen für die einzelnen Schadensszenarien zu bestimmen.

Dafür beschreibt der BSI Standard typische Schadensszenarien, denen Schäden, die bei dem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für einen Geschäftsprozess bzw. eine Anwendung einschließlich ihrer Daten entstehen können, zugeordnet werden können und anhand derer die Abgrenzung der Schutzbedarfskategorien deutlicher wird:

- Verstoß gegen Gesetze/Vorschriften/Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung und
- finanzielle Auswirkungen

Häufig können **für einen Schaden mehrere Schadensszenarien** zutreffen. Beispielsweise kann der Ausfall einer Anwendung die Aufgabenerfüllung beeinträchtigen, was direkte finanzielle Einbußen nach sich zieht und gleichzeitig auch zu einem Imageverlust führt.

Die Schadensszenarien für jede Schutzbedarfskategorie (normal, hoch, sehr hoch) werden folgend beschrieben:

Schutzbedarfskategorie „normal“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des infor mationellen Selbstbestim mungsrechts	• Es handelt sich um personenbezogene Daten, durch deren Ver arbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt wer den kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeein trächtigung ist zu erwarten.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.

Schutzbedarfskategorie „hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des infor mationellen Selbstbestim mungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verar beitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu er warten.
6. Finanzielle Auswirkungen	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des infor mationellen Selbstbestim mungsrechts	• Es handelt sich um personenbezogene Daten, bei deren Verar beitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Gravierende Beeinträchtigungen der persönlichen Unversehrt heit sind möglich. • Gefahr für Leib und Leben.
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von allen Betroffenen als nicht tole rabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Außenwirkung	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden ist für die Institution existenzbedrohend

Diese Tabellen dienen lediglich als **Orientierung** und Beispiel, welchen Schutzbedarf ein potenzieller Schaden und seine Folgen erzeugen. Die Tabellen sollten vom jeweiligen Unternehmen auf die eigenen Gegebenheiten angepasst werden.

7. Technisch Organisatorische Maßnahmen (TOM)

7.1 Definition

Die DSGVO spricht in Art. 32 von geeigneten technischen und organisatorischen Maßnahmen, die der Verantwortliche unter Berücksichtigung u. a. des Stands der Technik und der Implementierungskosten zu treffen hat. Folglich wird einerseits stets zu prüfen bleiben, was beim jeweiligen Verfahren als Stand der Technik angesehen wird. Andererseits wird auch die Verhältnismäßigkeit einer Maßnahme hinsichtlich des Aufwands zu diskutieren sein. Weiterhin sollen, gem. Art. 32 DSGVO, mit den TOM die Sicherheit der Verarbeitung gewährleistet werden. Die TOM sind daher besonders relevant, wenn es zu einem (meldepflichtigen) Datenleck oder Datenschutzverstoß gekommen ist. Die TOM sollten dann den Beleg bringen können, dass stets angemessene Maßnahmen zum Schutz der Daten getroffen wurden und diese auch regelmäßig überwacht bzw. evaluiert und bei Bedarf erweitert/ angepasst wurden. Daraus resultiert, dass TOM bereits vor der Datenerhebung implementiert und umgesetzt werden sollten.

Eine kurze Zusammenfassung zeigt nachfolgend auf, worauf im Kern jeweils zu achten ist:

7.1.1 Technische Maßnahmen

Die Technischen Maßnahmen sind Bestandteil der TOM. Sie bilden Vorgaben und Rahmenbedingungen für die technische Umsetzung. Hier finden sich Maßnahmen, welche die Sicherheit der eingesetzten IT-Systeme sowie bis die Sicherheit des Gebäudes in dem sie sich befinden, gewährleisten. Technische Maßnahmen sind bspw.:

- Verschlüsselung sämtlicher Datenträger bzw. der Datenübermittlung
- Automatische und systematische Backups (Georedundanz beachten)
- Einsatz von Firewalls
- Einsatz USV (Notstrom, insb. wenn eigene Server betrieben werden)

7.1.2 Organisatorische Maßnahmen

Die organisatorischen Maßnahmen bilden die Rahmenbedingungen der technischen Verarbeitung. Organisatorische Maßnahmen sind u.a. Maßnahmen, aber auch Prozesse, welche sich im Qualitätsmanagement wiederfinden sollten, bzw. an das Qualitätsmanagement anknüpfen. Die Maßnahmen sollten daher realistisch umsetzbar und überprüfbar sein.

- Schulung der Mitarbeiter im Datenschutz (als Bestandteil eines Schulungskonzeptes)
- Vertraulichkeitsverpflichtung der Mitarbeiter (bspw. als fester Bestandteil im Einstellungsprozess)
- Vier-Augen-Prinzip
- Bestimmung der zugriffsberechtigten Personen

7.1.3 Auswahlkriterien

Jedes Unternehmen wird seinen eigenen, spezifischen Maßnahmenkatalog entwickeln müssen. Es gibt zwar Leitfäden und Modelle (Beispiele folgen im nächsten Kapitel), die Inhalte, der Umfang etc. müssen jedoch individuell erarbeitet werden und sollten gut in die Struktur des jeweiligen Unternehmens integriert werden, um eine Umsetzung ohne Widerstände gewährleisten zu können. Die Maßnahmen müssen nicht nur für die stattfindenden Verarbeitungen ein angemessenes Schutzniveau herstellen, sondern auch entsprechend der Kriterien dauerhaft angepasst und aktualisiert werden. Zu den Kriterien zählen der Stand der Technik, Implementierungskosten, die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen, sowie Art, Umfang, Umstände und Zweck der Verarbeitung.

Beispiele und Quellen:

Die Landesbeauftragte für Datenschutz (LfD) aus Niedersachsen hat einen Leitfaden zur Auswahl angemessener **z**ur **A**us**w**ahl **a**ngemessener **S**icherungsmaßnahmen(ZAWAS) bereitgestellt[4]. Im Wesentlichen sind folgende Bereiche ausführlich im Leitfaden abgebildet:

1. **Verarbeitungstätigkeit beschreiben**
   Fassen Sie zusammen, welche Zwecke mit der Verarbeitung verfolgt werden, welche Daten die Verarbeitung betrifft und beschreiben Sie den Ablauf der Verarbeitung (bei externen Verarbeitungen, siehe Kapitel 8).

2. **Rechtliche Grundlagen prüfen**
   Stellen Sie sicher, dass die Verarbeitung auf einer zulässigen Rechtsgrundlage basiert und die Grundsätze der DSGVO eingehalten werden. (Siehe auch Kapitel 3 und 4)

3. **Strukturanalyse durchführen**
   Ermitteln und beschreiben Sie die zu schützenden Objekte der Verarbeitungstätigkeit. Geben Sie außerdem deren Beziehung zueinander an. Zum Beispiel die IT-Systeme, das Gebäude oder spezifische Räume.

4. **Risiken identifizieren und Schadenswerte einschätzen**
   Bestimmen Sie Ereignisse, die zu einem Schaden führen können und bestimmen Sie den Schadenswert des Risikos anhand der Eintrittswahrscheinlichkeit und der Schwere des Risikos (Als Teil davon auch die DSFA, siehe Kapitel 6).

5. **Maßnahmen auswählen**
   Suchen Sie unter Berücksichtigung der oben genannten Kriterien nach geeigneten Maßnahmen, um die identifizierten Risiken einzudämmen. Achten Sie dabei auf die bestimmten Schadenswerte und wählen Sie geeignete Maßnahmen zur Prävention aus. Sie können sich am IT-Grundschutz-Kompendium, oder an den Maßnahmen des Standard-Datenschutzmodells orientieren (Siehe auch Kapitel 6 und 8)

6. **Restrisiko bewerten**
   Ermitteln Sie die bestehenden Restrisiken, wenn die nach Punkt 5 ausgewählten Maßnahmen implementiert wären. Sollte weiterhin ein hohes Risiko bestehen, müssen Sie neue Maßnahmen bestimmen, oder den Verarbeitungsprozess

[4] https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/zawas/praxisnahe-hilfe-zum-technisch-organisatorischen-datenschutz-173395.html

anpassen.

7. **Maßnahmen konsolidieren**
   Hierbei sollen nun alle Maßnahmen als Einheit betrachtet werden. Es kann sein, dass Maßnahmen überflüssig sind, weil eine andere Maßnahme ein besseres Schutzniveau gewährleistet. Konkretisieren Sie außerdem Maßnahmen, wenn bei der Gesamtbetrachtung das Ziel der Maßnahme nicht klar ist.

8. **Maßnahmen realisieren**
   Verteilen Sie Aufgaben und Verantwortlichkeiten und priorisieren Sie bei Budget- bzw. Personalknappheit Ihre Maßnahmen. Setzen Sie nun die festgelegten Maßnahmen um.

7.2. Beispiele Technische Maßnahmen (Auszug TTT Stand der Technik)[5]

7.2.1 Bewertung der Passwortstärke

Die Maßnahme simuliert praxisnah Angriffe auf sicher gespeicherte/gehashte Anmeldedaten und misst die objektive Widerstandsfähigkeit auf Grundlage mathematischer Methoden, persönlicher Verhaltensweisen u.a. Die Maßnahme unternimmt eine umfassende Inventur und Bewertung aller, auch unbekannter, Passwörter. Die Maßnahme ermittelt den Erfüllungsgrad der Compliance zu unternehmensinternen Richtlinien und unterstützt bzw. ermöglicht die Durchführung weiterer sicherheitsrelevanter Maßnahmen, wie zum Beispiel die Notifikation von Mitarbeitern bei Verwendung unsicherer Passwörter unter Einhaltung der DSGVO.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Die Maßnahme soll das Risiko des Missbrauchs von Kontoinformationen (Zugangsdaten) verhindern. 80% der IT-Sicherheitsvorfälle die zur Offenlegung von Account-Informationen - privater, personenbezogener Daten und Geschäfts-Daten führen, gehen auf das Konto schwacher und oder gestohlener Passwörter (Verizon Report 2017). Die Einhaltung statischer Passwort-Richtlinien für Benutzerkonten ist somit erwiesenermaßen keine geeignete Maßnahme für die Durchsetzung starker, sicherer Passwörter. Die Passwort-Richtlinie täuscht ein falsches Sicherheitsniveau vor.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

	Verfügbarkeit
X	Integrität
X	Vertraulichkeit
X	Authentizität

7.2.2 Beispiel Multifaktor Authentisierung

---

5 https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

Als Multi-Faktor-Authentifizierung (MFA) bezeichnet man den Nachweis der Identität eines Nutzers mit mehr als einem Faktor (z.B. Passwort + One-Time-Password (OTP) oder Passwort + Fingerabdruck +Sicherheitstoken).[6]

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

Wenn ein System lediglich mit einem Faktor (Ein-Faktor-Authentifizierung) gesichert ist, unterliegt die Nutzeridentität einem erhöhten Risiko des

• Identitätsdiebstahls,

• Identitätsmissbrauchs und

• Identitätsbetrugs.

Zur Absicherung von schutzwürdigen Computerzugriffen/Benutzeranmeldungen ist ein Faktor allein nicht ausreichend – die Methoden der digitalen Angreifer werden immer versierter und die möglichen Schäden aufgrund der fortschreitenden Vernetzung und Digitalisierung immer drastischer. 81% aller Datenverletzungen entstehen durch gestohlene oder schwache Passwörter (also Ein-Faktor-Authentifizierung). Diese sehr hohe Rate wird insbesondere ausgelöst durch:

• Menschliche Risiken im Umgang mit Passwörtern:

o unzureichende Qualität der Passwörter,

o zu häufiges Nutzen von ein und demselben Passwort,

o bewusste Passwortweitergabe (z.B. Teilen mit anderen Personen) oder

o unbewusste Passwortweitergabe (z.B. Aufschreiben).

• Technische Risiken im Umgang mit Passwörtern:

o "Man in the middle” Attacken,

o Phishing Attacken,

o Keylogger basierte Attacken,

o Brute Force Attacken, etc.

Der Einsatz von MFA-Lösungen kann diese Risiken erheblich reduzieren.

---

[6] DiGA Hersteller sind dazu angehalten 2 Faktoren umzusetzen

Neben dem klassischen Passwort sind diverse Methoden und Lösungen der Authentifizierung (MFA Systeme) verfügbar. Sie lassen sich in drei wesentliche Kategorien einteilen:

• Wissensbasierte Faktoren (z.B. Passwort, PIN, Passphrase, etc.)

• Besitzbasierte Faktoren (z.B. Sicherheitstoken, Smartcard, etc.)

• Biometrische Faktoren (z.B. Fingerabdruck, Iris, etc.)

MFA-Systeme kombinieren in der Regel jeweils zwei Methoden aus unterschiedlichen Kategorien zu einer Authentifizierungskette, wobei einige MFA-Systeme auch die Verkettung von beliebig vielen Methoden zulassen. Die Kombination von Methoden aus nur einer Kategorie ist nicht ratsam. Es ist zu beachten, dass nicht zwangsläufig alle Methoden aus diesen drei Kategorien, auch in ihrer Kombination gleichwertig sind. Jedoch stellt jegliche Kombination eine Verbesserung gegenüber dem Einsatz von Passwörtern allein dar. Welche Authentifizierungsmethoden kombiniert werden sollten, hängt vom Schutzbedarf der Anwendung bzw. Nutzeridentität sowie den technischen Voraussetzungen ab.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

	Verfügbarkeit
X	Integrität
X	Vertraulichkeit
X	Authentizität

7.2.3 Management mobiler, dienstlicher Geräte

Der Einsatz von Mobile Device Management (MDM)-Lösungen vermindert die Sicherheitsrisiken, die durch die unkontrollierte Nutzung mobiler **Endgeräte zu dienstlichen Zwecken entstehen**. MDM Lösungen ermöglichen es, die eingesetzten mobilen Geräte zentral administrieren und konfigurieren zu können.

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

1. Datenverlust: Wenn wichtige Daten auf den mobilen Geräten abgelegt werden und das Gerät verloren geht oder zerstört wird, muss das Unternehmen unter Umständen einen unwiederbringlichen Datenverlust hinnehmen.

2. Diebstahl: Wenn ein mobiles Endgerät gestohlen wird, kann der Dieb möglicherweise auf vertrauliche Unternehmensdaten zugreifen.

3. Schadsoftware: Durch die Verwendung von öffentlichen WLAN-Netzen, der Nichtinstallation verfügbarer Updates und durch die unkontrollierte Installation von Anwendungen aus teilweise fragwürdigen Quellen, werden mobile Geräte häufig mit Schadsoftware infiziert.

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Mobile Device Management (MDM)-Lösungen ermöglichen den Administratoren auf unterschiedliche Art und Weise die Kontrolle über die Nutzung und den Zugriff auf dienstlich genutzte Mobilgeräte nach zuvor definierten Sicherheitsrichtlinien. MDM-Lösungen können den Patchstatus der Mobilgeräte ermitteln und das Einspielen von Updates auslösen, sobald diese verfügbar sind und getestet wurden. Außerdem kann zentral ein adäquater Passwortschutz, ein regelmäßiges Backup und eine Geräteverschlüsselung erzwungen werden. Im Falle eines Diebstahls oder eines Verlusts des Geräts kann zusätzlich eine Zwangslöschung erfolgen, um die Vertraulichkeit der Unternehmensdaten zu schützen. Dem Administrator wird es ermöglicht, die Nutzerrechte des Mobilgeräts dahingehend zu setzen, dass eine Installation von Anwendungen aus beliebigen und potentiell unsicheren Quellen nicht erlaubt ist.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

X Verfügbarkeit

X Integrität

X Vertraulichkeit

Authentizität

7.3. Beispiel/ Auszug einer Checkliste zur Überprüfung der TOMs[7]

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Die Umsetzung kann mittels einer Tabelle überprüft und dokumentiert werden.

---

7 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjYkrbw0bfvAhU05eAKHSUwCEwQFjAAegQIAhAD&url=https%3A%2F%2Fwww.sage.com%2Fde-de%2F-%2Fmedia%2Ffiles%2Fsagedotcom%2Fgermany%2Fdocuments%2Fpdf%2Fsupport-und-service%2Fdsgvo%2Fvorlagen%2Ftom_mustervorlage.pdf%3Fla%3Dde-de%26hash%3D4131478865A08578830F33F28BF4FFCF&usg=AOvVaw3Z6F2Mz18Eng60vSAwFjem

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☐ Schlüsselregelung / Liste
☐ Automatisches Zugangskontrollsystem	☐ Empfang / Rezeption / Pförtner
☐ Biometrische Zugangssperren	☐ Besucherbuch / Protokoll der Besucher
☐ Chipkarten / Transpondersysteme	☐ Mitarbeiter- / Besucherausweise
☐ Manuelles Schließsystem	☐ Besucher in Begleitung durch Mitarbeiter
☐ Sicherheitsschlösser	☐ Sorgfalt bei Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	☐ Sorgfalt bei Auswahl Reinigungsdienste
☐ Absicherung der Gebäudeschächte	☐
☐ Türen mit Knauf Außenseite	☐
☐ Klingelanlage mit Kamera	☐
☐ Videoüberwachung der Eingänge	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen bitte hier beschreiben:

Weiterführende Informationen und Beispiele:

Johner Institut
https://github.com/johner-institut/it-security-guideline/blob/master/Guideline-IT-Security_DE.md

BSI
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03161/BSI-TR-03161.pdf;jsessionid=0B7B3A2B7488C1F64BC7B1E8A67A2D92.2_cid351?__blob=publicationFile&v=2

8. Umgang mit Auftragsverarbeitern

8.1 Abgrenzung zu eigenständiger und gemeinsamer Verantwortlichkeit

Beim Einsatz von Dienstleistern zur Verarbeitung von personenbezogenen Daten ist zu prüfen, ob es sich bei der Dienstleistung um eine Auftragsverarbeitung nach Artikel 28 DS-GVO handelt, eine gemeinsame Verantwortlichkeit nach Artikel 26 DS-GVO vorliegt oder es sich um eine Datenübermittlung zwischen eigenständigen Verantwortlichen handelt.

Die Abgrenzung kann sich, je nach Ausgestaltung der Verarbeitung, schwierig gestalten. Prinzipiell gilt als verantwortlich, wer Mittel und Zwecke der Verarbeitung festlegt, d.h. das “Womit” und “Wozu” der Datenverarbeitung (siehe “Verantwortlicher” i.s.d. Artikel 4 Nr. 7 DS-GVO). Im Umkehrschluss gilt das Unternehmen als Auftragsverarbeiter i.S.d. Artikel 4 Nr. 8 , welches keine Kontrolle über die Festlegung dieser Fragen hat.

Im Zweifel ist der Datenschutzbeauftragte zu konsultieren, wenn die Einordnung des Vertragsverhältnisses nicht ohne Weiteres möglich ist. Dabei kommt es nicht auf die Festlegung innerhalb des Vertrages an, d.h. eine Klausel die besagt, dass der Verarbeitung eine Auftragsverarbeitung zugrunde liegt, ist nicht ausschlaggebend zur Einschätzung des Sachverhaltes, sondern nur die tatsächliche Ausgestaltung der Verarbeitung.

Bei einer falschen Einschätzung können vermeintliche Auftragsverarbeiter im Nachhinein als Verantwortliche von der Aufsichtsbehörde eingeschätzt werden und entsprechend aufgrund der zwangsläufig damit einhergehenden mangelhaften Umsetzung ihrer Pflichten hinsichtlich der zugrunde liegenden Verarbeitung mit Bußgeldern belegt werden.

8.2 Eignungsprüfung

Vor Beauftragung des Dienstleisters ist die Eignung von dessen technischen und organisatorischen Maßnahmen zu prüfen und die Datenverarbeitung im Rahmen der zur erbringenden Dienstleistung mit einem Vertrag über die Auftragsverarbeitung **(AV-Vertrag)** zu definieren. Die Eignungsprüfung ist in regelmäßigen Abständen, mindestens jährlich, zu wiederholen und hinreichend zu dokumentieren.

8.2.1. Vertragsprüfung

8.2.1.1. AV-Vertrag (AVV)

Eine Auftragsverarbeitung setzt einen AV-Vertrag voraus, der darauf zu prüfen ist, ob die zwingend nach Art. 28 Abs. 3 DSGVO zu inkludierenden Inhalte enthalten sind. Es ist darauf zu achten, dass der Umfang der Regelungsinhalte die Vorgaben der DSGVO nicht unterschreitet. Dies kann insbesondere im internationalen Kontext, z.B. bei der Beauftragung von Dienstleistern außerhalb des europäischen Wirtschaftsraums auftreten, da hier gegebenenfalls auch lokale oder andere datenschutzrechtliche Sachverhalt in den AV-Vertrag eingebracht werden, die keine Relevanz für die Umsetzung der Vorgaben der DSGVO besitzen, oder diesen gar zuwider laufen.

Die Pflicht zum Abschluss eines AV-Vertrages trifft sowohl den Verantwortlichen als auch den Auftragsverarbeiter in gleichem Maße. Es ist daher nicht statthaft, darauf zu warten,

dass die andere Seite “den ersten Schritt” macht. Beide Seiten haben auf den Abschluss eines AV-Vertrages hinzuwirken. Ohne einen rechtskonformen AV-Vertrag dürfen personenbezogene Daten nicht an Auftragsverarbeiter übermittelt werden. Dies stellt einen erheblichen Verstoß gegen geltendes Datenschutzrecht dar.

Im Rahmen der wiederholten Eignungsprüfung ist der bereits abgeschlossene Vertrag auf geänderte rechtliche Vorgaben durch Weiterentwicklung des Rechts zu prüfen und festgestellte Defizite durch Vertragsänderungen bzw. den Abschluss eines neuen Vertrages zu beheben.

8.2.1.2. Hauptvertrag

In der Regel liegt dem AV-Vertrag ein Dienstleistungsvertrag zugrunde (Hauptvertrag), welcher unter Umständen ebenfalls datenschutzrechtlich relevante Regelungen enthält. Der Vertrag, aber auch alle weiteren in die Verträge eingebundenen Dokumente und Verweise sind auf inhaltliche Widersprüche zum AV-Vertrag zu prüfen. Häufig werden auch Teile der Anforderungen nach Art. 28 DSGVO in den Hauptvertrag vorverlagert, sodass hier ebenfalls zu prüfen ist, ob diese die Anforderungen an die DSGVO erfüllen.

8.2.2. Technische und organisatorische Maßnahmen

8.2.2.1. TOMs im Rahmen des AVV

Die abzuschließenden AV-Verträge müssen eine Aufstellung technischer und organisatorischer Maßnahmen (TOMs) beinhalten, welche die Anforderungen nach Art. 32 DSGVO erfüllen. Die Maßnahmen müssen hinreichend bestimmt sein. Dies ist dann der Fall, wenn dadurch die Datensicherheit erkennbar gewährleistet wird. Die Angabe, dass Maßnahmen vorliegen, ohne diese konkret zu benennen, ist indes nicht ausreichend.

Die Anforderungen an die Ausgestaltung der TOMs müssen dem Stand der Technik entsprechen und richten sich u.a. nach Art und Umfang der Verarbeitung, die Art der zu verarbeitenden Daten und weitere Umstände z.B. den Ort der Verarbeitung und ggfs. mit der Verarbeitung einhergehende Risiken. Sensible personenbezogene Daten, insbesondere solche nach Art. 9 DSGVO (Gesundheitsdaten) erfordern regelmäßig deutlich höhere Anforderungen an den umzusetzenden Stand der Technik.

Neben der Prüfung der TOMs sind Nachweise des Auftragsverarbeiters einzuholen, um die Umsetzung der TOMs gegenüber der Aufsichtsbehörde nachweisen zu können. Als Nachweise kann die Dokumentation des Auftragsverarbeiters (z.B. Datenschutzkonzepte, IT- und Datenschutzrichtlinien etc.), anerkannte Zertifikate für einschlägige Zertifizierungen und Audits bzw. Auditberichte dienen.

8.2.2.2. Zertifikate als Nachweise (ISO 27001, SOC I, SOC II, ISO 27017, ISO 27018)

Es gibt zahlreiche internationale Normen, welche eine standardisierte Umsetzung anerkannter Praktiken beschreiben und welche über Zertifikate als hinreichender Nachweis für TOMs gewertet werden können. Die Üblichsten sollen hier kurz behandelt werden.

ISO 27001 (IT-Sicherheit), ISO 27017 (IT-Sicherheit für Clouddienste), ISO 27018 (Sicherheit personenbezogener Daten bei Clouddiensteanbietern) sind die in Europa üblichsten Zertifizierungen nach einem internationalen Standard, bei welchem ein IT-Sicherheitsmanagementsystem (ISMS) nach festgelegten Kriterien aufgebaut und nachgewiesen wird. Insbesondere größere Unternehmen können solche Zertifizierungen vorweisen. Als Alternative zur ISO 27001 gibt es ferner den weniger gebräuchlichen und auf Deutschland beschränkten BSI-Grundschutz.

Im amerikanischen Bereich finden sich häufig auch Zertifizierungen nach SOC 1 und SOC 2 der Typen I und II. Beide Zertifizierungen entstammen dem US-amerikanischen Bereich der Finanzcompliance und werden bevorzugt von amerikanischen Unternehmen als Nachweise angeboten. Ferner bieten einige Dienstleister auch SOC 3-Berichte an,.

SOC 1 - Zertifizierungen konzentrieren sich hauptsächlich auf finanzielle Prozesse und Maßnahmen und sind regelmäßig von nur geringem Wert als Nachweis wirksamer TOMs.

SOC 2 - Zertifizierungen behandeln Maßnahmen zu IT-Sicherheit und Datenschutz und sind somit im Vergleich zu SOC 1 - Nachweisen deutlich brauchbarer.

SOC 3 - Diese Berichte sind für die Allgemeinheit bestimmt und daher weniger detailliert als SOC II-Berichte. Inwiefern brauchbare Informationen zur Prüfung des Datenschutzes enthalten sind, kann sich von Bericht zu Bericht unterscheiden.

Sowohl SOC 1 als auch SOC 2 - Zertifizierungen können dem “Type I” oder “II” entsprechen. Type I - Zertifizierungen betrachten die Maßnahmen zu nur einem fixen Zeitpunkt, während Type II - Zertifizierungen zusätzlich zu den Prüfpunkten des Type I auch die Wirksamkeit der getroffenen Maßnahmen prüfen, aber über einen definierten Zeitraum hinweg. Type II - Zertifizierungen sind daher deutlich umfangreicher und diese den Type I - Zertifizierungen vorzuziehen.

Auch wenn SOC 2 Type II - Zertifizierungen deutlich umfangreicher ausfallen als die Type I - Variante, sind diese nicht vergleichbar mit ISO 27001- Zertifizierungen. Während die ISO 27001 konkret umzusetzende Maßnahmen vorgibt, gibt SOC 2 keine solche Maßnahmen vor. Vielmehr entscheidet das sich zu zertifizierende Unternehmen, welche Prozesse und Maßnahmen für den eigenen Geschäftsbetrieb notwendig sind und lässt nur diese zertifizieren.

Aufgrund dessen fallen auch SOC 2 - Berichte entsprechend unterschiedlich aus. Diese sind daher hinreichend sorgfältig darauf zu prüfen, ob sämtliche notwendigen TOMs auch entsprechend dadurch nachgewiesen wurden. Andernfalls müssen weitere Nachweise angefordert werden. Eine bloße Prüfung des Zertifikats ist aus denselben Gründen nicht ausreichend.

Die Prüfung von ISO-Zertifizierungen gestaltet sich anders und prinzipiell deutlich einfacher. Jedes Zertifikat sollte geprüft werden, ob die darauf angegebene Gültigkeitsdauer noch nicht abgelaufen ist. ISO-Zertifikate sind regelmäßig drei Jahre gültig. Wenn die Gültigkeitsdauer noch vor dem Ende der Verarbeitung endet, sollte das aktuelle Zertifikat zeitnah vom Dienstleister angefordert werden.

Ferner enthalten ISO - Zertifikate einen Geltungsbereich. Es ist zu prüfen, ob dieser auch die Prozesse erfasst, über welche die Daten verarbeitet werden sollen. Der Geltungsbereich kann sich auf einzelne Standorte, Büros, juristische Personen, einzelne Dienstleistungen oder einzelne Prozesse beziehen. Wird die Verarbeitung nicht vom Geltungsbereich erfasst, so ist das Zertifikat als Nachweis für die TOMs nicht einschlägig.

Ist nicht erkennbar, ob der Geltungsbereich einschlägig ist, kann vom Dienstleister auch die Anwendbarkeitserklärung (SOA - Statement of Applicability) angefordert werden, welche den Geltungsbereich ausführlich definiert. Allerdings gilt dieses Dokument nicht selten als Betriebsgeheimnis, weswegen zahlreiche Unternehmen es nur gegen Unterzeichnung einer Geheimhaltungserklärung (NDA) anbieten oder gar nicht zur Verfügung stellen.

Zertifikate werden von einem Zertifizierer ausgestellt, welcher ebenfalls auf dem Zertifikat angegeben wird. Unterwirft sich der Zertifizierer den Vorgaben und Prüfungen von Akkreditierungsstellen, so wird auch die Akkreditierungsstelle auf dem Zertifikat angegeben (z.B. in Deutschland die DAKKS).

Akkreditierungsstellen halten online Mitgliederlisten vor. Es sollte geprüft werden, ob der Zertifizierer auch von der angegebenen Akkreditierungsstelle als zugelassen geführt wird. Ist dies nicht der Fall oder ist keine Akkreditierungsstelle angegeben, so ist das Zertifikat mit Vorsicht zu genießen, da der Zertifizierer nicht von einer unabhängigen Stelle kontrolliert wird. In solchen Fällen lässt sich der Nachweis u.a. über die Prüfung der einschlägigen Dokumente des ISMS führen.

8.2.3. Auftragsverarbeitung in Drittländern

Länder außerhalb der Europäischen Union gelten als Drittländer, für welche in einem gesonderten Schritt sichergestellt werden muss, dass ein angemessenes Datenschutznievau vorliegt. Für bestimmte Länder hat die EU-Kommission in Form eines Angemessenheitsbeschlusses ein dem der DSGVO vergleichbares Datenschutzniveau festgestellt. Dazu zählen aktuell Andorra, Argentinien, Kanada (nur für kommerzielle Organisationen), Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay und Japan. Die Vereinigten Staaten von Amerika gehören seit dem Fall des Privacy Shields nicht mehr dazu.

Für die Beauftragung von Auftragsverarbeitern in Drittländern gelten dieselben obigen, in diesem Kapitel erwähnten Verpflichtungen. Aufgrund des unsicheren Datenschutzniveaus in solchen Ländern sind jedoch zusätzliche Garantien zur Einhaltung des Datenschutzes notwendig, welche im Folgenden beschrieben werden.

Für DiGA-Hersteller ist zu beachten, dass die im Folgenden erwähnten Garantien nicht ausreichen, um eine Auftragsverarbeitung von Gesundheitsdaten, die im Rahmen der DiGA erhoben werden, abzusichern. Eine solche Datenverarbeitung darf in solchen Fällen nur in Ländern der EU oder in jenen mit Angemessenheitsbeschluss der EU-Kommission erfolgen.

8.2.3.1. Verbindliche interne Datenschutzvorschriften

Unternehmen können eigene interne, rechtlich verbindliche Datenschutzvorschriften (“Binding Corporate Rules”, nachfolgend BCR genannt) erlassen und das darin beschriebene Datenschutzniveau von der EU-Kommission genehmigen lassen. BCR stellen eine geeignete Garantie zur Sicherstellung eines angemessenen Datenschutzniveaus dar. Insbesondere bei großen internationalen Konzernen besteht die Chance, dass diese von der EU-Kommission genehmigte BCR vorweisen können und somit deren Beauftragung erheblich erleichtern. Die EU-Kommission stellt auf ihrer Webseite eine Liste von Unternehmen mit genehmigten BCR zur Verfügung. Allerdings stammt die Liste vom 24.05.2018 und ist damit nicht mehr aktuell.

8.2.3.1. Standardvertragsklauseln

Ein weiteres Instrument zur Sicherstellung geeigneter Garantien sind von der EU-Kommission herausgegebene oder von der Datenschutzaufsichtsbehörde genehmigte Standardvertragsklauseln.

Am 4.6.2021 wurde als Ersatz für die drei bisher gültigen Fassungen eine Neufassung der SCCs beschlossen. Diese müssen ab dem 27.9.2021 zwingend für alle neu abgeschlossenen Verträge anstelle der bisherigen SCCs zum Einsatz kommen. Für bestehende Verträge, in denen die alten SCC bereits vereinbart wurden, gilt jedoch eine Übergangsfrist von 18 Monaten. Entsprechend müssen bis spätestens zum 26.12.2022 diese Altverträge auf die Neufassung umgestellt werden.

Auch wenn gerade bei großen US-Anbietern davon auszugehen ist, dass die Umstellung ihrerseits automatisch passieren wird, ist eine entsprechende Prüfung dringend anzuraten.

Eine der wesentlichsten Änderung der neuen SCC ist deren modularer Aufbau. Neben den beiden bekannten Transferszenarien Verantwortlicher -> Verantwortlicher und Verantwortlicher -> Auftragsverarbeiter, sind nun auch die Konstellation Auftragsverarbeiter in de EU -> Auftragsverarbeiter und Auftragsverarbeiter -> Verantwortlicher vorgesehen. Zunächst muss also festgestellt werden, welches der vier Module für den konkreten Anwendungsfall das richtige ist[8].

Bei dem wohl häufigsten Fall einer Datenübertragung als Verantwortlicher hin zu einem Auftragsverarbeiter (Modul Zwei) wären alle Elemente aus den Anhängen 1 bis 3 in den Vertragstext aufzunehmen. In dieser Fassung erfüllen die SCC dann alle Voraussetzungen einer Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO, so dass diese nicht noch zusätzlich abgeschlossen werden muss.

Die neuen SCC beziehen sich auch bereits auf das Schrems II-Urteil des EuGH. Neu hinzugekommen sind nun weitreichende Pflichten beider Parteien die Rechtsvorschriften und Gepflogenheiten im Drittland einer Risikoabschätzung (Transfer Impact Assessment) zu unterziehen und fortlaufend beobachten. Kann der Datenimporteur den Pflichten aus den SCC nicht mehr nachkommen, müssen die schon im Schrems II-Urteil geforderten zusätzlichen Maßnahmen ergriffen werden. Zudem hat der Datenimporteur die Pflicht,

[8] Eine praktische Aufteilung der Module in Einzeldokumente findet sich hier: https://iapp.org/resources/article/eu-standard-contractual-clauses-word-documents/.

Auskunftsverlangen der Behörden des Drittlandes dem Datenexporteur umgehend mitzuteilen und deren Rechtmäßigkeit gerichtlich überprüfen zu lassen.

Damit übernehmen die SCC zwar bereits einige der Vorschläge, die auch in der Empfehlung 01/2020 des EDSA zur Umsetzung zusätzlicher Maßnahmen enthalten sind. Zu beachten ist aber, dass dennoch stets eine Betrachtung im Einzelfall stattzufinden hat, ob mit den getroffenen MAßnahmen ein angemessenes Schutzniveau gewährleistet werden kann[9]. Die neuen SCC sind damit ebenfalls nicht zwingend ausreichend zur Gewährleistung eines angemessenen Datenschutzniveaus. Zumindest nach Meinung einiger Datenschutzbehörden ist das in Bezug auf Übermittlungen in die USA auch der Fall. Hier müssen weiterhin zusätzliche Maßnahmen wie Verschlüsselung oder Pseudonymisierung ergriffen werden.

Auch die neuen SCCs stellen allerdings keinen gleichwertiger Ersatz für einen Angemessenheitsbeschluss der Europäischen Kommission dar. Die gilt auch für nationalstaatliche Regelung nach § 35 Abs. 7 SGB I. Entsprechend können die SCCS für die Verarbeitung bzw. den Transfer ins Drittland von Gesundheitsdaten von DiGA-Herstellers und Telemedizinanbietern nicht herangezogen werden!

8.2.4. Audit

Die Eignung von Auftragsverarbeitern zur Verarbeitung der vom Verantwortlichen bereitgestellten personenbezogenen Daten muss vom Verantwortlichen vor dem Einsatz des Dienstleisters und sodann in regelmäßigen Abständen festgestellt und überprüft werden.

Die Vorabprüfung wird durch die unter Punkt 8.2 beschriebenen Aspekte der Vertragsprüfung, inklusive technischer und organisatorischer Maßnahmen unter Zuhilfenahme verfügbarer Zertifikate, Konzepte, Richtlinien und Leitlinien in vielen Fällen ausreichend sein.

Bestehen Anhaltspunkte auf Risiken oder erkennbare Unwägbarkeiten, z.B. nach einer bekannt gewordenen Datenpanne, so kann die Prüfung auch Vor-Ort erfolgen. Auftragsverarbeiter sind gemäß Art. 28 Abs. 3 lit. h) DSGVO und durch die Bestimmungen des AV-Vertrags verpflichtet, solche Prüfungen zu dulden.

Allerdings kann es vorkommen, dass Auftragsverarbeiter versuchen dieses Recht des Verantwortlichen im AV-Vertrag zu beschränken. So sind Regelungen, die das Inspektionsrecht auf nur eine Überprüfung im Jahr beschränken, ein Vor-Ort-Audit ganz ausschließen, oder die Kosten dafür dem Verantwortlichen aufbürden, bedenklich und sollten entsprechend nachverhandelt werden. Nach Ansicht der Berliner Datenschutzbehörde sind solche Beschränkungen rechtswidrig, wenn eine solche Überwachung insbesondere durch ein Verschulden des Auftragsverarbeiters ausgelöst wird.

Ist eine reine Dokumentenprüfung nicht zielführend um notwendige Fragen zu beantworten, so kann eine Inspektion vor Ort erfolgen. Der zeitliche Vorlauf, welcher dem Auftragsverarbeiter dabei zur Vorbereitung eingeräumt werden sollte, ist um so kürzer je gewichtiger die Gründe für die Überprüfung sind. Eine anhaltende Datenpanne kann ein

[9] PRESSEMITTEILUNG der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 21. Juni 2021: https://www.datenschutzkonferenz-online.de/media/pm/2021_pm_neue_scc.pdf.

sehr kurzfristiges Audit mit nur wenigen Tagen Vorlaufzeit rechtfertigen, während eine regelmäßige Überprüfung, die nicht anlassbezogen erfolgt auch mit einer Frist von mehreren Wochen vereinbart werden kann. Die Inspektion sollte strukturiert erfolgen (Ablaufplan mit benannten Ansprechpartnern) und mit einem Bericht zu Nachweiszwecken abgeschlossen werden. Festgestellte Mängel sind dem Auftragsverarbeiter mitzuteilen und diesen unter angemessener Fristsetzung zur Behebung aufzufordern. Die Behebung der Mängel ist vom Auftragsverarbeiter nachzuweisen. Ist der Nachweis nicht möglich oder nicht überzeugend, so kann der Verantwortliche sich im Rahmen einer weiteren Inspektion davon überzeugen und diese dokumentieren.

8.3. Unterauftragsverarbeitung

Setzt ein Auftragsverarbeiter selbst einen Auftragsverarbeiter ein, um personenbezogene Daten zu verarbeiten, so spricht man von Unterauftragsverarbeitung. Da auch Verantwortliche für datenschutzrechtliche Verstöße von Unterauftragsverarbeitern zur Verantwortung gezogen werden können, sind Verantwortliche gehalten, auch die Unterauftragsverarbeitung entsprechend abzusichern. Dies erfolgt regelmäßig im Rahmen des AV-Vertrags. Eine solche Regelung ist jedoch nicht verpflichtend, weswegen der Vertrag entsprechend darauf geprüft und bei Bedarf angepasst werden sollte.

Insbesondere ist es empfehlenswert den Auftragsverarbeiter zu verpflichten, in seinen Verträgen mit den Unterauftragsverarbeitern das Recht auf Einforderung von Nachweisen und Durchführungen von Inspektionen durch den Verantwortlichen zu vereinbaren.

Gleichzeitig sind sämtliche an der Verarbeitung beteiligten Unterauftragsverarbeiter mindestens mit Firma, Adresse und Art der Datenverarbeitungen in die bestehenden AV-Verträge aufzunehmen. Es empfiehlt sich jedoch auch Kontaktdaten zum jeweiligen DSB mit aufzunehmen. Nicht ausreichend ist indes eine bloße Auflistung von Diensten, die in Anspruch genommen werden, ohne die konkrete juristische Person dahinter zu identifizieren.

Ferner müssen Regelungen getroffen werden, die den Auftragsverarbeiter und dessen Unterauftragsverarbeiter verpflichten, rechtzeitige Meldung zu erstatten, wenn Unterauftragsverarbeiter gewechselt oder hinzugefügt werden. Dem Verantwortlichen steht hinsichtlich solcher Änderungen ein Einspruchsrecht zu, welches sich per Gesetz an keine Einschränkungen knüpft. Allerdings finden sich in AV-Verträgen nicht selten Regelungen, welche das Einspruchsrecht an hohe Bedingungen knüpfen oder entsprechend reduzieren. Hier ist zu prüfen, inwiefern Art und Umfang der Datenverarbeitung die Akzeptanz solcher Einschränkungen erlaubt.

8.4 Informationen zur Nutzung von Cloud-Infrastrukturen

- **Die folgenden Hinweise gelten nur für DiGA-Hersteller -**

8.4.1 Hintergrund und bisherige Interpretation des BfArM

- DSGVO: Die DSGVO erlaubt grundsätzlich eine Datenverarbeitung personenbezogener Daten innerhalb der Europäischen Union (EU). Eine Verarbeitung außerhalb der EU in einem sog. Drittstaat ist zulässig, sofern ein vergleichbares Schutzniveau im Drittstaat durch einen Angemessenheitsbeschluss nach Artikel 45 DSGVO besteht.
- DiGA Verordnung: Die Digitale Gesundheitsanwendungen-Verordnung (DiGAV) beschränkt analog zu den für Krankenkassen geltenden Regeln (§ 80 SGB X) den Ort der Datenverarbeitung für die von der DiGA nach § 4 Abs. 2 DiGAV verarbeiteten Daten auf die Bundesrepublik Deutschland, die Mitgliedstaaten der EU, die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR) und die Schweiz und Staaten, für die ein Angemessenheitsbeschluss nach Artikel 45 DSGVO vorliegt (nachfolgend **“sichere Staaten**” genannt). Das heisst:
    a. Eine Verarbeitung personenbezogener Daten außerhalb der EU allein auf Basis von Standardvertragsklauseln (Artikel 46 DSGVO), (Binding Corporate Rules (Artikel 47), oder Ausnahmen gemäß Artikel 49 DSGVO ist für DiGA nicht zulässig (vgl. § 4 Abs. 3 DiGAV).
    b. In einer aktuellen Liste der Staaten, für die ein Angemessenheitsbeschluss nach Artikel 45 DSGVO vorliegt, wurden bisher die USA aufgeführt. Hier galt der Angemessenheitsbeschluss für Unternehmen, die unter den EU-US Privacy Shield fallen, welches mit der Entscheidung des EuGH vom 16.07.2020 für nicht ausreichend erklärt wurde. Da § 4 Absatz 3 DiGAV grundsätzlich nur die Verarbeitung von personenbezogenen Daten in Drittstaaten zulässt, wenn ein Angemessenheitsbeschluss nach Artikel 45 DSGVO vorliegt, ist eine Verarbeitung von personenbezogenen Daten in den USA im Rahmen von DiGA seitdem nicht mehr zulässig. Eine Lösung über Standardvertragsklauseln ist nicht gangbar. Weiterhin ist eine Datenverarbeitung in den USA im Rahmen einer DiGA nach (datenschutzrechtlicher) Patienteneinwilligung gemäß DSGVO regelmäßig nicht zulässig.
- Problematik von “Grenzfällen”:
    a. Viele DiGA-Hersteller haben schon vor dem Schrems II auf die Cloud-Infrastrukturen etablierter Anbieter mit US amerikanischem Mutterkonzern (d.h. bspw. Google Cloud, Amazon Web Services, Microsoft Azure) gesetzt, welche durch ihre europäischen Entitäten i.d.R. der DS-GVO verpflichtet
    b. Allerdings steht dieser Rechtsverpflichtung immer auch der sog. “Cloud Act” entgegen, welcher amerikanische Unternehmen verpflichten kann, unter gewissen Voraussetzungen und bei Vorlage einer richterlichen Verfügung Daten aus ihren Rechenzentrum offenzulegen, unabhängig davon, in welcher Geographie und welcher rechtlichen Sub-Einheit diese gespeichert und verwaltet liegen. Mehr Information und eine rechtliche Einschätzung zu diesem Konflikt kann man auch hier nachlesen

Bis zum 28.01.2021 wurde auf dieser Basis die Nutzung von Cloud Infrastrukturen von Dienstleistern, die zwar örtlich und rechtlich innerhalb der EU agieren (bspw. Amazon Luxemburg mit AWS RZ innerhalb der EU) verweigert.

8.4.2. Handreichung des BfArM am 28.01.2021

Nach einer Abstimmung mit dem Bundesgesundheitsministerium hat das BfArM hier am 28.01.2021 eine offizielle Rechtsauffassung formuliert, welche Klarheit bzgl. der für Hersteller schaffen kann.

Achtung: Diese Positionierung und Einschätzung steht unter dem Vorbehalt, dass eine für den DiGa Hersteller zuständige Landesdatenschutzbehörde *(Anm. rechtlich verantwortlich und "weisungsbefugt" für einen DiGa Hersteller ist immer der Landesdatenschutzbeauftragte des Bundeslandes, in dem der Hersteller ansässig ist, bspw. Hamburg)* diese Ansicht nicht teilen muss, d.h. es kann vorkommen, dass diese die nachfolgenden Interpretationen nicht teilen und den Hersteller dadurch zwingen können, ein anderes Set-Up zu wählen.

Zusammenfassung:

Dienstleister (z.B. Betreiber von Rechenzentren) welche innerhalb der DiGa zum Einsatz kommen

- mit (selbständiger) Niederlassung in sicheren Staaten (z.B. Google Limited Ireland),
- aber einem Mutterkonzern in den USA (z.B. Google LLC),
- dürfen aufgrund des EuGH-Urteils und den 2 Vorgaben der DiGAV (nur) unter bestimmten Voraussetzungen für die Verarbeitung von personenbezogenen Daten herangezogen werden

Eine Inanspruchnahme kommt allein unter Beachtung strenger Anforderungen in Betracht, die hinreichende Gewähr für die Unterbindung einer Datenübertragung aus dem Geltungsbereich der DSGVO an das Mutterunternehmen bieten (s. FAQ). Auch für jegliche Tools, die im Rahmen der Nutzung der DiGA ggfs. zum Einsatz kommen, muss dabei ein Datenfluss von personenbezogenen Daten in die USA vollumfassend ausgeschlossen werden.

8.4.3. Mögliche Ansätze zur technischen Umsetzung

Für die Sicherstellung dieser Anforderungen beschreibt das BfArM u.a. die Möglichkeiten und Voraussetzungen (Auswahl):

- Es existiert ein Vertrag zur Auftragsverarbeitung nach §28 DS-GVO mit einer innerhalb sicherer Staaten registrierten juristischen Person des Cloud-Anbieters (z.B. Google Ireland Limited)
- Speicherung und Verarbeitung der Daten in einem Rechenzentrum des Anbieters innerhalb sicherer Staaten (z.B. AWS Datacenter Frankfurt a.M.)
- Weitere technische oder organisatorische Maßnahmen zur Sicherstellung der o.G. Kriterien **[Achtung: diese Kriterien müssen beide erfüllt sein gemäß einem zu erwarteten Update des BfArM]**:
    a. Verschlüsselung der Daten nach neuestem Stand der Technik (siehe hier Informationen zum Verschlüsselungsverfahren und eigene Schlüsselverwaltung des DiGa-Herstellers unabhängig oder außerhalb des Einflussbereiches des Cloud-Anbieters, z.B. Customer-Managed Encryption Keys, CMEK (siehe 9.4.3.3)
    b. Vertragliche Zusicherung des Anbieters, keine Daten in unsichere Drittländer zu leiten, sofern nicht ein höchstrichterlicher Beschluss vorliegt und ein Übereinkommen mit dem Drittland gem. Art. 48 DSGVO existiert.

Andere Konstrukte wie bspw. Standardvertragsklauseln (SCCs), Binding Corporate Rules (BCRs) oder andere Garantien sind nicht zulässig. *Es ist grundsätzlich davon auszugehen, dass es keine lediglich vertragliche Lösung mit in der EU ansässigen Tochterunternehmen von US-Konzernen gibt, welche die Anforderungen des BfArMs erfüllt.*

8.4.3.1 Sonderthema “3rd Party Appstore” (d.h. Google Play, Apple Appstore)

Bei der Bereitstellung einer DiGA, die auf einer mobilen App basiert, müssen Hersteller regelmäßig auf den Appstore der jeweiligen Plattform zurückgreifen. Die Verarbeitung bestimmter personenbezogener Daten der Store-Betreiber außerhalb des Einflussbereiches des DiGA-Herstellers (d.h. bspw. nicht in einem Rechenzentrum in einem sicheren Staat, nicht im Schlüsselverwaltungsbereich des Herstellers) wird dahingehend akzeptiert,

- dass personenbezogene Daten, die bei der Anmeldung der DiGA vom Nutzer erhoben werden keine Gesundheitsdaten darstellen und, getrennt von den diesen innerhalb der DiGA gespeichert werden.
- dass bei der Nutzung von Push Nachrichten (welche i.d.R. ebenfalls auch auf den Servern der Anbieter versendet werden) keine gesundheitsbezogenen Daten enthalten sind (z.B. “Dein Blutdruck von 158/120 ist eindeutig zu hoch!”)

8.4.3.2 Welche Möglichkeit des eigenen Key Managements sollte ich verwenden?

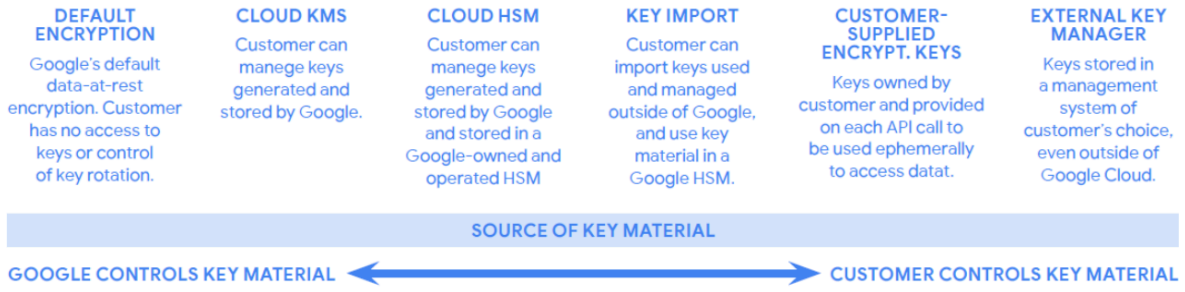
Diese Fragestellung ist sehr davon abhängig,

- Welche Ressourcen (finanziell, organisatorisch, Entwickler, DevOps) dem DiGA-Hersteller zur Verfügung stehen

- welche Möglichkeiten der Cloud-Anbieter erlaubt, selbst anbietet, von extern integrieren lässt
- wie die Datenstruktur innerhalb der DiGa aufgebaut ist
- wie viele Daten verschlüsselt werden müssen und können

Beispiel Google Cloud Infrastruktur:

Google verschlüsselt “ab Werk” bereits alle Daten “at rest”, d.h., die in Datenbanken und Hardware abgelegt sind, mit dem eigenen Encryption Verfahren (Default Encryption). Hierfür hat jedoch Google den “Verschlüsselungs-Key” selbst in der Hand, d.h. Google kannim Zweifel (bspw. bei Aufforderung im Rahmen des FISA oder CLOUD-Acts durch eine US Behörde) die Daten entschlüsseln und weitergeben. Daher ist es für DiGA-Hersteller beim Einsatz solcher Dienstleister geboten, diese Schlüssel selbst zu verwalten (siehe markierte Verfahren) (Customer-Supplied Encryption Keys, External Key Manager).



Das Verschlüsseln und Verwalten von Schlüsseln in diesen zwei Stufen kann man grob in folgende Schritte zusammenfassen, welche dann

- entweder durch einen eigenen Service des DiGA-Herstellers erledigt (d.h. Customer Supplied Encrypted Keys and Management CMEK)
- oder von einem externen Key Provider (z.B. Equinix, Ionic, Thales, Fortanix) übernommen werden.
- Einzelaspekte der technischen Umsetzung sind u.a.: Key generation, Key storage, Key distribution and installation, Key usage, Key rotation, Key backup, Key recovery, Key revocation, Key suspension, Key destruction.

Hier ist vom DiGA-Hersteller abzuwägen, ob er selbst ein solches Schlüsselmanagement entwickeln, verwalten und übernehmen will oder dafür einen Anbieter (“key as a Service”) in Anspruch nimmt. Grob kann man dies wie folgt nach Vor-und Nachteilen einteilen:

CMEK (selbst entwickelt)	**CMEK (mit ext. Key Provider)**
+ Geringe externe Kosten pro Verschlüsselung **+ Volle Kontrolle über Verschlüsselungsmechanismus** **+ Keine Steuerung externer**	**+ Maximale Compliance und Audit-Proof (weil professionelle Anbieter selbst zertifiziert sind)** **+ Einfache Einbindung in Systeme** **+ Keine eigene DevOps**

Services	**Maintenance notwendig** **+ Hoch skalierbar** **+ Kontrolle der Schlüssellokalisierung (key provenance) und gute SLA**
- Hoher Entwicklungs- und Maintenanceaufwand (Anpassungen, Kryptographie, Schutz vor Angreifern) **- Bei Verlust oder Fehlern im Key Management besteht Gefahr, Kontrolle oder Zugriff auf Daten vollständig zu verlieren !!!** **- Entwicklung kryptographisches Key Management für sich nicht zu unterschätzen in Komplexität**	**- Oft sehr hohe Kosten für Verschlüsselungspakete und einzelne Transaktionen** **- Synchronisation von externem Key Provider mit eigenem Rechenzentrum wichtig, um Latenz und dadurch ggf. Fehler in der Ansprache der APIS zu vermeiden (bspw. sollte ein Google RZ in Frankfurt und ein Key Provider RZ in Australien vermieden werden)**