Bundesministerium
für Wirtschaft
und Energie

# Orientierungshilfe zum Gesundheits-datenschutz

**Impressum**

**Herausgeber**
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

**Stand**
November 2018

**Druck**
Druck- und Verlagshaus Zarbock GmbH & Co. KG,
60386 Frankfurt am Main

**Gestaltung**
PRpetuum GmbH, 80801 München

**Bildnachweis**
Getty Images
baranozdemir / S. 54
Gregory Huczynski / EyeEm / S. 73
imaginima / S. 80
Ralf Hiemisch / S. 18
rolfo eclaire / S. 19
suedhang / S. 82
Tinpixels / S. 51
Vertigo3d / S. 68
Westend61 / S. 14, S. 61
Yuichiro Chino / Titel

**Diese und weitere Broschüren erhalten Sie bei:**
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

**Zentraler Bestellservice:**
Telefon: 030 182722721
Bestellfax: 030 18102722721



Bundesministerium
für Wirtschaft
und Energie

# Orientierungshilfe zum Gesundheits-datenschutz

# Überblick

## Für wen ist die Orientierungshilfe gedacht und worin unterstützt Sie die Orientierungshilfe?

Die Gesundheitswirtschaft ist einer der größten deutschen Wirtschaftssektoren. In ihrer Weiterentwicklung spielt die Digitalisierung eine zunehmend bedeutsame Rolle. Etablierte Unternehmen entwickeln neue digitale Lösungen, junge Start-ups treiben kreative Ideen und innovative Geschäftsmodelle voran. Gleichzeitig gilt der erfolgreiche Eintritt in den Gesundheitsmarkt aufgrund der regulatorischen Anforderungen als schwierig und findet nicht immer im gewünschten Umfang statt. Vor diesem Hintergrund bietet die Digitalisierung der Gesundheitswirtschaft ein besonderes Potenzial, dessen Realisierung durch das BMWi aktiv unterstützt werden soll.

Eine besondere Herausforderung für digitale Produkte stellen dabei die datenschutzrechtlichen Anforderungen dar. Das gilt erst recht, seitdem die europäische Datenschutz-Grundverordnung (DSGVO) am 25.05.2018 in Kraft getreten ist. Der Datenschutz ist im Bereich der Gesundheitswirtschaft besonders bedeutsam, da Gesundheitsdaten sensibel sind und deswegen umfassend zu schützen sind. Entwickler von digitalen Produkten sollten diese datenschutzrechtlichen Anforderungen frühzeitig berücksichtigen, damit ihre Produkte nicht zu einem späteren Zeitpunkt aufwendig angepasst werden müssen.

Die Orientierungshilfe zum Datenschutz für Gesundheitsdaten soll Entwicklern und Anbietern von digitalen Gesundheitsprodukten daher einen Einstieg in diesen wichtigen Bereich bieten. Sie stellt sowohl die allgemeinen datenschutzrechtlichen Anforderungen als auch die Bestimmungen für besondere Bereiche, wie z. B. die automatisierte Entscheidungsfindung, Big-Data-Anwendungen und die Entwicklung von Apps dar. Um die erforderliche Praxisnähe zu gewährleisten, ist sie in Abstimmung mit Unternehmen aus der Digitalwirtschaft entstanden. Zur Vertiefung wird auf frei erhältliche Darstellungen, Checklisten und Musterformularen von Behörden und Verbänden verwiesen. Neben der ausführlichen Darstellung im Dokument, das heruntergeladen werden kann, finden sich auf dieser Seite noch FAQs sowie ein Glossar zu den zentralen Begriffen des Datenschutzrechts in der Gesundheitswirtschaft.

Die Darstellung wendet sich an alle Unternehmen, die Gesundheitsdaten erheben und verarbeiten. Dabei wird der Begriff der Gesundheitsdaten sehr weit verstanden, um den sensiblen Gesundheitsdaten den bestmöglichen Schutz zuzugestehen (Teil 1 der Orientierungshilfe).

## Allgemeine Anforderungen

### Rechtfertigungsgründe für die Verarbeitung von Gesundheitsdaten

Die Verarbeitung von personenbezogenen Daten ist nur erlaubt, wenn besondere Rechtfertigungsgründe vorliegen. Bei den sensiblen Gesundheitsdaten gelten neben den allgemeinen datenschutzrechtlichen Anforderungen zusätzliche Voraussetzungen. Die Orientierungshilfe stellt die praxisrelevanten Rechtfertigungsgründe und möglichen Ausnahmetatbestände anhand von konkreten Beispielen vor (Teil 2 A.I der Orientierungshilfe). Es werden insbesondere die Anforderungen an die in der Praxis überaus bedeutsame Einwilligung erläutert und eine entsprechende Best Practice dargestellt.

### Organisatorische Maßnahmen zum Schutz der Gesundheitsdaten

Unternehmen, die mit sensiblen Gesundheitsdaten umgehen, müssen organisatorische Vorkehrungen treffen, um den Schutz dieser Daten zu gewährleisten. Diese Vorkehrungen fangen mit einer Verpflichtung der Beschäftigten auf das Datengeheimnis und der Erstellung eines Verzeichnisses aller Datenverarbeitungsvorgänge an. Eine wesentliche Anforderung ist die Bestellung einer bzw. eines Datenschutzbeauftragten, der das Unternehmen beim Datenschutz berät und den Kontakt mit den zuständigen Aufsichtsbehörden hält (Teil 2 A.II der Orientierungshilfe).

Welche Maßnahmen konkret zu treffen sind, ist mit Hilfe einer risikobasierten Datenschutz-Folgenabschätzung zu ermitteln. Die Orientierungshilfe stellt das dazu erforderliche Verfahren dar und verweist auf weitere Leitfäden und praktische Anwendungsfälle (Teil 2 A.VI der Orientierungshilfe).

### Maßnahmen zur Wahrung der Nutzerrechte

Zu ihrem Schutz werden den Betroffenen verschiedene Rechte gewährt. Sie müssen von den Unternehmen zunächst durch eine Datenschutzerklärung über die Datenverarbeitung informiert werden. Darüber hinaus können die Betroffenen Auskünfte über ihre Daten verlangen und/oder die Berichtigung oder Löschung ihrer Daten fordern. Sie können der weiteren Verarbeitung ihrer Daten (teilweise) widersprechen oder deren Übertragung an einen anderen Anbieter fordern. Unternehmen müssen deswegen bei der Produktentwicklung sicherstellen, dass sie diesen Rechten der Betroffenen auch entsprechen können. Neben der Erläuterung der einzelnen Betroffenenrechte und deren Bedeutung enthält die Orientierungshilfe zu diesem Zweck auch Vorschläge für entsprechende Konzepte (Teil 2 A.III der Orientierungshilfe).

### Vorgaben zur Datensicherheit

Gerade im Gesundheitsbereich ist die Datensicherheit von entscheidender Bedeutung. Die Betroffenen und die Öffentlichkeit reagieren überaus sensibel, wenn es zu Datenpannen kommt. Durch die DSGVO wird das erforderliche Schutzniveau verbindlich konkretisiert. In der Orientierungshilfe werden diese Vorgaben näher erläutert und Beispiele für geeignete Sicherheitsmaßnahmen sowie ein Vorgehen und die damit verbundenen Anforderungen bei Datenpannen vorgestellt. Zudem wird auf weitere Leitlinien von Datenschutzbehörden und Verbänden verwiesen (Teil 2 A.IV und A.V der Orientierungshilfe).

## Arbeitsteilige Datenverarbeitung

Die zunehmende Komplexität der Datenverarbeitung führt dazu, dass die Verarbeitung in vielen Fällen arbeitsteilig durchgeführt wird.

### Gemeinsame Datenverantwortlichkeit

Bei der arbeitsteiligen Datenverarbeitung durch mehrere Beteiligte sind grundsätzlich die allgemeinen datenschutzrechtlichen Anforderungen zu beachten. Die Orientierungshilfe erläutert, wie nach den allgemeinen Regeln eine Vereinbarung über die Zusammenarbeit abgeschlossen und Betroffene entsprechend informiert werden können (Teil 2 A.VII der Orientierungshilfe).

### Auftragsverarbeitung durch spezialisierte Dienstleister

Anders liegt die Sache, wenn sich ein Unternehmen bei der Verarbeitung von Gesundheitsdaten von spezialisierten (technischen) Dienstleistern unterstützen lässt. Das kann insbesondere der Fall bei der Nutzung von Cloud-Diensten sein. Für eine solche Datenverarbeitung durch Dienstleister sieht die DSGVO gewisse Privilegierungen und Ausnahmen von den strengen Voraussetzungen für den Austausch von Gesundheitsdaten mit anderen Unternehmen vor. Um in den Genuss dieser Erleichterungen zu kommen, muss der Dienstleister als weisungsgebundener Auftragsverarbeiter unter Beachtung bestimmter Vorgaben beauftragt werden. Die Orientierungshilfe stellt den Umfang der Privilegierung sowie die Voraussetzungen für diese Auftragsverarbeitung anhand von konkreten Beispielen vor. Ein besonderes Augenmerk wird auf Dienstleister im Ausland gelegt, wobei zwischen dem EU-Ausland, den privilegierten Drittländern, den USA und den sonstigen Drittländern unterschieden wird (Teil 2 C der Orientierungshilfe).

## Anforderungen bei besonderen Datenarten

Die Anforderungen an den Datenschutz können bei besonderen Datenarten variieren. Während bei Daten, die dem Berufsgeheimnis unterfallen, noch strengere Regeln gelten, können die Vorgaben bei erfolgreich anonymisierten Daten entfallen.

### Daten, die dem Berufsträgergeheimnis unterliegen

Besondere Anforderungen sind für die Daten von Ärzten und anderen Heilberufen zu beachten. Denn diese Heilberufe unterliegen besonderen Schweigepflichten, deren Verletzung auch strafrechtlich sanktioniert werden kann. Es muss deswegen neben den datenschutzrechtlichen Vorschriften auch geprüft werden, ob die Verarbeitung von Gesundheitsdaten in diesen Fällen berufsrechtlich zulässig ist (Teil 2 B der Orientierungshilfe).

### Anonymisierung der Daten

Bei anonymen oder anonymisierten Daten entfallen die Vorgaben der DSGVO, weil kein Personenbezug hergestellt werden kann. Es sollte jedoch gerade bei Gesundheitsdaten nicht vorschnell davon ausgegangen werden, dass eine Anonymisierung vorliegt. Die hinter den Daten stehende Person darf nicht mehr mit vertretbarem Aufwand identifizierbar sein. Dabei liegt eine Identifizierbarkeit noch vor, wenn die natürliche Person mittels Informationen von Dritten ermittelt werden kann. Da Informationen über den Gesundheitszustand höchst individuell sind, können Personen gerade auf dieser Datengrundlage vergleichsweise leicht ermittelt werden. Die Orientierungshilfe stellt deswegen unterschiedliche Verfahren vor, mit denen sich Gesundheitsdaten erfolgreich anonymisieren lassen (Teil 2 F.II der Orientierungshilfe).

## Anforderungen für besondere Produkte

Die datenschutzrechtlichen Anforderungen können auch danach variieren, welche Produktart angeboten wird.

### Vorgaben für Apps

Das Angebot von Apps bildet einen wesentlichen Teil der digitalen Gesundheitswirtschaft (mhealth). Mit Hilfe von mobilen Geräten kann der Nutzer Gesundheitsdienste von überall nutzen. Allerdings können damit besondere Risiken für seine Gesundheitsdaten einhergehen. Die Orientierungshilfe stellt dar, welchen datenschutzrechtlichen Anforderungen besondere Aufmerksamkeit gewidmet werden sollte und welche rechtlichen Anforderungen zusätzlich zu berücksichtigen sind (Teil 2 D der Orientierungshilfe).

### Besondere Anforderungen an Profiling und automatisierte Entscheidungsfindung

Innovative digitale Gesundheitsprodukte nutzen häufig Profiling und automatisierte Entscheidungsfindungen zur Unterstützung der Diagnose oder Therapieempfehlung. Es werden bestimmte persönliche Aspekte einer natürlichen Person bewertet, um deren Gesundheit zu analysieren. Theoretisch kann auf dieser Grundlage eine Diagnose ohne Beteiligung eines Menschen erfolgen. Für derartige Anwendungen gelten aufgrund der damit verbundenen Auswirkungen für die Betroffenen jedoch besonders strenge Voraussetzungen. Die Orientierungshilfe erläutert, unter welchen Voraussetzungen die Verwendung derartiger Hilfsmittel zulässig ist und welche Sicherheitsvorkehrungen getroffen werden müssen (Teil 2 E der Orientierungshilfe).

### Big-Data-Auswertungen

Besondere Fortschritte in der Medizin werden aufgrund von Big-Data-Anwendungen erwartet. Durch die Analyse einer Vielzahl von Daten können neue Wirkungszusammenhänge erkannt werden. Sofern nicht ausnahmsweise anonymisierte Daten vorliegen, unterliegen derartige Anwendungen jedoch besonderen datenschutzrechtlichen Anforderungen. Die Orientierungshilfe führt in diese Problematik ein und zeigt erste Lösungsmöglichkeiten auf (Teil 2 F.I der Orientierungshilfe).

## Nachweis der Datenschutz-Compliance

Für Unternehmen ist es von entscheidender Bedeutung, im Zweifelsfall die Einhaltung der datenschutzrechtlichen Vorgaben nachweisen zu können. Dafür ist zunächst eine umfassende Dokumentation erforderlich. Darüber hinaus bieten unterschiedliche Stellen eine Prüfung der datenschutzrechtlichen Vorgaben an und erteilen entsprechende Bescheinigungen oder Zertifizierungen. Auf eine Übersicht über derartige Stellen wird in der Orientierungshilfe verwiesen (Teil 3 der Orientierungshilfe).

*Das Forschungsvorhaben „Orientierungshilfe zum datenschutzrechtlichen Umgang mit Gesundheitsdaten“ ist von der Rechtsanwaltskanzlei lindenpartners verfasst worden.*

# Inhalt

# Teil 1


Herz
HF /min
30
EKG
ST mm
II V1 aVL II
D1 Art mmHg Sys
36/35
D2 ZVD mmHg Kontr.
(-5)
Kein Nullabgleich
Entropie
RE 49
SE 44
T1 34.0 38.0
T1
36.5

# Für wen ist die Orientierungshilfe gedacht?

Die Orientierungshilfe richtet sich primär an Unternehmen, die Gesundheitsdaten für digitale Produkte verarbeiten. Die Orientierungshilfe bietet einen Überblick über die wesentlichen dabei zu beachtenden datenschutzrechtlichen Anforderungen.

## I. Was sind Gesundheitsdaten?

Gesundheitsdaten sind besonders sensible Daten. Das Datenschutzrecht behandelt sie daher als eine besondere Kategorie personenbezogener Daten.

Von Gesundheitsdaten spricht man, wenn es sich um Daten handelt, die sich

- auf eine natürliche Person beziehen (Personenbezug) und
- Informationen zu deren Gesundheitszustand enthalten (Gesundheitsbezug).

### 1. Personenbezug

Unter „personenbezogenen Daten“ versteht man Informationen, die sich auf eine bestimmte natürliche Person beziehen (Artikel 4 Nr. 1 DSGVO). Nur solche Daten unterliegen dem Datenschutz. Keine natürlichen Personen sind z. B. juristische Personen wie eine GmbH oder eine AG.

Ein Personenbezug kann bereits bestehen, wenn die natürliche Person, auf die sich die Information bezieht, erst mit weiteren Hilfsmitteln (z. B. Suchmaschinen) identifizierbar ist. Das ist etwa bei Pseudonymen der Fall, wenn ein Unternehmen über Mittel verfügt, mithilfe derer man herausfinden kann, welche Person sich hinter dem Pseudonym verbirgt. Dabei kommt es nicht darauf an, ob nur bestimmte Personen in einem Unternehmen (etwa der Leiter der IT) diesen Bezug herstellen können oder ob das Unternehmen überhaupt ein Interesse daran hat, die Person hinter dem Pseudonym zu identifizieren. Der Begriff „Personenbezug“ ist daher sehr weit zu verstehen.

#### 1.1 Beispiele

- Persönliche Angaben (z. B. Name, Alter, Fotos)
- Sachliche Angaben (z. B. Kreditwürdigkeit, Vertragsbeziehungen)
- Geodaten
- Online-Kennungen (z. B. IP-Adressen, Cookies)

#### 1.2 Kein Personenbezug bei Anonymisierung

Das Datenschutzrecht findet dagegen keine Anwendung, wenn die Daten in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Es ist allerdings Vorsicht bei der Annahme geboten, bestimmte Daten seien bereits „anonym“, nur weil man z. B. den Namen der Person entfernt hat. Die Anforderungen an eine Anonymisierung sind streng. Solange eine Re-Identifizierung der Person, auf die sich die Daten ursprünglich bezogen, möglich ist, sind die Daten grundsätzlich nicht anonym.

### 2. Gesundheitsbezug

Gesundheitsdaten sind nur solche personenbezogenen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Artikel 4 Nr. 15 DSGVO).

Der Begriff „Gesundheitsdaten“ wird sehr weit verstanden. Das soll der gesteigerten Schutzbedürftigkeit dieser sensiblen Daten Rechnung tragen. Erfasst sind jegliche Informationen, die die Gesundheit einer Person unter allen Aspekten – körperlichen wie psychischen – betreffen:

### 2.1 Beispiele

Gesundheitsdaten umfassen z. B. Informationen, die von der Untersuchung eines Körperteils oder aus genetischen Daten abgeleitet wurden. Die Informationen können sich auf Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder den biomedizinischen Zustand der betroffenen Person beziehen.

Zu den Gesundheitsdaten zählen auch Vermutungen zu bestimmten Veranlagungen des Betroffenen aufgrund familiärer Vorbelastungen, die Messung von Gesundheitsdaten in Fitnessstudios sowie Daten, die von Fitness- und Health-Apps sowie Smart Watches erfasst werden.

Auch das Lichtbild einer Person kann ein Gesundheitsdatum sein, beispielsweise wenn daraus hervorgeht, dass die betroffene Person eine Brille trägt.

### 2.2 Zeitpunkt

Informationen über den gegenwärtigen Gesundheitszustand sind ebenso erfasst wie Informationen über den früheren oder künftigen Gesundheitszustand der betroffenen Person.

### 2.3 Herkunft

Die Herkunft des Datums ist für die Einstufung als Gesundheitsdatum nicht entscheidend. Das Datum kann also Gesundheitsdatum sein, wenn es beispielsweise von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder der Person selbst stammt. Es ist aber auch jede andere Herkunft denkbar.

### 2.4 Mittelbare Rückschlüsse

Gesundheitsdaten liegen schließlich auch dann vor, wenn mittelbar über andere Daten ein Rückschluss auf den Gesundheitszustand möglich ist. Das ist beispielsweise der Fall, wenn Informationen zum Aufenthalt in einer Klink oder gesundheitsrelevanten Einrichtung, zur Teilnahme an Patienten- oder Selbsthilfegruppen oder zu einem Kuraufenthalt verarbeitet werden. Immer dann, wenn Rückschlüsse auf den gesundheitlichen Zustand des Betroffenen möglich sind, liegen grundsätzlich Gesundheitsdaten vor.

### 3. Weiterführende Links

- **Bayerische Landesdatenschutzbehörde**, Besondere Kategorien personenbezogener Daten, Artikel 9 DSGVO, August 2016: https://www.lda.bayern.de/media/baylda_ds-gvo_6_special_categories.pdf
- **DSK**, Besondere Kategorien personenbezogener Daten, März 2018: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_17_Besondere-Kategorien.pdf
- **ICO**, What is personal data? (engl.): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
- **EU-Kommission**, Was sind personenbezogene Daten?: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_de

## II. Wann unterliegt die Verwendung von Gesundheitsdaten den Vorgaben der DSGVO?

Wenn ein Unternehmen Gesundheitsdaten in irgendeiner Art und Weise nutzt oder verwendet, muss es hierfür die Vorgaben der DSGVO beachten.

Denn die DSGVO gilt in sachlicher Hinsicht immer dann, wenn Gesundheitsdaten „verarbeitet“ werden (Artikel 2 DSGVO). „Verarbeiten“ ist sehr weit zu verstehen und meint grundsätzlich jeden Vorgang im Zusammenhang mit personenbezogenen Daten (Artikel 4 Nr. 2 DSGVO).

**Beispiele:** Erfasst sind insbesondere die Verwendung, das Erheben, das Erfassen, das Ordnen, die Speicherung, die Veränderung, das Abfragen, die Offenlegung durch Übermittlung, die Bereitstellung, der Abgleich und die Löschung von Daten.

## III. Für welche Unternehmen gelten die Vorschriften der DSGVO?

Die Vorschriften der DSGVO gelten nur für diejenigen Unternehmen, die in ihren räumlichen Anwendungsbereich fallen (Artikel 3 DSGVO).

### 1. In der EU tätige Unternehmen

Die DSGVO ist z. B. anwendbar, soweit ein Unternehmen in einem Mitgliedstaat der Europäischen Union (etwa in Deutschland) niedergelassen ist und die Verarbeitung der Daten im Rahmen der Tätigkeit dieser Niederlassung erfolgt.

Eine „Niederlassung" in diesem Sinne kann bereits vorliegen, wenn das Unternehmen eine effektive und tatsächliche Tätigkeit in der EU mittels einer festen Einrichtung ausübt. Die Rechtsform der Niederlassung ist nicht entscheidend, insbesondere muss es sich nicht um eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handeln.

**Beispiel:** Unselbständige Zweigstelle eines US-Unternehmens in Deutschland.

### 2. EU als Marktort

Ist das Unternehmen nicht in der EU niedergelassen, kann die DSGVO dennoch anwendbar sein. Das ist etwa der Fall, wenn ein Unternehmen Daten einer Person, die sich in der EU befindet, im Zusammenhang damit verwendet, dass es

- dieser betroffenen Person Waren oder Dienstleistungen anbietet, egal ob kostenpflichtig oder unentgeltlich,

**Beispiele:** kostenlose Gesundheits-App, Cloud-Angebote, Vergleichsportal, Social-Media-Angebote.

oder

- das Verhalten dieser betroffenen Person beobachtet.

**Beispiele:** Tracking und Profiling im Internet durch Analyse-Tools, die durch Cookies die individuelle Rückverfolgung der Nutzer ermöglichen und zum Zwecke der individuellen Werbung (Targeted Advertising) erfolgen.

Es spielt jeweils keine Rolle, welche Staatsangehörigkeit die betroffene Person besitzt, solange sie sich nur physisch in der EU befindet.

### 3. Weiterführende Links

- **DSK**, Kurzpapier zum Marktortprinzip: Regelungen für außereuropäische Unternehmen, Juli 2017: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_7_Marktortprinzip.pdf

# Teil 2

# Welche rechtlichen Anforderungen sind zu beachten?

Die Orientierungshilfe soll einen Überblick über die datenschutzrechtlichen Anforderungen für digitale Produkte im Gesundheitssektor bieten. Sie kann keine Rechtsberatung im Einzelfall ersetzen. Im Zweifelsfall sollten Unternehmen die für sie zuständige Datenschutzaufsichtsbehörde kontaktieren, die innerhalb des geltenden Rechtsrahmens eigenständig die jeweilige Zweifelsfrage beurteilen kann.

Die Orientierungshilfe ist nach einem Baukastenprinzip strukturiert:

- Die Grundvoraussetzungen erläutern, welche datenschutzrechtlichen Anforderungen von allen Unternehmen, die Gesundheitsdaten verarbeiten, zu erfüllen sind (A.).
- Auf die Grundvoraussetzungen bauen fünf Schwerpunktthemen auf. Diese können für mit Gesundheitsdaten arbeitende Unternehmen – abhängig von dem Geschäftsmodell – eine mehr oder weniger große Bedeutung haben. Die Schwerpunktthemen sind:
  - Umgang mit Daten, die dem Berufsträgergeheimnis unterliegen (B.),
  - Einschaltung von externen Dienstleistern in die Verarbeitung von Gesundheitsdaten (C.),
  - Umgang mit Gesundheits-Apps (D.),
  - Nutzung automatisierter Entscheidungsmechanismen mit Bezug auf Gesundheitsdaten (E.) und
  - Einsatz von Big-Data-Analysen unter Einbeziehung von Gesundheitsdaten (F.).

Das Baukastensystem soll es Unternehmen erleichtern, gezielt diejenigen Punkte herauszugreifen und nachzulesen, die die eigene Situation widerspiegeln oder für das eigene Geschäftsmodell besonders relevant sind.

## A. Grundvoraussetzungen

### I. Die Verarbeitung von Gesundheitsdaten erfordert eine Ausnahme und eine Rechtsgrundlage

#### 1. Worum geht es?

Ein zentraler Grundsatz im Datenschutzrecht besagt, dass man personenbezogene Daten nur dann speichern, übermitteln oder anderweitig verarbeiten darf, wenn hierfür eine gesetzliche Rechtsgrundlage besteht. Die infrage kommenden Rechtsgrundlagen sind in der DSGVO aufgelistet (Artikel 6). Als Rechtsgrundlage kommt z. B. die Einwilligung der Person, deren Daten genutzt werden, oder ein Vertrag mit ihr in Betracht.

Bei Gesundheitsdaten gelten jedoch weitaus strengere Regeln als bei einfachen personenbezogenen Daten. Gesundheitsdaten sind sensible, besonders schützenswerte Daten und werden im Gesetz als „besondere Kategorie“ personenbezogener Daten behandelt. Grundsätzlich ist es untersagt, Gesundheitsdaten zu verarbeiten. Dieses Verbot gilt nur dann nicht, wenn einer der gesetzlich geregelten Ausnahmefälle gegeben ist (Artikel 9 Abs. 2–4 DSGVO).

Neben der allgemeinen Rechtsgrundlage für die Verarbeitung muss somit zusätzlich ein Ausnahmetatbestand gerade für die Verarbeitung von Gesundheitsdaten bestehen.

## 2. Was ist zu tun?

Wer Gesundheitsdaten verarbeiten möchte, muss sicherstellen, dass ein spezifischer Ausnahmetatbestand erfüllt ist und er zudem eine Rechtsgrundlage vorweisen kann. Ohne eine derartige „doppelte" Rechtfertigung ist die Verarbeitung von Gesundheitsdaten rechtswidrig und kann sanktioniert werden.

### 2.1 Prüfungsschritte (Übersicht)

Um sicherzustellen, dass die gesetzlichen Voraussetzungen erfüllt sind, bietet es sich an, zunächst die strengeren Regeln speziell für Gesundheitsdaten und sodann die allgemeinen Regeln zu prüfen:

- **Schritt 1:** Kann ich meine geplante Verarbeitung von Gesundheitsdaten auf einen der Ausnahmetatbestände in Artikel 9 Abs. 2–4 DSGVO stützen? Wenn nein, ist die geplante Datenverarbeitung verboten. Wenn ja, weiter mit Schritt 2.

- **Schritt 2:** Sind zusätzlich die Voraussetzungen einer Rechtsgrundlage für die Datenverarbeitung nach Artikel 6 DSGVO erfüllt? Wenn nein, ist die geplante Datenverarbeitung verboten. Wenn ja, ist die Datenverarbeitung erlaubt.

### 2.2 Zu Schritt 1: Liegt eine Ausnahme vom Verbot der Verarbeitung von Gesundheitsdaten vor?

Als Grundregel gilt, dass Gesundheitsdaten nicht verarbeitet werden dürfen. Nur wenn eine oder mehrere der gesetzlichen Ausnahmen einschlägig ist/sind, greift diese Grundregel nicht und das Verbot ist aufgehoben.

#### 2.2.1 Systematik der Ausnahmen

Die einzelnen Ausnahmen sind unterschiedlich strukturiert.

a) Einstufige Ausnahmen
Teilweise sind die Voraussetzungen für eine Ausnahme einstufig und unmittelbar aus dem Text der DSGVO ableitbar. Eine solche Ausnahme besteht etwa bei Gesundheitsdaten, deren Verarbeitung zur Geltendmachung oder Verteidigung von Rechtsansprüchen erforderlich ist.

**Beispiel:** Ein Krankenhaus wird wegen eines angeblichen Behandlungsfehlers von einem Patienten auf Schadensersatz verklagt. Das Krankenhaus möchte Daten zur Behandlung des Patienten vorlegen, um sich zu entlasten. Soweit diese Datenverarbeitung zur Verteidigung der behaupteten Rechtsansprüche des Patienten erforderlich ist, greift eine Ausnahme und das Verbot ist aufgehoben (Artikel 9 Abs. 2 lit. f DSGVO).

b) Mehrstufige Ausnahmen
Viele andere Ausnahmen sind dagegen mehrstufig aufgebaut und dienen als eine Art Brücke zum bereichsspezifischen Recht. Sie verweisen auf andere Spezialgesetze, die die Verarbeitung von Gesundheitsdaten erlauben können.

Solche Spezialgesetze können sich aus dem europäischen Recht (z. B. einer EU-Verordnung) oder dem nationalen Recht des jeweiligen EU-Mitgliedstaates (für Deutschland siehe unten 2.2.2) ergeben. Nur wenn auch die jeweiligen Voraussetzungen eines solchen Spezialgesetzes erfüllt sind, besteht eine Ausnahme vom Verarbeitungsverbot.

**Beispiel:** Ein Unternehmen darf Gesundheitsdaten für statistische Zwecke verarbeiten, wenn ein Spezialgesetz dies erlaubt (Artikel 9 Abs. 2 lit. j DSGVO). Ein solches Spezialgesetz findet sich in § 27 Abs. 1 BDSG-neu. Nur wenn auch die Voraussetzungen dieses § 27 Abs. 1 BDSG-neu erfüllt sind, ist das Verbot der Verarbeitung aufgehoben.

#### 2.2.2 Welche nationalen Ausnahmen gibt es?

Gesundheitsdaten werden in den EU-Mitgliedstaaten unterschiedlich geschützt. Das liegt daran, dass die DSGVO selbst zwar einheitlich für alle EU-Mitgliedstaaten gilt, aber gerade im Bereich der Gesundheitsdaten (Artikel 9 DSGVO) viele sogenannte Öffnungsklauseln enthält.

Diese Öffnungsklauseln räumen den EU-Mitgliedstaaten weitreichende Freiräume ein, eigene nationale Regelungen dazu zu treffen, wann und inwieweit ein Unternehmen Gesundheitsdaten nutzen darf. Die Mitgliedstaaten dürfen somit eigene Rechtsgrundlagen für die Datenverarbeitung schaffen. Auch in Deutschland gibt es zahlreiche bereichsspezifische Regelungen zur Zulässigkeit der Verarbeitung von Gesundheitsdaten.

a) Rechtsgrundlagen in Bundesgesetzen
Einige wichtige Beispiele für Ausnahmen in Bundesgesetzen sind:

- das **neue Bundesdatenschutzgesetz BDSG-neu** (z. B. § 27 BDSG-neu bei wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken),
- die **Regelungen in den Sozialgesetzbüchern**, insbesondere allgemein zur Verarbeitung von Sozialdaten (§§ 67a ff. SGB X), im SGB V zur gesetzlichen Krankenversicherung (z. B. §§ 284 ff. SGB V) oder im SGB XI zur gesetzlichen Pflegeversicherung (z. B. §§ 93 ff. SGB XI),
- das **Infektionsschutzgesetz** (z. B. § 9 InfSchG),
- das **Transplantationsgesetz** (z. B. §§ 13 ff. TPG),
- das **Medizinproduktegesetz** (z. B. § 20 Abs. 1 Nr. 2 MPG),
- das **Transfusionsgesetz** (z. B. § 14 TFG) oder
- das **Versicherungsvertragsgesetz** (z. B. § 213 VVG).

b) Rechtsgrundlagen in Landesgesetzen
In Deutschland sind für das Gesundheitswesen primär die Länder zuständig. Es gibt daher zahlreiche landesrechtliche Regelungen, die datenschutzrechtliche Vorschriften enthalten, wie z. B.

- **Psychisch-Kranken-Gesetze** (z. B. §§ 84 ff. PsychKG Berlin),
- **Maßregelvollzugsgesetze** (z. B. Artikel 34 BayMRVG),
- **Krankenhausgesetze** (§ 24 Abs. 4 LKG Berlin),
- **kirchliches Recht bei Krankenhäusern** in kirchlicher Trägerschaft,
- **Krebsregistergesetze**,
- **Gesundheitsdienstgesetze**.

#### 2.2.3 Zusätzliche Einschränkungen der Ausnahmen durch nationales Recht

Die einzelnen EU-Mitgliedstaaten können aber nicht nur eigene Ausnahmen schaffen. Sie haben zudem die Möglichkeit, für die Verarbeitung von Gesundheitsdaten zusätzliche Bedingungen, einschließlich Beschränkungen, festzulegen (Artikel 9 Abs. 4 DSGO).

Unternehmen sollten daher immer genau prüfen, ob es in ihrem Bereich spezifische nationale Gesetze auf Bundes- oder Länderebene gibt, die sich auf die Zulässigkeit des Umgangs mit Gesundheitsdaten auswirken.

Solche zusätzlichen Einschränkungen können auch dazu führen, dass Ausnahmen, die sich unmittelbar aus der DSGVO ergeben, durch nationale Regelungen weiter eingeschränkt werden.

**Beispiel:** Schriftformerfordernis für Einwilligungen bei genetischen Untersuchungen. In Deutschland müssen Einwilligungen in genetische Untersuchungen nicht nur ausdrücklich erfolgen (vgl. Artikel 9 Abs. 2 lit. a DSGVO), sondern zudem in Schriftform gegenüber dem verantwortlichen Arzt erteilt werden (§ 8 Abs. 1 des Gesetzes über genetische Untersuchungen bei Menschen).

### 2.3 Zu Schritt 2: Gibt es eine Rechtsgrundlage für die Datenverarbeitung?

Im zweiten Schritt muss das Unternehmen prüfen, ob es eine gesetzliche Rechtsgrundlage für die geplante Datenverarbeitung gibt (Artikel 6 DSGVO).

#### 2.3.1 Wichtige Rechtsgrundlagen

Die wichtigsten Rechtsgrundlagen für Unternehmen, die Gesundheitsdaten verarbeiten, sind:

- die Einwilligung der Person, deren Daten verarbeitet werden. Wie diese Einwilligung ausgestaltet sein muss (z. B. Inhalt, Form etc.), ist in der DSGVO geregelt (vgl. Artikel 4 Nr. 11, Artikel 7 und Artikel 8 DSGVO);
- ein Vertrag mit der Person, deren Daten verarbeitet werden. Das gilt jedoch nur, soweit es erforderlich ist, die Daten zu verarbeiten, um den Vertrag zu erfüllen;
- eine rechtliche Verpflichtung, der der Verantwortliche unterliegt und zu deren Erfüllung die Verarbeitung erforderlich ist;

- eine Interessensabwägung, die zugunsten desjenigen ausgeht, der die Daten verarbeiten möchte. Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

#### 2.3.2 Überschneidungen von Ausnahmen und Rechtsgrundlagen

Die Ausnahmen vom Verbot der Verarbeitung von Gesundheitsdaten (Schritt 1) überschneiden sich teilweise mit den Rechtsgrundlagen (Schritt 2).

So z. B. bei der Einwilligung: Sie kann in Schritt 1 eine Ausnahme vom Verbot, Gesundheitsdaten zu nutzen, begründen (Artikel 9 Abs. 2 lit. a DSGVO). Hierzu muss sie ausdrücklich erteilt worden sein, aber auch die allgemeinen Anforderungen an die Einwilligung erfüllen. Liegen diese Voraussetzungen vor, dient die Einwilligung in Schritt 2 der Prüfung gleichzeitig auch als Rechtsgrundlage dafür, diese Daten zu verarbeiten.

Da die Voraussetzungen der Ausnahmen vom Verbot der Verarbeitung von Gesundheitsdaten bereits sehr streng sind, geht mit der Einhaltung dieser Voraussetzungen in vielen Fällen auch die gleichzeitige Erfüllung der Voraussetzungen einer Rechtsgrundlage (Artikel 6 DSGVO) einher. Teilweise wird daher sogar vertreten, dass eine (normale) Rechtsgrundlage (Artikel 6 DSGVO) nicht erforderlich ist, wenn bereits ein Ausnahmetatbestand (Artikel 9 Abs. 2 DSGVO) erfüllt ist.

### 2.4 Beispielsfall zur Prüfung der Zulässigkeit

Das Unternehmen A-Sports betreibt einen professionellen Sports-Blog. A-Sports hat über Twitter erfahren, dass sich der bekannte Fußballspieler Toni K. einen Kreuzbandriss zugezogen hat, und möchte in einem nächsten Post darüber berichten. Ist das datenschutzrechtlich zulässig?

**Schritt 1:** Grundsätzlich ist es dem Unternehmen A-Sports datenschutzrechtlich untersagt, über den Kreuzbandriss zu berichten. Denn A-Sports möchte Gesundheitsdaten einer anderen Person nutzen.

Toni K. hat allerdings die Information zu der Verletzung über seinen offiziellen Twitter-Account persönlich bekannt gegeben. Er hat ein Gesundheitsdatum insoweit offensichtlich öffentlich gemacht. Die Information zum Kreuzbandriss ist dann keine „sensible“ Information mehr.

Damit liegt eine Ausnahme vor, und das Verbot, diese Information zu nutzen, ist aufgehoben (Artikel 9 Abs. 2 lit. e DSGVO).

**Schritt 2:** A-Sports darf den Post gleichwohl nur veröffentlichen, wenn hierfür eine datenschutzrechtliche Rechtsgrundlage besteht.

Als Rechtsgrundlage kann das Unternehmen eine Interessensabwägung anführen (Artikel 6 Abs. 1 lit f. DSGVO), da das öffentliche Interesse an der Information und die Pressefreiheit das Interesse des Toni K. an seiner Privatsphäre in diesem konkreten Fall überwiegen. Denn einerseits ist der Pressefreiheit eine große Bedeutung zuzumessen und besteht wegen der Bekanntheit des Toni K. ein großes öffentliches Interesse an seiner Verletzung. Andererseits kann das Interesse des Toni K. an seiner Privatsphäre als vergleichsweise geringer eingestuft werden, da er selbst die Information bereits veröffentlicht hat.

Das Unternehmen A-Sports kann sich also darauf berufen, dass die Interessenabwägung zu seinen Gunsten ausgeht. Damit ist die Veröffentlichung des Posts auch von einer datenschutzrechtlichen Rechtsgrundlage gedeckt.

## 3. Typische Beispiele für eine zulässige Verarbeitung von Gesundheitsdaten

Im Folgenden werden typische Ausnahmetatbestände und Rechtsgrundlagen, auf deren Grundlage Unternehmen Gesundheitsdaten verarbeiten dürfen, erläutert.

### 3.1 Einwilligung

#### 3.1.1 Worum geht es?

Eine Verarbeitung von Gesundheitsdaten ist erlaubt, wenn die Person, deren Daten verarbeitet werden, ihre ausdrückliche Einwilligung hierzu erteilt. Die betroffene Person muss zum Ausdruck bringen, dass sie mit der konkreten Verarbeitung einverstanden ist.

Eine wirksame Einwilligung ist dabei zugleich Ausnahme vom Verbot, Gesundheitsdaten zu verarbeiten, und Rechtsgrundlage für die Datenverarbeitung.

Die Einwilligung ist für viele Unternehmen die bedeutendste Ausnahme und realistischste Möglichkeit, Gesundheitsdaten zulässig zu verarbeiten.

### 3.1.2 Was ist zu tun?

Der Verantwortliche sollte von dem Betroffenen – dem Nutzer seiner Dienste – eine Einwilligungserklärung einholen. Dabei muss er sicherstellen, dass die Einwilligung ausdrücklich und freiwillig erfolgt und der Betroffene über Umstände und Folgen seiner Einwilligung hinreichend informiert ist.

a) Zweckgebundenheit
Die Einwilligung muss sich auf einen oder mehrere bestimmte Zwecke beziehen. Eine Lockerung erfährt das Erfordernis der Zweckbindung allerdings im Forschungsbereich. Dort besteht die Möglichkeit eines sogenannten *„broad consent“*. Hintergrund des *„broad consent“* ist, dass im Forschungsbereich häufig bei Erhebung der personenbezogenen Daten noch nicht eindeutig dargestellt werden kann, zu welchen Zwecken diese Daten genutzt werden. Daher soll es Studienteilnehmern möglich sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht (Erwägungsgrund 33 der DSGVO).

b) Art und Weise der Erteilung
Die Einwilligung muss ausdrücklich erklärt werden. Es reicht nicht aus, dass die betroffene Person durch schlüssiges Verhalten oder stillschweigend zu verstehen gibt, dass sie mit der Verarbeitung einverstanden ist.

Eine bestimmte Form ist nicht vorgeschrieben. Eine Einwilligung kann daher auch mündlich erteilt werden. Die Einverständniserklärung muss allerdings unmissverständlich und nachweisbar sein.

c) Freiwilligkeit
Damit die betroffene Person eine wirksame Einwilligung erteilen kann, muss der Verantwortliche gewährleisten, dass die Einverständniserklärung freiwillig, d. h. ohne Zwang erfolgt. Die betroffene Person muss eine echte Wahl haben hinsichtlich der Fragen, ob, inwieweit und wem sie die Verarbeitung ihrer Daten gestattet.

An der Freiwilligkeit kann es fehlen, wenn dem Betroffenen eine Leistung nur unter der Bedingung angeboten wird, dass er in eine Nutzung der Daten einwilligt, die für die Erbringung des Dienstes gar nicht erforderlich ist (sogenanntes Kopplungsverbot).

d) Informiertheit
Erforderlich ist, dass die betroffene Person darüber informiert ist, was mit ihren Daten geschieht. Die Einwilligungserklärung kann in AGB enthalten sein, muss dann aber in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen und von anderen Sachverhalten klar zu unterscheiden sein (Artikel 7 Abs. 2 DSGVO).

e) Widerruflichkeit
Darüber hinaus muss der Verantwortliche den Betroffenen darüber informieren, dass ein Widerruf der Einwilligung jederzeit möglich ist. Der Widerruf der Einwilligung muss genauso leicht erfolgen können wie die Erteilung der Einwilligungserklärung selbst.

Ein Widerruf bedeutet zunächst lediglich, dass die jeweilige Datenverarbeitung in Zukunft nicht mehr erfolgen darf. Das heißt aber nicht zwingend, dass auch der gesamte zivilrechtliche Vertrag rückabgewickelt werden muss.

### 3.1.3 Best Practice

- Die Einwilligungserklärung kann mit anderen Erklärungen verbunden werden, muss in diesem Fall aber von dem Verantwortlichen besonders hervorgehoben werden, z. B. durch Fettdruck, Rahmen oder eine Schattierung. Werden diese Vorgaben beachtet, kann die Einwilligung etwa auch Bestandteil von Allgemeinen Geschäftsbedingungen (AGB) sein.

- Für den Betroffenen muss deutlich werden, dass er eine Einwilligungserklärung abgibt und welche Konsequenzen das hat. Ein Button mit der Aufschrift „Jetzt geht’s los“ reicht nicht aus.

- Der Betroffene soll die Möglichkeit erhalten, zumutbar Kenntnis über den Inhalt der Erklärung zu erlangen und nicht mit einer Informationsflut überfordert werden. Um eine solche Informationsüberladung zu vermeiden, kann die Einwilligungserklärung ggf. auf den wesentlichen Kern reduziert werden und im Übrigen auf eine verlinkte ausführlichere Darstellung (z. B. in der Datenschutzerklärung) verwiesen werden.

#### 3.1.4 Wichtige Rechtsvorschriften

- **Artikel 4 Nr. 11 DSGVO** (Definition)
- **Artikel 6 Abs. 1 lit. a DSGVO** (Einwilligung als Rechtsgrundlage)
- **Artikel 7 DSGVO** (Bedingungen für die Einwilligung)
- **Artikel 8 DSGVO** (Einwilligung bei Kindern)
- **Artikel 9 Abs. 2 lit. a DSGVO** (Einwilligung als Ausnahme vom Verbot, Gesundheitsdaten zu verarbeiten)

#### 3.1.5 Weiterführende Links

- **Artikel-29-Gruppe**, Leitlinien zur Einwilligung, April 2018: https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Artikel-29-Gruppe/wp259-rev-0_1_DE.PDF
- **Bayerische Landesdatenschutzbehörde**, Die Einwilligung nach der DSGVO, Mai 2018: https://www.datenschutz-bayern.de/datenschutzreform2018/einwilligung.pdf
- **GDD-Praxishilfe DS-GVO XIII**: Einwilligung, Mai 2018: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_13.pdf
- **GMDS/DMI**, Anforderungen an eine Einwilligung, August 2016: http://ds-gvo.gesundheitsdatenschutz.org/download/einwilligung.docx
- **GMDS/GDD**, Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU Datenschutz-Grundverordnung, Ziff. 5.1 zur Einwilligung, Mai 2017: https://www.gdd.de/arbeitskreise/datenschutz-und-datensicherheit-im-gesundheits-und-sozialwesen/materialien-und-links/datenschutzrechtliche-anforderungen-an-die-medizinische-forschung-unter-beru-cksichtigung-der-eu-datenschutz-grundverordnung/datenschutzrechtliche-anforderungen-an-die-medizinische-forschung-unter-beru-cksichtigung-der-eu-datenschutz-grundverordnung
- **ICO**, Consent at a glance (engl.): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent
- **IHK Berlin**, Hinweise zur Einwilligung: https://www.ihk-berlin.de/Service-und-Beratung/recht_und_steuern/vertragsrecht_online_recht/datenschutzgrundverordnung/einwilligung/4005120
- **Bitkom**, Hinweise zur Einwilligung, Oktober 2016: https://www.bitkom-consult.de/news/%E2%80%9Eja-ich-will%E2%80%9C-%E2%80%93-einwilligungen-nach-der-neuen-eu-datenschutzgrundverordnung

### 3.2 Offensichtlich öffentlich gemachte Daten

#### 3.2.1 Worum geht es?

Hat die Person, um deren Daten es geht, ihre Gesundheitsdaten offensichtlich öffentlich gemacht, so kann eine Verarbeitung auch ohne ausdrückliche Einwilligung oder Kontakt zu dieser Person erlaubt sein.

#### 3.2.2 Was ist zu tun?

a) Öffentliche Gesundheitsdaten

Der Verantwortliche muss zunächst prüfen, ob die betroffene Person ihre Gesundheitsdaten offensichtlich öffentlich gemacht hat.

Eine Person hat ihre Gesundheitsdaten öffentlich gemacht, wenn die Daten dem Zugriff einer unbestimmten Anzahl von Personen ohne wesentliche Zulassungsschranke offenstehen.

**Beispiel:** Ein Patient berichtet in frei zugänglichen Foren des Internets oder auf allgemein einsehbaren Plattformen in sozialen Netzwerken über von ihm erlittene Nebenwirkungen eines Medikaments. Informationen zu Nebenwirkungen, die Dritte (und somit nicht der Betroffene selbst) öffentlich gemacht haben, oder Daten aus geschützten Bereichen in den sozialen Netzwerken können dagegen nicht ohne Weiteres verarbeitet werden.

b) Rechtsgrundlage

Im zweiten Schritt bedarf es zudem einer Rechtsgrundlage für die Verarbeitung. In Betracht kommt als Rechtsgrundlage regelmäßig eine Interessensabwägung. Sind Informationen im Internet frei verfügbar, so spricht das Recht auf Information dafür, dass auch ihre Nutzung datenschutzrechtlich grundsätzlich erlaubt ist. Die Interessensabwägung muss jedoch immer einzelfallbezogen erfolgen und die Rechte und Interessen des Betroffenen hinreichend berücksichtigen.

#### 3.2.3 Best Practice

Der Verantwortliche sollte dokumentieren, woher die Gesundheitsdaten stammen, um auf diese Weise nachweisen zu können, dass die Daten tatsächlich öffentlich gemacht wurden. Auch die Rechtsgrundlage für die Verarbeitung, z. B. die Interessensabwägung, sollte dokumentiert werden.

#### 3.2.4 Wichtige Rechtsvorschriften

- **Artikel 9 Abs. 2 lit. e DSGVO** (Ausnahme vom Verbot, öffentliche Gesundheitsdaten zu verarbeiten)
- **Artikel 6 Abs. 1 lit. f DSGVO** (Interessensabwägung als typische Rechtsgrundlage zur Verarbeitung öffentlicher Daten)

### 3.3 Maßnahmen für die individuelle Gesundheit

#### 3.3.1 Worum geht es?

Eine Erlaubnis für die Verarbeitung von Gesundheitsdaten kann vorliegen, wenn die Verarbeitung der individuellen Gesundheitsversorgung dient. Das gilt aber nur dann, wenn ein Spezialgesetz die Datenverarbeitung legitimiert oder ein Vertrag mit einem Angehörigen des Gesundheitsberufs (z. B. Arzt) zugrunde liegt.

Im Vordergrund dieser Ausnahme steht das individuelle Interesse an der gesundheitlichen Versorgung und der damit verbundenen Abwicklung. So sollen z. B. bei routinemäßigen Krankheitsfälle Gesundheitsdaten im Interesse des Betroffenen schnell bearbeitet werden können.

#### 3.3.2 Was ist zu tun?

Das Unternehmen muss prüfen, ob die mehrstufigen Voraussetzungen der Ausnahme erfüllt sind. In der Regel liegt dann auch eine Rechtsgrundlage zur Verarbeitung vor.

a) Erforderlichkeit der Datenverarbeitung für bestimmten Zweck

Die Daten dürfen nur verarbeitet werden, wenn dies zu einem der in Artikel 9 Abs. 2 lit. h DSGVO genannten Zwecke erforderlich ist. Zu diesen Zwecken zählen z. B.:

- Sämtliche Formen medizinischer Versorgung präventiver, diagnostischer, kurativer und nachsorgender Artikel
- Im Zusammenhang mit gesundheitsbezogenen Handlungen erforderliche Verwaltungstätigkeit und die Arbeit von Abrechnungsstellen und Apotheken.

b) Spezialgesetz oder Vertrag mit einem Angehörigen eines Gesundheitsberufs

Die jeweilige Zweckbestimmung muss sich entweder aus dem Recht der Union oder dem eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs ergeben.

Das Unternehmen muss daher prüfen, ob es (i) ein Gesetz oder (ii) einen Vertrag mit einem Angehörigen eines Gesundheitsberufs gibt, welches bzw. welcher die Verarbeitung der Gesundheitsdaten erlaubt.

**Beispiele:**

- Behandlungsvertrag zwischen einem Arzt und einem Patienten.
- Verarbeitung von Daten, die medizinische Leistungserbringer den Krankenkassen und den Kassenärztlichen Vereinigungen mitteilen (sogenannte Leistungsdaten), auf der Grundlage von §§ 294 ff. SGB V.

c) Verarbeitung nur bei Geheimhaltungspflicht
Es muss schließlich gewährleistet sein, dass nur Personen, die einem Berufsgeheimnis oder einer sonstigen Geheimhaltungspflicht unterliegen, die Gesundheitsdaten verarbeiten. Solche Geheimhaltungspflichten können sich unmittelbar aus dem Gesetz ergeben oder von Stellen, die nach nationalem Recht hierfür zuständig sind, erlassen werden, wie Aufsichtsbehörden oder berufsständische Organisationen.

In Deutschland gibt es Regeln zum Berufsgeheimnis in § 203 StGB und in den Heilberufsordnungen für Ärzte, Apotheker oder Psychologen in Form des sogenannten Patientengeheimnisses.

**Beispiele:** Ärzte, Psychotherapeuten, Medizinische Fachangestellte, Krankenschwestern und Krankenpfleger, Hebammen, Masseure, Krankengymnasten, medizinisch-technische Assistenten sowie berufsmäßig tätige Gehilfen.

d) Rechtsgrundlage
Liegen die Voraussetzungen dieser Ausnahme vor, besteht regelmäßig auch eine Rechtsgrundlage für die Verarbeitung.

- Rechtsgrundlagen sind bei der Verarbeitung aufgrund eines Gesetzes typischerweise die Erfüllung einer Rechtspflicht oder die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Artikel 6 Abs. 1 lit. c bzw. lit. e. DSGVO).

- Bei der Verarbeitung aufgrund eines Vertrages ist regelmäßig auch die Rechtsgrundlage der Vertragserfüllung miterfüllt (Artikel 6 Abs. 1 lit. b DSGVO).

#### 3.3.3 Wichtige Rechtsvorschriften

- **Artikel 9 Abs. 2 lit. h DSGVO**
(Ausnahme bei Versorgung im Gesundheitsbereich)

- **Artikel 6 Abs. 1 lit. b, c, e DSGVO**
(typische Rechtsgrundlagen)

- **§ 630a ff. BGB** (zivilrechtlicher Behandlungsvertrag)

- **§ 203 StGB** (zum Berufsgeheimnis)

### 3.4 Forschungszwecke oder statistische Zwecke

Eine Verarbeitung von Gesundheitsdaten kann erlaubt sein, wenn sie zu wissenschaftlichen Forschungszwecken oder statistischen Zwecken erforderlich ist. Diese Ausnahmen spielen vor allem für Big-Data-Analysen eine Rolle. Zu Einzelheiten siehe Ziff. F.I.2.1.3.

## II. Anpassung der Unternehmensorganisation

### 1. Verpflichtung der Mitarbeiter auf das Datengeheimnis

Unternehmen sollten sicherstellen, dass alle Mitarbeiter zur Wahrung des Datengeheimnisses und zur Beachtung der geltenden datenschutzrechtlichen Anforderungen verpflichtet werden. Ein entsprechendes **Muster** findet sich hier (bzw. unter weiterführende Links).

Die Verpflichtung muss bei der Aufnahme der Tätigkeit erfolgen. Sie sollte daher spätestens am ersten Arbeitstag vorgenommen werden.

Die Verpflichtung dient dazu, den Beschäftigten deutlich zu machen, dass sie im Rahmen der täglichen Aufgabenerfüllung mit besonders sensiblen Gesundheitsdaten arbeiten und die datenschutzrechtlichen Reglementarien zum Umgang mit diesen Daten von allen Mitarbeitern eingehalten werden müssen.

#### 1.1 Wichtige Rechtsvorschriften

- **Artikel 28 Abs. 3 DSGVO, Artikel 29 DSGVO, Artikel 32 Abs. 4 DSGVO**.

#### 1.2 Weiterführende Links

- **DSK**, Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO, Mai 2018: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_19_Verpflichtung-Beschaeftigte.pdf

## 2. Einsetzung eines Datenschutzbeauftragten

### 2.1 Worum geht es?

Unternehmen, die mit Gesundheitsdaten arbeiten, sind in einigen Fällen gesetzlich verpflichtet, einen Datenschutzbeauftragten zu bestellen.

### 2.2 Was ist zu tun?

Unternehmen müssen prüfen, ob sie zur Bestellung eines Datenschutzbeauftragen gesetzlich verpflichtet sind, und sodann eine geeignete Person mit dieser Aufgabe betrauen.

#### 2.2.1 Frage des „Ob“

In welchen Fällen die Bestellung eines Datenschutzbeauftragten erforderlich ist, ergibt sich aus Artikel 37 Abs. 1 DSGVO und § 38 Abs. 1 BDSG. Typische Konstellationen bei Gesundheitsdaten:

a) Umfangreiche Verarbeitung von Gesundheitsdaten
Besteht eine Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung von Gesundheitsdaten, muss ein Datenschutzbeauftragter benannt werden.

- **Kerntätigkeiten** sind Tätigkeiten, die von herausragender Bedeutung für die Erreichung der Unternehmensziele sind – etwa, weil das Unternehmen ohne diese Tätigkeit nicht in der Lage wäre, seine Produkte oder Dienstleistungen anzubieten. Hingegen handelt es sich bei Hilfs- oder Nebentätigkeiten, die dem eigentlichen Geschäftszweck untergeordnet sind, nicht um Kerntätigkeiten.

- Als **umfangreich** kann die Verwendung der Gesundheitsdaten gelten, wenn große Mengen an Gesundheitsdaten verarbeitet werden oder eine große Anzahl von Personen betroffen ist und aufgrund der Sensibilität der Daten ein hohes Risiko besteht. Indikatoren können dabei sein: Wie viele Datensätze werden verarbeitet? Sind viele Unternehmen als Verantwortliche oder Auftragsverarbeiter beteiligt? Welche geografische Reichweite hat die Datenverarbeitung? Dabei soll die Datenverarbeitung regelmäßig nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten betrifft und durch einen einzelnen Arzt erfolgt.

b) Mindestens zehn Personen verarbeiten Daten
Unternehmen, die ständig mindestens zehn Personen mit der automatisierten Verarbeitung von personenbezogenen Daten (egal ob Gesundheitsdaten oder andere Daten) beschäftigen, müssen einen Datenschutzbeauftragten bestellen.

Wann eine „ständige“ Beschäftigung mit der automatisierten Datenverarbeitung anzunehmen ist, ist – auch unter den zuständigen Datenschutzbeauftragten der Länder – umstritten. Falls diese Frage eine Rolle spielen kann, sollte sie mit dem jeweils zuständigen Landesdatenschutzbeauftragten abgeklärt werden.

Nach dieser Vorschrift besteht in vielen Unternehmen eine Pflicht zur Bestellung eines Datenschutzbeauftragten. Beschäftigte, die nicht mit der automatisierten Datenverarbeitung betraut sind, stellen aufgrund der fortschreitenden Digitalisierung in den meisten Unternehmen die Ausnahme dar. Nur solche Beschäftigte, die keinerlei Zugang zu Datenverarbeitungssystemen mit personenbezogenen Daten haben, können insoweit außer Betracht bleiben. Für die Zahl der relevanten Beschäftigten spielt es keine Rolle, ob es sich um Voll- oder Teilzeitbeschäftigte oder z. B. freie Mitarbeiter oder Praktikanten handelt.

c) Datenschutz-Folgenabschätzung
Nehmen Unternehmen Datenverarbeitungen vor, die einer Datenschutz-Folgenabschätzung unterliegen (vgl. hierzu Ziff. V), hat dieser Umstand ebenfalls zur Folge, dass ein Datenschutzbeauftragter zwingend zu bestellen ist.

#### 2.2.2 Frage des „Wie“

a) Wer kommt in Betracht?
Bei der Auswahl des Datenschutzbeauftragten ist die berufliche Qualifikation und insbesondere das Fachwissen auf dem Gebiet des Datenschutzrechts bzw. der Datenschutzpraxis ausschlagegebend:

- Das erforderliche Niveau des Fachwissens hängt von Art und Umfang der Datenverarbeitungsvorgänge und dem erforderlichen Schutz der Daten ab.

- Es kann ausreichend sein, wenn der Datenschutzbeauftragte nur in einem Teilbereich über eigene Qualifikation verfügt und im Übrigen auf fachkundige Mitarbeiter oder externen Rechtsrat zurückgreifen kann, solange er selbst in der Lage ist, das Große und Ganze selbst zu verstehen.

- Auch sollte der Mitarbeiter zuverlässig sein.

Unternehmen können entweder eine im Unternehmen tätige Person zum Datenschutzbeauftragten benennen (interner Datenschutzbeauftragter) oder hierfür einen Dritten beauftragen (externer Datenschutzbeauftragter).

b) Zeitlicher Umfang
Der Datenschutzbeauftragte muss seine Funktion nicht zwingend in Vollzeit erfüllen. Er kann vielmehr auch mit anderen Aufgaben im Unternehmen betraut sein. Wichtig ist aber, dass dem Datenschutzbeauftragten ein ausreichender Teil seiner Arbeitszeit für die Erfüllung seiner datenschutzrechtlichen Aufgaben zur Verfügung steht.

c) Kein Interessenkonflikt
Aufgaben und Pflichten des Datenschutzbeauftragten dürfen nicht zu einem Interessenkonflikt führen. Ein solcher Interessenkonflikt liegt jedenfalls dann vor, wenn der Datenschutzbeauftragte von ihm zu verantwortende Datenverarbeitungsvorgänge selbst überwachen und damit sich selbst kontrollieren würde.

**Beispiele:** Der Datenschutzbeauftragte darf daher grundsätzlich nicht gleichzeitig Geschäftsführer/Vorstand, Marketing- oder Vertriebsleiter, Leiter der IT-Abteilung oder der Personalverwaltung sein.

d) Prozess der Bestellung
Ein **Muster** für die Bestellung eines internen Datenschutzbeauftragen kann hier (bzw. unter den weiterführenden Links) abgerufen werden. Das Unternehmen muss die Kontaktdaten des Datenschutzbeauftragten veröffentlichen und der zuständigen Aufsichtsbehörde mitteilen. Der Name des Datenschutzbeauftragten gehört nicht zu den Kontaktdaten und muss daher nicht mitgeteilt werden.

- Die **Mitteilung an Aufsichtsbehörden** kann in der Regel über deren Online-Formulare erfolgen, so z. B. für Hamburg hier (bzw. unter den weiterführenden Links).

- Die **Veröffentlichung** kann auf der Homepage (z. B. im Impressum oder in der Datenschutzerklärung) erfolgen.

## 2.3 Stellung und Pflichten des Datenschutzbeauftragten

### 2.3.1 Stellung im Unternehmen

Der Datenschutzbeauftragte ist eine interne Kontrollinstanz und muss bei datenschutzrechtlichen Fragestellungen im Unternehmen einbezogen werden. Unternehmen sind nach der DSGVO verpflichtet, dem Datenschutzbeauftragten die erforderlichen Ressourcen, wie beispielsweise Mitarbeiter, EDV, Fachliteratur, Reisekosten und ggf. externe Beratung, zur Verfügung zu stellen.

Dem Datenschutzbeauftragten dürfen in Bezug auf seine Aufgabe keine Weisungen erteilt werden und er darf wegen seiner Tätigkeit nicht abberufen oder benachteiligt werden. Ferner muss ihm Zugang zu den personenbezogenen Daten/Verarbeitungsvorgängen im Unternehmen ermöglicht werden.

**Beispiel:** Der Datenschutzbeauftragte muss Zutritt zu allen Räumlichkeiten haben, in denen Daten verarbeitet werden. Ferner muss er technischen Zugriff auf alle Programme haben und es ist ein unmittelbarer Kontakt zu der höchsten Managementebene einzurichten.

### 2.3.2 Pflichten des Datenschutzbeauftragten

a) Zentrale Aufgaben
Der Datenschutzbeauftragte ist verpflichtet, das Unternehmen über die gesetzlichen Vorgaben nach der DSGVO sowie nach den sonstigen Datenschutzvorschriften zu unterrichten und zu deren Einhaltung zu beraten.

Er muss die Einhaltung der Vorgaben des Datenschutzes durch den Verantwortlichen überwachen und fungiert als Kontaktstelle zu der zuständigen Aufsichtsbehörde.

b) Risikoorientierte Tätigkeit
Bei der Erfüllung seiner Aufgaben muss der Datenschutzbeauftragte dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung tragen (sogenannte Pflicht zur risikoorientierten Tätigkeit). Der Datenschutzbeauftragte muss seine Tätigkeiten daher je nach Risiko für die Rechte und Freiheiten der betroffenen Personen priorisieren und seine Bearbeitungszeiten entsprechend planen.

Wird der Datenschutzbeauftragte etwa bei einer Datenschutz-Folgenabschätzung konsultiert, die wegen einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten durchgeführt wird, hat diese Aufgabe Vorrang vor weniger dringenden Aufgaben.

c) Verschwiegenheit
Der Datenschutzbeauftragte ist zur Verschwiegenheit verpflichtet.

### 2.4 Wichtige Rechtsvorschriften

Artikel 37 bis 39 DSGVO, § 38 BDSG.

### 2.5 Weiterführende Links

2.5.1 Leitfäden

- **ULD**, Datenschutzbeauftragte, Mai 2018: https://www.datenschutzzentrum.de/uploads/praxisreihe/PraxisReihe-2-Datenschutzbeauftragte.pdf
- **GDD**, Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung, November 2016: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_1.pdf
- **DSK**, Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern, Januar 2018: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/kurzpapiere/DSK_KPNr_12_Datenschutzbeauftragte.pdf
- **Artikel-29-Gruppe**, Leitlinien in Bezug auf Datenschutzbeauftragte, April 2017: https://datenschutz-hamburg.de/assets/pdf/wp243rev01_de.pdf
- **IHK Stuttgart**, Bestellung einer/s betrieblichen Datenschutzbeauftragten: https://www.stuttgart.ihk24.de/Fuer-Unternehmen/recht_und_steuern/Datenschutzrecht/der-betriebliche-datenschutzbeauftragte2/3810788#titleInText0

2.5.2 FAQ

- **LDI**, FAQ zum Datenschutzbeauftragten, Mai 2018: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzbeauftragte/Inhalt/Datenschutzbeauftragte_nach_der_DS-GVO_und_der_JI-RL/Inhalt/FAQ_zum_Datenschutzbeauftragten/FAQ_ein_Dokument.pdf
- **BayLDA**, FAQ zum Datenschutzbeauftragten im medizinischen Bereich. https://www.lda.bayern.de/media/FAQ_DSB_im_medizinischen_Bereich.pdf
- **HmbBDI**, Meldung eines Datenschutzbeauftragten: https://datenschutz-hamburg.de/meldung-dsb

## 3. Rechenschafts- und Dokumentationspflicht

### 3.1 Worum geht es?

Ein Unternehmen, das mit Gesundheitsdaten (und/oder anderen personenbezogenen Daten) arbeitet und über die Zwecke und Mittel der Datenverarbeitung entscheidet, ist „Verantwortlicher“ im Sinne der DSGVO und muss daher „Rechenschaft“ über diese Datenverarbeitung ablegen:

- Das Unternehmen muss hierzu zum einen die Einhaltung der datenschutzrechtlichen Vorgaben sicherstellen.
- Zum anderen muss es auch jederzeit zeigen und nachweisen können, dass es die Vorgaben einhält und welche Compliance-Maßnahmen ergriffen wurden, um Verstöße gegen die datenschutzrechtlichen Bestimmungen zu vermeiden. Anhand dieser Nachweise können die Aufsichtsbehörden wiederum kontrollieren, ob die Unternehmensorganisation den Anforderungen des Datenschutzrechts genügt.

Ein zentraler Bestandteil der Rechenschaftspflicht ist die ordnungsgemäße Dokumentation der datenschutzrechtlich relevanten Prozesse im Unternehmen im Wege eines Verzeichnisses von Verarbeitungstätigkeiten (auch „Verarbeitungsverzeichnis“ genannt).

## 3.2 Was ist zu tun?

Unternehmen müssen die zur Einhaltung der DSGVO erforderlichen Prozesse implementieren und nachweisen bzw. dokumentieren, insbesondere durch ein Verarbeitungsverzeichnis. Ein Verarbeitungsverzeichnis kann auch dann zu erstellen sein, wenn das Unternehmen nicht selbst verantwortlich ist, sondern als Auftragsverarbeiter für ein anderes Unternehmen (vgl. Ziff. C.I) tätig wird.

### 3.2.1 Sicherstellung einer DSGVO-konformen Verarbeitung

Das verantwortliche Unternehmen steht dafür ein, dass die von ihm und/oder seinem Auftragsverarbeiter durchgeführte Verarbeitung von (Gesundheits-)Daten rechtskonform ist und insbesondere alle Grundsätze der Datenverarbeitung (vgl. Ziff. IX) eingehalten werden.

Um die Einhaltung der datenschutzrechtlichen Anforderungen laufend zu gewährleisten, muss das verantwortliche Unternehmen geeignete technische und organisatorische Maßnahmen (siehe Ziff. IV.2.2.1) ergreifen:

- Die Auswahl dieser Maßnahmen erfolgt auf der Grundlage des risikobasierten Ansatzes (vgl. hierzu auch Ziff. IV.2.1.1). Das beutet, dass der Verantwortliche Art, Umfang, Umstände und Zwecke der Datenverarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen und bewerten muss.

- Gefordert sind nur verhältnismäßige Vorkehrungen. Das bedeutet, dass die Maßnahmen von einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten und den damit verbundenen Risiken abhängig sind.

Konkretere Regelungen zu den zu treffenden technischen und organisatorischen Maßnahmen, mit denen die DS GVO sachgerechten Datenschutz erreichen will, finden sich in den Regelungen zu Datenschutz „by design and default“ (siehe Ziff. D.II.2) und zur Datensicherheit (siehe Ziff. IV).

### 3.2.2 Nachweis- und Dokumentationspflichten

Die Einhaltung der datenschutzrechtlichen Anforderungen ist vom verantwortlichen Unternehmen nachzuweisen. Der Nachweis wird insbesondere durch umfassende Dokumentation erbracht.

a) Verzeichnis der Verarbeitungstätigkeiten

Verarbeitet ein Unternehmen Gesundheitsdaten, so ist es gesetzlich verpflichtet, ein Verzeichnis aller seiner Datenverarbeitungstätigkeiten zu führen. Das gilt auch, wenn das Unternehmen die Daten im Auftrag und auf Weisung für ein anderes Unternehmen als Auftragsverarbeiter verarbeitet.

*aa) Muster und Inhalt*

Der notwendige Inhalt des Verzeichnisses ergibt sich aus Artikel 30 Absatz 1 DSGVO (Verantwortliche) bzw. Artikel 30 Absatz 2 DSGVO (Auftragsverarbeiter). Bei Erstellung des Verzeichnisses können folgende **Muster** (siehe auch unter den weiterführenden Links) weitere Orientierung bieten:

- Muster für Unternehmen, die als Verantwortlicher Daten verarbeiten

- Muster für Unternehmen, die als Auftragsverarbeiter Daten verarbeiten

**Erläuterungen** zum Ausfüllen der Muster finden Sie hier (siehe auch unter den weiterführenden Links).

*bb) Verfügbarkeit*

Das Verarbeitungsverzeichnis muss nicht veröffentlicht werden. Es ist allerdings der Aufsichtsbehörde jederzeit auf Anfrage zur Verfügung zu stellen.

*cc) Form*

Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen.

*dd) Beispiel*

Wie ein ausgefülltes Verarbeitungsverzeichnis aussehen kann, zeigt dieses Beispiel.

b) Nachweis und Dokumentation im Übrigen

Mit der Erstellung des Verarbeitungsverzeichnisses sind noch nicht alle gesetzlich geforderten Dokumentations- und Nachweispflichten bereits erfüllt. Vielmehr muss das Unternehmen zu allen relevanten Datenverarbeitungen, Prozessen und Strukturen im Unternehmen nachweisen können, dass diese im Einklang mit den gesetzlichen Anforderungen an den Datenschutz stehen.

**Beispiele:** Das Vorhandensein von erforderlichen Einwilligungen, datenschutzfreundliche Technikgestaltung oder Voreinstellungen, das Ergebnis einer erforderlichen Datenschutz-Folgen-Abschätzung und die Gewährleistung der Datensicherheit müssen durch entsprechende Dokumentationen nachgewiesen werden.

Zudem kann die Einhaltung genehmigter Verhaltensregeln (Artikel 40 DSGVO) oder eines genehmigten Zertifizierungsverfahrens (Artikel 42 DSGVO) als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen (vgl. zur Zertifizierung Teil 3 – A.II).

### 3.3 Wichtige Rechtsvorschriften

Artikel 5 Abs. 2 DSGVO (Rechenschaftspflicht), Artikel 24 DSGVO (Verantwortung des für die Verarbeitung Verantwortlichen), Artikel 30 DSGVO (Verarbeitungsverzeichnis).

### 3.4 Weiterführende Links

#### 3.4.1 Verantwortlichkeiten

- **GDD**, Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung, Dezember 2016: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_2.pdf

#### 3.4.2 Verarbeitungsverzeichnis

- **Bitkom**, Leitfaden: Das Verarbeitungsverzeichnis (nebst Mustern und Beispielen), April 2017: https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html
- **DSK**, Musterformulare zu Verarbeitungsverzeichnissen: https://datenschutz-hamburg.de/dsgvo-information/verzeichnis-verarbeitungstaetigkeiten
- **GDD**, Verzeichnis von Verarbeitungstätigkeiten, April 2017: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf
- **DSK**, Kurze Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Juni 2017: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_1_Verzeichnis_Verarbeitungstaetigkeiten.pdf
- **DSK**, Ausführliche Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Februar 2018: https://www.datenschutzzentrum.de/uploads/dsgvo/Hinweise-zum-Verzeichnis-von-Verarbeitungstaetigkeiten.pdf
- **KBV**, Ausfüllbeispiel für ein Verarbeitungsverzeichnis, März 2018: https://www.kbv.de/media/sp/Praxisinformation_Datenschutz_Verarbeitungsverzeichnis_Ausfuellbeispiel.pdf

## 4. Einsetzung eines Vertreters bei nicht in der EU niedergelassenen Unternehmen

Ist ein Unternehmen (ob als Verantwortlicher oder Auftragsverarbeiter) nicht in der EU niedergelassen, so muss es u. U. einen Vertreter in der EU bestimmen. Einzelheiten sind in Artikel 27 DSGVO geregelt.

# III. Rechte der Betroffenen und Pflichten gegenüber Betroffenen

Personen, deren Gesundheitsdaten (oder auch andere personenbezogene Daten) verarbeitet werden, stehen eine Reihe von gesetzlichen Rechten zu – die sogenannten Betroffenenrechte. Diese Rechte können im Vorfeld, während und nach der Datenverarbeitung bestehen.

Aus den Betroffenenrechten ergeben sich entsprechende gesetzliche Pflichten, welche die für die Datenverarbeitung verantwortlichen Unternehmen befolgen müssen. Teilweise müssen Unternehmen dabei von sich aus tätig werden (z. B. Erteilung von Informationen über die Datenverarbeitung, Löschung von Daten), teilweise (nur) auf Verlangen des Betroffenen (z. B. Recht auf Auskunft, Recht auf Datenübertragung).

## 1. Rahmenregelungen (Fristen, Form u. a.)

### 1.1 Worum geht es?

Artikel 12 DSGVO stellt Rahmenregelungen hinsichtlich transparenter Information, Kommunikation und Modalitäten auf, die Unternehmen grundsätzlich bei allen Betroffenenrechte berücksichtigen müssen.

### 1.2 Was ist zu tun?

Die Rahmenregelungen enthalten u. a. Vorschriften zu Form, Fristen, Ausnahmen, Entgelten sowie Identitätsnachweisen im Zusammenhang mit der Geltendmachung von

Betroffenenrechten. Insbesondere folgende Vorschriften sind zu beachten:

- Macht eine betroffene Person von ihren Betroffenenrechten Gebrauch, muss das verantwortliche Unternehmen der betroffenen Person Informationen über die daraufhin ergriffenen Maßnahmen zur Verfügung stellen. Die Information muss unverzüglich, in jedem Fall aber innerhalb eines Monats, nachdem das Betroffenenrecht geltend gemacht worden ist, erteilt werden. Die Frist kann in bestimmten Fällen um weitere zwei Monate verlängert werden (Artikel 12 Abs. 3 DSGVO).

  Innerhalb der Frist sollte die betroffene Person in jedem Fall eine Statusmeldung zu ihrem Antrag erhalten. Der Anspruch der betroffenen Person muss daher nicht zwingend auch innerhalb der Frist erfüllt werden. Es handelt sich bei der Frist wohl nicht um eine Erledigungsfrist. Die rechtliche Einordnung ist allerdings noch nicht abschließend geklärt.

- Will das verantwortliche Unternehmen dem Antrag der betroffenen Person (z. B. auf Berichtigung) nicht nachkommen, so muss es die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit unterrichten, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

- Betroffene Personen müssen die ihnen zustehenden Betroffenenrechte unentgeltlich geltend machen können. Das verantwortliche Unternehmen darf hierfür daher grundsätzlich keine Bearbeitungsgebühren o. ä. verlangen. Nur in bestimmten Ausnahmefällen darf ein angemessenes Entgelt verlangt werden (vgl. hierzu Artikel 12 Abs. 5 DSGVO).

## 2. Informationspflichten

### 2.1 Worum geht es?

Unternehmen müssen Transparenz darüber herstellen, wie sie personenbezogene Daten verarbeiten. Sie müssen daher Personen, deren personenbezogene Daten sie verarbeiten, bestimmte Informationen über die Datenverarbeitung zur Verfügung stellen. Die Information muss proaktiv mitgeteilt werden – also unabhängig davon, ob der Betroffene eine solche Information verlangt.

**Beispiel:** Ein Unternehmen kommt seinen Informationspflichten nach, indem es eine Datenschutzerklärung/Privacy Policy in seiner Gesundheits-App zur Verfügung stellt und darin umfassend erläutert, wie und in welchem Umfang personenbezogene Daten im Zusammenhang mit der App verarbeitet werden.

### 2.2 Was ist zu tun?

Welche Informationspflichten gelten, hängt davon ab, ob das Unternehmen die Daten bei der betroffenen Person selbst erhebt oder nicht. In beiden Fällen muss zudem über Widerspruchsrechte informiert werden.

#### 2.2.1 Inhalt der Informationspflicht

Der Inhalt der mitzuteilenden Informationen ergibt sich unmittelbar aus Artikel 13 oder Artikel 14 DSGVO, je nachdem, ob es sich um eine Direkterhebung handelt oder nicht.

- Soweit die Datenerhebung mit Kenntnis oder unter Mitwirkung der betroffenen Person erfolgt, werden die Daten bei dem Betroffenen erhoben. In diesem Fall ergeben sich die von dem Unternehmen zu beachtenden Informationspflichten aus Artikel 13 DSGVO.

**Beispiele:** Der Betroffene gibt Informationen zu Vorerkrankungen direkt in eine vom Verantwortlichen angebotene App ein.

- Soweit die Daten dagegen nicht bei dem Betroffenen erhoben werden, sondern z. B. von Dritten stammen, ist Artikel 14 DSGVO einschlägig.

**Beispiele:** Ein Unternehmen wertet Daten aus, welche die betroffenen Personen in sozialen Netzwerken selbst veröffentlicht haben.

- Die mitzuteilenden Informationen sind in beiden Fällen weitestgehend identisch; der Verantwortliche muss aber im Rahmen von Artikel 14 DSGVO zusätzlich über die Kategorien der verarbeiteten Daten aufklären. Der maßgebliche Zeitpunkt der Erteilung der Information und die Ausnahmebestimmungen sind dagegen sehr unterschiedlich. Außerdem muss in beiden Fällen auf ein möglicherweise bestehendes Widerspruchsrecht (vgl. hierzu Ziff. 9.) hingewiesen werden.

Ein kumuliertes **Muster** der IHK München für beide Fälle der Datenerhebung nebst Erläuterungen der einzelnen Informationspflichten kann hier abgerufen (bzw. unter den weiterführenden Links gefunden) werden.

### 2.2.2 Art und Weise der Informationserteilung

Bei der Erteilung der Informationen ist insbesondere Folgendes zu beachten:

- Die Informationen, die sich auf Datenverarbeitungen beziehen, müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden.

- Die Mitteilung kann schriftlich oder elektronisch erfolgen. Somit kann die Information grundsätzlich auch über eine Website erfolgen. Auch die Übergabe eines Datenträgers ist denkbar. Die Information kann auch mündlich erfolgen. Eine mündliche Informationserteilung sollte jedoch immer dokumentiert werden.

- Der Hinweis auf möglicherweise bestehende Widerspruchsrechte (vgl. Ziff. 9.) muss ausdrücklich sowie in einer verständlichen und von anderen Informationen getrennten Form erfolgen, z. B. durch deutliche grafische Hervorhebung wie Rahmung oder Fettdruck. Unter Berücksichtigung dieser Voraussetzungen kann es sich anbieten, den Hinweis im selben Dokument zusammen mit den übrigen Informationen zu erteilen.

- Die Informationen sind unentgeltlich zur Verfügung zu stellen.

### 2.2.3 Zulässiger Medienbruch

Abhängig von der konkreten Verarbeitungssituation ist es häufig nicht möglich, der betroffenen Person umfangreiche Informationen (etwa in Form eines mehrseitigen Abdrucks der Datenschutzerklärung) zur Verfügung zu stellen. Allzu umfangreiche Informationen können den Betroffenen außerdem überfordern. Vor diesem Hintergrund kann es sich anbieten, die Informationen nicht in einem Dokument, sondern in mehreren Stufen und ggf. mittels verschiedener Medien zu erteilen. Zur Frage, welche Informationen in diesen Fällen der betroffenen Person möglichst unmittelbar mitgegeben werden sollten (1st level) und welche Informationsgehalte ggf. auf einer gesonderten Website bzw. per Faxabruf etc. vorgehalten werden können (2nd level), bieten diese Muster-Informationen bzw. die hier abrufbare Praxishilfe (S. 6) weitere Orientierung (siehe auch unter den weiterführenden Links).

### 2.2.4 Zeitpunkt der Informationspflicht

Werden die Daten direkt bei der betroffenen Person erhoben, muss die Information „zum Zeitpunkt“ der Erhebung der Daten erfolgen. Erfassungsakt und Information können daher zeitlich zusammenfallen.

Erhebt der Verantwortliche die Daten nicht direkt bei der betroffenen Person, muss die Information spätestens einen Monat nach Erlangung der Daten erfolgen (Artikel 14 Abs. 3 DSGVO).

Ferner ist zu beachten, dass der Verantwortliche spätestens zum Zeitpunkt der ersten Kommunikation mit der betroffenen Person diese auf etwaige Widerspruchsrechte gemäß Artikel 21 Abs. 1 und Abs. 2 DSVO hinweisen muss (Artikel 21 Abs. 4 DSVO).

### 2.2.5 Ausnahmen von der Informationspflicht

Die Informationspflicht besteht nicht, wenn und soweit der Betroffene bereits über die Informationen verfügt. Weitere Ausnahmen von der Informationspflicht im Falle der indirekten Erhebung können sich aus Artikel 14 Abs. 5 DSGVO u. a. bei unverhältnismäßigem Aufwand ergeben.

Zudem enthält das BDSG in speziellen Fällen weitere Ausnahmen, vgl. § 29 BDSG bei entgegenstehenden Geheimhaltungspflichten, § 32 BDSG bei beabsichtigten Weiterverarbeitungen sowie § 33 BDSG bei Gefährdung zivilrechtlicher Ansprüche.

Will sich ein Unternehmen auf eine Ausnahme berufen, sollte es in der Lage sein, nachzuweisen, dass die Voraussetzungen der Ausnahme erfüllt sind.

### 2.3 Weiterführende Links

#### 2.3.1 Leitfäden

- **GDD**, Praxishilfe zu Informations- und Transparenzpflichten bei der Datenverarbeitung, April 2018: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf
- **ULD**, Informationspflichten, Mai 2018: https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-4-Informationspflichten.pdf
- **DSK**, Informationspflichten, Januar 2018: https://www.saechsdsb.de/images/stories/sdb_inhalt/behoerde/oea/DSK_KPNr_10_Informationspflichten.pdf
- **Artikel-29-Gruppe**, Guidelines on transparency under Regulation 2016/679, April 2018 (engl.): https://datenschutz-hamburg.de/assets/pdf/wp260rev01_en.pdf

#### 2.3.2 Muster

- **GDD**, Praxishilfe zu Informations- und Transparenzpflichten bei der Datenverarbeitung, April 2018: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf (dort S. 9 ff.)
- **ULD**, Informationspflichten, Mai 2018: https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-4-Informationspflichten.pdf (Muster-Informationen als Vertragsanlage sowie Muster-Datenschutzhinweise für Website)
- **Prof. Dr. Thomas Hoeren/Deutsches Forschungsnetz**, Musterdatenschutzerklärung für Websitebetreiber nach den Vorgaben der DSGVO, April 2018: https://www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/Musterdatenschutzerk%C3%A4rung-nach-der-DSGVO.docx
- **IHK München**, Muster-Informationspflichten nach Artikel 13 DSGVO (Datenerhebung direkt beim Betroffenen) und nach Artikel 14 DSGVO (Datenerhebung über Dritte), Mai 2018: https://www.ihk-muenchen.de/ihk/documents/Anhänge-Recht/IHK_Muster-Informationspflicht-nach-Art.-13-und-14-DSGVO-3.pdf
- **BLTK-Musterdatenschutzerklärung für Praxis-Websites**: https://www.bltk.de/fileadmin/user_upload/Tieraerzte/Praxis/EU-DSGVO/BLTK-Datenschutzvorlage_pdf.pdf

## 3. Auskunftsanspruch

### 3.1 Worum geht es?

Die betroffene Person kann nach der DSGVO Auskunft über die sie betreffende Datenverarbeitung verlangen. Unternehmen müssen daher darauf vorbereitet sein, dass ein Betroffener sein Recht auf Auskunft hinsichtlich der ihn betreffenden (Gesundheits-)Daten geltend macht und dabei auch eine Kopie seiner Daten verlangt. Eine Verweigerung der Auskunft ist nur in Ausnahmefällen möglich.

Der entscheidende Unterschied zu den Informationspflichten (vgl. Ziffer 2.) und Wesenskern des Auskunftserteilung ist dabei, dass der Betroffene nicht nur die Metadaten („Wie“) der Verarbeitung abfragen, sondern vielmehr auch materielle Auskunft hinsichtlich der konkret verarbeiteten (Gesundheits-)Daten verlangen kann.

### 3.2 Was ist zu tun?

Wenn Personen Auskunft über die Verarbeitung ihrer Daten verlangen, muss das Unternehmen in einem ersten Schritt Auskunft darüber erteilen, ob es überhaupt (Gesundheits-)Daten der jeweiligen Person verarbeitet.

Wo dies der Fall ist, muss das Unternehmen in einem zweiten Schritt über das „Was“ und „Wie“ (Metadaten) der Verarbeitung aufklären. Die in der Auskunft mitzuteilenden Inhalte ergeben sich hinsichtlich des „Was“ aus Artikel 15 Abs. 1 Hs. 2 und Abs. 3 DSGVO, hinsichtlich des „Wie“ aus Artikel 15 Abs. 1 Hs. 2 lit. a–h sowie Abs. 2 DSGVO.

#### 3.2.1 Art und Weise der Auskunftserteilung

Verlangt der Betroffene Auskunft, muss der Verantwortliche dem Betroffenen die in Artikel 15 Abs. 1 DSGVO genannten Informationen zur Verfügung stellen. Der Betroffene kann zudem eine Kopie seiner (Gesundheits-)Daten, die Gegenstand einer Verarbeitung sind, verlangen. Die erste Kopie ist unentgeltlich zur Verfügung zu stellen, für alle weiteren Kopien kann der Verantwortliche ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen. Weitere

Einzelheiten zu Zeitpunkt sowie Art und Weise der Auskunftserteilung ergeben sich aus Artikel 12 DSGVO und Artikel 15 Abs. 3 DSGVO.

#### 3.2.2 Ausnahmen

Das Unternehmen kann in bestimmten Fällen die Auskunft ganz oder teilweise verweigern. Beispiele:

- Missbrauch der Auskunftspflicht (offenkundig unbegründete oder exzessive Anträge, vgl. Artikel 12 Abs. 5 S. 2 lit. b DSGVO);
- entgegenstehende Berufsgeheimnisse;
- fehlende Zuordenbarkeit der antragstellenden Person trotz zusätzlicher Bereitstellung identifizierender Informationen (vgl. Artikel 11 Abs. 2 DSGVO und Artikel 12 Abs. 6 DSGVO);
- bereichsspezifische Ausnahmen, z. B. bei Forschungszwecken oder statistischen Zwecken (§ 27 Abs. 2 BDSG), Geheimhaltungspflichten (§ 29 Abs. 1 S. 2 BDSG), Speicherung nur zur Aufbewahrung bzw. Datensicherung oder nicht-automatisierte Verarbeitung (§ 34 BDSG), Steuergeheimnis (§ 32c AO) und Sozialgeheimnis (§ 83 SGB X).

Das Recht auf Erhalt einer Kopie kann zudem durch Rechte und Freiheiten anderer Personen (z. B. Geschäftsgeheimnisse, Recht des geistigen Eigentums) beschränkt sein (Artikel 15 Abs. 4 DSGVO).

### 3.3 Weiterführende Links

- **DSK**, Auskunftsrecht der betroffenen Person, Artikel 15 DSGVO, Juli 2017: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_6_Auskunftsrecht.pdf

## 4. Berichtigungsanspruch

### 4.1 Worum geht es?

Nach der DSGVO kann der Betroffene die Berichtigung seiner personenbezogenen Daten verlangen. Unternehmen können daher Berichtigungsansprüchen des Betroffenen ausgesetzt sein, wenn die jeweiligen (Gesundheits-)Daten, die sie verarbeiten, unrichtig oder unvollständig sind.

### 4.2 Was ist zu tun?

Unternehmen müssen die Prozesse in ihrem Unternehmen so einrichten, dass sie einem Berichtigungsverlangen des Kunden fristgerecht nachkommen können.

- (Gesundheits-)Daten sind unrichtig, wenn die in Rede stehenden Informationen zum Zeitpunkt der Geltendmachung des Berichtigungsanspruchs nicht mit der Tatsachenlage übereinstimmen. Unrichtige Daten müssen richtiggestellt werden (Artikel 16 Satz 1 DSGVO).

**Beispiel:** Wenn sich der Familienname einer Person nachträglich durch Heirat ändert, kann diese Person eine entsprechende Korrektur verlangen.

- (Gesundheits-)Daten sind unvollständig, falls sie in Bezug auf die konkrete Verarbeitung derart lückenhaft sind, dass der mit der Verarbeitung verfolgte Zweck nicht (mehr) erreicht wird. Das kann etwa der Fall sein, wenn das Fehlen von Daten im konkreten Verarbeitungszusammenhang in Missverständnissen oder Irreführungen resultiert. Der Betroffene hat in diesem Fall einen Anspruch auf Vervollständigung, der auch auf Berücksichtigung von ergänzenden Erklärungen des Betroffenen selbst gehen kann (Artikel 16 Satz 2 DSGVO).

Bereichsspezifische Ausnahmen existieren z. B. bei Verarbeitungen zu Forschungszwecken/statistischen Zwecken (§ 27 Abs. 2 BDSG).

## 5. Nachberichtspflicht

### 5.1 Worum geht es?

Hat ein Unternehmen (Gesundheits-)Daten einem Empfänger (z. B. Auftragnehmer) offengelegt, können für das Unternehmen zusätzliche Nachberichts- bzw. Mitteilungspflichten entstehen, wenn die Daten nach der Weitergabe berichtigt, gelöscht oder eingeschränkt werden.

### 5.2 Was ist zu tun?

Es ist zu unterscheiden zwischen Mitteilungspflichten gegenüber dem Empfänger einerseits und gegenüber der betroffenen Person andererseits.

- Der Verantwortliche muss allen Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung oder Löschung oder Einschränkung der Datenverarbeitung mitteilen. Eine Ausnahme besteht, wenn die Mitteilung unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. Auf eine Anfrage oder einen Antrag des Empfängers kommt es nicht an.
- Außerdem muss der Verantwortliche die betroffene Person über die zu benachrichtigenden Empfänger der Daten unterrichten. Das gilt aber nur, wenn die betroffene Person diese Unterrichtung verlangt.

## 6. Löschungsanspruch

### 6.1 Worum geht es?

Unternehmen müssen die erforderlichen Prozesse implementieren, um die (Gesundheits-)Daten des Betroffenen eigenständig und/oder auf Verlangen der betroffenen Person gemäß den gesetzlichen Bestimmungen zu löschen.

Hat ein Unternehmen die von einem Löschverlangen erfassten Daten öffentlich gemacht, kann das Unternehmen zudem verpflichtet sein, andere Verantwortliche über das Löschverlangen zu informieren („Recht auf Vergessenwerden“).

### 6.2 Was ist zu tun?

Bei der Umsetzung der Vorgaben ist zwischen Löschungspflichten und Informationspflichten zu unterscheiden. Sollen personenbezogene Daten gelöscht werden, ist immer genau zu prüfen, ob die Daten möglicherweise (noch) nicht gelöscht werden müssen, da eine Verarbeitung aus anderen Gründen erlaubt ist (Ausnahmetatbestände).

#### 6.2.1 Löschungspflicht

Das verantwortliche Unternehmen muss die (Gesundheits-) Daten in folgenden Fällen unverzüglich löschen:

- Zweckerledigung (d. h. die Daten sind nicht mehr notwendig, um den Zweck zu erfüllen, für den die Daten erhoben wurden); oder
- Widerruf der Einwilligung in die Verarbeitung der (Gesundheits-)Daten; oder
- berechtigter Widerspruch gegen die Verarbeitung (vgl. Artikel 21 DSGVO); oder
- unrechtmäßige Verarbeitung (z. B. nachträglicher Wegfall der Rechtsgrundlage der Verarbeitung); oder
- rechtliche Verpflichtung zur Löschung; oder
- Datenerhebung in Bezug auf angebotene Dienste der Informationsgesellschaft bei Minderjährigen; der Regelungsgehalt dieses Tatbestandes ist jedoch noch nicht abschließend geklärt.

Die Pflicht zur Löschung besteht unabhängig davon, ob die betroffene Person die Löschung verlangt hat oder nicht.

Die Löschung hat unverzüglich zu erfolgen, d. h. ohne unangemessene Verzögerung. Wann eine Verzögerung unangemessen ist, legt die DSGVO nicht fest und muss daher anhand der Umstände des Einzelfalls beurteilt werden.

#### 6.2.2 Pflicht zur Information Dritter („Recht auf Vergessenwerden“)

Ein Unternehmen, das (Gesundheits-)Daten öffentlich gemacht hat und nach Ziff. 6.2.1 zu deren Löschung verpflichtet ist, muss andere Verantwortliche, die die jeweiligen Daten verarbeiten, darüber informieren, dass der Betroffene von ihnen die Löschung aller Links, Kopien oder Replikationen verlangt hat. Zu beachten ist:

- Voraussetzung für diese Mitteilungspflicht ist, dass die betroffene Person gegenüber dem Unternehmen zumindest die Löschung seiner Daten verlangt hat. Hierin wird in der Regel ein umfassendes Löschverlangen gesehen, das auch die Geltendmachung des Rechts auf Vergessenwerden mitumfasst.

- Das „Recht auf Vergessenwerden“ zieht keine (weitere) Löschungspflicht für das verantwortliche Unternehmen nach sich. Die Verpflichtung ist erfüllt, wenn der Verantwortliche den betroffenen Drittverantwortlichen das Löschverlangen mitgeteilt hat. Es muss also nicht darauf hingewirkt werden, dass die Empfänger der Mitteilung die Daten auch tatsächlich löschen.

a) Hintergrund der Regelung
Selbst wenn der Verantwortliche (Gesundheits-)Daten ordnungsgemäß bei sich löscht, besteht im Falle einer vorherigen Veröffentlichung dieser Daten weiterhin ein Risiko, dass Dritte auf die Daten zugreifen können. Von einer Veröffentlichung spricht man, wenn Daten einem unbestimmten Personenkreis zugänglich gemacht werden, also beispielsweise im Internet frei verfügbar bereitgestellt wurden. Der Betroffene soll in diesem Fall davor geschützt werden, dass seine Daten trotz Löschung weiterhin im Internet für jedermann verfügbar sind.

b) Umfang der Mitteilungspflicht
Die Mitteilungspflicht beschränkt sich darauf, angemessene Maßnahmen zu treffen, um Dritte von dem Löschverlangen in Kenntnis zu setzen. Diese Maßnahmen müssen zumutbar sein. Dabei sind die verfügbaren Technologien und die Implementierungskosten zu berücksichtigen. Eine aufwendige unmittelbare Kontaktaufnahme mit einer Vielzahl anderer Verantwortlicher wird in der Regel nicht erforderlich sein.

### 6.2.3 Ausnahmen

In bestimmten Ausnahmefällen besteht keine Pflicht zur Löschung der Daten (und insoweit auch kein Recht auf Vergessenwerden). Umfangreiche Ausnahmetatbestände sind in Artikel 17 Abs. 3 DSGVO geregelt. Weitere Ausnahmen können sich aus § 35 BDSG ergeben (z. B. nicht automatisierte Datenverarbeitung, schutzwürdige Belange der betroffenen Person).

Hintergrund der Ausnahmen ist eine Abwägung widerstreitender Rechtspositionen. Die Ausnahmetatbestände erfassen vor allem Konstellationen, in denen die fortdauernde Speicherung der Daten für die Wahrung von Rechten und Interessen der Öffentlichkeit oder des Verantwortlichen selbst erforderlich ist.

Insbesondere folgende Ausnahmefälle können aus Unternehmenssicht wichtig sein:

a) Erfüllung rechtlicher Verpflichtungen
Eine Ausnahme von der Löschungspflicht besteht, wenn die Verarbeitung für die Erfüllung bestimmter rechtlicher Verpflichtungen erforderlich ist. Rechtliche Verpflichtungen, die in der Praxis regelmäßig einer Löschung entgegenstehen, sind bereichsspezifische bzw. steuer- und handelsrechtliche Aufbewahrungspflichten.

**Beispiele:** Aufbewahrungspflichten im Rahmen des ärztlichen Behandlungsvertrags (vgl. § 630f BGB), im Handelsrecht (§§ 238, 257 HGB) oder im Steuerrecht (§ 147 AO).

Ferner kann in Fällen, in denen Daten eigentlich wegen Zweckerledigung gelöscht werden müssten, eine Ausnahme bestehen, wenn satzungsmäßige oder vertragliche Aufbewahrungsfristen vereinbart worden sind (vgl. hierzu § 35 Abs. 3 BDSG).

b) Öffentliche Gesundheit
Die Löschungspflicht kann entfallen, wenn die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich ist (Artikel 9 Abs. 2 lit. h und i sowie Artikel 9 Abs. 3 DSGVO).

c) Forschungszwecke, statistische Zwecke
Eine Ausnahme von der Löschungspflicht kann bestehen, wenn die Verarbeitung der (Gesundheits-)Daten zu Forschungszwecken oder statistischen Zwecken erforderlich ist, soweit die Löschung voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt.

d) Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
Eine Löschungspflicht besteht nicht, wenn die Verarbeitung personenbezogener Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Auch außergerichtliche Verfahren sind erfasst.

**Beispiel:** Die Speicherung kann weiterhin erforderlich und zulässig sein, soweit dem Unternehmen ein Rechtsstreit droht und die einschlägige zivilrechtliche Verjährungsfrist noch nicht abgelaufen ist.

Ausreichend dürfte sein, dass ein entsprechender Rechtsstreit hinreichend wahrscheinlich erscheint. Bei der Erstellung der Prognose sind insbesondere die Eintrittswahrscheinlichkeit, das Gewicht der möglichen Ansprüche und die Belange des Betroffenen abzuwägen.

### 6.3 Best Practice

Der Verantwortliche muss seinen Datenbestand laufend daraufhin überprüfen, ob eine Löschungspflicht besteht.

Um den Löschpflichten der DSGVO gerecht zu werden, sollten die Unternehmen sogenannte Löschkonzepte (z. B. nach DIN 66398) entwickeln, welche es ermöglichen, in regelmäßigen Abständen Löschungen durchzuführen.

### 6.4 Weiterführende Links

- **DSK**, Recht auf Löschung und Recht auf Vergessenwerden, August 2017: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/08/DSK_KPNr_11_Recht-auf-Vergessenwerden.pdf

- **GDD**, DIN 66398 – Löschen mit Konzept, November 2017: https://www.gdd.de/eforen/karlsruhe/intern/sitzungs-unterlagen/sitzung-vom-21-11.2016/folien-loeschkonzept-dr-hammer

- **BayLDA**, FAQ: Gesammelte Antworten zur EU-Datenschutz-Grundverordnung (DSGVO), Wie lösche ich DSGVO-konform Daten von Festplatten?: https://www.ihk-nuernberg.de/de/Geschaeftsbereiche/Innovation-Umwelt/IuK-E-Business/Datenschutz/eu-datenschutz-grundverordnung/fragen-an-das-baylda-zur-ausgestaltung-der-dsgvo-in-der-praxis/

- **ico**, Guide to the General Data Protection Regulation (GDPR), Juni 2018 (engl.), S. 116 ff.: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

- **Verbraucherzentrale**, Musterbrief Löschung personenbezogener Daten, April 2018: https://www.verbraucherzentrale-niedersachsen.de/sites/default/files/medien/141/dokumente/Musterbrief%20Löschung%20nach%20Art.%2017%20DSGVO%20%28Löschung%20personenbezogener%20Daten%29.pdf

## 7. Einschränkung der Verarbeitung

### 7.1 Worum geht es?

Unternehmen können auf Verlangen der betroffenen Person verpflichtet sein, die Verarbeitung von (Gesundheits-) Daten einzuschränken (Artikel 18 DSGVO). Im Falle einer Einschränkung werden die Daten zwar nicht gelöscht. Sie dürfen aber nur noch in sehr begrenztem Umfang weiterverarbeitet werden.

### 7.2 Was ist zu tun?

Verlangt eine betroffene Person die Einschränkung der Verarbeitung, ist zu prüfen, ob die gesetzlichen Voraussetzungen des Anspruchs erfüllt sind. Ist das der Fall, muss das Unternehmen die Verarbeitung der (Gesundheits-)Daten einschränken. Aufhebungen der getroffenen Einschränkungen sind mitteilungspflichtig.

#### 7.2.1 Prüfung der Voraussetzungen

Die Einschränkung der Verarbeitung der (Gesundheits-) Daten kann verlangt werden, wenn einer der vier folgenden Fälle gegeben ist (vgl. hierzu Artikel 18 Abs. 1 DSGVO):

- Bestreiten der Richtigkeit der Daten durch die betroffene Person, solange die Prüfung der Richtigkeit andauert (vgl. auch Ziff. 4);

- unrechtmäßige Verarbeitung durch das verantwortliche Unternehmen, wenn der Betroffene die (in diesem Fall typischerweise erforderliche) Löschung der Daten ablehnt;

- vom Betroffenen initiierte Verhinderung einer Löschung, wenn der Verantwortliche die Daten nicht mehr benötigt, der Betroffene zur Geltendmachung von Rechtsansprüchen aber auf sie angewiesen ist;

- Widerspruch der betroffenen Person, solange die Prüfung der Berechtigung des Widerspruchs nach Artikel 21 Abs. 1 DSGVO andauert.

Der Betroffene muss zudem formlos einen entsprechenden Antrag stellen.

#### 7.2.2 Umsetzung der Einschränkung

Besteht eine Pflicht zur Einschränkung der Verarbeitung, so sind die jeweiligen Daten zunächst als gesperrt zu markieren. Die Einschränkung kann dann beispielweise wie folgt umgesetzt werden:

- Übertragung der Daten auf ein anderes Verarbeitungssystem;
- Sperrung der Daten für Nutzer;
- vorübergehende Entfernung veröffentlichter Daten von einer Website.

In automatisierten Dateisystemen soll grundsätzlich durch technische Mittel sichergestellt werden, dass gesperrte personenbezogene Daten in keiner Weise weiterverarbeitet oder verändert werden können. Auf die Tatsache einer Beschränkung sollte im System unmissverständlich hingewiesen werden.

Im Falle einer Einschränkung dürfen die betroffenen personenbezogenen Daten – abgesehen von der weiterhin zulässigen Speicherung – nur noch verarbeitet werden, wenn

- die betroffene Person einwilligt, oder
- die Verarbeitung der Geltendmachung von Rechtsansprüchen, dem Schutze einer anderen natürlichen oder juristischen Person oder einem wichtigen öffentlichen Interesse dient.

#### 7.2.3 Mitteilungspflicht bei Aufhebung der Einschränkung

Eine betroffene Person, die eine Einschränkung erwirkt hat, muss von dem Verantwortlichen unterrichtet werden, bevor die Einschränkung wieder aufgehoben wird.

## 8. Datenübertragung

### 8.1 Worum geht es?

Der Betroffene kann nach der DSGVO unter bestimmten Voraussetzungen die Übertragung seiner personenbezogenen Daten verlangen. Unternehmen müssen aus diesem Grund darauf vorbereitet sein, dass ein Betroffener eine solche Datenübertragung verlangt.

Das Recht auf Datenübertragbarkeit soll dem Betroffenen erlauben, seine (Gesundheits-)Daten, die er dem verantwortlichen Unternehmen bereitgestellt hat, von diesem Unternehmen heraus zu verlangen.

Zudem darf die betroffene Person diese Daten einem anderen Unternehmen (neuer Verantwortlicher) übermitteln, ohne dabei behindert zu werden. Soweit es technisch machbar ist, kann der Betroffene dabei auch verlangen, dass die Übermittlung direkt von einem verantwortlichen Unternehmen zu dem anderen erfolgt.

### 8.2 Was ist zu tun?

Macht ein Betroffener einen Anspruch auf Datenübertragung geltend, müssen Unternehmen überprüfen, ob die Voraussetzungen für eine solchen Anspruch (vgl. hierzu Artikel 20 DSGVO) erfüllt sind. Wesentliche Voraussetzungen sind u. a., dass

- die Grundlage der Datenverarbeitung eine Einwilligung oder ein Vertrag ist, und
- der Betroffene die Daten dem Unternehmen selbst bereitgestellt hat, und
- die Verarbeitung bei dem Unternehmen mithilfe automatisierter Verfahren erfolgt.

Besteht der Anspruch, müssen die Unternehmen die (Gesundheits-)Daten in einem strukturierten, gängigen und maschinenlesbaren Format bereitstellen.

### 8.3 Weiterführende Links

- **Artikel-29-Gruppe**, Leitlinien zum Recht auf Datenportabilität, 16/EN WP242, Dezember 2016: https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2017/07/WP242de_Art_29-Gruppe_Datenubertragbarkeit.pdf
- **Stiftung Datenschutz**, Praktische Umsetzung des Rechts auf Datenübertragbarkeit, rechtliche, technische und verbraucherbezogene Implikationen, Januar 2018: https://www.stiftungdatenschutz.org/fileadmin/Redaktion/Datenportabilitaet/stiftungdatenschutz_abschlussbericht_Hyperlinks_20180124_01_web.pdf

## 9. Widerspruch gegen die Verarbeitung

### 9.1 Worum geht es?

Das Widerspruchsrecht erlaubt es der betroffenen Person in bestimmten Fällen, eine eigentlich zulässige Datenverarbeitung mit Blick auf die Zukunft zu unterbinden. Der Betroffene kann sich so im Einzelfall auch gegen eine im Grundsatz rechtmäßige Verarbeitung zur Wehr setzen. Der Widerspruch ist nicht zu verwechseln mit dem Widerruf der Einwilligung (vgl. hierzu unter Ziff. I.3.1).

### 9.2 Was ist zu tun?

Unternehmen müssen sich darauf einstellen, dass der Betroffene einer Datenverarbeitung widerspricht. Jeder Widerspruch ist zu prüfen. Ist der Widerspruch berechtigt, darf das Unternehmen die Daten nicht mehr verarbeiten (Artikel 21 DSGVO).

#### 9.2.1 Beispiele für Widerspruchsrechte

Widerspruchsrechte bestehen nur in bestimmten, gesetzlich festgelegten Fällen. Diese sind in Artikel 21 DSGVO geregelt und von dem Unternehmen im Falle eines Widerspruchs zu prüfen. Wichtige Beispiele:

- Ein Widerspruchsrecht kann bestehen, soweit Rechtsgrundlage für die Verarbeitung der (Gesundheits-)Daten eine Interessensabwägung ist (Artikel 6 Abs. 1 lit. f DSGVO, vgl. z. B. Ziff. I.2.3). Die betroffene Person kann zudem einer Datenverarbeitung, die zu Forschungszwecken oder zu statistischen Zwecken erfolgt (vgl. Ziff. F.I.2.1.3), widersprechen.

  Voraussetzung ist in diesen beiden Fällen jedoch, dass der Widerspruch aus Gründen erfolgt, die sich aus der besonderen Situation des Betroffenen ergeben. Damit ist gemeint, dass in Bezug auf die jeweilige Person im Vergleich zu anderen Betroffenen eine atypische Konstellation bestehen muss, die ihren individuellen Interessen ein besonderes Gewicht verleiht. Das kann etwa der Fall sein, wenn durch eine fortgesetzte Datenverarbeitung – nunmehr – eine Gefahr für Leib und Leben der betroffenen Person besteht. Eine besondere Situation liegt außerdem vor, wenn die Datenverarbeitung zu ethischen, sozialen, gesellschaftlichen oder familiären Zwangssituationen führt.

- Ein Widerspruchsrecht besteht zudem bei einer Verarbeitung zum Zwecke der Direktwerbung. Hier müssen neben der Erklärung des Widerspruchs keine weiteren Voraussetzungen erfüllt sein. Ein Widerspruch gegen die Verarbeitung zum Zwecke der Direktwerbung ist daher immer möglich.

#### 9.2.2 Ausnahmen

Das Unternehmen muss im Falle eines Widerspruchs zudem immer prüfen, ob ein Ausnahmefall vorliegt. In besonderen Fällen können die Interessen des Unternehmens an der Verarbeitung überwiegen (vgl. Artikel 21 Abs. 1 S. 2, Abs. 6 DSGVO). Dies gilt jedoch nicht für den Widerspruch gegen Verarbeitungen zum Zwecke der Direktwerbung.

#### 9.2.3 Folgen

Ergibt die Prüfung des Unternehmens, dass die Voraussetzungen eines Widerspruchsrechts erfüllt sind und auch kein Ausnahmefall vorliegt, so ist der Widerspruch berechtigt. Dies führt dazu, dass die Verarbeitungsgrundlage entfällt und das Unternehmen die Daten nicht mehr verarbeiten darf.

## IV. Verpflichtung zur Datensicherheit

### 1. Worum geht es?

Eines der zentralen Anliegen der DSGVO ist die Sicherheit der für die Verarbeitung personenbezogener (Gesundheits-) Daten genutzten Systeme. Um dieses Ziel zu verwirklichen, haben sowohl der Verantwortliche als auch der Auftragsverarbeiter geeignete technische und organisatorische Schutzmaßnahmen im Wege einer eigenständigen Risikobewertung zu bestimmen, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Auswahl der erforderlichen Maßnahmen ist eine Balance zwischen Schutzaufwand und Risiko zu finden.

### 2. Was ist zu tun?

Anhand des Schutzbedarfs der Daten muss ein angemessenes Schutzniveau ermittelt werden, um sodann die erforderlichen Maßnahmen zur Gewährleistung des angemessenen Schutzniveaus treffen und nachweisen zu können.

#### 2.1 Ermittlung des angemessenen Schutzniveaus anhand eines risikobasierten Ansatzes

Zunächst ist der Schutzbedarf für die bei dem Unternehmen vorhandenen personenbezogenen Daten zu ermitteln. Der Schutzbedarf ergibt sich insbesondere aus der Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen sowie der Eintrittswahrscheinlichkeit einer Verletzung und orientiert sich an den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit. Zur Bestimmung eines angemessenen Schutzniveaus sind sodann neben den Risiken auch die wirtschaftlichen Interessen des Unternehmens und der Stand der Technik zu berücksichtigten.

##### 2.1.1 Risiken für die Rechte und Freiheiten des Betroffenen

Zur Beurteilung des angemessenen Schutzniveaus müssen Unternehmen eigenverantwortlich eine Risikobewertung dahingehend vornehmen, wie hoch sie die Risiken für die Rechte und Freiheiten derjenigen einschätzen, deren Daten sie verarbeiten. Damit sind sämtliche Grundrechte und Grundfreiheiten des Betroffenen erfasst – nicht nur, aber insbesondere das Recht auf Achtung des Privatlebens sowie das Recht auf Schutz personenbezogener Daten. Weitere Orientierung zur Beurteilung von Risiken bietet dieses Kurz-Papier der DSK.

a) Typische Risiken

Die Datensicherheit kann beispielsweise durch die Vernichtung, den Verlust, die Veränderung oder die unbefugte Offenlegung von bzw. den unbefugten Zugang zu den Daten des Betroffenen beeinträchtigt werden.

Typische Folgen einer solchen Beeinträchtigung der Datensicherheit sind z. B. die Diskriminierung von Personen, Identitätsdiebstahl oder -betrug, finanzielle Verluste, die unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Profilbildung mit Standortdaten sowie der Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen.

b) Grundsätze der Risikobeurteilung

Das Risiko ist das Produkt aus der Schwere eines möglichen Schadens für die betroffene Person sowie aus der Wahrscheinlichkeit, dass es zu einem entsprechenden Schadensereignis kommt.

- Die Schwere eines möglichen Schadens beurteilt sich nach dem Gewicht des bedrohten Rechts bzw. der bedrohten Freiheit sowie danach, welche Schäden ihnen aus der Verarbeitung erwachsen können. Dabei sind sowohl materielle als auch immaterielle Schäden von Bedeutung.

  Je sensibler die Daten sind, desto größer ist die mögliche Schadenshöhe. Bei Gesundheitsdaten ist grundsätzlich von einer besonderen Schadenshöhe auszugehen.

- Die zudem zu berücksichtigende Eintrittswahrscheinlichkeit meint den statistischen Erwartungswert, mit dem ein bestimmtes Schadensereignis eintreten wird.

c) Verarbeitungsspezifische Faktoren bei der Risikobestimmung

Zur Bestimmung des Risikos sind zudem die Bezugsgrößen Art, Umfang, Umstände und Zweck der Verarbeitung heranzuziehen:

- Art der Verarbeitung: Artikel 4 Nr. 2 DSGVO nennt insbesondere das Erheben, das Erfassen, die Übermittlung, das Ordnen, die Speicherung, das Löschen und die Vernichtung.

- Umfang der Verarbeitung: Menge der Personen, deren Daten in die Verarbeitung einfließen, sowie Menge der Daten, die dabei über eine Person erhoben werden. Dabei ist zu berücksichtigen, dass Daten umso engmaschiger miteinander verknüpft werden können, je größer die

Datenmenge ist. Der Aussagegehalt einer Datenanalyse steigt zudem mit der wachsenden Anzahl von Personen, die in eine vergleichende Betrachtung einbezogen werden.

- Umstände der Verarbeitung: Gemeint sind alle tatsächlichen und rechtlichen Gegebenheiten, die die Einzelheiten des Verarbeitungsprozesses bestimmen.

- Zwecke der Verarbeitung: Hiermit sind die Ziele gemeint, die mit der Verarbeitung verfolgt werden. Diese legt der Verantwortliche selbst fest.

#### 2.1.2 Wirtschaftliche Interessen und Stand der Technik

Für die Bestimmung des angemessenen Schutzniveaus spielen neben dem Risiko für die Rechte und Freiheiten des Betroffenen auch die wirtschaftlichen Interessen des Unternehmens, insbesondere die Implementierungskosten, eine Rolle. Implementierungskosten sind die wirtschaftlichen Ressourcen, die der Verarbeiter aufwenden muss, um die Maßnahme in sein Verarbeitungssystem zu integrieren. Die Höhe der Implementierungskosten kann als Grenze der dem Unternehmen noch zumutbaren Sicherheitsmaßnahmen zu berücksichtigen sein.

Schließlich muss der Stand der Technik berücksichtigt werden. Nur solche Maßnahmen, die technisch verfügbar sind und Marktstandards entsprechen, müssen ergriffen werden. Umgekehrt muss der Verarbeiter diesen Anforderungen aber auch genügen. Hinsichtlich des Stands der Technik können sich Unternehmen an den BSI-Grundsätzen bzw. der ISO 27000-Normenreihe orientieren.

### 2.2 Maßnahmen zur Herstellung eines angemessenen Schutzniveaus

Auf Grundlage des ermittelten Schutzbedarfs sind sodann geeignete technische und/oder organisatorische Maßnahmen zu treffen, die einen angemessenen Schutz vor den Risiken gewährleisten. Die Maßnahmen müssen laufend überprüft und aktualisiert werden.

#### 2.2.1 Was sind technische und organisatorische Maßnahmen?

Unter technischen Maßnahmen versteht man Vorkehrungen, die sich auf den Vorgang der Verarbeitung von Daten erstrecken, wie z. B. bauliche Maßnahmen, die den Zutritt Unbefugter verhindern sollen, oder Steuerungen des Software- oder Hardwareprozesses der Verarbeitung, etwa durch Maßnahmen der Zugriffs- oder Weitergabekontrolle wie Verschlüsselung oder Passwortsicherung.

Organisatorische Maßnahmen beziehen sich insbesondere auf die äußeren Rahmenbedingungen zur Gestaltung des technischen Verarbeitungsprozesses, etwa die Einhaltung des Vieraugenprinzips, das Wegschließen von Datenträgern, Protokollierungen von Tätigkeiten und Stichprobenroutinen. Dazu können auch Schulungen der Mitarbeiter oder Verpflichtungserklärungen gehören.

#### 2.2.2 Beispiele für geeignete Maßnahmen

Technische und organisatorische Maßnahmen, die zur Herstellung eines angemessenen Schutzniveaus beitragen können, sind u. a.:

- Pseudonymisierung und Verschlüsselung;

- Maßnahmen zur dauerhaften Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang;

- Maßnahmen zur raschen Widerherstellung der Verfügbarkeit der personenbezogenen Daten bei einem physischen oder technischen Zwischenfall;

- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die Aufzählung ist lediglich beispielhaft. Es steht grundsätzlich im Ermessen des Verantwortlichen, welche konkreten Maßnahmen er zur Gewährleistung eines angemessenen Schutzniveaus ergreift. Entscheidend ist, ob ein angemessenes Schutzniveau erreicht wird, nicht aber, ob ein bestimmter Maßnahmenkatalog abgearbeitet worden ist.

#### 2.2.3 Verarbeitung durch unterstellte Personen

Der Verantwortliche und der Auftragsverarbeiter müssen zudem sicherstellen, dass die ihnen unterstellten natürlichen Personen, die Zugang zu personenbezogenen Daten haben, diese nur entsprechend den Vorgaben des Verantwortlichen verarbeiten. Entsprechende Weisungen sollten bereits bei Aufnahme der Tätigkeit unter Berücksichtigung der zu beachtenden datenschutzrechtlichen Vorgaben erteilt werden.

### 2.3 Nachweis der Konformität

Das Unternehmen hat nachzuweisen, dass es die Sicherheit der Verarbeitung gewährleistet (siehe zur Rechenschaftspflicht bereits Ziff. II.3). Für den Nachweis der Erfüllung der Verpflichtung zur Herstellung eines angemessenen Schutzniveaus kann auch die Einhaltung genehmigter Verhaltensregeln (Artikel 40 DSGVO) oder eines genehmigten Zertifizierungsverfahrens (Artikel 42 DSGVO) als Faktor herangezogen werden (siehe zur Zertifizierung Teil 3 – A.II).

## 3. Wichtige Rechtsvorschriften

Artikel 32 DSGVO (Sicherheit der Verarbeitung)

## 4. Weiterführende Links

- **Bitkom**, Leitfaden zur Datensicherheit, Mai 2017: https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf
- **Bundesärztekammer/Kassenärztliche Bundesvereinigung, Sicherheitsempfehlungen**, Juni 2018: https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Telemedizin_Telematik/Sicherheit/Schweigepflicht_Technische_Anlage_2018.pdf
- **Kassenärztliche Bundesvereinigung**, Fragen und Antworten zur Datensicherheit, Mai 2018: http://www.kbv.de/html/datensicherheit.php
- **DSK**, Kurz-Papier zum Risiko für die Rechte und Freiheiten natürlicher Personen unter der DSGVO, April 2018: https://www.lda.bayern.de/media/dsk_kpnr_18_risiko.pdf
- **ico**, Security at a glance (engl.): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/
- **LDI NRW**, Technische Anforderungen an technische und organisatorische Maßnahmen beim E-Mail-Versand: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Technische-Anforderungen-an-technische-und-organisatorische-Massnahmen-beim-E-Mail-Versand/Technische-Anforderungen-an-technische-und-organisatorische-Massnahmen-beim-E-Mail-Versand.html
- **ENISA**, Smartphone Secure Development Guideline, Februar 2017 (engl.): https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016
- **ULD**, Das Standard-Datenschutzmodell (SDM): https://www.datenschutzzentrum.de/sdm

## V. Umgang mit Datenpannen

### 1. Worum geht es?

Bei der Verletzung personenbezogener Daten (sogenannte Datenpannen) bestehen für Unternehmen in bestimmten Fällen gesetzliche Meldepflichten.

Eine Datenpanne liegt vor, wenn die Datensicherheit verletzt wurde, indem personenbezogenen Daten vernichtet wurden, verloren gegangen sind, verändert wurden oder es zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten gekommen ist (Artikel 4 Nr. 12 DSGVO). Unerheblich ist, wer für die Verletzung verantwortlich ist.

**Beispiel:** Eine Datenpanne liegt beispielsweise vor, wenn Gesundheitsdaten fehlerhaft übermittelt oder gestohlen wurden oder wenn das verarbeitende Unternehmen „gehackt" wurde.

### 2. Was ist zu tun?

Unternehmen unterliegen bei einer Datenpanne ggf. einer Meldepflicht gegenüber der Aufsichtsbehörde und gegenüber den von der Datenpanne betroffenen Personen.

#### 2.1 Meldung an die Aufsichtsbehörde

Verantwortliche Unternehmen müssen Datenpannen grundsätzlich der zuständigen Aufsichtsbehörde melden.

- Die Meldung hat unverzüglich (möglichst binnen 72 Stunden) zu erfolgen und muss mindestens die in Artikel 33 Abs. 3 DSGVO aufgezählten Informationen enthalten. Die Frist beginnt zu dem Zeitpunkt, zu welchem dem Unternehmen die Datenschutzverletzung bekannt geworden ist.
- In weniger schwerwiegenden Fällen, die zu keinem Risiko für die betroffenen Personen führen, ist die Meldung entbehrlich.
- (Auch geringfügige) Datenpannen sind umfassend zu dokumentieren.

Einzelheiten ergeben sich aus Artikel 33 DSGVO.

#### 2.2 Meldung an den Betroffenen

Hat eine Datenpanne voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche unverzüglich den Betroffenen über diese Datenpanne.

- Die Meldepflicht gegenüber der betroffenen Person besteht damit erst bei einem deutlich erhöhten Risiko für die persönlichen Rechte und Freiheiten. Diese wesentliche Voraussetzung ist z. B. in der Regel noch nicht erfüllt, wenn personenbezogene Daten mit einem relativ geringen Vertraulichkeitsgrad unberechtigt übermittelt werden. Ggf. kann aber die Aufsichtsbehörde von dem Verantwortlichen verlangen, eine Mitteilung an den Betroffenen nachzuholen.
- „Unverzüglich" bedeutet, dass eine angemessene und sorgfältige Prüfung vor einer Benachrichtigung des Betroffenen nicht zu einer Fristverletzung führen muss. Vielmehr muss der Einzelfall betrachtet werden.

Einzelheiten und Ausnahmen sind in Artikel 33 DSGVO geregelt.

#### 2.3 Sonderfall: Datenpanne beim Auftragsverarbeiter

Für Datenpannen bei Auftragsverarbeitern besteht eine Sonderregelung. Den Auftragsverarbeiter selbst trifft keine Meldepflicht gegenüber der Aufsichtsbehörde oder gegenüber dem Betroffenen. Vielmehr muss der Auftragsverarbeiter Verletzungen im Rahmen der Auftragsverarbeitung unverzüglich an den Verantwortlichen melden. Dieser wird dann ggf. selbst anzeigepflichtig gegenüber der Aufsicht bzw. mitteilungspflichtig gegenüber dem Betroffenen.

### 3. Weiterführende Links

- **BayLDA**, September 2016: https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf
- **Artikel-29-Gruppe**, Guidelines on Personal data breach notification, Februar 2018 (engl.): https://datenschutz-hamburg.de/assets/pdf/wp250rev01_enpdf.pdf

## VI. Durchführung einer Datenschutz-Folgenabschätzung (Impact Assessment)

### 1. Worum geht es?

Sind mit einer geplanten Verarbeitung von (Gesundheits-) Daten hohe Risiken für die betroffene Person verbunden, muss das verantwortliche Unternehmen in bestimmten Fällen vorab eine sogenannte Datenschutz-Folgenabschätzung (nachfolgend auch **DSFA**) durchführen.

Die DSFA soll sicherstellen, dass der Verantwortliche mögliche Folgen bestimmter kritischer Datenverarbeitungen vorab analysiert und Maßnahmen für den Schutz der betroffenen Personen festlegt, um so das Risiko auf ein angemessenes Maß zu reduzieren.

Für die Verarbeitung von Gesundheitsdaten spielt die DSFA aufgrund der Sensibilität dieser Daten eine wichtige Rolle. Jede umfangreiche Verarbeitung von Gesundheitsdaten erfordert bereits eine DSFA. Unternehmen, die mit Gesundheitsdaten arbeiten, sollten daher die Regelungen zur DSFA immer im Blick haben.

### 2. Was ist zu tun?

Unternehmen müssen prüfen, ob die von ihnen geplante Verarbeitung besonders risikoreich ist. Eine erforderliche DSFA hat die angedachten Prozesse zu beschreiben, beinhaltet eine Risikobewertung sowie Maßnahmen zur Risikominimierung.

#### 2.1 Stufe 1: Risikobewertung – DSFA erforderlich? (Vorprüfung)

Der Verantwortliche muss zunächst ermitteln, ob mit der Form der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen einhergeht. Methodisch unterscheidet sich die Risikobewertung im Rahmen der DSFA nicht von der Risikoanalyse zur Gewährleistung des dem Risiko angemessenen Schutzniveaus.

In den hier abrufbaren Leitlinien der Artikel-29-Datenschutzgruppe (siehe auch unter den weiterführenden Links) werden neun Kriterien genannt, die der Verantwortliche zur Prüfung heranziehen kann, ob voraussichtlich ein hohes Risiko besteht.

**Beispiel:** Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen (Nr. 8 der Leitlinien der Artikel-29-Gruppe).

##### 2.1.1 Hohes Risiko bei Gesundheitsdaten und Profiling

Einer eigenen Risikobewertung bedarf es in folgenden Fällen nicht, da jeweils bereits nach der gesetzgeberischen Wertung generell von einem hohen Risiko auszugehen und somit stets eine DSFA durchzuführen ist (Artikel 35 Abs. 3 DSGVO):

- Umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten (insbesondere auch Gesundheitsdaten). Wann eine Verarbeitung „umfangreich“ ist, wird in Erwägungsgrund 91 der DSGVO näher erläutert. Demnach sollen umfangreiche Verarbeitungsvorgänge erfasst werden, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren.

**Beispiel:** Nicht umfangreich ist eine Verarbeitung, die Daten von Patienten betrifft und durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufes erfolgt. In diesem Fall dürfte eine Datenschutz-Folgenabschätzung daher nicht vorgeschrieben sein (EW 91 der DSGVO).

- Systematisch und umfassend durchgeführte Profilingmechanismen (vgl. Artikel 35 Abs. 3 lit. a DSGVO).

##### 2.1.2 Weitere Beispiele für Datenverarbeitungen mit hohem Risiko

Die deutschen Aufsichtsbehörden haben eine Liste weiterer Verarbeitungsvorgänge vorgelegt, für die generell von einem hohen Risiko auszugehen und daher stets eine DSFA durchzuführen ist (vgl. Artikel 35 Abs. 4 DSGVO). Diese Liste kann hier abgerufen werden (siehe auch unter den weiterführenden Links).

## 2.2 Stufe 2: Folgenabwägung

Kommt die Vorprüfung zu dem Ergebnis, dass ein hohes Risiko für die Rechte und Freiheiten des Betroffenen besteht oder eines der gesetzlichen Regelbeispiele einschlägig ist, ist eine DSFA durchzuführen. Ziel der DSFA ist es, aufzuzeigen, dass dem ermittelten hohen Risiko für den Betroffenen mit angemessenen Schutzmaßnahmen begegnet wird. Die DFSA ist zu Dokumentationszwecken zu verschriftlichen. Drei wesentliche Bestandteile muss die DSFA mindestens enthalten (Artikel 35 Abs. 7 DSGVO).

### 2.2.1 Systematische Beschreibung des Verarbeitungsvorgangs

Erforderlich ist zunächst eine systematische Beschreibung der geplanten Verarbeitungsvorgänge. Damit wird der Gegenstand der DSFA erfasst. Ähnlich gelagerte Vorgänge mit ähnlichen Risiken können zusammengefasst werden. Der zu adressierende Verarbeitungsvorgang ist zu identifizieren und muss einem konkreten Zweck sowie der maßgeblichen Rechtsgrundlage zugeordnet werden. Dabei kann eine Orientierung an den Eintragungen im Verzeichnis von Verarbeitungstätigkeiten erfolgen. Zudem sind die vom Verantwortlichen mit der Verarbeitung verfolgten berechtigten Interessen zu benennen. Deren Benennung sollte mit Blick auf die im zweiten Teil vorzunehmende Verhältnismäßigkeitsprüfung generell erfolgen und nicht nur dann, wenn der identifizierte Verarbeitungsvorgang auf der Grundlage einer Interessenabwägung (Artikel 6 Abs. 1 lit. f DSGVO) gerechtfertigt werden kann.

### 2.2.2 Bewertung

Im zweiten Teil der DSFA sind Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck darzulegen. Es ist also eine Verhältnismäßigkeitsprüfung im weiteren Sinne vorzunehmen. Dabei ist zu ermitteln, ob der Verarbeitungsvorgang unter Berücksichtigung des Zwecks geeignet, erforderlich und angemessen ist.

Darüber hinaus muss eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Person erfolgen. Wurde eine solche Analyse bereits im Rahmen der Vorprüfung vorgenommen, so kann an dieser Stelle auf die entsprechende Dokumentation verwiesen werden. Ist hingegen eines der Regelbeispiele einschlägig oder das Verfahren in der Liste der Datenschutzbehörden aufgeführt, muss eine Risikobewertung für die gegenständlichen Verarbeitungsvorgänge durchgeführt werden.

Allerdings ist zu berücksichtigen, dass sich die DSFA nicht auf die für die Datensicherheit maßgeblichen Schutzziele und nicht auf die technischen Aspekte beschränken darf. Vielmehr ist der Verarbeitungsvorgang im Rahmen der DSFA einer umfassenden Rechtmäßigkeitsprüfung zu unterziehen. Insoweit sind sämtliche Vorgaben der DSGVO als Schutzziele einzubeziehen. Hierzu gehören etwa die Transparenzvorgaben (Artikel 13, 14 DSGVO) sowie die Anforderungen an die automatisierte Einzelentscheidung (Artikel 22 Abs. 3 DSGVO).

### 2.2.3 Beschreibung der Abhilfemaßnahmen

Schließlich sind die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen zu benennen. Es kommen insoweit insbesondere Garantien, Sicherheitsvorkehrungen und Verfahren in Betracht; vgl. zu möglichen Maßnahmen auch Ziff. IV.2.2 und die Auflistung in Artikel 32 Abs. 1 lit. a bis d DSGVO.

Eine notwendige Abhilfemaßnahme kann aber etwa auch – mit Blick auf die Transparenzanforderungen – eine Ergänzung in der nach Artikel 13 und 14 DSGVO geschuldeten Information oder die Implementierung eines Prozesses zur Kontaktaufnahme sein, die dem Kunden die Ausübung seines Widerspruchsrechts ermöglicht.

Bei Änderung bestehender Verfahren und bei veränderten Risiken ist die DSFA gegebenenfalls erneut durchzuführen (Artikel 35 Abs. 11 DSGVO).

## 2.3 Dokumentation der DSFA

Der Verantwortliche muss die DSFA dokumentieren, um seiner Rechenschaftspflicht zu genügen. Hierzu sind die beschriebenen Bestandteile der DSFA einschließlich der jeweiligen Prüfungsergebnisse in einem entsprechenden Dokument o.ä. festzuhalten. Dabei sollte der Verantwortliche auch die Perspektive der zuständigen Aufsichtsbehörde vor Augen haben. Diese sollte die Risikobewertung und die Angemessenheit der ergriffenen Abhilfemaßnahmen anhand der Dokumentation nachvollziehen können.

## 2.4 Konsultation der Aufsichtsbehörden

Kommt der Verantwortliche im Rahmen der DSFA zu dem Ergebnis, dass die Verarbeitung zwar mit hohen Risiken verbunden ist, diese aber nicht mit – in Bezug auf verfüg-

bare Technologien und Implementierungskosten – vertretbaren Mitteln eingedämmt werden können, muss er vor Verarbeitungsbeginn die Aufsichtsbehörde konsultieren (Artikel 36 Abs. 1 DSGVO).

### 2.5 Einbindung von Datenschutzbeauftragtem und Auftragsverarbeitern

Die Durchführung der DSFA obliegt dem Unternehmen als Verantwortlichem. Der betriebliche Datenschutzbeauftragte überwacht die Durchführung der DSFA und nimmt auf Anfrage seine Beratungsaufgabe wahr. Die Verlagerung einer Datenverarbeitung auf einen Auftragsverarbeiter entbindet den Verantwortlichen nicht von der Durchführung einer DSFA, die datenschutzrechtliche Verantwortung verbleibt bei ihm. Der Auftragsverarbeiter muss den Verantwortlichen aber bei der Durchführung der Folgenabschätzung unterstützen.

## 3. Best Practice

Unternehmen, die Gesundheitsdaten verarbeiten, sollten sich auf die Durchführung einer DSFA einstellen.

Der Datenschutzbeauftragte muss den Verantwortlichen dahingehend überwachen, dass er seine Mitarbeiter hinsichtlich der Pflicht zur Durchführung einer DSFA hinreichend schult und entsprechende Zuständigkeiten organisatorisch festlegt. Die Durchführung der DSFA muss durch den Datenschutzbeauftragten überwacht werden, d. h. er muss beurteilen, ob die Bestandteile der Dokumentation zur DSFA zutreffend, vollständig und funktionsfähig sind. Diese Überwachung ist zu dokumentieren.

Möchte das Unternehmen neue Datenverarbeitungsverfahren einführen, sollten möglichst früh auch die für die Risikoanalyse relevanten Informationen ermittelt bzw. von den beauftragten Auftragsverarbeitern eingeholt werden. Die Auftragsverarbeiter sind insoweit zur Unterstützung der Unternehmen verpflichtet.

## 4. Weiterführende Links

### 4.1 Leitfäden

- **DSK**, Kurz-Papier zur Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO, Juli 2017: https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf
- **Bitkom**, Leitfaden Datenschutzfolgenabschätzung, Mai 2017: https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf
- **Artikel 29 Gruppe**, WP-248-Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) (inkl. Übersicht zu nationalen und EU-weit geltenden Rahmenbestimmungen/Standard-Datenschutzmodellen und Checklisten), Oktober 2017: https://www.datenschutz-bayern.de/technik/orient/wp248.pdf
- **GDD**, Voraussetzungen der Datenschutz-Folgenabschätzung, November 2017: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf
- **IHK Hannover**, Newsletter DSFA, Dezember 2017: https://www.hannover.ihk.de/fileadmin/data/Dokumente/Themen/Recht/Newsletter_Nr_14_Datenschutzfolgenabschätzung.pdf
- **Datenschutzbehörde Rheinland-Pfalz**, Hinweise zur Datenschutz-Folgenabschätzung nach Artikel 35 Datenschutz-Grundverordnung, Dezember 2017: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Hinweise_DSFA_20171205.pdf
- **Forum Privatheit**, White Paper Datenschutz-Folgenabschätzung, Mai 2016: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf
- **ULD**, Das Standard-Datenschutzmodell (SDM): https://www.datenschutzzentrum.de/sdm/

### 4.2 Anwendungsfälle und Beispiele

- **ULD/DSK**, Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO, Mai 2018: https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf

- **ULD**, Planspiel zur Datenschutz-Folgenabschätzung gem. Artikel 35 DSGVO, November 2017: https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf

## VII. Gemeinsame Datenverantwortlichkeit

### 1. Worum geht es?

Die zunehmende Komplexität von Datenverarbeitungsvorgängen führt dazu, dass die Verarbeitung von Daten in vielen Fällen arbeitsteilig durchgeführt wird. Das kann etwa durch Anweisung an einen Dienstleister passieren, wie bei der Auftragsverarbeitung.

Die Arbeitsteilung kann aber auch zu einem von mehreren Beteiligten gemeinsam verfolgten Zweck und mit von ihnen gemeinsam festgelegten Mitteln durchgeführt werden (vgl. hierzu Ziff. C.I.2.2). Unter der DSGVO gibt es kein Privileg für diese gemeinsame Verantwortlichkeit (Artikel 26 DSGVO). Gemeinsam verantwortliche Unternehmen bleiben im Verhältnis zueinander „Dritte". Ein Austausch von Daten zwischen zwei gemeinsam Verantwortlichen ist daher – wie jede andere Datenverarbeitung – rechtfertigungsbedürftig.

### 2. Was ist zu tun?

Liegt im Einzelfall eine gemeinsame Datenverantwortlichkeit vor (vgl. hierzu Ziff. C.I.2.2), so haben die beteiligten Unternehmen insbesondere eine die gemeinsame Verarbeitung regelnde Vereinbarung abzuschließen und Informationspflichten zu beachten (vgl. zu Einzelheiten Artikel 26 DSGVO).

### 2.1 Vereinbarung

Sind die Voraussetzungen einer gemeinsamen Verantwortlichkeit gegeben, müssen die gemeinsam Verantwortlichen eine Vereinbarung schließen, aus der sich ergibt, welche tatsächlichen Aufgaben, Funktionen und Beziehungen die Betroffenen gegenüber dem jeweiligen Verantwortlichen haben und welcher der Verantwortlichen welche Pflichten der DSGVO erfüllt.

Im Außenverhältnis gegenüber dem Betroffenen schränkt diese Vereinbarung die jeweilige Verantwortlichkeit der beteiligten Unternehmen nicht ein. Die Vereinbarung regelt vielmehr vornehmlich das Innenverhältnis zwischen den verantwortlichen Unternehmen.

### 2.2 Informationspflichten

Die zuvor genannte Vereinbarung zwischen den Verantwortlichen muss den Betroffenen in ihren wesentlichen Zügen zur Verfügung gestellt werden. Ziel ist es, Transparenz für den Betroffenen herzustellen, um es ihm zu erleichtern, seine Rechte geltend machen zu können. Die entsprechenden Informationen können etwa zusammen mit den nach den Artikeln 13 und 14 DSGVO mitzuteilenden Informationen zur Verfügung gestellt werden.

### 3. Weiterführende Links

- **Bitkom**, Leitfaden zu Joint Controllership, April 2017: https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-Joint-Controllership-online.pdf

- **DSK**, Kurzpapier zur Gemeinsamen Verantwortlichkeit, März 2018: https://www.lda.bayern.de/media/dsk_kpnr_16_gemeinsam_verantwortliche.pdf

## VIII. Datenübermittlung in Drittländer

Wollen Unternehmen (Gesundheits-)Daten in ein Land außerhalb der EU übermitteln, z. B. in die USA, müssen neben dem per se erforderlichen Rechtsgrund für eine Datenübermittlung weitere besondere Voraussetzungen erfüllt sein. Da eine solche Drittlandübermittlung vor allem beim Einsatz von Dienstleistern relevant wird, wird dieser Aspekt unter Ziff. C.II.2 näher beleuchtet.

## IX. Datenschutzgrundsätze

### 1. Worum geht es?

Die DSGVO hält in Artikel 5 einen Katalog an Datenschutzgrundsätzen vor. Diese Grundsätze konkretisieren das Ziel der DSGVO, natürliche Personen bei der Verarbeitung personenbezogener Daten sowie den freien Verkehr solcher Daten zu schützen.

Die Datenschutzgrundsätze stellen nicht bloß schlichte Programmsätze dar, sondern definieren verbindliche Maßstäbe für die Verarbeitung personenbezogener Daten. Sie spielen beispielsweise bei Wertungsfragen eine Rolle und können dazu dienen, Zweifelsfragen bei der Anwendung konkreter Regelungen der DSGVO aufzulösen.

Gleichwohl dürfte in der Rechtspraxis eine isolierte Ahndung der sehr allgemein formulierten Grundsätze eher selten in Betracht kommen, da sie weitgehend durch die verschiedenen Einzelbestimmungen der DSGVO konkretisiert werden (z. B. Rechtsgrundlagen nach Artikel 6 DSGVO).

### 2. Was ist zu tun?

Bei der Verarbeitung von Gesundheitsdaten (oder anderen Daten) müssen nicht nur konkrete Vorschriften, sondern auch die allgemeinen Grundsätze der Datenverarbeitung berücksichtigt werden (Artikel 5 DSGVO).

#### 2.1 Rechtmäßigkeit (Erforderlichkeit einer Verarbeitungsgrundlage)

Daten müssen rechtmäßig verarbeitet werden. Das bedeutet, dass bei der Verarbeitung von Gesundheitsdaten immer eine Ausnahme (Artikel 9 DSGVO) und eine Rechtsgrundlage (Artikel 6 DSGVO) vorliegen muss.

#### 2.2 Fairness

Daten müssen nach den Grundsätzen von Treu und Glauben verarbeitet werden. Es gilt somit ein Fairnessgebot, wonach Gesundheitsdaten und andere Daten nur verarbeitet werden dürfen, soweit dies erforderlich bzw. verhältnismäßig ist.

#### 2.3 Transparenz

Die Datenverarbeitung muss in einer für die betroffene Person nachvollziehbaren Weise erfolgen. Der Grundsatz der Transparenz schlägt sich insbesondere in den Informationspflichten und Auskunftsrechten (Artikeln 12 bis 15 DSGVO, vgl. Ziff. III.2 und III.3) nieder.

#### 2.4 Zweckbindung/-änderung

Personenbezogene Daten (einschließlich Gesundheitsdaten) dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden.

Eine Zweckänderung im Verlauf der Verarbeitung kann unter bestimmten Voraussetzungen zulässig sein. Entscheidend ist die Kompatibilität des neuen Zwecks mit dem alten Zweck (sogenannter Kompatibilitätstest, siehe zu den Voraussetzungen Artikel 6 Abs. 4 DSGVO). Für eine solche Kompatibilität spricht u.a. das Vorhandensein von geeigneten Garantien zum Schutz der Betroffenen wie z. B. die Verschlüsselung oder die Pseudonymisierung (Artikel 6 Abs. 4 Buchst. e DSGVO). Ferner gilt eine Zweckänderung bei Weiterverarbeitungen z. B. zu wissenschaftlichen Forschungszwecken oder für statistische Zwecke grundsätzlich als nicht unvereinbar mit den ursprünglichen Zwecken (Artikel 5 Abs. 1 lit. b DSGVO i. V. m. 89 Abs. 1 DSGVO). In diesen Fällen sprechen gute Gründe dafür, dass für die Weiterverarbeitung keine andere gesonderte Rechtsgrundlage als diejenige für die Erhebung der personenbezogenen Daten erforderlich ist (vgl. Erwägungsgrund 50 S. 2 der DSGVO). Diese Frage ist allerdings umstritten und sollte, falls sie eine Rolle spielen kann, mit der jeweils zuständigen Datenschutzbehörde abgeklärt werden.

#### 2.5 Datenminimierung

Personenbezogene Daten, einschließlich Gesundheitsdaten, müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dieser Grundsatz schlägt sich etwa in der Verpflichtung zu Datenschutz by design and by default nieder (vgl. hierzu Ziff.D.II.2).

### 2.6 Datenrichtigkeit

Es ist erforderlich, die Richtigkeit und ggf. Aktualität der Daten zu gewährleisten. Dazu sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Der Grundsatz der Datenrichtigkeit findet insbesondere Ausprägung im Recht auf Berichtigung (vgl. hierzu Ziff. III.4).

### 2.7 Grundsatz der zeitlichen Begrenzung der Speicherung

Der Grundsatz der Speicherbegrenzung korreliert mit dem Grundsatz der Zweckbindung und ergänzt diesen um die Anforderung, dass der Personenbezug von Daten nur so lange bestehen darf, wie dies für den jeweils festgelegten Zweck erforderlich ist. Das bedeutet, dass grundsätzlich umgehend nach Erfüllung des Primärzwecks der Personenbezug aufzuheben ist. Das ist etwa möglich, indem eine Anonymisierung erfolgt. Etwas anderes gilt ggf., wenn die DSGVO eine Weiterverarbeitung zu anderen Zwecken zulässt. Verarbeitungen zu wissenschaftlichen Forschungszwecken oder für statistische Zwecke erfahren hier eine Privilegierung (Artikel 5 Abs. 1 b DSGVO).

### 2.8 Datensicherheit als datenschutzrechtlicher Grundsatz der Integrität und Vertraulichkeit

Es gilt der Grundsatz der Integrität und der Vertraulichkeit. Unternehmen müssen Daten in einer Weise verarbeiten, in der ein angemessenes Sicherheitsniveau durch geeignete technische und organisatorische Maßnahmen gewährleistet wird. Konkretisiert wird dieser Grundsatz vor allem in den gesetzlichen Anforderungen an die Datensicherheit, vgl. hierzu Ziff. IV.

## X. Datenschutz „by design and default“

Eines der erklärten Ziele der Datenschutzgrundverordnung ist der Schutz personenbezogener Daten durch die datenschutzkonforme Ausgestaltung der Informations- und Kommunikationssysteme nach dem Grundsatz Datenschutz „by design and default“ (Artikel 25 DSGVO).

- Das verantwortliche Unternehmen hat schon „by design“, also bei Konzeptionierung, durch geeignete (insbesondere technische) Maßnahmen, und „by default“, also durch geeignete Voreinstellungen, zu gewährleisten, dass die Datenschutzgrundsätze (vgl. Ziff. IX), wie etwa der Grundsatz der Datenminimierung und der Zweckbindung, wirksam umgesetzt werden.

- Die Vorschrift in Artikel 25 DSGVO konkretisiert somit die nach Artikel 24 DSGVO bestehende allgemeine Pflicht, technische und organisatorische Prozesse zum Schutz personenbezogener Daten frühzeitig zu implementieren (siehe Ziff. II.3.2.1). Dabei legt sie einen inhaltlichen Schwerpunkt darauf, dass die Einhaltung der datenschutzrechtlichen Vorgaben schon bei der architektonischen Konzipierung sowie Entwicklung der Datenverarbeitungsvorgänge und den Grundeinstellungen, wie sie dem Nutzer präsentiert werden, Berücksichtigung finden muss.

Da dieser Grundsatz bei Apps eine wichtige Rolle spielt, wird er unter Ziff. D.II.2 näher beleuchtet.

## B. Umgang mit Daten, die dem Berufsträgergeheimnis unterliegen

### I. Worum geht es?

Ärzte unterliegen der ärztlichen Schweigepflicht, die das besondere Vertrauensverhältnis zwischen Patienten und Arzt schützen soll. Patienten sollen sich ihrem Arzt oder ihrer Ärztin uneingeschränkt anvertrauen können. Mit dieser gesetzlichen Schweigepflicht korrespondiert das durch § 203 StGB geschützte Patientengeheimnis, das entsprechende Verstöße des Arztes oder eines Angehörigen eines anderen Heilberufs gegen diese Verschwiegenheitspflicht strafrechtlich sanktioniert.

**Beispiel:** A ist Hausarzt und betreibt seit 35 Jahren eine kleine Praxis in Berlin. Bisher hat er die Patientenakten manuell in Form eines Karteikartenregisters geführt. A entschließt sich, alle Patientendaten zukünftig elektronisch zu verwalten. Hierfür möchte A das Unternehmen D beauftragen, das auch die (Fern-)Wartung des Praxis-IT-Systems übernehmen und die Patientendaten in einer Cloud speichern will. A stellt sich die Frage, ob eine Weitergabe der Daten seiner Patienten an D mit seiner ärztlichen Pflicht zur Verschwiegenheit vereinbar ist.

Bisher erlaubte das Strafrecht dem Arzt – außer in gesetzlich geregelten Sonderfällen oder bei Einwilligung des Patienten – grundsätzlich nur, Patientendaten solchen Mitarbeitern zu offenbaren, die organisatorisch in seine Sphäre eingegliedert waren (z. B. Praxisangestellte, eigene EDV-Mitarbeiter). Das Gesetz verwendete hierfür den Begriff der berufsmäßig tätigen Gehilfen.

Im Zuge der Digitalisierung wird es auch für größere Einrichtungen allerdings zunehmend unausweichlich, sich externer Spezialisten für die Bewältigung der Aufgaben zu bedienen. Hierzu gehört etwa die Bereitstellung und Pflege (inkl. Fernwartung) informationstechnischer Anlagen und entsprechend ausgestatteter medizinischer Geräte sowie die Speicherung von Daten auf externen Anlagen (wie z. B. in einer Cloud). Eine solche Hinzuziehung externer Dienstleister ist nach Auffassung des Gesetzgebers grundsätzlich berechtigt.

Mit Wirkung zum 9. November 2017 hat der Gesetzgeber daher die Möglichkeiten von Ärzten und sonstigen Berufsgeheimnisträgern, sich bei ihrer beruflichen Tätigkeit der Mitwirkung dritter Personen zu bedienen, ausgeweitet. Berufsgeheimnisträger dürfen fremde Geheimnisse nicht nur – wie bisher – gegenüber den bei ihnen berufsmäßig tätigen Gehilfen offenbaren, sondern unter bestimmten Voraussetzungen auch gegenüber sonstigen Personen offenlegen, die an ihrer beruflichen Tätigkeit mitwirken (§ 203 Abs. 3 S. 2 StGB). Das Gesetz verwendet hierfür den Begriff der sonstigen mitwirkenden Personen.

### II. Was ist zu tun?

Der folgende Abschnitt soll einen Überblick darüber geben, unter welchen Voraussetzungen ein Arzt oder ein Angehöriger eines anderen Heilberufs im Sinne des § 203 Abs. 1 Nr. 1 StGB Patientendaten gegenüber externen Hilfspersonen als sogenannte sonstige mitwirkende Personen offenbaren darf.

#### 1. Zwei-Stufen-Prüfung

Die DSGVO steht weiterhin grundsätzlich unabhängig neben dem Strafrecht. Die Zulässigkeit ist also in zwei Stufen zu prüfen:

- **Stufe 1:** Ist die geplante Weitergabe der Daten datenschutzrechtlich zulässig (vgl. unter Ziff. A.I und Abschnitt C)? Wenn nein, ist die Verarbeitung verboten. Wenn ja, weiter mit Stufe 2.

- **Stufe 2:** Ist die geplante Verarbeitung auch strafrechtlich nach Maßgabe des § 203 StGB zulässig?

**Beispiel:** Eine datenschutzrechtlich zulässige Weitergabe von Patientendaten an einen IT-Dienstleister (Stufe 1) kann gleichwohl einen Strafrechtsverstoß (Stufe 2) darstellen. Das wäre etwa dann der Fall, wenn der Arzt die Patientendaten an den IT-Dienstleister weitergibt, ohne diesen zuvor als mitwirkende Person zur Geheimhaltung verpflichtet zu haben (§ 203 Abs. 4 S. 2 Nr. 1 StGB).

## 2. Voraussetzungen für die straffreie Einschaltung von externen Hilfspersonen

Der Berufsgeheimnisträger darf fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an seiner beruflichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist (§ 203 Abs. 3 S. 2 StGB). Zudem ist dafür Sorge zu tragen, dass die sonstige mitwirkende Person zur Geheimhaltung verpflichtet wird. Die folgenden Unterabschnitte sollen hierzu einen Überblick geben.

### 2.1 Fremde Geheimnisse

Verarbeitet ein Angehöriger eines Heilberufes Gesundheitsdaten seines Patienten, handelt es sich bei diesen Daten oftmals auch gleichzeitig um für ihn fremde Patientengeheimnisse, die strafrechtlich geschützt sind. Die Begriffe Gesundheitsdaten (Datenschutzrecht) und Patientengeheimnisse (Strafrecht) überschneiden sich häufig, sind jedoch nicht identisch.

- Der strafrechtliche Schutz erstreckt sich (nur) auf fremde Geheimnisse, von denen ein Angehöriger eines Heilberufes in Ausübung seiner Tätigkeit (also nicht als Privatperson) Kenntnis erlangt hat. Unter fremden Geheimnissen versteht man dabei Tatsachen, die sich auf eine andere Person beziehen, nur einem begrenzten Personenkreis bekannt sind und an denen ein sachlich begründetes Geheimhaltungsinteresse des Betroffenen besteht.

- Gesundheitsdaten sind alle Daten, aus denen Informationen über den Gesundheitszustand einer natürlichen Person hervorgehen – unabhängig von ihrer Vertraulichkeit und unabhängig davon, ob Berufsgeheimnisträger involviert sind. In der Regel ist der Begriff der Patientengeheimnisse daher wesentlich enger als der der Gesundheitsdaten.

### 2.2 Mitwirkung an der beruflichen Tätigkeit

Die externe Hilfsperson muss in die berufliche Tätigkeit des Berufsgeheimnisträgers eingebunden werden und Beiträge dazu leisten.

**Beispiele:** Unter die mitwirkenden Tätigkeiten fallen insbesondere Schreibarbeiten, Rechnungswesen, Annahme von Telefonanrufen, Aktenarchivierung und -vernichtung sowie Outsourcing von IT-Arbeiten und Inanspruchnahme von Cloud-Diensten.

### 2.3 Erforderlichkeit des Offenbarens

Der Arzt muss prüfen, ob und inwieweit das Offenbaren der Patientendaten an den IT-Dienstleister für dessen Inanspruchnahme als sonstige mitwirkende Person erforderlich ist.

Die Rechtfertigung reicht grundsätzlich nur so weit, wie bestimmte Informationen für die konkrete Tätigkeit der externen Hilfsperson erforderlich sind. Auch gegenüber dem IT-Spezialisten ist ein Offenbaren (im Sinne der bloßen Ermöglichung der Kenntnisnahme) erforderlich, damit der Berufsgeheimnisträger dessen Tätigkeit überhaupt sinnvoll in Anspruch nehmen kann. Kann der Arzt – wie häufig – nicht einschätzen, welche Informationen für die Dienstleistungen des externen Vertragspartners erforderlich sind, sollte die Vereinbarung mit diesem vorsehen, dass das Unternehmen und dessen ausführende Mitarbeiter sich nur insoweit Kenntnis von Patienteninformationen verschaffen, wie dies zur Vertragserfüllung erforderlich ist (vgl. auch unter Ziff. III.).

Nicht zu prüfen ist hingegen, ob die Inanspruchnahme der externen Dienstleistung selbst erforderlich ist. Das wirtschaftliche Interesse von Berufsgeheimnisträgern etwa an der Nutzung von Cloud-Diensten ist auch nach der Gesetzesbegründung grundsätzlich berechtigt.

### 2.4 Geheimhaltungsverpflichtung

Der Arzt muss zur Abwendung seiner eigenen Strafbarkeit nach § 203 Abs. 4 S. 2 Nr. 1 StGB auch dafür Sorge tragen, dass die sonstige mitwirkende Person zur Geheimhaltung verpflichtet wird. Dies bedeutet, dass der Arzt

- die von ihm extern beauftragte mitwirkende Person selbst zur Geheimhaltung verpflichtet und
- diese mitwirkende Person gleichzeitig auch dazu verpflichten muss, dass diese wiederum
  - ihre ausführenden Mitarbeiter
  - und – bei Gestattung einer Unterbeauftragung – ihre Unterauftragnehmer in gleicher Weise zur Geheimhaltung verpflichtet.

Der Öffnung in § 203 Abs. 3 S. 2 StGB korrespondiert eine „Verlängerung" des strafrechtlichen Geheimnisschutzes. Die Strafrechtsdrohung erstreckt sich auch auf die sonstigen mitwirkenden Personen. Ein spezifischer Hinweis auf das eigene Strafbarkeitsrisiko der mitwirkenden Person nach § 203 Abs. 4 S. 1 und S. 2 Nr. 2 StGB ist nach dem Wortlaut der gesetzlichen Regelung nicht erforderlich, sollte aber vorsorglich erfolgen.

### 2.5 Umsetzung bei mehrstufigen Unterauftragsverhältnissen

Der Berufsgeheimnisträger muss nicht selbst mit sämtlichen Subunternehmern und deren ausführenden Mitarbeitern Geheimhaltungsvereinbarungen schließen.

Die Strafrechtsandrohung verlangt nach ihrem Wortlaut nur, dass der Berufsgeheimnisträger dafür Sorge trägt, dass der Auftragnehmer zur Geheimhaltung verpflichtet wurde (vgl. § 202 Abs. 4 S. 2 Nr. 1 StGB). Der Berufsgeheimnisträger kann entweder die mitwirkende Person selbst zur Geheimhaltung verpflichten oder dies auch auf andere übertragen. Entsprechendes gilt für mitwirkende Personen, die sich einer weiteren mitwirkenden Person bedienen und die hierbei die Strafandrohung in § 203 Abs. 4 S. 2 Nr. 2 StGB trifft.

### 3. Weitere Einschränkungen durch die berufsrechtliche Verschwiegenheitsverpflichtung?

Gelegentlich wird die Auffassung vertreten, dass die Neuregelung in § 203 Abs. 3 S. 2 StGB zwar Ärzten strafrechtlich unter bestimmten Voraussetzungen erlaube, auch externe Unternehmen mitwirken zu lassen, dass diese Mitwirkung von Externen aber mangels entsprechender Änderung der Berufsordnungen – wie bisher auch – die berufsrechtliche Schweigepflicht verletzen würde.

Diese restriktive Sichtweise steht allerdings nicht im Einklang damit, dass die Bundesärztekammer (BÄK) die Neuregelung und die damit verbundene Öffnung bereits im Gesetzgebungsverfahren ausdrücklich begrüßt und nunmehr in einschlägigen Hinweisen mit Stand 16.02.2018 auch berufsrechtlich nachvollzogen hat (siehe Link unten unter Ziff. V). Die ärztliche Schweigepflicht im Sinne der Musterberufsordnung werde – so die Begründung der BÄK – durch die gesetzliche Offenbarungsbefugnis in § 203 Abs. 3 S. 2 StGB eingeschränkt. Das Auslegungsergebnis der BÄK ist überzeugend und dürfte auch für die Regelungen in den Berufsordnungen der Landesärztekammern gelten.

## III. Best Practice

Zu Beweiszwecken sollte die Geheimhaltungsverpflichtung zwischen Arzt und mitwirkender Person (z. B. IT-Dienstleister) in schriftlicher Form erfolgen. Gleiches gilt für die vertragliche Verpflichtung des mitwirkenden Unternehmens, die für den Arzt eingesetzten Mitarbeiter und – soweit vom Arzt gestattet – etwaige Unterauftragnehmer ihrerseits zur Geheimhaltung zu verpflichten.

Ärzte werden häufig nicht einschätzen können, in welchem Umfang der Mitarbeiter eines IT-Dienstleisters Zugriff auf Patientendaten benötigt. Daher sollte in einem Vertrag über die jeweilige Dienstleistung schriftlich vereinbart werden, dass das Unternehmen und dessen ausführende Mitarbeiter sich nur insofern Kenntnis von Informationen über Patienten verschaffen, wie dies für die Vertragserfüllung erforderlich ist. Diese Vereinbarung kann in den Vertrag über eine Auftragsdatenverarbeitung aufgenommen werden (vgl. Hinweise BÄK, S. A4, unter Ziff. V).

### IV. Wichtige Rechtsvorschriften

- **§ 203 StGB** (Privat-, insbes. Patientengeheimnis)
- **§ 9 Abs. 1** (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) bzw. die entsprechenden (unmittelbar Rechtswirkung entfaltenden) Bestimmungen der Berufsordnungen der Landesärztekammern wie z. B. § 9 Abs. 1 der Berufsordnung der Ärztekammer Berlin

### V. Weiterführende Links

- **Bitkom**, IT-Einsatz durch Berufsgeheimnisträger – Muster zur Umsetzung der Neuregelung des § 203 StGB, August 2018: https://www.bitkom.org/Bitkom/Publikationen/Muster-zur-Umsetzung-des-Gesetzes-zur-Neuregelung-des-Schutzes-von-Geheimnissen-bei-der-Mitwirkung-Dritter-an-der-Berufsausuebung-schweigepflichtiger-Personen.html
- **Bundesärztekammer/Kassenärztliche Bundesvereinigung**: Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis (Stand 16.02.2018), Deutsches Ärzteblatt 2018; 115(10): A-453 / B-395 / C-395: https://www.aerzteblatt.de/archiv/196630/Hinweise-und-Empfehlungen-zur-aerztlichen-Schweigepflicht-Datenschutz-und-Datenverarbeitung-in-der-Arztpraxis
- **Begründung der Bundesregierung zur Neuregelung des § 203 StGB** vom 12.04.2017, BT-Drucks. 18/11936, insbes. S. 17 f., 20-23, 26-30: https://dip21.bundestag.de/dip21/btd/18/119/1811936.pdf

## C. Einschaltung von externen Dienstleistern

### I. Worum geht es?

Im Gesundheitsbereich sind viele Unternehmen bei der Verarbeitung von Gesundheitsdaten auf die Unterstützung von spezialisierten (technischen) Dienstleistern angewiesen. Speichert ein Unternehmen z. B. Gesundheitsdaten bei einem Cloud-Anbieter, erhält der Cloud-Anbieter dabei regelmäßig Zugriff auf Gesundheitsdaten und verarbeitet diese.

Für eine solche Datenverarbeitung durch Dienstleister sieht die DSGVO gewisse Privilegierungen und Erleichterungen von den strengen Voraussetzungen für den Austausch von Gesundheitsdaten mit anderen Unternehmen vor.

Um in den Genuss dieser Erleichterungen zu kommen, muss der Dienstleister als weisungsgebundener Auftragsverarbeiter entsprechend der datenschutzrechtlichen Vorgaben beauftragt werden (Artikel 28 DSGVO).

#### 1. Wie funktioniert die Privilegierung von Auftragsverarbeitern?

Möchte ein Unternehmen Gesundheitsdaten seiner Kunden einem externen Dienstleister weitergeben bzw. offenlegen, muss es für diese Datenverarbeitung normalerweise eine gesonderte Ausnahme nebst Rechtsgrundlage vorweisen

können, wie z. B. eine ausdrückliche Einwilligung des Kunden in die Datenweitergabe an den Dienstleister (Artikel 6 und 9 DSGVO, vgl. unter Ziff. A.I).

Anders dagegen bei der Auftragsverarbeitung: Setzt das Unternehmen den Dienstleister als weisungsgebundenen Auftragsverarbeiter ein und sind die weiteren Vorgaben der Auftragsverarbeitung erfüllt, so wird der Dienstleister datenschutzrechtlich besonders eng an das Unternehmen gebunden. Diese enge Bindung bewirkt, dass die Datenweitergabe zulässig ist, ohne dass es einer gesonderten Ausnahme und Rechtsgrundlage (Artikel 6 und 9 DSGVO) bedarf – obwohl der Dienstleiter ein externes Unternehmen ist. Liegt eine solche Auftragsverarbeitung vor, ist daher allein entscheidend, ob das Unternehmen selbst die Gesundheitsdaten verarbeiten darf. Ist das der Fall, darf es sich zur Erfüllung dieser Aufgabe auch eines externen Dienstleisters bedienen.

Bei der Auftragsverarbeitung werden das Unternehmen und der Dienstleiter somit als eine datenschutzrechtliche Einheit angesehen. Für die gemeinsame Verarbeitung der Gesundheitsdaten durch diese Einheit ist in erster Linie das Unternehmen verantwortlich.

**Beispiel:** Ein Unternehmen bietet Kunden an, die für ihre Gesundheitsvorsorge relevanten Termine, Mitteilungen etc. mittels einer App zentral zu verwalten. Die Termine und Mitteilungen sind Gesundheitsdaten, die das Unternehmen für den Kunden verarbeitet. Die Datenverarbeitung wird durch eine ausdrückliche Einwilligung des Kunden legitimiert.

Mit der Wartung der App will das Unternehmen einen externen technischen Dienstleister beauftragen. Der Dienstleister soll, soweit erforderlich, zur Behebung von individuellen Störungen auch Zugriff auf die vom Kunden gespeicherten Gesundheitsdaten erhalten. Ist das datenschutzrechtlich zulässig?

- Normalerweise wäre hier zu prüfen, ob die Zugriffsgewährung an den Dienstleister und die Arbeit des Dienstleisters mit den Gesundheitsdaten unter eine gesonderte Ausnahme für die Verarbeitung von Gesundheitsdaten fallen und eine Rechtsgrundlage besteht. Hierzu wäre etwa eine zusätzlich ausdrückliche Einwilligung des Kunden in die Einbeziehung des Dienstleisters denkbar.
- Besteht dagegen zwischen Unternehmen und Dienstleister ein wirksames Auftragsverarbeitungsverhältnis für die Wartung, so entfällt diese Prüfung der Zulässigkeit der Offenlegung. Der Dienstleister wird privilegiert. Solange das Unternehmen selbst auf die Gesundheitsdaten zwecks Wartung der App zugreifen darf, kann es diese Aufgabe auch von dem Dienstleister durchführen lassen. Einer ausdrücklichen Einwilligung des Kunden in die Einbeziehung des Dienstleisters bedarf es nicht.

Zu beachten ist allerdings, dass die Privilegierung nur den Bereich des Datenschutzes betrifft. Die besonderen zusätzlichen Vorschriften für Daten, die dem Berufsträgergeheimnis unterliegen, werden von der datenschutzrechtlichen Privilegierung nicht erfasst und müssen daher auch bei der Einbindung von Dienstleistung zusätzlich geprüft werden (vgl. unter Abschnitt B.).

### 2. In welchen Konstellationen kommt eine Auftragsverarbeitung in Betracht?

Die Einbindung eines Dienstleisters wird nur privilegiert, wenn die Anforderungen der DSGVO an eine Auftragsverarbeitung eingehalten werden. „Auftragsverarbeiter“ kann nur sein, wer die Gesundheitsdaten im Auftrag des verantwortlichen Unternehmens verarbeitet. Vor allem muss dazu ein Auftragsverarbeitungsvertrag zwischen dem Unternehmen und dem Dienstleister bestehen. Einzelheiten hierzu sogleich unter Ziff. II.

Zu beachten ist, dass nicht jeder Datenaustausch zwischen Unternehmen als Auftragsverarbeitung eingeordnet werden kann. Die Auftragsverarbeitung kommt nicht in allen Konstellationen in Betracht. Ein wesentliches Merkmal der Auftragsverarbeitung ist, dass der Dienstleister die Gesundheitsdaten nach Weisung des Unternehmens verarbeitet. Zwar kann auch der Auftragsverarbeiter über einen gewissen Entscheidungsspielraum verfügen und in begrenztem Umfang eigenverantwortlich handeln. Das Unternehmen muss aber weiter entscheiden können, wie die Daten verarbeitet werden und zu welchem Zweck.

In folgenden Fällen scheidet daher eine Auftragsverarbeitung aus:

### 2.1 Keine Auftragsverarbeitung, wenn der Dienstleister Verantwortlicher ist

Eine Auftragsverarbeitung kommt nicht in Betracht, wenn der Dienstleister wesentliche Entscheidungen in Bezug auf die von ihm übernommene Datenverarbeitung selbst trifft, er also die Zwecke und Mittel der Verarbeitung festlegt. In diesem Fall ist der Dienstleister selbst Verantwortlicher (Artikel 24 DSGVO, Artikel 4 Nr. 7 DSGVO). Er kann dann nicht Auftragsverarbeiter sein.

**Beispiel:** Ein Dienstleister ist Betreiber einer Website. Er legt fest, unter welchen Bedingungen Inhalte in die Website eingestellt werden dürfen, und bestimmt die Abläufe der Website. Ein solcher Dienstleister ist als Verantwortlicher und nicht als Auftragsverarbeiter einzuordnen. Denn obwohl nicht er, sondern das Unternehmen darüber entscheidet, welche konkreten Inhalte auf der Website eingestellt werden, trifft er gleichwohl wesentliche Entscheidungen darüber, wie die Daten verarbeitet werden.

Unterliegt der Dienstleister hingegen umfangreichen Weisungen, die ihm wenig Spielraum lassen, spricht dies dafür, dass eine Auftragsverarbeitung möglich ist.

Ein Auftragsverarbeiter wird zudem wie ein Verantwortlicher behandelt, wenn er sich über den Auftrag bzw. die Weisung des Verantwortlichen hinwegsetzt und unabhängig vom Willen des Verantwortlichen selbst die Zwecke und Mittel der Verarbeitung festlegt.

### 2.2 Keine Auftragsverarbeitung bei gemeinsamer Verantwortlichkeit

Eine Auftragsverarbeitung kommt nicht in Betracht, wenn das Unternehmen und der Dienstleister gemeinsam wesentliche Entscheidungen in Bezug auf die Datenverarbeitung treffen. In diesem Fall legen beide die Zwecke und die Mittel der Verarbeitung fest. In einer solchen Situation sind datenschutzrechtlich beide Unternehmen gemeinsam verantwortlich. Das bedeutet, dass keines der Unternehmen privilegiert wird.

**Beispiel 1:** Ein Pharmaunternehmen beauftragt eine Arzneimittelstudie. Es bestimmt das Studienprotokoll und legt grundlegende Faktoren der Studie wie Gegenstand und Verlauf fest. Das beauftragte Studienzentrum führt die Studie jedoch weitgehend autonom durch und behält letztendlich auch die erhobenen Daten. In diesem Fall spricht viel dafür, dass das Pharmaunternehmen und das Studienzentrum gemeinsam Verantwortliche sind.

**Beispiel 2:** Unterhält ein Unternehmen eine Fanpage bei einem sozialen Netzwerk wie Facebook, so legt das Unternehmen Kriterien für die Erhebung von Statistiken fest und bezeichnet Kategorien von Personen, deren personenbezogene Daten von Facebook ausgewertet werden sollen. Facebook erhält dabei Einblicke in die Nutzung seiner Dienste, um sein Werbekonzept zu verbessern. Das Unternehmen erhält von Facebook im Gegenzug Besucherstatistiken. Das Unternehmen ist in diesem Fall gemeinsam mit Facebook für die Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage verantwortlich.

Wenn sie gemeinsame Verantwortliche sind, treffen Unternehmen zusätzliche Pflichten, sich gegenseitig abzustimmen. Sie müssen in transparenter Form vereinbaren, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Personen angeht. Einzelheiten sind in Artikel 26 DSGVO geregelt.

## II. Was ist zu tun?

Unternehmen, die externe Dienstleister in ihre Verarbeitung von Gesundheitsdaten als privilegierte Auftragsverarbeiter einbinden wollen, müssen die folgenden Voraussetzungen erfüllen (II.1). Zusätzliche Vorgaben können bestehen, wenn Dienstleister außerhalb der EU in Anspruch genommen werden sollen (II.2).

### 1. Voraussetzungen für den Einsatz von Auftragsverarbeitern

Unternehmen müssen einen Dienstleister wählen, der zuverlässig ist, und sodann mit ihm einen Auftragsverarbeitungsvertrag abschließen.

### 1.1 Auswahl des Dienstleisters

Das verantwortliche Unternehmen hat einen Dienstleister auszuwählen, der zuverlässig ist.

Ein Dienstleister ist zuverlässig, wenn er hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die datenschutzrechtlichen Vorschriften nicht verletzt werden. Damit ist gemeint, dass der Dienstleister ausreichende Nachweise vorlegen muss, die eine sorgfältige und gewissenhafte Erbringung seiner Tätigkeit unter Einhaltung der Vorgaben der DSGVO wahrscheinlich erscheinen lassen.

Wie weit diese Auswahlpflicht geht und wie sie in der Praxis umgesetzt werden soll, ist noch nicht vollständig geklärt. Es werden jedoch keine unverhältnismäßigen Anforderungen an den Auswahlprozess gestellt werden.

**Beispiel:** Bei der Auswahl dürfen Unternehmen berücksichtigen, dass es sich ggf. um einen auf dem Markt bekannten und bewährten Dienstleister handelt. Bei Dienstleistern, die in der EU sitzen und der Aufsicht europäischer Datenschutzbehörden unterliegen, darf zudem grundsätzlich davon ausgegangen werden, dass sich der Dienstleister an die für ihn geltenden Gesetze und datenschutzrechtlichen Bestimmungen hält.

#### 1.1.1 Zertifizierungen als Garantien?

Der Auftragsverarbeiter kann seine Zuverlässigkeit durch die Einhaltung von genehmigten Verhaltensregeln für bestimmte Branchen (Artikel 40 DSGVO) oder durch eine Zertifizierung (Artikel 42 DSGVO) belegen.

Eine Zertifizierung ist ein wesentlicher Indikator für die Zuverlässigkeit des Dienstleisters; allerdings ist auch bei zertifizierten Unternehmen letztendlich immer eine Gesamtbeurteilung des Dienstleisters ausschlaggebend. Zertifikate können es Unternehmen zudem erleichtern, die sorgfältige Auswahl zu dokumentieren und somit ihrer Dokumentationspflicht (Artikel 5 Abs. 2 DSGVO) nachzukommen.

Hinsichtlich der Zertifizierung muss darauf geachtet werden, dass diese durch einen akkreditierten Zertifizierer ausgestellt wird. Zum jetzigen Zeitpunkt ist jedoch noch keine Akkreditierung eines Zertifizierers erfolgt. Eine Zertifizierung im Sinne von Artikel 42 DSGVO ist daher derzeit noch nicht möglich (vgl. Teil 3 – B.I).

#### 1.1.2 Überprüfungen

Auch nach Erteilung eines Auftrags muss das Unternehmen die Zuverlässigkeit des Dienstleisters im Blick behalten, z. B. durch Durchführung von Überprüfungen des Auftragsverarbeiters.

### 1.2 Auftragsverarbeitungsvertrag

Das Unternehmen (als der Verantwortliche) und der Dienstleister (als der Auftragsverarbeiter) müssen einen Auftragsverarbeitungsvertrag schließen.

#### 1.2.1 Inhalt

Der Inhalt dieses Vertrages muss den folgenden zwingenden Mindestanforderungen genügen (Artikel 28 Abs. 3 DSGVO):

a) Grundlegende Festlegungen zum Umfang der beauftragten Datenverarbeitung

Der Vertrag muss Gegenstand, Dauer, Art und Zweck der Verarbeitung (z. B. Cloud-Computing-Dienstleistungen für zwei Jahre) sowie die Art der personenbezogenen Daten und die Kategorien betroffener Personen (z. B. Gesundheitsdaten der Kunden) festlegen. Vor allem bezüglich des Gegenstandes und der Dauer sind auch Verweise auf bereits bestehende Hauptverträge denkbar.

b) Rechte und Pflichten der Beteiligten

Es müssen zumindest alle in Artikel 28 Abs. 3 Buchst. a bis h DSGVO aufgelisteten Rechte und Pflichten vertraglich vereinbart werden.

Hierzu zählen vor allem die Weisungsbefugnis des Auftraggebers und die Pflicht des Auftragsverarbeiters, die Weisungen zu dokumentieren.

Erforderlich sind außerdem jedenfalls vertragliche Regelungen zur Vertraulichkeit, zu Datensicherheitsmaßnahmen des Auftragsverarbeiters, zur Vergabe von weiteren Aufträgen (Unteraufträgen) durch den Auftragsverarbeiter, zu Unterstützungspflichten des Auftragsverarbeiters, zur Rückgabe bzw. Löschung der Daten nach Beendigung des Auftrags und zu Informationsrechten und Kontrollbefugnissen des Auftraggebers.

#### 1.2.2 Form

Der Vertrag ist schriftlich oder in einem elektronischen Format abzufassen.

Mit „elektronischem Format“ ist nicht gemeint, dass die strengen Anforderungen der elektronischen Form gemäß § 126a BGB eingehalten werden müssen. Welche konkreten Anforderungen das elektronische Format erfüllen muss und ob das elektronische Format auch bei der Inanspruchnahme von Unterauftragnehmern durch den Auftragsverarbeiter ausreicht, ist im Einzelnen noch nicht geklärt.

### 1.3 Best Practice

Unternehmen sollten sich möglichst eng am Wortlaut des Artikel 28 Abs. 3 DSGVO orientieren und einen der unter Ziffer III.2 aufgeführten Muster-Auftragsverarbeitungsverträge als Grundlage verwenden.

## 2. Zusätzliche Besonderheiten bei Dienstleistern im EU-Ausland

### 2.1 Worum geht es?

Die DSGVO gewährleistet einen umfassenden Schutz personenbezogener Daten innerhalb der EU/des EWR. Dieser Schutz soll nicht dadurch umgangen werden können, dass Daten in Staaten mit geringeren datenschutzrechtlichen Schutzvoraussetzungen übermittelt werden.

Sollen Daten an Unternehmen in einem Land außerhalb der EU/des EWR, also in ein sogenanntes „Drittland“ (oder „Drittstaat“), übermittelt werden, so ist dies nur unter besonderen Voraussetzungen möglich (Artikel 44 ff. DSGVO). Diese besonderen Voraussetzungen gelten zusätzlich zu den allgemeinen Zulässigkeitsvorschriften für Datenübermittlungen, da auch diese eine Datenverarbeitung darstellen.

Diese Systematik gilt für alle Konstellationen von Datenübermittlungen in Drittländer, also auch für Übermittlungen an einen Verantwortlichen außerhalb der EU. Für außerhalb der EU sitzende Auftragsverarbeiter ist die Thematik aber besonders praxisrelevant.

### 2.2 Was ist zu tun?

Das Unternehmen, das einen Dienstleister außerhalb der EU als Auftragsverarbeiter einsetzen möchte, muss sicherstellen, dass das durch die DSGVO gewährleistete Datenschutzniveau durch die Übermittlung in das Drittland nicht untergraben wird.

Diese zusätzliche Verpflichtung (Artikel 44 ff. DSGVO) tritt somit neben die Einhaltung der allgemeinen Anforderungen an die Auftragsverarbeitung (siehe dazu Ziff. 1).

Zur Sicherstellung eines angemessenen Datenschutzniveaus bietet die DSGVO verschiedene Möglichkeiten:

#### 2.2.1 Privilegierte Drittländer (Artikel 45 DSGVO)

Für bestimmte Drittländer hat die EU-Kommission mittels sogenannter Angemessenheitsbeschlüsse entschieden, dass dort generell oder für bestimmte Daten von einem angemessenen Datenschutzniveau auszugehen ist. Solange es einen solchen EU-Kommissionbeschluss gibt und soweit die jeweiligen Daten erfasst sind, sind die Unternehmen daher davon befreit, selbst zusätzliche Maßnahmen zur Sicherstellung eines angemessenen Datenschutzniveaus zu treffen.

Angemessenheitsbeschlüsse existieren (teilweise mit Einschränkungen) derzeit für folgende Drittländer:

- Andorra
- Argentinien
- Australien (PNR-Daten)
- Färöer
- Guernsey
- Isle of Man
- Israel
- Jersey

- Kanada
- Neuseeland
- Schweiz
- Uruguay

### 2.2.2 Sonderfall USA

In beschränktem Umfang sind auch Unternehmen in den USA privilegiert.

Eine Übermittlung der Daten an ein Unternehmen in den USA kann grundsätzlich ohne zusätzliche Maßnahmen zur Sicherung des angemessenen Datenschutzniveaus erfolgen, wenn und soweit sich das jeweilige US-Unternehmen unter dem sogenannten Privacy Shield zertifiziert hat.

Eine Liste der zertifizierten US-Unternehmen kann unter folgendem Link abgerufen werden: https://www.privacy-shield.gov/list.

**Beispiel:** Im obigen Beispielsfall (s. Ziff. I.1) wird mit der weisungsgebundenen Wartung der App ein US-Unternehmen als externer technischer Dienstleister beauftragt. Dabei soll es auch zu Datenübermittlungen in die USA kommen.

Es ist in diesem Fall nicht ausreichend, dass das Unternehmen mit dem Dienstleister einen Auftragsverarbeitungsvertrag schließt. Das Unternehmen muss zusätzlich prüfen, ob die Übermittlung in die USA (also in ein Drittland) erlaubt ist.

Ist das US-Unternehmen jedoch unter dem Privacy Shield registriert, sind keine zusätzlichen Maßnahmen zur Absicherung des Datenschutzniveaus notwendig und die Beauftragung des US-Unternehmens auf Grundlage eines Auftragsverarbeitungsvertrags ist erlaubt.

Ist das US-Unternehmen nicht unter dem Privacy Shield zertifiziert, sind zusätzliche Garantien erforderlich oder es muss ein besonderer Ausnahmefall vorliegen (siehe hierzu sogleich).

### 2.2.3 Sonstige Drittländer

Fehlt es an einer Privilegierung durch Angemessenheitsbeschluss oder Privacy Shield, muss das Unternehmen entweder bestimmte Garantien zur Absicherung des Datenschutzniveaus vorsehen oder es muss eine Ausnahmekonstellation vorliegen.

a) Garantien
Welche Garantien ausreichend sind, ist in Artikel 46 DSGVO geregelt.

- **Standarddatenschutzklauseln:** In der Praxis sind gerade für kleinere Unternehmen vor allem die sogenannten Standarddatenschutzklauseln von großer Bedeutung. Standarddatenschutzklauseln sind Musterverträge, die von der Kommission entworfen wurden; hierzu zählen auch solche Musterverträge, die bereits vor Geltung der DSGVO erlassen wurden. Schließen die beteiligten Unternehmen diese Musterverträge – zusätzlich zum Auftragsverarbeitungsvertrag – ab, können sie dadurch die erforderlichen Garantien für die Übermittlung in das Drittland erbringen.

  Es existieren unterschiedliche Standarddatenschutzklauseln je nach Verhältnis der an der Übermittlung Beteiligten. Die Standarddatenschutzklauseln für die Konstellation der Übermittlung von einem Verantwortlichen (Auftraggeber) an einen Auftragsverarbeiter (Dienstleister) sind unter folgendem Link abrufbar:

  https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02010D0087-20161217

- **Sonstige Garantien:** Andere geeignete Garantien können dagegen mit einem hohen Aufwand bzw. einem langen behördlichen Genehmigungsverfahren verbunden sein. Das gilt z. B. für die verbindlichen internen Datenschutzvorschriften (sogenannte Binding Corporate Rules). Ein genehmigter Zertifizierungsmechanismus, der grundsätzlich auch als Garantie in Betracht kommt, existiert derzeit noch nicht (für mehr Informationen zu Zertifizierungen siehe unter Teil 3 – B.I).

b) Ausnahmen
In bestimmten Ausnahmefällen kann die Übermittlung in ein Drittland auch ohne Garantien für ein angemessenes Datenschutzniveau zulässig sein. Diese Ausnahmefälle sind in Artikel 49 DSGVO geregelt.

**Beispiel:** Ein in Deutschland tätiges Unternehmen vermittelt Kuraufenthalte in Sri Lanka, die auf die individuelle Gesundheit der Kunden zugeschnitten sind. Die Übermittlung von Buchungsdaten eines Reisenden an das Kurhotel in Sri Lanka wäre zulässig, soweit die Übermittlung für die Erfüllung des Vertrags zwischen dem Reisenden und dem deutschen Unternehmen erforderlich ist. Ein Ausnahmefall für eine zulässige Drittlandübermittlung könnte zudem auch dann vorliegen, wenn der Reisende in die Übermittlung seiner Buchungsdaten nach Sri Lanka ausdrücklich eingewilligt hat, nachdem er über die für ihn bestehenden möglichen Risiken derartiger Datenübermittlungen nach Sri Lanka unterrichtet wurde.

### 2.3 Best Practice

Werden Daten an einen Dienstleister in einem Drittland übermittelt, ist nach einer zwei-Stufen-Prüfung vorzugehen:

Auf der ersten Stufe ist zu prüfen, ob die jeweilige Datenübermittlung an den Dienstleister nach den allgemeinen Voraussetzungen der DSGVO zulässig ist, ob also die Anforderungen an die Auftragsverarbeitung eingehalten sind (Artikel 28 DSGVO). Diesbezüglich gibt es keinen Unterschied zwischen einer Übermittlung an Unternehmen innerhalb der EU oder an ein Unternehmen in einem Drittstaat.

Erst auf der zweiten Stufe ist dann zu prüfen, ob und unter welchen Voraussetzungen eine Übermittlung in ein Drittland stattfinden darf (Artikel 44 ff. DSGVO).

## III. Weiterführende Links

### 1. Leitfäden zur Auftragsverarbeitung

- **Bitkom**, Begleitende Hinweise zu der Anlage Auftragsverarbeitung, Leitfaden, Mai 2017: https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-LF-Auftragsverarbeitung-online.pdf
- **DSK**, Auftragsverarbeitung, Januar 2018: https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf
- **GDD**, Praxishilfe für Auftragsverarbeiter nach Artikel 28 DSGVO, Februar 2018: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_12.pdf
- **BayLDA**, Was ist Auftragsverarbeitung und was nicht?: https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf
- **BayLDA**, FAQ zu Arztpraxis und Auftragsverarbeitung: https://www.lda.bayern.de/media/FAQ_Auftragsverarbeitung_Arzt.pdf
- **BvD**, Umgang mit Altverträgen bzgl. Auftragsverarbeitung (ADV-Verträge), Juni 2017: https://www.bvdnet.de/wp-content/uploads/2017/07/17_Umgang_Altvertraege.doc
- **IHK Saarland**, Auftragsverarbeitung nach der DSGVO, März 2018: https://www.saarland.ihk.de/ihk-saarland/Integrale?SID=CRAWLER&MODULE=Frontend.Media&ACTION=ViewMediaObject&Media.PK=7451&Media.Object.ObjectType=full

### 2. Musterverträge zur Auftragsverarbeitung

- **BvD**, Muster-Auftragsverarbeitungs-Vertrag für das Gesundheitswesen, Juni 2017: https://www.bvdnet.de/wp-content/uploads/2017/07/Muster-AV-Vertrag.pdf
- **GDD**, Vertragsmuster zur Auftragsverarbeitung, April 2017: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf
- **ULD**, Mustervereinbarung für einen Vertrag zur Auftragsverarbeitung, April 2018: https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-3-ADV.pdf

### 3. Datenübermittlung in Drittländer

- **DSK**, Datenübermittlung in Drittländer, September 2017: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_4_Datenuebermittlung-Drittlaender.pdf.
- **EU-Kommission**, Informationen zu Standarddatenschutzklauseln (engl.): https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en


## D. Angebot einer (Gesundheits-)App

### I. Worum geht es?

Die umfangreiche Verarbeitung von Gesundheitsdaten ist ein charakteristischer Faktor der Entwicklungen im Bereich **eHealth**, also der gesundheitsnahen Dienstleistungen, die mit modernen Informations- und Telekommunikationstechnologien erbracht werden. Das gilt vor allem für die durch Mobilgeräte elektronisch unterstützte Gesundheitsversorgung (**mHealth**).

Speziell im mobilen Bereich stellen Unternehmen den Nutzern dabei mittels leicht zugänglicher Software bestimmte eHealth-Funktionalitäten und gesundheitsrelevante Anwendungsmöglichkeiten bereit (**Gesundheits-Apps**), die – häufig in großem Umfang – Gesundheitsdaten der Nutzer verwenden. Der datenintensive Charakter von Apps geht mit entsprechenden Risiken für den Schutz der Gesundheitsdaten der Nutzer einher.

Aufgrund des einfachen Zugangs zu Apps, deren breiten Nutzungsmöglichkeiten und der weitgehenden Undurchsichtigkeit der Vorgänge im Umgang mit den Daten der Nutzer kommt dem Datenschutzrecht bei Apps daher eine entscheidende Rolle zu.

### II. Was ist zu tun?

Grundsätzlich gelten für Gesundheits-Apps die gleichen datenschutzrechtlichen Anforderungen wie bei jeder anderen Verarbeitung von Gesundheitsdaten. Daneben sollten Unternehmen, die Apps im Bereich eHealth (bzw. mHealth) entwickeln oder anbieten wollen, einige datenschutzrechtliche Besonderheiten beachten. Der nachfolgende Abschnitt stellt diese übersichtsartig dar.

#### 1. Zulässigkeit der Datenverarbeitung

Wie jede Verarbeitung personenbezogener Daten, muss auch die Datenverarbeitung im Rahmen von Gesundheits-Apps die allgemeinen datenschutzrechtlichen Zulässigkeitsvoraussetzungen erfüllen. Das bedeutet, dass für die Verarbeitung von Gesundheitsdaten im Zusammenhang mit der App eine gesetzliche Ausnahme nebst Rechtsgrundlage (Artikel 6 und 9 DSGVO, siehe ausführlich Ziff. A.I.) bestehen muss. Fehlt eine solche, verstößt der App-Anbieter gegen das Datenschutzrecht und muss mit Sanktionen durch Aufsichtsbehörden (z. B. Geldbußen) sowie Abmahnungen von Konkurrenten rechnen.

##### 1.1 Verarbeitungsgrundlage ist typischerweise eine Einwilligung

Die wichtigste gesetzliche Verarbeitungsgrundlage ist in der Praxis die (ausdrückliche) Einwilligung des Betroffenen (Artikel 9 Abs. 2 lit. a DSGVO, siehe Ziff. A.I.3.1). Die Einwilligung muss eingeholt werden, bevor die jeweilige Datenverarbeitung beginnt. Im Idealfall sollten erforderliche Einwilligungen daher bereits vor dem Download der App eingeholt werden.

Dass die Gesundheitsdaten zum Zweck der Gesundheitsvorsorge verarbeitet werden sollen, reicht dagegen in der Regel nicht aus, um eine Zulässigkeit zu begründen. Denn die Gesundheitsvorsorge ist nur dann als Ausnahme vom Verbot der Verarbeitung von Gesundheitsdaten einschlägig, wenn z. B. ein (Berufs-)Geheimnisträger die Verarbeitung verantwortet (Artikel 9 Abs. 3 DSGVO).

###### 1.1.1 Einwilligung bei mehreren Nutzern

Problematisch können Fälle sein, in denen mehrere Personen auf das mobile Gerät zugreifen können, die Einwilligung

aber nur einmal bei der erstmaligen Ausführung der App eingeholt wurde. Zu beachten ist, dass die Einwilligung sich immer nur auf diejenige Person bezieht, die sie abgegeben hat. Dieses Problem kann technisch z. B. durch die Einrichtung einer Benutzerverwaltung gelöst werden, mit der Einwilligungen auch für mehrere Nutzer eingeholt werden können.

#### 1.1.2 Einwilligung bei Kindern

Minderjährige sind nach der DSGVO besonders schutzwürdig, da sie die Risiken der Verarbeitung personenbezogener Daten im Zweifel schlechter einschätzen können als Erwachsene. Wird die App von Kindern genutzt, gelten daher besondere Anforderungen an die Einwilligung (Artikel 8 DSGVO).

Ein Kind kann nur dann wirksam in die Verarbeitung seiner Daten einwilligen, wenn es das 16. Lebensjahr vollendet hat. Ansonsten bedarf es der Einwilligung des Trägers der elterlichen Verantwortung. App-Anbieter müssen insbesondere sicherstellen, dass eine Verifikation der Träger der elterlichen Verantwortung stattfindet.

#### 1.1.3 Einwilligung bei Standortdaten

Für die Verwendung von Standortdaten gelten besonders strenge datenschutzrechtliche Anforderungen, da solche Daten Bewegungsprofile ermöglichen. Die Erhebung und Verarbeitung von Standortdaten erfordert regelmäßig eine gesonderte Einwilligung – unabhängig davon, ob sie im Zusammenhang mit Gesundheitsdaten verarbeitet werden.

Greift eine App auf Standortdaten zu, sollte zudem darauf geachtet werden, dass der exakte Standort des Nutzers nur insoweit bestimmt werden kann, wie dies für die Nutzung der App erforderlich ist. Die zeitlichen Abschnitte, in denen Standortdaten gesammelt werden, sollten möglichst begrenzt werden. Gleichzeitig sollte die Speicherung dieser Standortdaten lokal auf dem Endgerät erfolgen und nicht an den App-Anbieter übermittelt werden. Standardmäßig sollte die Standortermittlung ausgeschaltet sein.

Ferner sollte der Nutzer durch einen permanenten Warnhinweis erkennen können, dass die Standortermittlung eingeschaltet ist. Schließlich ist über Standortdaten in der Datenschutzerklärung (vgl. Ziff. 4) sehr detailliert im Sinne größtmöglicher Transparenz zu informieren. Weitergehende Informationen enthält die Orientierungshilfe des Düsseldorfer Kreises unter Ziff. III.2.

### 1.2 Verarbeitung anderer Daten

Soweit andere personenbezogene Daten, die keine Gesundheitsdaten sind, verarbeitet werden, bedarf es nach allgemeinen Grundsätzen einer Rechtsgrundlage (Artikel 6 DSGVO, siehe auch Ziff. A.I.2.3).

Besonders praxisrelevant ist vor allem die Rechtsgrundlage der Vertragserfüllung (Artikel 6 Abs. 1 lit. b DSGVO). Danach ist die jeweilige Datenverarbeitung zulässig, soweit sie für die Erfüllung eines Vertrags mit dem betroffenen Nutzer (z. B. zur Bereitstellung der Dienste der App oder zur Abrechnung) oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist. Bei Apps können in diese Kategorie der erforderlichen Datenverarbeitung typischerweise u. a. folgende personenbezogenen Daten fallen:

- Personenbezogene Daten, die zur Begründung, inhaltlichen Ausgestaltung oder Änderung des Vertrags über die Nutzung der App erforderlich sind.

**Beispiele:** Typische Daten in diesem Sinne sind z. B. Kontakt- und Zahlungsdaten bei zahlungspflichtigen Apps, Passwörter, IP-Adressen etc.

- Personenbezogene Daten, die für die eigentliche Nutzung der App benötigt werden, wie z. B. Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Inhalte.

**Beispiele:** Typische Nutzungsdaten sind etwa die in den Browser eingegebenen URLs, Suchanfragen bei Suchmaschinen oder Cookies, durch die der Anbieter erfährt, dass der Nutzer bereits zu einem früheren Zeitpunkt auf ein Angebot zugegriffen hat. Auch Standortdaten können für die Nutzung bestimmter App-Funktionen erforderlich sein – etwa, wenn der Nutzer einer Jogging-App sich die bisher zurückgelegte Laufstrecke und den aktuellen Standort auf einer Karte anzeigen lassen möchte.

### 1.3 Analyse von Nutzerverhalten/Tracking

Auch wenn in der App das Nutzerverhalten gemessen bzw. getrackt werden soll, gelten die allgemeinen Rechtmäßig-

keitsvoraussetzungen. Zu beachten ist allerdings, dass in diesem Zusammenhang verschiedene Aspekte umstritten sind und sich die Rechtslage in naher Zukunft voraussichtlich ändern wird, wenn die sogenannte E-Privacy-Verordnung in Kraft tritt.

#### 1.3.1 Geltende Rechtslage

Derzeit kommt es für die Beurteilung der Rechtmäßigkeit von Reichweitenmessung und des Einsatzes von Tracking-Mechanismen, die das Verhalten von betroffenen Nutzern im Internet nachvollziehbar machen, auf die allgemeinen Vorschriften der DSGVO (insbesondere Artikel 6 und 9 DSGVO) an. Die §§ 12, 13, 15 TMG werden dagegen nicht mehr angewendet, da sie von der DSGVO verdrängt werden.

Personenbezogene Daten, die keine Gesundheitsdaten sind, dürfen daher im Rahmen von Tracking-Mechanismen bzw. für Nutzeranalysen verwendet werden, soweit dies für die Nutzung der App und damit für die Erfüllung des mit dem Nutzer geschlossenen Vertrags erforderlich ist.

**Beispiel:** Um den Nutzer bei der „Selbststeuerung" seines Handygebrauchs zu unterstützen, erstellt eine App für den Nutzer Übersichten, aus denen der Nutzer erkennen kann, zu welchen Tagesezeiten oder an welchen Orten bestimmte Apps besonders häufig genutzt werden.

Werden personenbezogene Daten hingegen nicht für die Vertragserfüllung benötigt, bedarf es nach der umstrittenen Ansicht der deutschen Datenschutzbehörden (siehe hierzu den Link unter Ziff. III.1) jedenfalls dann einer vorherigen Einwilligung des Nutzers, wenn

- Tracking-Mechanismen eingesetzt werden, die das Verhalten von konkreten betroffenen Personen im Internet nachvollziehbar machen, oder
- wenn Nutzerprofile erstellt werden.

In diesen Fällen sollte daher eine Einwilligung des Nutzers eingeholt werden, bevor z. B. Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.

Soweit Gesundheitsdaten getrackt oder analysiert werden, ist aufgrund der dann geltenden strengeren Anforderungen nach Artikel 9 DSGVO typischerweise ohnehin eine Einwilligung erforderlich (vgl. oben Ziff. 1.1)

#### 1.3.2 Anstehende Änderung des Rechtsrahmens durch die E-Privacy-Verordnung

Auf europäischer Ebene wird derzeit die sogenannte E-Privacy-Verordnung beraten, ein neues Gesetz, das u. a. die Datenverarbeitung im Internet und den berechtigten Zugriff auf Endgeräte bereichsspezifisch regeln soll. Ziel der E-Privacy-Verordnung ist, einen wirksamen Schutz der Privatsphäre zu gewährleisten und innovative Anwendungen nicht unangemessen zu behindern. Tritt sie in Kraft, wird sie voraussichtlich neben der DSGVO und unmittelbar in allen EU-Mitgliedstaaten gelten. Insbesondere die Zulässigkeit des Webtrackings und des Zugriffs auf Endgeräte wird sich dann nach den Vorgaben der E-Privacy-Verordnung richten.

### 2. Datenschutz by design/Datenschutz by default

Zwei zentrale Grundsätze einer DSGVO-konformen Datenverarbeitung, die insbesondere bei der Programmierung von Apps besonders relevant werden, sind Datenschutz by design und Datenschutz by default:

- Anwendungen und Systeme müssen von Beginn an schutzbedarfs- bzw. risikoorientiert konzipiert und technisch umgesetzt werden. Diesen Ansatz nennt man Datenschutz by design.
- Zudem soll nach dem Prinzip „Datenschutz durch datenschutzfreundliche Voreinstellungen" ein angemessenes Datenschutzniveau für Nutzer durch datenschutzfreundliche Grundeinstellungen gewährleistet werden (Datenschutz by default).

Zur Implementierung der beiden Grundsätze sind insbesondere folgende Maßnahmen ratsam:

#### 2.1 Datensparsamkeit

Soweit möglich, sollte der Nutzer die App anonym nutzen können. Sind anonyme Daten nicht ausreichend, sollten die Daten zumindest möglichst weitgehend pseudonymisiert werden.

Im Übrigen sollte die Verarbeitung von Gesundheitsdaten minimiert werden und auf das tatsächlich notwendige Maß reduziert werden, gerade auch in den Voreinstellungen der App.

Zu solchen Minimierungsmaßnahmen gehört etwa die standardmäßige Unterbindung von Cookies bzw. Setzung von Cookies erst mit der Bestätigung durch den Nutzer. Eine standardmäßige Deaktivierung der Ortungsfunktion in der App ermöglicht, dass erst nach Aktivierung/Zustimmung durch den Nutzer dessen aktueller Standort verwendet werden kann. Vor dem ersten Start der App sollten keine Daten versendet werden, soweit dies nicht für den Download oder die Installation technisch erforderlich ist.

**Beispiel:** Eine App analysiert die Stimmlage des Nutzers, um Rückschlüsse auf dessen physische Verfassung zu ziehen. Wenn der Nutzer die App startet, erfolgt noch kein Zugriff des Handys auf das Mikrofon. Vielmehr muss der Nutzer erst von sich aus eine ausdrückliche Zugriffsberechtigung erteilen, wenn er die App tatsächlich nutzt. Das Mikrofon wird sodann durch die App nur so lange eingeschaltet, wie es erforderlich ist, um eine ausreichende Datenbasis für die Analyse zu schaffen.

### 2.2 Zweckbindung

Gesundheitsdaten werden ausschließlich zu den jeweils konkret benannten Zwecken verarbeitet und Zugriffsberechtigungen werden lediglich im Rahmen dieser Zwecke verlangt. Weiterverarbeitungen der Daten zu anderen Zwecken sind innerhalb der gesetzlichen Vorgaben der DSGVO und des BDSG (etwa zu Forschungszwecken) zulässig.

**Beispiel:** Eine App analysiert die Stimmlage des Nutzers, um Rückschlüsse auf dessen physische Verfassung zu ziehen. Anhand einer kurzen Aufnahme der Stimme wird die tägliche Stimmungslage aufgrund von Vergleichsgruppen ermittelt und dem Nutzer angezeigt.

Der Zugriff auf das Mikrofon des Handys erfolgt nur zu dem Zweck, täglich die konkreten Aufnahmen als Basis für die Zuordnung einer Stimmungslage zu erstellen. Sobald die Stimmungslage bewertet wurde, wird die jeweilige Aufnahme für die Zwecke der App nicht mehr benötigt und sodann (wegen Fortfall des Zwecks) gelöscht.

### 2.3 Aggregierung

Daten sollten wenn möglich aggregiert und Gruppen statt Einzelpersonen zugeordnet werden. So wird ein Rückschluss auf individuelle Informationen zu einer bestimmten Person erschwert.

### 2.4 Kontrolle und Transparenz

Der Nutzer sollte jederzeit in der Lage sein, zu kontrollieren und zu überblicken, welche Gesundheitsdaten über ihn gesammelt werden. Die Benutzeroberflächen sollten entsprechend transparent ausgestaltet sein und es dem Nutzer ermöglichen, die Datenschutzeinstellungen jederzeit und ohne Komplikationen zu ändern:

- Apps sollten alle datenschutzrechtlichen Einstellungen und Informationen an einer leicht auffindbaren Stelle bündeln, z. B. unter einem Menüpunkt „Datenschutz“.
- Der Nutzer sollte einsehen können, welche Einwilligungen (wie Zugriffsberechtigungen oder Zustimmungen in das Setzen von Tracking- oder Analyse-Cookies) er erteilt hat, und solche Einwilligungen/Zugriffsberechtigungen jederzeit innerhalb der App widerrufen können. Das Datensendeverhalten der App sollte möglichst kontrollierbar sein und Einschränkungen ermöglichen.

**Beispiel:** Eine App analysiert die Stimmlage des Nutzers, um Rückschlüsse auf dessen physische Verfassung zu ziehen. Unter dem Menüpunkt Datenschutz kann der Nutzer sehen, in welchem Umfang er der App Zugriff auf das Mikrofon des Handys gewährt hat, und diesen Zugriff jederzeit rückgängig machen.

- Nutzer sollten wenn möglich selbständig Daten sperren bzw. löschen können bzw. über Löschungsoptionen informiert werden.
- Updates sollten bereits getroffene Datenschutzeinstellungen respektieren. Soweit Updates mit einer zusätzlichen oder anderen Datenverarbeitung einhergehen, sollte hierauf transparent hingewiesen werden.

### 2.5 Frühzeitige Prüfung des Datenschutzes und der Datensicherheit

Die Einhaltung der datenschutzrechtlichen Anforderungen sollte nicht erst geprüft werden, wenn die App bereits vollständig programmiert ist.

Oftmals können in der Anfangsphase datenschutzrechtlich relevante Weichenstellungen noch ohne Schwierigkeiten vorgenommen werden. Nachträgliche Eingriffe in den fertigen Code können dagegen mit erheblichem Aufwand und hohen Kosten verbunden sein.

Bei der Programmierung von Apps sollten daher der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte frühzeitig eingebunden werden, um die Einhaltung der datenschutzrechtlichen Anforderungen sicherzustellen und Compliance-Kosten zu reduzieren. Die Einbindung des Datenschutzbeauftragten und des IT-Sicherheitsbeauftragten sollte zudem dokumentiert werden.

## 3. Datensicherheit

Für das datenschutzkonforme Angebot von Apps ist es elementar, dass durch technische und organisatorische Maßnahmen ein angemessenes Sicherheitsniveau gewährleistet ist (Artikel 32 DSGVO, vgl. hierzu bereits Ziff. A.IV). Wichtige Themen bei der Datensicherheit in Apps sind insbesondere unverzügliche Einspielung von sicherheitsrelevanten Patches und Updates, sichere Passwörter, Auto-Log-out, Verschlüsselung der Datenübertragungen, Anforderungen an lokale Speicherung, Einbindung fremder Webseiten und Backend-Schutz.

Die eingesetzte Technologie muss die Einhaltung der Datenschutzgrundsätze dauerhaft gewährleisten. Das heißt, dass es eines regelmäßigen Abgleichs der eingesetzten Technik mit dem geltenden Recht und dem Stand der Technik bedarf, um ggf. Nachbesserungen im Standard vorzunehmen. Beispiele für diese Nachbesserung können ein höherer Verschlüsselungsstandard oder ein stärkeres Authentifizierungsverfahren sein.

Weitergehende Informationen zur Datensicherheit bei Apps bietet u. a. der Leitfaden “Smartphone Secure Development Guideline” der ENISA (European Union Agency for Network and Information Security) sowie die Leitfäden der Artikel-29- Gruppe (S. 18 ff.) und des Düsseldorfer Kreises (S. 21 ff.), siehe hierzu die Links unter Ziff. III.1.

## 4. Information

Rechtlich zwingend erforderlich ist eine Datenschutzerklärung. Zu empfehlen ist zudem ein nutzerfreundlicher One-Pager. Es können ferner weitere Informationspflichten, wie z. B. typischerweise die Impressumspflicht, bestehen.

### 4.1 Datenschutzerklärung

Die Informationspflichten der DSGVO gelten auch für die Datenverarbeitung in Apps (Artikel 13, 14, 21 DSGVO, siehe hierzu Ziff. A.III.2). Als Leitlinie für die Zusammenstellung der Information kann die unter Ziff. III.1 aufgelistete **Musterdatenschutzerklärung** für Websitebetreiber dienen.

- Die Datenschutzerklärung muss App-spezifisch sein, also die besondere Datenerhebung und -nutzung durch die App erläutern. Hierzu zählen z. B. Datenerhebung mittels Kameras, verschiedenen Sensoren des jeweiligen Endgerätes oder Wearables und Zugriff auf im Telefon gespeicherte Kontakte oder Bilder.

- Die Datenschutzerklärung sollte möglichst frühzeitig einsehbar sein und daher bereits im App Store zur Verfügung gestellt werden. Eine Kenntnisnahme erst nach der Installation genügt nicht, da bei erster Inbetriebnahme der App schon Zugriff auf personenbezogene Daten erfolgen kann.

- Die Datenschutzerklärung sollte auch in der App an zentraler Stelle platziert und leicht aufzufinden sein.

### 4.2 One-Pager

Empfehlenswert ist es, zusätzlich zur rechtlich verpflichtenden Datenschutzerklärung eine Kurzinformation bereitzustellen, die alle wesentlichen Punkte der Datenverarbeitung anschaulich zusammenfasst (sogenannte One-Pager). Ein kommentiertes **Muster** für einen solchen One-Pager findet sich unter Ziff. III.1.

Um Apps informiert und selbstbestimmt nutzen zu können, sollten Nutzer jederzeit in der Lage sein zu verstehen, wie Gesundheitsdaten verarbeitet werden und wer Kenntnis von den Gesundheitsdaten erhält. Gerade bei Apps, deren zentraler Zweck in der Verarbeitung großer Mengen oder besonders sensibler Gesundheitsdaten liegt, kann es für die

Nutzer schwierig sein, den Kern der Datenverarbeitung anhand einer ausführlichen Datenschutzerklärung schnell nachzuvollziehen.

Der One-Pager kann vor diesem Hintergrund dazu dienen, die Datenverarbeitung verbraucherfreundlich, anschaulich und transparent aufzubereiten, um Vertrauen zu schaffen sowie die Nutzerakzeptanz zu erhöhen. Er sollte einen ersten, strukturierten Überblick bieten und den Nutzern, ggf. über ein gestuftes Modell (Layered-Approach), Zugang zu ausführlicheren Erklärungen in der Datenschutzerklärung verschaffen. Auch der One-Pager sollte vor dem Download und der Installation zugänglich sein.

### 4.3 Impressumspflicht

Apps mit Online-Anbindung, die (Gesundheits-)Daten aufbereiten, fallen als elektronische Informations- und Kommunikationsdienste regelmäßig unter den Anwendungsbereich des Telemediengesetzes (vgl. § 1 TMG). Zu beachten ist in diesen Fällen insbesondere die Impressumspflicht bei geschäftsmäßig angebotenen Apps (Informationspflichten nach § 5 TMG). Hierzu können auch kostenlose Apps gehören. Das Impressum muss leicht als solches erkennbar, unmittelbar (d. h. ohne längeres Suchen) erreichbar und ständig verfügbar sein.

Ein **Leitfaden** zur Impressumspflicht findet sich unter Ziff. III.1.

### 5. Anforderungen der App Stores

Neben gesetzlichen Anforderungen stellen auch die verschiedenen App Store-Betreiber wie z. B. Apple und Google in ihren Developer Agreements durchaus umfangreiche datenschutzrechtliche Vorgaben auf. Will ein Unternehmen die App in einem App Store bereitstellen, sollte es daher darauf achten, dass die jeweiligen Anforderungen eingehalten werden.

## III. Weiterführende Links

### 1. Muster und Hilfen zu Informationspflichten

- **Prof. Dr. Thomas Hoeren/Deutsches Forschungsnetz**, Musterdatenschutzerklärung für Websitebetreiber nach den Vorgaben der DSGVO, April 2018: https://www.uni-muenster.de/Jura.itm/hoeren/itm/wp-content/uploads/Musterdatenschutzerk%C3%A4rung-nach-der-DSGVO.docx

- **BMJV/Nationaler IT-Gipfel**, „One-Pager" – Kommentiertes Muster für transparente Datenschutzhinweise, November 2015: https://www.bmjv.de/SharedDocs/Downloads/DE/Verbraucherportal/OnePager/11192915_OnePager-Datenschutzhinweise.pdf?__blob=publicationFile&v=3

- **BMJV**, Leitfaden zur Impressumspflicht, April 2016: https://www.bmjv.de/DE/Verbraucherportal/DigitalesTelekommunikation/Impressumspflicht/Impressumspflicht_node.html

### 2. Leitfäden zu Apps und Datenschutz

- **Medizinische Hochschule Hannover** (gefördert durch das Bundesministerium für Gesundheit), Leitfaden zu Chancen und Risiken von Gesundheits-Apps, April 2016: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/A/App-Studie/CHARISMHA_gesamt_V.01.3-20160424.pdf

- **ENISA**, Smartphone Secure Development Guideline, Februar 2017 (engl.): https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016

- **ENISA**, Privacy and data protection in mobile applications, Januar 2018 (engl.): https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications

- **BMJV**, Verbraucherfreundliche Best Practice bei Apps, u. a. mit Bezug zum Datenschutzrecht, Februar 2017: https://www.bmjv.de/SharedDocs/Downloads/DE/Service/StudienUntersuchungenFachbuecher/Apps_Best_Practise_StiWa_DE.pdf?__blob=publicationFile&v=1

- **Nationaler IT-Gipfel**, Thesenpapier zu Privacy by Design, November 2015: https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/11162016_IT_Gipfel_Thesenpapier.pdf?__blob=publicationFile&v=1

- **Berliner Beauftragte für Datenschutz**, Hinweise zur Verarbeitung von Nutzungsdaten durch Blogs bzw. Webseiten, Juli 2018: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/themen-a-z/n/Nutzungsdaten/20170705-Hinweise-Nutzungsdaten.pdf

- **DSK**, Zur Anwendbarkeit des TMG für nichtöffentliche Stellen ab dem 25. Mai 2018, April 2018: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf

- **Zum alten Datenschutz-Recht vor Geltung der DSGVO**: Düsseldorfer Kreis, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, Juni 2014: https://www.lda.bayern.de/media/oh_apps.pdf

- **Zum alten Datenschutz-Recht vor Geltung der DSGVO**: Artikel-29-Gruppe, Stellungnahme zu Apps auf intelligenten Endgeräten, Februar 2013 (engl.): https://iapp.org/media/pdf/resource_center/wp202_Apps-smart-devices_02-2013.pdf

- **Zum alten Datenschutz-Recht vor Geltung der DSGVO**: EU-Kommission, DRAFT Privacy Code of Conduct on mobile health apps, August 2016 (engl.): https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

### 3. Allgemeine Informationen zu (Gesundheits-)Apps

- **Bundesinstitut für Arzneimittel und Medizinprodukte**, Orientierungshilfe Medical Apps, Oktober 2015: https://www.bfarm.de/DE/Medizinprodukte/Abgrenzung/MedicalApps/_node.html;jsessionid=5023A558770724433C1A522025D70163.1_cid329

- **Bundesinstitut für Arzneimittel und Medizinprodukte**, Unterstützung für App-Entwickler, Juni 2016: https://www.bfarm.de/SharedDocs/Downloads/DE/Service/Termine-und-Veranstaltungen/dialogveranstaltungen/dialog_2016/160608/02_Folien_Raemsch-Guenther.pdf?__blob=publicationFile&v=3

- **Bitkom/bvitg/ZVEI**, Checkliste: Medical Apps und digitale Gesundheitsanwendungen als Medizinprodukt, Juni 2017: https://www.bvitg.de/wp-content/uploads/bvitg_bitkom_ZVEI_Handlungsempfehlung_Checkliste_Medical_App_2017.pdf

- **EU-Kommission**, Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices, Juli 2016 (engl.): https://ec.europa.eu/docsroom/documents/17921/attachments/1/translations/en/renditions/native

- **Bundesministerium für Gesundheit**, FAQ zur elektronischen Gesundheitskarte und zum E-Health-Gesetz, März 2018: https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health-gesetz/faq-e-health-gesetz.html


## E. Profiling und automatisierte Entscheidungsfindung

### I. Worum geht es?

Bereits heute sind zahlreiche Unternehmen in der Lage, anhand der vorhandenen Datenbestände umfassende Persönlichkeitsprofile (z. B. zu Kunden oder Mitarbeitern) zu erstellen. Von der Verwendung solcher Profile können Risiken für das Persönlichkeitsrecht der Betroffen ausgehen. Gleiches gilt, wenn Daten von Betroffenen im Rahmen automatisierter Einzelentscheidungen – etwa auf Grundlage von Algorithmen – ausgewertet werden. Für den Einsatz solcher Methoden (z. B. beim Einsatz von KI-Lösungen) gelten daher besondere datenschutzrechtliche Vorgaben.

#### 1. Profiling

Unter Profiling im Gesundheitsbereich ist jede automatisierte Verarbeitung personenbezogener Daten zu verstehen, die bestimmte persönliche Aspekte einer natürlichen Person bewertet, um etwa deren Gesundheit zu analysieren und vorherzusagen (Artikel 4 Nr. 4 DSGVO). Damit sind insbesondere drei Aspekte entscheidend:

- Es muss eine automatisierte Form der Datenverarbeitung stattfinden.
- Es müssen personenbezogene Daten (z. B. Gesundheitsdaten) bei der Verarbeitung verwendet werden.
- Das Ziel muss die Vorhersage von Interessen und Verhaltensweisen bzw. die Bewertung persönlicher Aspekte einer natürlichen Person sein.

Im Allgemeinen geht es also darum, Informationen über Personen automatisch zu sammeln und auszuwerten, um sie einer bestimmten Kategorie zuzuordnen. Hierbei können Algorithmen (d. h. eine Zusammenstellung von Regeln zur Lösung eines Problems) eingesetzt werden. Profiling setzt im Vergleich zu einer automatisierten Entscheidungsfindung nicht zwingend voraus, dass am Ende des Vorgangs eine Entscheidung getroffen wird. Automatisierte Entscheidungen können auf Grundlage von Profiling getroffen werden, müssen es aber nicht.

**Beispiel:** Automatisches Verfahren zur (Vor-)Auswahl von geeigneten Organempfängern aufgrund von Kompatibilität, Dringlichkeit etc.; automatische Einordnung von Versicherten in bestimmte Kategorien aufgrund von Informationen über ihren Lebensstil (Bewegung, Ernährung etc.).

#### 2. Automatisierte Entscheidungen ohne menschliches Eingreifen

Für automatisierte Entscheidungen gelten besondere datenschutzrechtliche Anforderungen, wenn es um rein automatisierte Entscheidungen geht, also um Entscheidungen auf Grundlage einer Verarbeitung von personenbezogenen Daten, bei denen keine Überprüfung durch einen Menschen stattfindet (Artikel 22 DSGVO).

Umgekehrt bedeutet das: Entscheidet ein Mensch auf der Grundlage eines durch einen Computer entwickelten Entscheidungsvorschlags, stellt dies noch keine „automatisierte“ Entscheidung im Sinne der DSGVO dar. Die durch den Menschen getroffene Entscheidung muss inhaltlicher Art sein, darf sich also nicht nur auf die Überprüfung der technischen Abläufe o. ä. beziehen. Der menschliche Entscheider muss das Wissen und die Befugnis haben, den automatisiert entwickelten Entscheidungsvorschlag nicht bzw. abgeändert umzusetzen. Verbleiben entsprechende Spielräume für menschliche Entscheidungen, finden die restriktiven Vorgaben in Artikel 22 DSGVO auf die automatisierte Entscheidungsvorbereitung keine Anwendung.

**Beispiel:** Eine Diagnoseempfehlung, die automatisch aufgrund der Symptome erstellt wird, beruht nicht ausschließlich auf der automatisierten Verarbeitung, wenn sie noch von dem behandelnden Arzt überprüft wird. Anders sähe es aus, wenn die Diagnoseempfehlung von einer Sprechstundenhilfe an den Patienten lediglich übergeben würde.

### 3. Kombination von Profiling und automatisierter Entscheidung

Häufig werden Profiling und automatisierte Entscheidungen kombiniert. Zunächst wird ein (automatisiertes) Profiling durchgeführt. Auf Grundlage der hierdurch gewonnenen Erkenntnisse wird dann eine automatisierte Entscheidung getroffen. Sofern diese automatisierte Entscheidung ohne menschliche Einwirkung erfolgt und nachteilige Auswirkungen für den Betroffenen haben kann, gelten strenge datenschutzrechtliche Regeln (Artikel 22 DSGVO).

## II. Was ist zu tun?

Zunächst sind die allgemeinen datenschutzrechtlichen Anforderungen zu beachten, die bei jeder Verwendung von Profiling und automatisierter Entscheidung gelten. Zusätzliche Anforderungen gelten für automatisierte Entscheidungen, die ohne menschliches Eingreifen ergehen.

### 1. Allgemeine Anforderungen

Allgemein sind bei der Verwendung von Profiling und automatisierten Entscheidungen entsprechende Anpassungen der Rechtfertigungsgründe und der Betroffenenrechte vorzunehmen.

#### 1.1 Rechtmäßigkeit der Datenverarbeitung

Die Rechtfertigungsgründe für die Datenverarbeitung (vgl. Ziff. A.I) müssen auch das Profiling und die automatisierte Entscheidungsfindung als Form der Datenverarbeitung umfassen.

**Beispiel:** Ein Arzt bietet eine App an, mit deren Hilfe Nutzer einsehen können, wie viele Kalorien sie täglich einnehmen. Die Datenverarbeitung basiert auf einer ausdrücklichen Einwilligung der Nutzer. Soll die App eine Profiling-Funktion enthalten, die automatisch die individuelle Kalorieneinnahme über einen längeren Zeitraum auswertet und mit bestimmten Durchschnittswerten vergleicht, muss die Einwilligung des Nutzers dieses Profiling mitumfassen.

#### 1.2 Betroffenenrechte

Das Profiling und automatisierte Entscheidungen müssen bei den Rechten der Betroffenen berücksichtigt werden:

##### 1.2.1 Information, Widerspruchsrecht

Findet eine automatisierte Entscheidungsfindung statt, so muss die erforderliche Information des Betroffenen (Ziff. A.III.2) hierüber aufklären. Dazu gehören aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Artikel 13 Abs. 2 lit. f DSGVO; Artikel 14 Abs. 2 lit. g DSGVO). Der Betroffene muss nachvollziehen können, wie das Auswertungsverfahren im Grundsatz funktioniert (z. B. ob die von ihm erhobenen Daten mit bestimmten Musterprofilen abgeglichen werden). Geschäftsgeheimnisse – etwa der eingesetzte Algorithmus – müssen aber nicht offengelegt werden.

Zudem kann eine besondere Information bzgl. Widerspruchsrechten erforderlich sein, wenn ein Fall des Artikel 21 DSGVO vorliegt (siehe Ziff. A.III.9). Zu beachten ist allerdings, dass nicht jedes Profiling zu einem Widerspruchsrecht führt, sondern nur die in Artikel 21 DSGVO genannten Fälle des Profilings. Ein Widerspruchsrecht besteht daher beispielsweise, wenn Profiling auf Grundlage einer Interessensabwägung durchgeführt wird, zum Zwecke der Direktwerbung erfolgt oder zu Zwecken der Statistik bzw. Forschung eingesetzt wird.

##### 1.2.2 Auskunft

Der Betroffene kann im Rahmen seines Auskunftsrechts (vgl. Ziff. A.III.3) Informationen zu den ihn betreffenden Datenverarbeitungen anfordern. Dabei kann er insbesondere Informationen über das Bestehen einer automatisierten Entscheidungsfindung verlangen. Hierzu gehören auch aussagekräftige Informationen über die involvierte Logik

sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Artikel 15 Abs. 1 lit. h DSGVO).

#### 1.2.3 Berichtigung/Löschung

Der Betroffene kann in bestimmten Fällen die Berichtigung und die Löschung der Daten (vgl. Ziff. A.III.6) verlangen (Artikel 16 DSGVO und Artikel 17 DSGVO). Das gilt sowohl für die eingegebenen Daten (Input) als auch für die daraus resultierende Einordnung oder Entscheidung (Output).

**Beispiel:** Aufgrund eines Computerprogramms wird ein Betroffener in die Gruppe eingeordnet, die die höchste Wahrscheinlichkeit für eine Herzerkrankung aufweist. Dieses „Profil" ist nicht falsch, selbst wenn der Betroffene nicht am Herzen erkrankt ist. Es wird nur ausgesagt, dass eine erhöhte Wahrscheinlichkeit für die Erkrankung besteht. Der Betroffene kann zur Vervollständigung ergänzende Erklärungen abgeben, z. B. zusätzliche Daten zur Verfügung stellen oder falsch erhobene Daten berichtigen lassen.

### 2. Automatisierte Entscheidungen ohne menschliche Einwirkung

Für automatisierte Entscheidungen ohne menschliche Einwirkung gelten besondere, zusätzliche Anforderungen.

Sofern automatisierte Entscheidungen gegenüber den Betroffenen rechtliche Wirkungen entfalten oder sie in ähnlicher Weise beeinträchtigen, ist die Verwendung automatisierter Entscheidungen nur unter bestimmten Voraussetzungen erlaubt. Allgemein ist von einer erheblichen Beeinträchtigung auszugehen, wenn der Betroffene durch die Entscheidung in seiner wirtschaftlichen oder persönlichen Entfaltung nachhaltig gestört wird.

**Beispiel:** Aufgrund seines mit Hilfe einer App erfassten Verhaltens im Alltag (Bewegung, Ernährung etc.) wird die Prämie für die private Krankenversicherung eines Betroffenen automatisch erhöht.

Eine automatisierte Entscheidungsfindung ohne menschliche Einwirkungen ist bei der Verarbeitung von Gesundheitsdaten nur zulässig, wenn folgende Voraussetzungen kumulativ erfüllt sind:

- Die zugrundeliegende Datenverarbeitung muss aufgrund einer Einwilligung des Betroffenen (Artikel 9 Abs. 2 lit. a DSGVO) oder auf Grundlage eines erheblichen öffentlichen Interesses (Artikel 9 Abs. 2 lit. g DSGVO) erfolgen (Artikel 22 Abs. 4 DSGVO).

- Die automatisierte Entscheidung muss (a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich sein, (b) aufgrund besonderer Rechtsvorschriften zulässig sein oder (c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgen (Artikel 22 Abs. 2 DSGVO).

- Es müssen angemessene Maßnahmen ergriffen werden, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren.

#### 2.1 Anforderungen an die zugrundeliegende Datenverarbeitung

Bei Gesundheitsdaten ist eine automatisierte Entscheidung nicht bei allen Formen der Datenverarbeitung zulässig.

Vielmehr darf eine automatisierte Entscheidung nur auf Grundlage einer Datenverarbeitung erfolgen, die entweder

- durch eine ausdrückliche Einwilligung des Betroffenen (Artikel 9 Abs. 2 lit. a DSGVO, vgl. hierzu Ziff. A.I.3.1) gedeckt ist, oder

- auf einem Spezialgesetz zur Wahrung eines erheblichen öffentlichen Interesses (Artikel 9 Abs. 2 lit. g DSGVO) beruht. Ein solches Spezialgesetz ist z. B. § 37 Abs. 2 BDSG, der den Versicherungsunternehmen eine automatisierte Entscheidung auch auf Grundlage einer Verarbeitung von Gesundheitsdaten erlaubt.

Kann die Datenvereinbarung hingegen (nur) auf Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin (Artikel 9 Abs. 2 lit. h DSGVO) bzw. auf Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Artikel 9 Abs. 2 lit. i) gestützt werden, rechtfertigt dies noch keine automatisierte Entscheidungsfindung. Vielmehr muss der Verantwortliche in einer solchen Konstellation sicherstellen, dass zusätzlich die Voraussetzungen nach einer der beiden genannten Ausnahmeregelungen erfüllt sind, z. B. durch die (zusätzliche) Einholung einer Einwilligung des Betroffenen.

## 2.2 Anforderungen an die Entscheidung

Eine automatisierte Entscheidung ist datenschutzrechtlich nur zulässig, wenn eine der nachfolgenden Voraussetzungen vorliegt (Artikel 22 Abs. 2 DSGVO). Die Entscheidung muss

- für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich sein,
- aufgrund besonderer Rechtsvorschriften zulässig sein oder
- mit ausdrücklicher Einwilligung der betroffenen Person erfolgen.

### 2.2.1 Erforderlich für Abschluss oder Erfüllung eines Vertrags

Eine automatisierte Entscheidungsfindung ist zulässig, wenn sie für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Es soll damit den praktischen Anforderungen von Massengeschäften Rechnung getragen werden. Die automatisierte Entscheidung muss dabei nicht Vertragsgegenstand sein. Es sind auch Fälle erfasst, bei denen eine Bearbeitung durch einen Menschen aufgrund der Datenmengen (nahezu) unmöglich ist.

**Beispiel:** Die Arbeit als Astronaut erfordert verschiedene körperliche und gesundheitliche Voraussetzungen. Gleichwohl gehen bei einer Ausschreibung zehntausende Bewerbungen ein. Damit die geeigneten Bewerbungen herausgefiltert werden können, wird eine automatisierte Entscheidungsfindung eingesetzt.

### 2.2.2 Zulässigkeit aufgrund besonderer Rechtsvorschriften

Die automatisierte Entscheidungsfindung ist zudem zulässig, wenn sie aufgrund von anwendbaren Rechtsvorschriften im Recht der EU oder der Mitgliedstaaten zulässig ist.

Deutschland hat mit der Regelung in § 37 BDSG für Gesundheitsdaten eine solche Sondernorm § 37 BDSG erlassen. § 37 BDSG ermöglicht zu Gunsten der Versicherungswirtschaft die automatisierte Abrechnung von Versicherungsleistungen der privaten Krankenversicherung. Automatisierte Entscheidungen auf Grundlage der Verarbeitung von Gesundheitsdaten sind bei der Leistungserbringung nach Versicherungsvertrag möglich, wenn

- einem Begehren des Betroffenen stattgegeben wird (§ 37 Abs. 1 Nr. 1 BDSG) oder
- die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht (§ 37 Abs. 1 Nr. 2 BDSG).

Es müssen zudem angemessene Maßnahmen zur Wahrung der Betroffeneninteressen getroffen werden. Diese Voraussetzung entspricht der Voraussetzung in Artikel 22 Abs. 3 DSGVO (vgl. Ziff. 2.3).

### 2.2.3 Einwilligung

Die automatisierte Entscheidungsfindung ist zudem zulässig, wenn sie aufgrund einer ausdrücklichen Einwilligung erfolgt. Es sind bei der Einwilligung zur automatisierten Entscheidungsfindung die gleichen Anforderungen zu stellen wie bei der Einwilligung in die allgemeine Datenverarbeitung (vgl. auch Ziff. A.I.3.1). Die Einwilligung muss insbesondere ausdrücklich und freiwillig erfolgen und der Betroffene muss über Umstände und Folgen seiner Einwilligung hinreichend informiert werden.

## 2.3 Umsetzung von angemessenen Sicherheitsmaßnahmen

Setzt der Verantwortliche Verfahren zur automatisierten Entscheidungsfindung ein, muss er angemessene Sicherheitsmaßnahmen zur Wahrung der Rechte, Freiheiten und Interessen des Betroffenen vorsehen (Artikel 22 Abs. 3 DSGVO und § 37b Abs. 1 Nr. 2 und Abs. 2 Satz 2 BDSG).

### 2.3.1 Mindestmaßnahmen

Zur angemessenen Wahrung der Interessen der Betroffenen muss der Verantwortliche zumindest die folgenden Maßnahmen treffen:

a) Recht auf Kontrolle durch Mensch
Der Verantwortliche muss sicherstellen, dass eine automatisiert getroffene Entscheidung auf entsprechende Nachfragen des Betroffenen noch einmal von einem Menschen kontrolliert wird. Der zuständige Mitarbeiter muss in der Lage sein, die Entscheidung inhaltlich zu kontrollieren und ggf. abzuändern. In der Praxis müssen also ausreichend qualifizierte Mitarbeiter vorhanden und mit entsprechenden Entscheidungsbefugnissen ausgestattet sein.

b) Recht auf Anhörung

Der Verantwortliche muss sicherstellen, dass der Betroffene seinen eigenen Standpunkt darlegen kann (etwa um besondere Umstände darlegen zu können, die seine Situation von vergleichbaren Konstellationen unterscheiden). Der Standpunkt des Betroffenen muss auch entsprechend zur Kenntnis genommen werden. In der Praxis kann das Anhörungsrecht im Rahmen eines Anmeldeprozesses etwa durch ein entsprechendes Kommentarfeld geschaffen werden, über das der Nutzer seinen Standpunkt erläutern kann. Ausreichend ist aber auch ein entsprechender Hinweis, verbunden mit der Angabe einer postalischen oder elektronischen Adresse, an die sich der Betroffene wenden kann.

c) Recht auf Überprüfung

Der Betroffene muss die Entscheidung „anfechten" können. Dies bedeutet, dass der Verantwortliche eine automatisiert getroffene Entscheidung einer nochmaligen inhaltlichen Bewertung unterziehen muss, sofern der Betroffene dies verlangt. Diese ist durch einen Menschen durchzuführen. Das Recht auf Überprüfung überschneidet sich daher mit dem Recht auf Kontrolle durch einen Menschen.

### 2.3.2 Zusätzliche Maßnahmen

Neben diesen spezifisch geregelten Anforderungen muss auch allgemein sichergestellt sein, dass die automatisierte Entscheidung fair und transparent erfolgt. Daraus lassen sich insbesondere folgende Anforderungen ableiten:

- Es muss ein geeignetes mathematisches oder statistisches Verfahren verwendet werden (EG 71 DSGVO).
- Es sollen technische und organisatorische Maßnahmen vorgesehen sein, mit denen Korrekturen von unrichtigen Daten ermöglicht und das Risiko von Fehlern minimiert werden (EG 71 DSGVO).
- Es ist sicherzustellen, dass die automatisierte Entscheidungsfindung keine diskriminierende Wirkung hat (EG 71 DSGVO).
- Kinder sollen von automatisierten Entscheidungen nicht betroffen sein (EG 71 DSVO).

## III. Best Practice

### 1. Information

Es sollte sichergestellt werden, dass der Betroffene hinreichend Informationen über die Logik erhält, die hinter dem Profiling bzw. der automatisierten Entscheidungsfindung steht. Dabei sollte die Information klar und verständlich sein. Beispielsweise ist es sinnvoll, die Kategorien der Daten zu benennen, die für das Profiling bzw. die automatisierte Entscheidungsfindung verwendet werden. Es sollte erklärt werden, wie Profile erstellt werden, insbesondere, welche Statistiken für die Profilerstellung eingesetzt werden und ggf. warum das Profiling für die automatische Entscheidung relevant ist. Dabei kann eine visuelle Darstellung dieser Informationen für den Betroffenen hilfreich sein.

### 2. Angemessene Sicherheitsmaßnahmen

Bei dem Einsatz automatischer Entscheidungen sind angemessene Sicherheitsmaßnahmen zu wählen. Beispielsweise ist zu empfehlen,

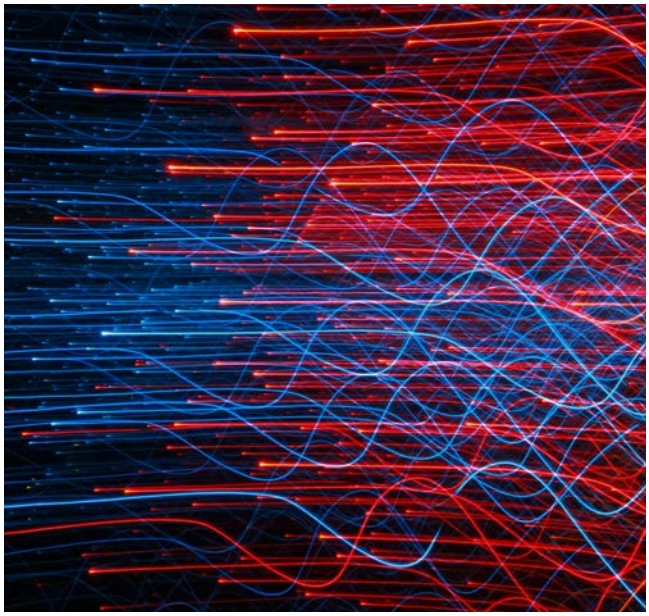
- regelmäßig Qualitätsprüfungen durchzuführen, um sicherzustellen, dass die Betroffenen fair behandelt und nicht diskriminiert werden;
- Algorithmen, die durch sogenannte selbstlernende Systeme entwickelt wurden, dahingehend zu überprüfen, dass sie die beabsichtigte Aufgabe erfüllen und keine fehlerhaften oder diskriminierenden Entscheidungen produzieren;
- externen Prüfern die nötigen Informationen zu verschaffen, damit diese verstehen, wie ein ggf. eingesetzter Algorithmus oder selbstlernendes System funktioniert;
- von Dritten vertragliche Zusicherungen über die Konformität mit geltendem Recht einzuholen, wenn deren Algorithmen verwendet werden;
- Anonymisierungs- oder Pseudonymisierungs-Techniken einzusetzen.

### IV. Wichtige Rechtsvorschriften

- **Artikel 4 Ziff. 4 DSGVO** (Definition Profiling)
- **Artikel 8 DSGVO/EG 38** (besonderer Schutz von Kindern bei Profiling)
- **Artikel 13/14 DSGVO/EG 60** (Informationspflicht bei Profiling), **Artikel 15 DSGVO/EG 63** (Auskunftspflicht bei Profiling), **Artikel 21 DSGVO** (Widerspruchsrecht bei Profiling)
- **Artikel 35 DSGVO/EG 91** (Berücksichtigung von Profiling bei der DSFA)
- **Artikel 13 Abs. 2 lit. f/14 Abs. 2 lit. g DSGVO/EG 61** (Informationspflicht bei automatisierten Entscheidungen)
- **Artikel 15 Abs. 1 lit. h DSGVO/EG 63** (Auskunftspflicht bei automatisierten Entscheidungen)
- **Artikel 22 DSGVO** (Automatisierte Entscheidungen im Einzelfall einschließlich Profiling)
- **Artikel 35 Abs. 3 lit. a DSGVO/EG 91** (Berücksichtigung von Profiling bei der DSFA)
- **§ 37 BDSG** (Automatisierte Entscheidungen im Einzelfall)

### V. Weiterführende Links

- **Artikel-29-Gruppe**, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Februar 2018 (engl.): http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
- **EU-Kommission**, Könnte ich von einer automatisierten Entscheidungsfindung im Einzelfall, einschließlich Profiling, betroffen sein?: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_de
- **ICO**, What is automated individual decision-making and profiling? (engl.): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling



## F. Anwendung Big Data und Anonymisierung

Anbieter von digitalen Produkten sind häufig daran interessiert, die im Rahmen der Nutzung des Produkts erhobenen Daten – ggf. unter Anwendung von Profiling und automatisierten Entscheidungen (vgl. oben Abschnitt E.) – mittels Big-Data-Techniken zu analysieren. Aus Sicht des europäischen Gesetzgebers eröffnet der Big-Data-Ansatz große Chancen – etwa um neue Erkenntnisse in Bezug auf weit verbreitete Krankheiten wie Herz-Kreislauf-Erkrankungen, Krebs und Depression zu generieren (vgl. EG 157 der DSGVO).

Gleichzeitig müssen bei der Anwendung von Big-Data-Techniken die datenschutzrechtlichen Anforderungen eingehalten werden.

### I. Big Data ohne Anonymisierung

#### 1. Worum geht es?

Unter Big Data ist eine Form der Datenanalyse zu verstehen, die es erlaubt, mit einer hohen Verarbeitungsgeschwindigkeit aus großen und unstrukturierten Datenmengen Gesetzmäßigkeiten, Korrelationen und Kausalitäten zu erkennen und daraus neue Informationen zu generieren. Die Daten können dabei aus vielfältigen Quellen, wie Texten, Sensor- und Audiodaten, stammen.

## 2. Was ist zu tun?

Bei der Datenanalyse mittels Big Data muss die damit verbundene Datenverarbeitung entsprechend der allgemeinen Regeln gerechtfertigt sein (vgl. Ziff. A.I) und die Betroffenenrechte (vgl. Ziff. A.III) müssen gewahrt werden. Da bei der Datenanalyse mittels Big Data bereits begrifflich eine Vielzahl von Daten analysiert wird, stellen sich allerdings besondere Herausforderungen bei der Einhaltung der datenschutzrechtlichen Vorgaben. Zusätzlich sind ggf. die Voraussetzungen für Profiling und automatisierte Entscheidungen zu berücksichtigen (vgl. Abschnitt E.).

### 2.1 Ausnahme und Rechtsgrundlage

Für die Verarbeitung von personenbezogenen Gesundheitsdaten ist im Rahmen von Big-Data-Anwendungen in einer zweistufigen Prüfung sicherzustellen, dass (1) ein Ausnahmetatbestand für die Verarbeitung von Gesundheitsdaten und (2) eine Rechtsgrundlage für die allgemeine Datenverarbeitung vorliegen (vgl. Ziff. A.I). Für typischerweise zulässige Verarbeitungen von Gesundheitsdaten (vgl. Ziff. A.I.3) sind bei Big-Data-Analysen Besonderheiten zu berücksichtigen.

#### 2.1.1 Einwilligung, Broad Consent

Gesundheitsdaten können auf Grundlage einer ausdrücklichen Einwilligung im Rahmen von Big-Data-Analysen verarbeitet werden. Die Einwilligung muss u. a. zweckgebunden und informiert erfolgen (vgl. Ziff. A.I.3.1).

Eine Information über den konkreten Zweck der Verarbeitung setzt allerdings voraus, dass dieser bereits zum Zeitpunkt der Erhebung der Daten bekannt ist. Gerade im Rahmen von Forschungsprojekten kann aber zunächst unklar sein, wie und mit welchem konkreten Ziel die Daten im Rahmen der Forschung genutzt werden sollen.

In derartigen Konstellationen stellt sich die Frage, wie der Einwilligende dennoch ausreichend informiert werden kann. Dabei kann die Figur des sogenannten „Broad Consent“ für Forschungsprojekte eine wichtige Erleichterung bieten. Erwägungsgrund 33 der DSGVO führt hierzu aus: Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.

#### 2.1.2 Offensichtlich öffentlich gemachte Gesundheitsdaten

Die Auswertung von Gesundheitsdaten im Rahmen von Big-Data-Analysen ist auf erster Prüfungsstufe zulässig, wenn die betroffene Person die zugrundeliegenden Gesundheitsdaten offensichtlich öffentlich gemacht hat. Eine Verarbeitung kann dann auch ohne ausdrückliche Einwilligung oder Kontakt zu dieser Person erlaubt sein (vgl. Ziff. A.I.3.2).

Auf zweiter Prüfungsstufe können Big-Data-Analysen in einer solchen Konstellation häufig auf eine Interessensabwägung nach Artikel 6 Abs. 1 lit. f DSGVO gestützt werden. Für die Zulässigkeit der Verarbeitung spricht dabei, dass in solchen Fällen nicht von einer erhöhten Schutzbedürftigkeit des Betroffenen ausgegangen werden kann. Andererseits können Rechte und Interessen der Betroffenen überwiegen, wenn aufgrund der Vielzahl der in die Analyse einfließenden Informationen umfangreiche Einblicke in die Persönlichkeitsstruktur gewonnen werden.

#### 2.1.3 Forschungszwecke oder statistische Zwecke

Die DSGVO verfolgt einen forschungsfreundlichen Ansatz. Eine Verarbeitung von Gesundheitsdaten im Rahmen von forschungsorientierter Big-Data-Analyse ist auch ohne Einwilligung der Betroffenen erlaubt, wenn die nachfolgenden Voraussetzungen kumulativ erfüllt sind:

- Die Datenverarbeitung dient wissenschaftlichen Forschungszwecken oder statistischen Zwecken,
- die Datenverarbeitung ist zur Erreichung dieser Zwecke erforderlich,
- ein entsprechendes Spezialgesetz ist einschlägig (z. B. § 27 BDSG),
- es sind geeignete Garantien zum Schutz der Betroffenen implementiert, und
- es besteht eine Rechtsgrundlage für die Datenverarbeitung.

a) Forschungszwecke oder statistische Zwecke
Im ersten Schritt müssen Unternehmen überprüfen, ob die angestrebte Verarbeitung von Gesundheitsdaten unter den Begriff „wissenschaftliche Forschungszwecke“ oder „statistische Zwecke“ fällt.

*aa) Wissenschaftliche Forschung*
Der Begriff „wissenschaftliche Forschungszwecke“ ist weit zu verstehen. Es sind auch die angewandte und privat finanzierte Forschung sowie Auftragsforschung in und für die Industrie erfasst.[25] Erforderlich ist nur, dass mit der Verarbeitung ein ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit angestrebt wird.

*bb) Statistik*
Mit „statistischen Zwecken“ ist jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Verarbeitung von (Gesundheits-)Daten gemeint. Dabei sind drei wichtige Punkte zu beachten:

- Die Ergebnisse der Verarbeitung zu statistischen Zwecken dürfen keine personenbezogenen Daten mehr enthalten, sondern müssen aggregierte Daten sein. Erst mit der Trennung der personenbezogenen Merkmale und deren Löschung entfällt in der Regel der Personenbezug.

- Die Ergebnisse oder die ihnen zugrundeliegenden personenbezogenen Daten dürfen nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden. Sobald es darum geht, Aussagen über identifizierbare Personen zu erhalten, handelt es sich nicht mehr um statistische Zwecke.

- Werden dagegen abstrakte, also von einzelnen Personen unabhängige Erkenntnisse gewonnen, können die Ergebnisse für verschiedene Zwecke, so auch für wissenschaftliche Forschungszwecke verwendet werden.

b) Erforderlichkeit
Die Verarbeitung muss für die wissenschaftlichen Forschungszwecke oder statistischen Zwecke erforderlich sein. Dies ist der Fall, wenn es kein milderes (d. h. in die Rechte des Betroffenen weniger eingreifendes) Mittel gibt, welches den gleichen Erfolg mit vergleichbarem Aufwand erreicht.

c) Spezialgesetz
Das Unternehmen muss sich schließlich auf ein Spezialgesetz berufen können, das die Verarbeitung von Gesundheitsdaten zu Forschungszwecken oder statistischen Zwecken erlaubt, und die jeweiligen Voraussetzungen einhalten.

*aa) § 27 BDSG*
Als Grundlage für die Verarbeitung der Gesundheitsdaten zu Forschungszwecken oder statistischen Zwecken können Unternehmen insbesondere § 27 BDSG heranziehen.

Eine Verarbeitung nach dieser Regelung setzt voraus, dass die Interessen des verantwortlichen Unternehmens an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen.

**Beispiel:** Das Interesse an der wissenschaftlichen Forschung kann überwiegen, wenn ein Forschungsvorhaben erhebliche Verbesserungen für die Gesundheit oder die soziale Sicherheit der Bevölkerung mit sich bringt.

*bb) Bereichsspezifische Spezialgesetze*
Weitere nationale Spezialgesetze zur Forschung sind etwa in den Sozialgesetzbüchern (z. B. §§ 67b Abs. 3, 67c Abs. 2 Nr. 2, Abs. 5 und § 75 SGV X) oder im Transplantationsgesetz (z. B. § 14 Abs. 2a, § 15g Abs. 2 TPG) zu finden.

d) Maßnahmen zum Schutz der Betroffenen
Ein besonderes Augenmerk müssen Unternehmen darauf legen, geeignete Garantien für die Rechte und Freiheiten der betroffenen Person zu implementieren (Artikel 89 Abs. 1 DSGVO). Es müssen hierzu insbesondere geeignete technische und organisatorische Maßnahmen getroffen werden, die gewährleisten, dass die Datenverarbeitung dem Zweck angemessen ist und auf das notwendige Maß beschränkt wird (Datenminimierung). Sofern möglich, sind Daten daher zu pseudonymisieren. Der Personenbezug der Daten ist so früh wie möglich zu entfernen.

Hinzu kommen die im jeweiligen Spezialgesetz vorgeschriebenen Vorkehrungen zum Schutz der Betroffenen. So bestehen etwa in § 27 BDSG Vorgaben, wie die Datenverarbeitung organisiert werden muss, ob bzw. wann die Gesundheitsdaten zu anonymisieren sind und wie die Daten gespeichert werden müssen. Außerdem ist im Falle von § 27 BDSG der Maßnahmenkatalog des § 22 Abs. 2 S. 2 BDSG einzuhalten,

der beispielhaft zehn mögliche Maßnahmen zum Schutz der Betroffenen auflistet, unter anderem die Zugangsbeschränkung und Verschlüsselung der Daten.

e) Rechtsgrundlage
Sind die zuvor genannten Voraussetzungen erfüllt, besteht in aller Regel auch eine Rechtsgrundlage für die geplante Verarbeitung, insbesondere in Gestalt der Interessensabwägung (Artikel 6 Abs. 1 lit. f DSGVO).

**Beispiel:** Das Spezialgesetz nach § 27 BDSG setzt bereits voraus, dass die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person erheblich überwiegen müssen. Ist das der Fall, dürften auch die Voraussetzungen der Rechtsgrundlage der Interessensabwägung (Artikel 6 Abs. 1 lit. f DSGVO) erfüllt sein.

f) Wichtige Rechtsvorschriften
- **Artikel 9 Abs. 2 lit. j DSGVO** und **§ 27 BDSG** (Ausnahmetatbestand bei wissenschaftlichen Forschungszwecken und statistischen Zwecken)
- **Artikel 89 DSGVO** (Geeignete Garantien)
- **Artikel 6 Abs. 1 lit. f DSGVO** (typische Rechtsgrundlage bei Forschung/Statistik)

### 2.2 Betroffenenrechte

Im Zusammenhang mit Big-Data-Analysen müssen die Verantwortlichen den Rechten der Betroffenen Beachtung schenken (vgl. Ziff. A.III). Angesichts der typischerweise zu analysierenden Datenmengen stellt dies eine besondere Herausforderung dar. Sofern die Big-Data-Analyse der wissenschaftlichen Forschung oder statistischen Zwecken dient, können zwar Ausnahmen von den Betroffenenrechten gegeben sein (vgl. Artikel 89 Abs. 2 und 3 DSGVO, § 27 Abs. 2 BDSG); eine spezifische Ausnahme für wissenschaftliche Forschung oder statistische Zwecke kommt für die Informationsrechte und Löschungspflichten jedoch nicht in Betracht.

Insbesondere ist daher bei Big-Data-Analysen Folgendes zu beachten:

#### 2.2.1 Informationsrechte

Die betroffene Person ist grundsätzlich umfassend zu informieren (vgl. Ziff. A.III.2), etwa über die Zwecke und die Rechtsgrundlage der Verarbeitung.

Auf die Information kann nur ausnahmsweise verzichtet werden, wenn Daten nicht bei der betroffenen Person erhoben wurden und die Erteilung einer Information einen unverhältnismäßigen Aufwand erfordern würde (Artikel 14 Abs. 5 lit. b DSGVO). Dies kann etwa im Falle von Auswertungen öffentlich zugänglicher Daten der Fall sein. Werden etwa Daten verarbeitet, welche betroffene Personen über Twitter selbst öffentlich gemacht haben, kann eine Information des Betroffenen regelmäßig unterbleiben, da die Datenerhebung ohne Beteiligung des Betroffenen erfolgt und mit einem unverhältnismäßigen Aufwand für den Verantwortlichen verbunden wäre.

#### 2.2.2 Löschungspflicht

Es besteht grundsätzlich die Pflicht, personenbezogene Daten unverzüglich zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (vgl. Ziff. A.III.6). Etwas anderes gilt, wenn die Daten für weitere Zwecke auf Grundlage der DSGVO oder des BDSG weiterverarbeitet werden dürfen.

### 2.3 Datenschutz-Folgenabschätzung

Big-Data-Analysen im Gesundheitsbereich erfordern in der Regel eine Datenschutz-Folgenabschätzung (vgl. Ziff. A.VI), da typischerweise eine umfangreiche Verarbeitung von Gesundheitsdaten erfolgt. Eine Checkliste für eine Big-Data-Datenschutz-Folgenabschätzung ist in englischer Sprache hier erhältlich (S. 99 ff.) (bzw. unter den weiterführenden Links).

## II. Anonymisierung

### 1. Worum geht es?

Anonymisierte Gesundheitsdaten fallen nicht in den Anwendungsbereich des Datenschutzrechts und können daher auch ohne Einhaltung der datenschutzrechtlichen Vorgaben im Rahmen von Big-Data-Analysen ausgewertet werden.

### 2. Was ist zu tun?

Die Anonymisierung stellt eine Verarbeitung personenbezogener Daten dar, für die ein Rechtfertigungsgrund vorliegen muss. An den eigentlichen Prozess der Anonymisierung von Gesundheitsdaten werden zudem hohe Anforderungen gestellt.

#### 2.1 Ausnahmetatbestand und Rechtsgrundlage

Die Anonymisierung stellt eine Datenverarbeitung dar, für die bei Gesundheitsdaten eine Ausnahme vom Verbot der Datenverarbeitung sowie eine Rechtsgrundlage erforderlich ist (vgl. Ziff. A.I).

Als Ausnahmetatbestände kommen insbesondere eine Einwilligung sowie die Verarbeitung zugunsten von wissenschaftlicher Forschung oder statistischen Zwecken (§ 27 BDSG) in Betracht. Zu beachten ist, dass durch die Anonymisierung gerade der Personenbezug der Daten entfernt wird. Es ist somit im Regelfall – sofern keine Aufbewahrungspflichten bestehen – kein gewichtiges Interesse erkennbar, das gegen eine Anonymisierung spricht.

#### 2.2 Anonymisierung

Die datenschutzrechtlichen Vorgaben gelten nicht für solche Gesundheitsdaten, die in einer Weise so modifiziert worden sind, dass kein Personenbezug mehr besteht, die betroffene Person also nicht oder nicht mehr identifiziert werden kann. Ist der Personenbezug aufgehoben, spricht man von anonymisierten Daten.

##### 2.2.1 Hohe Anforderungen an Anonymisierung von Gesundheitsdaten

Um festzustellen, ob eine natürliche Person (noch) identifizierbar ist, sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.

Die Anonymisierung von ursprünglich personenbezogenen (Gesundheits-)Daten erfordert daher, dass eine Identifizierung des Betroffenen praktisch nicht mehr durchführbar ist, weil sie z. B. einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde.

Ist eine Identifizierung hingegen mit vertretbarem Aufwand möglich, handelt es sich nicht um anonymisierte Daten. Dies kann etwa auch dann der Fall sein, wenn und solange eine Identifizierung mit Hilfe von Informationen erfolgen kann, die bei Dritten eingeholt werden können. Auch die zum Zeitpunkt der Verarbeitung verfügbaren Technologien sind zu berücksichtigen.

Die Aufhebung des Personenbezugs ist bei Gesundheitsdaten besonders schwierig, da Gesundheitsdaten häufig sehr individuell sind und der Betroffene daher häufig anhand weniger Zusatzinformationen identifiziert werden kann.

**Beispiel:** Die bloße Entfernung von Namen und Adresse reicht für eine Anonymisierung grundsätzlich nicht. Durch die verbleibenden Informationen lässt sich häufig der Personenbezug wiederherstellen. Das gilt insbesondere, wenn es sich um sehr spezielle Informationen handelt, z. B. Kauf eines Medikaments für eine seltene Krankheit und eine hiermit in Verbindung stehende Postleitzahl des Wohnorts.

Welche Maßnahmen für eine erfolgreiche Anonymisierung erforderlich sind, kann nur im jeweiligen Einzelfall bestimmt werden. Die bloße Entfernung des Namens und der Adresse der Person ist in aller Regel nicht ausreichend. Vielmehr sind besondere Anonymisierungstechniken zu verwenden und ggf. miteinander zu kombinieren.

##### 2.2.2 Anonymisierungstechniken

Zur Anonymisierung können unterschiedliche Techniken angewandt und ggf. miteinander kombiniert werden. Gesetzliche Vorgaben für die zu verwendenden Techniken bestehen nicht. Die hier genannten Techniken dienen als Beispiele und stellen keinen abschließenden Katalog dar.

a) Randomisierung

Bei Randomisierungstechniken werden die Daten teilweise verändert, um den Bezug zu einer konkreten Person zu beseitigen. Die Daten sind dann zwar immer noch singulär, d. h. jeder Datensatz kann immer noch einem Datensubjekt zugeordnet werden. Es ist aber schwieriger, den Datensatz einer bestimmten Person zuzuordnen.

Möglichkeiten der Randomisierung sind z. B.:

- **Veränderung einzelner Werte** für bestimmte Attribute, so dass sie weniger genau sind, sich aber an der Gesamtverteilung nichts ändert.

**Beispiel:** Die Körpergröße einer Person wurde auf den nächsten Zentimeter genau gemessen. Der anonymisierte Datensatz stellt die Körpergröße nur auf +/- 10 cm genau dar.

- **Vertauschung einzelner Werte** für bestimmte Attribute, so dass die Werte einem anderen Datensubjekt zugeordnet werden.

**Beispiel:** Die genau gemessenen Körpergrößen werden jeweils anderen Datensubjekten zugeordnet.

b) Verallgemeinerung

Bei Verallgemeinerungstechniken werden die Attribute der betroffenen Personen verallgemeinert, indem der jeweilige Maßstab oder die Größenordnung (z. B. eine Region anstatt einer Stadt, ein Monat anstatt einer Woche) geändert wird. Es können dann keine einzelnen Werte einer bestimmten Person zugeordnet werden, ggf. kann eine Person aber in eine bestimmte Gruppe eingeordnet werden.

Möglichkeiten der Verallgemeinerung sind z. B.:

- Zusammenfassung von mehreren Datensubjekten zu Gruppen in der Weise, dass die gemeinsamen Attribute ein Stück weit verallgemeinert werden.

**Beispiel:** Anstatt Personen mit demselben Geburtstag werden Personen mit demselben Geburtsjahr zusammengefasst.

- Sicherstellung einer ausreichenden Diversität der Werte für einzelne Attribute innerhalb der gebildeten Gruppen.

**Beispiel:** Es ist sicherzustellen, dass nicht Gruppen gebildet werden, bei denen alle in demselben Jahr geborenen Patienten dieselbe Diagnose erhalten haben. Denn in diesem Fall könnte man bereits allein anhand des Geburtsjahres auf die Diagnose schließen. Ggf. muss die Gruppe vergrößert werden.

Es ist sinnvoll, Datenklassen zu bilden und in jedem Einzelfall zu überprüfen, ob ein Rückschluss auf eine konkrete Person möglich ist. Ist eine Identifizierung weiterhin möglich, muss eine abstraktere Datenklasse gewählt werden. Keine Anonymisierung liegt vor, wenn der Verantwortliche mit weiteren (ggf. bei Dritten) verfügbaren Daten einen Personenbezug herstellen kann.

Bei der Übermittlung anonymisierter Daten an einen Empfänger muss zudem berücksichtigt werden, ob der Empfänger über Mittel verfügt, die Personenbeziehbarkeit wiederherzustellen.

### 3. Best Practice

Allgemeine Aussagen zu einer Best Practice bei der Anonymisierung von Datenbeständen lassen sich kaum treffen, da es auf die konkreten Umstände ankommt (z. B. um welche Daten geht es und welche Mittel stehen dem Verantwortlichen zur Verfügung).

Die Anonymisierung von Gesundheitsdaten kann sinnvoll sein, wenn die maßgeblichen Informationen effektiv genutzt werden können, ohne dass bekannt sein muss, auf wen sich diese Informationen beziehen. Gleichzeitig leidet bei jeder Anonymisierung die Qualität der Daten. Denn bestimmte Ursachenzusammenhänge werden entfernt oder unkenntlich gemacht, um die Identifikation zu verhindern.

Aus datenschutzrechtlicher Sicht können folgende Elemente zu einer Anonymisierung beitragen:

- Kombination unterschiedlicher Anonymisierungstechniken

- Entfernung seltener Attribute (z. B. seltene Krankheiten)
- Bei einer Verallgemeinerung sollte keine Beschränkung auf ein Generalisierungskriterium für das gleiche Attribut erfolgen. Vielmehr ist die Auswahl der Generalisierungskriterien von der Verteilung der jeweiligen Werte abhängig.

### 4. Wichtige Rechtsvorschriften/-erwägungsgründe

- **Erwägungsgrund 26 der DSGVO** (Anonymisierung)
- **Artikel 6 und 9 DSGVO** (Verarbeitungsgrundlagen)

### III. Weiterführende Links

- **ico**, Big Data, artificial intelligence, machine learning and data protection, September 2017: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
- **gmds/GDD**, Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU-DSGVO, 9.5, Mai 2017: https://www.gdd.de/arbeitskreise/datenschutz-und-datensicherheit-im-gesundheits-und-sozialwesen/materialien-und-links/datenschutzrechtliche-anforderungen-an-die-medizinische-forschung-unter-beru-cksichtigung-der-eu-datenschutz-grundverordnung
- **Europarat**, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, Januar 2017 (engl.): https://rm.coe.int/16806ebe7a
- **Universität Kiel**, Vorschlag einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland, September 2017: https://www.uni-kiel.de/medinfo/documents/TWMK%20Vorschlag%20DInfMedForsch%20v1.9%20170927.pdf
- **MPI für Bildungsforschung**, Datenschutzrechtliche Anforderungen der DSGVO an die Verwendung von Gesundheitsdaten in der Forschung, Juli 2017: https://www.eaid-berlin.de/wp-content/uploads/2017/07/Vortrag-EAID-17-07-06_Katrin_Schaar.pdf
- **Zum alten Recht vor Geltung der DSGVO**: Artikel-29-Gruppe, Opinion on Anonymisation Techniques, Mai 2014 (engl.): https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/WP216_Opinion52014AnonymisationTechniques.html

## G. Weiterführende Links zu themenübergreifenden Informationen

### I. Leitfäden/Allgemeine Informationen zur DSGVO

- **Handelskammer Hamburg**, Übersicht zur DSGVO, Mai 2018: https://www.hk24.de/produktmarken/beratung-service/recht_und_steuern/wirtschaftsrecht/medien_it_recht/datenschutzgrundverordnung/3740520
- **BfDI**, Überblick über die Regelungen der DSGVO, Juni 2018: https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1.html?nn=5217204
- **BayLDA**, Anforderungen der Datenschutz-Grundverordnung (DSGVO) an kleine Unternehmen und Vereine, inkl. Mustern (z. B. für Arztpraxis), https://www.lda.bayern.de/de/kleine-unternehmen.html
- **Artikel-29-Gruppe**, Leitlinien für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters, April 2017: https://datenschutz-hamburg.de/assets/pdf/wp244rev01_de.pdf
- **GDD**, Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung, Dezember 2016: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_2.pdf
- **ico**, Guide to the General Data Protection Regulation (GDPR), Juni 2018 (engl.): https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf
- **ico**, Key definitions of the GDPR (engl.): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions
- **GDD**, Zusammenschau der DSGVO und des BDSG, Mai 2017: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_6.pdf
- **Berliner Beauftragte für Datenschutz**, Infothek mit diversen Orientierungshilfen und Ratgebern: https://www.datenschutz-berlin.de/infothek-service.html

### II. FAQ

- **BayLDA**, FAQ: Gesammelte Antworten zur EU-Datenschutz-Grundverordnung (DSGVO): https://www.ihk-nuernberg.de/de/Geschaeftsbereiche/Innovation-Umwelt/IuK-E-Business/Datenschutz/eu-datenschutz-grundverordnung/fragen-an-das-baylda-zur-ausgestaltung-der-dsgvo-in-der-praxis/
- **Bitkom**, Was muss ich wissen zur EU-Datenschutz-Grundverordnung, September 2016: https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/161109-EU-DS-GVO-FAQ-03.pdf
- **Datenschutzbehörde Rheinland-Pfalz**, Fragen zur Datenschutz-Grundverordnung: https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordnung/faq

### III. Checklisten

- **BMWi**, DSGVO, Checkliste für die Umsetzung in Unternehmen, Februar 2018: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/datenschutzgrundverordnung.pdf?__blob=publicationFile&v=16

- **DSK**, Maßnahmenplan DSGVO für Unternehmen, Juli 2017: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_8_Massnahmenplan.pdf

- **ULD**, Selbst-Check für Arzt- und Zahnarztpraxen, November 2017: https://www.datenschutzzentrum.de/uploads/medizin/arztpraxis/171101_Selbst_Check.pdf

### IV. Daten im Gesundheitswesen

- **vbw**, Rechtliche Aspekte der Digitalisierung im Gesundheitswesen, Augsut 2017: https://www.vbw-bayern.de/vbw/Aktionsfelder/Standort/Soziale-Sicherung/Digitalisierung-Heckmann-Studie.jsp

- **gmds/GDD**, Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU-DSGVO, Mai 2017: https://www.gdd.de/arbeitskreise/datenschutz-und-datensicherheit-im-gesundheits-und-sozialwesen/materialien-und-links/datenschutzrechtliche-anforderungen-an-die-medizinische-forschung-unter-beru-cksichtigung-der-eu-datenschutz-grundverordnung

# Teil 3

# Wie lässt sich die Einhaltung der Anforderungen kontrollieren?

## A. Worum geht es?

Um zu **überprüfen, ob** ein Produkt bzw. Dienstleistung datenschutzkonform ist, und **nachzuweisen, dass** dieses Produkt bzw. Dienstleistung die Vorschriften des Datenschutzes erfüllt, kann eine Zertifizierung eingeholt werden. Für eine Zertifizierung überprüft ein objektiver Dritter (sogenannte Zertifizierungsstelle) die datenschutzrechtlichen Anforderungen und bescheinigt deren Einhaltung.

Bei den Zertifizierungen ist zu unterscheiden, ob sie von einer akkreditierten Zertifizierungsstelle (DSGVO-Zertifizierung) oder von einem Zertifikateanbieter ohne Akkreditierung vergeben werden. Beide Varianten können für ein Unternehmen vorteilhaft sein. Ein Teil der Vorteile wird jedoch nur durch eine Zertifizierung durch eine akkreditierte Zertifizierungsstelle vermittelt.

### I. Allgemeine Vorteile von Datenschutz-Zertifierungen, Siegeln und Prüfzeichen

Eine datenschutzrechtliche Zertifizierung kann für ein Unternehmen allgemeine Vorteile haben, z. B.:

- Eine Zertifizierung kann Voraussetzung für die Zulässigkeit eines Produktangebots sein (z. B. Telemedizin).
- Eine Zertifizierung kann die Glaubwürdigkeit und das Vertrauen in die Sicherheit eines Produkts oder einer Dienstleistung sowohl gegenüber Kunden als auch gegenüber Investoren steigern.
- Durch die Überprüfung erhält ein Unternehmen mehr Sicherheit, dass seinProdukt bzw. die von ihm angebotene Dienstleistung die datenschutzrechtlichen Vorgaben einhält. Dadurch sinkt das Risiko eines sanktionsbewehrten Verstoßes.

### II. Vorteile einer Zertifizierung durch eine akkreditierte Stelle (DSGVO-Zertifizierung)

Eine Zertifizierung von einer akkreditierten Zertifizierungsstelle hat zusätzliche Vorteile, die in der DSGVO geregelt sind. Die Zertifizierung kann als Gesichtspunkt herangezogen werden, um die Erfüllung der datenschutzrechtlichen Pflichten nachzuweisen.

#### 1. Konkrete Nachweis-Erleichterungen

Zertifizierungen können Unternehmen in folgenden Fällen zum Nachweis der Einhaltung der datenschutzrechtlichen Vorgaben dienen:

- Pflicht des Verantwortlichen zum Nachweis, das Datenschutzrecht einzuhalten (Accountability-Prinzip, Artikel 24 Abs. 3 DSGVO)
- Erfüllung der Anforderungen für den Datenschutz durch Technikeinstellungen und durch datenschutzfreundliche Voreinstellungen (Privacy by Design und Privacy by Default, Artikel 25 Abs. 3 DSGVO)
- Garantie ausreichender technisch-organisatorischer Sicherheit bei Auftragsverarbeitern (Artikel 28 Abs. 5 DSGVO)
- Sicherheit der Datenverarbeitung (Artikel 32 Abs. 3 DSGVO)
- Datenübermittlung an ein Drittland (Artikel 46 Abs. 2 lit. f DSGVO)

Zudem kann die Einhaltung eines zertifizierten Verarbeitungsverfahrens sanktionsmindernd bei Entscheidung über die Verhängung einer Geldbuße und über deren Betrag berücksichtigt werden (Artikel 83 Abs. 2 lit. j DSGVO).

#### 2. Rechtswirkung

Die Zertifizierung durch eine akkreditierte Stelle ist gewichtiges Indiz dafür, dass das Unternehmen im geprüften Umfang die datenschutzrechtlichen Anforderungen einhält. In der Praxis ist damit zu rechnen, dass sich die Aufsichtsbehörden in der Regel umfassend auf Zertifizierungen verlassen werden, solange sie keine konkreten Hinweise auf Missstände haben. Die rechtliche Verantwortung für die Einhaltung der datenschutzrechtlichen Vorgaben bleibt allerdings trotz Zertifizierung voll bestehen. Ebenso behält die Aufsichtsbehörde sich all ihre rechtlichen Aufgaben und Befugnisse vor.

## B. Was ist zu tun?

Aufgrund der oben genannten Vorteile kann es in vielen Fällen sinnvoll sein, für ein Produkt oder eine Dienstleistung der Gesundheitswirtschaft eine Zertifizierung anzustreben.

Auf dem Markt gibt es aktuell verschiedene Anbieter, die datenschutzrechtliche Zertifizierungen hinsichtlich unterschiedlicher Kriterienkataloge ausstellen. Eine staatliche Prüfung findet grundsätzlich nur im Rahmen des – gegenwärtig noch nicht durchgeführten – Akkreditierungsverfahrens statt.

### I. Achtung: Derzeit keine Zertifizierung durch akkreditierte Stelle (DSGVO-Zertifizierung) möglich

Gegenwärtig sind noch keine Zertifizierungsstellen für die Konformitätsbewertung nach der DSGVO akkreditiert, da die entsprechenden Akkreditierungsanforderungen noch nicht abgestimmt sind. Nach Aussagen der Deutschen Akkreditierungsstelle können deswegen Zertifikate, die eine Konformität mit den Anforderungen der EU-DSGVO bestätigen, noch nicht erworben werden.

Zwar könnten neben den Zertifizierungsstellen auch die Aufsichtsbehörden selbst DSGVO-Zertifizierungen vornehmen. Nach derzeitigem Informationsstand bietet aber keine Aufsichtsbehörde in Deutschland eine solche Zertifizierung an.

### II. Andere Zertifizierungen

Derzeit ist es lediglich möglich, sonstige Datenschutzsiegel, -prüfzeichen oder -zertifierungen mit den unter Ziff. A.I genannten allgemeinen Vorteilen zu erlangen.

Hierbei handelt es sich jedoch – trotz einer etwaigen Bezeichnung als Zertifizierung zur DSGVO o.ä. – nicht um DSGVO-Zertifizierungen, die als Faktor herangezogen werden, um die Erfüllung der datenschutzrechtlichen Pflichten nachzuweisen (vgl. Ziff A.II).

#### 1. Auswahl eines Anbieters

Auf dem Markt gibt es eine Reihe von Anbietern, die datenschutzrechtliche Zertifizierungen durchführen. Eine Übersicht über unterschiedliche Stellen, die sonstige Zertifizierungen mit datenschutzrechtlichem Bezug anbieten, kann in der Liste der Stiftung Datenschutz eingesehen werden.

Das Unabhängige Landeszentrum für Datenschutz führt überdies ein Register von anerkannten Sachverständigen, in dem auch Zertifizierungsstellen enthalten sind.

Die Zertifizierungen haben zum Teil unterschiedliche Schwerpunkte. Es werden Datenschutz-, Telekommunikations-, Multimedia- oder Verbraucherschutzrecht oder eine Kombination dieser Rechtsgebiete geprüft. Teilweise veröffentlichen die Zertifizierungsstellen ihre Anforderungskataloge. Ein Unternehmen kann somit einen geeigneten Anbieter für den eigenen Bedarf auswählen.

Sobald Zertifizierungsstellen zukünftig i.S.d. DSGVO akkreditiert sind, werden die angebotenen Zertifizierungsverfahren und Datenschutzsiegel in ein Register aufgenommen und in geeigneter Weise veröffentlicht.

#### 2. Ablauf eines Zertifizierungsverfahrens

Der Ablauf des Zertifizierungsverfahrens hängt vom gewählten Anbieter und vom begehrten Zertifikat ab. Grundsätzlich sieht der Ablauf folgendermaßen aus:

- Gemeinsame Festlegung der Ziele für die Zertifizierung
- Gemeinsame Analyse des gegenwärtigen Stands beim Datenschutz
- Optimierung des Datenschutzes durch das Unternehmen
- Prüfung und Bewertung des optimierten Datenschutzes durch die Zertifizierungsstelle, ggf. weitere Verbesserungsvorschläge
- Bei Erfüllung der Voraussetzungen der Zertifizierungsstelle wird das Zertifikat erteilt.

Die Prüfung selbst führt in der Regel ein selbständiger Gutachter durch, der keine Verbindung mit der zu prüfenden Einrichtung haben sollte und im Idealfall selbst als qualifiziert zertifiziert wurde. Der Gutachter legt die Ergebnisse der Zertifizierungsstelle vor, die dann wiederum das Datenschutz-Zertifikat verleiht.

Die Dauer dieses Prozesses hängt stark vom Umfang der Maßnahmen ab, die ein Unternehmen zur Einhaltung der datenschutzrechtlichen Anforderungen umsetzen muss.

### 3. Kosten der Zertifizierung

Über die Kosten einer Datenschutz-Zertifizierung lässt sich keine generelle Aussage treffen. Der Grund dafür ist zum einen die Vielzahl der Anbieter auf diesem Markt, die jeweils ihre eigenen Verfahren und Prüfsiegel haben. Zum anderen aber hängen die Kosten auch von der Intensität und Prüftiefe des Prozesses sowie der Komplexität des Gegenstandes ab: Wird nur ein bestimmtes IT-Produkt oder eine Dienstleistung geprüft oder steht der Datenschutz eines ganzen Unternehmens auf dem Prüfstand? Welche Größe und Verzweigung hat die Firma?


## C. Weiterführende Links

- **DSK**, Kurz-Papier zur Zertifizierung nach Artikel 42 DSGVO: https://www.lda.bayern.de/media/dsk_kpnr_9_zertifizierung.pdf
- **Stiftung Datenschutz**, Liste der Zertifizierer, Februar 2017: https://www.stiftungdatenschutz.org/fileadmin/Redaktion/PDF/Zertifizierungsuebersicht/SDS-Zertifizierungsuebersicht_02_2017.pdf
- **ULD**, Register der anerkannten Sachverständigen nach § 3 Abs. 3 DSGVO: https://www.datenschutzzentrum.de/guetesiegel/register-sachverstaendige/

# FAQ zur Orientierungshilfe

### 1. Handelt es sich bei den von mir verwendeten Daten um Gesundheitsdaten?

Um Gesundheitsdaten handelt es sich immer dann, wenn Sie Daten verwenden, die sich auf

- eine identifizierbare natürliche Person (Personenbezug) sowie
- die Gesundheit dieser Person beziehen und aus denen Informationen über ihren Gesundheitszustand hervorgehen (Gesundheitsbezug).

Das Datenschutzrecht behandelt Gesundheitsdaten per se als eine „besondere Kategorie" personenbezogener Daten und stellt mitunter höhere Anforderungen an ihre Verarbeitung als bei „normalen" Daten. Näheres hierzu finden Sie in Teil 1 I. der Orientierungshilfe.

### 2. Wann darf ich Gesundheitsdaten verwenden?

Bei Gesundheitsdaten gelten strengere Regeln als bei „normalen" personenbezogenen Daten. Wenn Sie Gesundheitsdaten verwenden möchten, müssen Sie sicherstellen, dass ein spezifischer Ausnahmetatbestand erfüllt ist und Sie eine Rechtsgrundlage vorweisen können. Ohne eine derartige „doppelte" Rechtfertigung ist die Verarbeitung von Gesundheitsdaten rechtswidrig und kann sanktioniert werden.

Ob Sie Gesundheitsdaten verwenden dürfen, sollten Sie daher in zwei Schritten prüfen:

- **Schritt 1:** Können Sie die geplante Verwendung von Gesundheitsdaten auf einen der Ausnahmetatbestände in Artikel 9 Abs. 2-4 DSGVO, wie zum Beispiel eine ausdrückliche Einwilligung der betroffenen Person, stützen? Wenn nein, ist die geplante Datenverarbeitung verboten. Wenn ja, weiter mit Schritt 2.
- **Schritt 2:** Sind zusätzlich die Voraussetzungen einer Rechtsgrundlage für die Datenverarbeitung nach Artikel 6 DSGVO erfüllt? Wenn nein, ist die geplante Verwendung der Daten verboten. Wenn ja, ist die Datenverarbeitung erlaubt.

Näheres hierzu finden Sie in Teil 2 A.I. der Orientierungshilfe.

### 3. Inwiefern muss ich meine Unternehmensorganisation anpassen?

Wenn Ihr Unternehmen Gesundheitsdaten verwendet, müssen Sie die Unternehmensorganisation vor allem in folgenden Punkten anpassen:

- Alle Beschäftigten sollten zur Wahrung des Datengeheimnisses und zur Beachtung der geltenden datenschutzrechtlichen Anforderungen verpflichtet werden.
- Sie müssen prüfen, ob Ihr Unternehmen zur Bestellung einer beziehungsweise eines Datenschutzbeauftragten gesetzlich verpflichtet ist, und sodann ggf. eine geeignete Person mit dieser Aufgabe betrauen.
- Ihr Unternehmen muss die zur Einhaltung der DSGVO erforderlichen Prozesse implementieren und nachweisen beziehungsweise dokumentieren, insbesondere durch ein Verarbeitungsverzeichnis. Ein Verarbeitungsverzeichnis kann auch dann zu erstellen sein, wenn Ihr Unternehmen nicht selbst verantwortlich ist, sondern als Auftragsverarbeiter für ein anderes Unternehmen tätig ist.

Näheres hierzu finden Sie in Teil 2 A.II. der Orientierungshilfe.

### 4. Wie muss ich mit Daten umgehen, die dem Berufsträgergeheimnis unterfallen?

Ärzte und Angehörige anderer Heilberufe unterliegen einer Schweigepflicht, die das besondere Vertrauensverhältnis zum Patienten schützen soll. Mit dieser gesetzlichen Schweigepflicht korrespondiert das durch § 203 StGB geschützte Berufsträgergeheimnis, das Verstöße gegen die Verschwiegenheitspflicht strafrechtlich sanktioniert. Die datenschutzrechtlichen Vorschriften der DSGVO stehen grundsätzlich unabhängig neben diesen strafrechtlichen Vorgaben.

Wenn Sie Daten, die dem Berufsträgergeheimnis unterliegen, an externe Hilfspersonen (wie z. B. Cloud-Dienste) weiterleiten möchten, müssen Sie daher die sogenannte Zwei-Stufen-Prüfung vornehmen:

- **Stufe 1:** Ist die geplante Weitergabe der Daten datenschutzrechtlich zulässig? Wenn nein, ist die Verarbeitung verboten. Wenn ja, weiter mit Stufe 2.

- **Stufe 2:** Ist die geplante Verarbeitung auch strafrechtlich nach Maßgabe des § 203 StGB zulässig?

Näheres hierzu finden Sie in Teil 2 B. der Orientierungshilfe.

### 5. Was muss ich bei der Einschaltung von externen Dienstleistern beachten?

Sie dürfen nur solche Dienstleister auswählen, die (auch gerade in datenschutzrechtlicher Hinsicht) zuverlässig sind. Außerdem müssen Sie einen Auftragsverarbeitungs-Vertrag mit dem Dienstleister abschließen. Der Inhalt dieses Vertrages muss den zwingenden Anforderungen genügen, die in Artikel 28 Abs. 3 DSGVO vorgegeben sind. Sie sollten möglichst einen der in der Orientierungshilfe verlinkten Muster-Auftragsverarbeitungsverträge als Grundlage verwenden.

Vorsicht ist schließlich geboten, wenn Sie Dienstleister außerhalb der Europäischen Union beauftragen möchten, da hier zusätzliche Vorgaben bestehen können.

Näheres hierzu finden Sie in Teil 2 C. der Orientierungshilfe.

### 6. Was muss ich bei der Programmierung einer App beachten?

Grundsätzlich gelten für Gesundheits-Apps die gleichen datenschutzrechtlichen Anforderungen wie bei jeder anderen Verwendung von Gesundheitsdaten. Daneben sollten Unternehmen, die Apps im Bereich Electronic Health (beziehungsweise MobileHealth) entwickeln oder anbieten wollen, jedoch einige datenschutzrechtliche Besonderheiten beachten. Das betrifft vor allem die Themen Zulässigkeit der Datenverarbeitung (zum Beispiel bei Tracking und Profiling), Datensicherheit, Informationspflichten (Stichwort: Datenschutzerklärung) und Anforderungen der App-Stores. Außerdem sollten Sie auf folgende Punkte achten:

- **Datenschutz durch Technikgestaltung:** Anwendungen und Systeme müssen von Beginn an schutzbedarfs- beziehungsweise risikoorientiert konzipiert und technisch umgesetzt werden. Diesen Ansatz nennt man Datenschutz by design.
- **Datenschutzfreundliche Voreinstellungen:** Zudem soll nach dem Prinzip „Datenschutz durch datenschutzfreundliche Voreinstellungen“ ein angemessenes Datenschutzniveau für Nutzer durch datenschutzfreundliche Grundeinstellungen gewährleistet werden (Datenschutz by default).

Näheres hierzu finden Sie in Teil 2 D. der Orientierungshilfe.

### 7. Was muss ich beim Einsatz von KI-Lösungen beachten?

Wenn Sie Künstliche-Intelligenz-Lösungen im Zusammenhang mit Gesundheitsdaten nutzen, müssen Sie in datenschutzrechtlicher Hinsicht vor allem darauf achten, ob durch die Datenanalyse Persönlichkeitsprofile von Personen erstellt werden (Stichwort: Profiling) und ob zum Beispiel durch Algorithmen computerbasierte Entscheidungen gegenüber der jeweiligen Person getroffen werden sollen (Stichwort: automatisierte Einzelentscheidungen). In diesen Fällen müssen Sie folgende Punkte prüfen:

**Schritt 1:** Zunächst müssen Sie die allgemeinen datenschutzrechtlichen Anforderungen beachten, die bei jeder Verwendung von Profiling beziehungsweise automatisierter Entscheidung gelten. Besonderheiten ergeben sich insofern vor allem bezüglich der Zulässigkeit der Verwendung der Gesundheitsdaten und bezüglich Betroffenenrechten.

**Schritt 2:** Zusätzliche Anforderungen gelten für automatisierte Entscheidungen immer dann, wenn sie ohne menschliches Eingreifen ergehen. Sofern solche automatisierten Entscheidungen gegenüber den betroffenen Personen rechtliche Wirkungen entfalten oder sie in ähnlicher Weise beeinträchtigen, ist die Verwendung automatisierter Entscheidungen bei der Verarbeitung von Gesundheitsdaten nur zulässig, wenn alle folgenden Voraussetzungen erfüllt sind:

- Die der automatisierten Entscheidung zugrundeliegende Verwendung der Gesundheitsdaten muss von einer ausdrücklichen Einwilligung des Betroffenen gedeckt sein oder auf der Grundlage eines Spezialgesetzes, das der Wahrung eines erheblichen öffentlichen Interesses dient, erfolgen.

- Die automatisierte Entscheidung muss (a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und Ihrem Unternehmen erforderlich sein oder (b) aufgrund besonderer Rechtsvorschriften zulässig sein oder (c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgen.

- Sie müssen angemessene Maßnahmen ergreifen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren.

Näheres hierzu finden Sie in Teil 2 E. der Orientierungshilfe.

### 8. Welche Anforderungen muss ich bei der Anwendung von Big-Data-Techniken beachten?

Da bei der Datenanalyse mittels Big Data eine Vielzahl von Gesundheitsdaten analysiert wird, stellen sich besondere Herausforderungen bei der Einhaltung der datenschutzrechtlichen Vorgaben. Sie müssen daher vor allem auf folgende Punkte achten:

- Zulässigkeit der Datenanalyse. Als mögliche gesetzliche Grundlage kommt auch hier eine ausdrückliche Einwilligung der betroffenen Personen in Betracht. Für Forschungszwecke können die Betroffenen durch den sogenannten „broad consent" ihre Einwilligung für ganze Bereiche wissenschaftlicher Forschung geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Zudem kann sich die Zulässigkeit auch daraus ergeben, dass die Gesundheitsdaten bewusst öffentlich gemacht wurden oder die Datenverarbeitung wissenschaftlichen Forschungszwecken beziehungsweise statistischen Zwecken dient.

- Betroffenenrechte. Die Einhaltung der Rechte der von der Datenverarbeitung betroffenen Personen stellt angesichts der typischerweise zu analysierenden Datenmengen eine besondere Herausforderung dar.

- Kombination mit Künstliche-Intelligenz-Lösungen. Zusätzlich sind gegebenenfalls die Voraussetzungen für Profiling und automatisierte Entscheidungen zu berücksichtigen (siehe auch FAQ Frage 7).

Alternativ können Sie prüfen, ob es möglich ist, im Rahmen der Big-Data-Analyse mit anonymisierten Datenbeständen zu arbeiten. Anonymisierte (Gesundheits-)Daten fallen nicht in den Anwendungsbereich des Datenschutzrechts und können daher auch ohne Einhaltung der datenschutzrechtlichen Vorgaben ausgewertet werden. Die hierzu notwendige Anonymisierung, d.h. die Aufhebung des Personenbezugs, ist bei Gesundheitsdaten jedoch besonders schwierig, da Gesundheitsdaten sehr individuell sein können und die betroffene Person daher häufig anhand weniger Zusatzinformationen identifiziert werden kann. Auch der Vorgang der Anonymisierung stellt zudem eine Datenverarbeitung dar, für die bei Gesundheitsdaten eine Ausnahme vom Verbot der Datenverarbeitung sowie eine Rechtsgrundlage erforderlich ist.

Näheres hierzu finden Sie in Teil 2 F. der Orientierungshilfe.

### 9. Welche Sicherheitsanforderungen muss ich beachten?

Der Sicherheit der personenbezogenen (Gesundheits-) Daten kommt in der DSGVO eine besonders hohe Bedeutung zu. Um die gesetzlichen Pflichten bezüglich Datensicherheit einzuhalten, muss Ihr Unternehmen geeignete technische und organisatorische Schutzmaßnahmen im Wege einer eigenständigen Risikobewertung festlegen und ein angemessenes Schutzniveau gewährleisten.

Im ersten Schritt müssen Sie hierzu anhand des Schutzbedarfs der Daten ermitteln, welches Schutzniveau für die Daten angemessen ist. Dabei müssen Sie eine Balance zwischen Aufwand und Risiko (zum Beispiel Folgen einer Datenpanne) finden. Im zweiten Schritt müssen Sie die Maßnahmen, die zur Gewährleistung dieses angemessenen Schutzniveaus notwendig sind, implementieren und dokumentieren.

Näheres hierzu finden Sie in Teil 2 A. IV. der Orientierungshilfe.

### 10. Wie kann ich nachweisen, dass ich die datenschutzrechtlichen Anforderungen einhalte?

Sie können eine Zertifizierung einholen. Bei einer Zertifizierung überprüft ein objektiver Dritter (sogenannte Zertifizierungsstelle), ob Ihr Unternehmen die datenschutzrechtlichen Anforderungen einhält, und stellt eine entsprechende Bescheinigung aus. Folgende zwei Arten der Zertifizierung sind zu unterscheiden:

- Besonders vorteilhaft sind die in der DSGVO genannten Zertifizierungen durch eine akkreditierte Zertifizierungsstelle. Denn solche Zertifizierungen sind im Gesetz ausdrücklich als wichtiger Anhaltspunkt für die Erfüllung der datenschutzrechtlichen Pflichten anerkannt. Derzeit sind aber solche Zertifizierungen noch nicht erhätlich.

- Gegenwärtig sind lediglich sonstige Datenschutzsiegel, -prüfzeichen oder -zertifierungen möglich. Auch diese haben verschiedene Vorteile für den Nachweis, dass Ihr Unternehmen datenschutzrechtlich compliant ist. Sie sind jedoch nicht gesetzlich anerkannt und entfalten daher auch nicht die gleiche Wirkung wie Zertifizierungen von einer akkreditierten Zertifizierungsstelle.

Näheres hierzu finden Sie in Teil 3 der Orientierungshilfe.

# Glossar

## 1. Anonymisierung

Unter **Anonymisierung** versteht man einen Vorgang, bei dem personenbezogene Daten in der Weise modifiziert werden, dass die Person, die hinter den persönlichen oder sachlichen Angaben steht, nicht bzw. nicht mehr identifiziert werden kann. Ist der Personenbezug aufgehoben, spricht man von anonymisierten Daten. Anonymisierte Daten fallen nicht in den Anwendungsbereich des Datenschutzrechts. Insofern sind sie abzugrenzen von (lediglich) pseudonymisierten Daten, bei denen eine Zuordnung zu einer spezifischen Person unter Hinzuziehung zusätzlicher Informationen möglich bleibt und die daher vollständig den Anforderungen des Datenschutzrechtes unterliegen.

Die Aufhebung des Personenbezugs ist bei Gesundheitsdaten besonders schwierig, da Gesundheitsdaten häufig sehr individuell sind und der Betroffene daher oft anhand weniger Zusatzinformationen identifiziert werden kann.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 F.II.)

## 2. Auftragsverarbeiter/Auftragsverarbeitungsvertrag

Als **Auftragsverarbeiter** bezeichnet man ein Unternehmen (oder eine andere Person bzw. Stelle), das als Dienstleister personenbezogene Daten im Auftrag eines anderen, für die Datenverarbeitung verantwortlichen Unternehmens verarbeitet, also zum Beispiel erhebt oder speichert (Artikel 4 Nr. 8 DSGVO). Der Auftragsverarbeiter verarbeitet die Daten als verlängerter Arm des Verantwortlichen nach dessen Weisung und in der Regel auf der Grundlage eines Auftragsverarbeitungsvertrages (Artikel 28 DSGVO). Er mag dabei zwar die physische Herrschaft über den Verarbeitungsprozess ausüben, entscheidet aber nicht selbst über die wesentlichen Zwecke sowie Mittel der Verarbeitung und wird daher datenschutzrechtlich privilegiert.

Der Verantwortliche dagegen muss sich das Handeln seines Auftragsverarbeiters datenschutzrechtlich so zurechnen lassen, als sei dieser Teil seines eigenen Unternehmens.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 C.I.)

## 3. Berufsgeheimnisträger

**Berufsgeheimnisträger** sind Angehörige einer Berufsgruppe, die gesetzlich zur Geheimhaltung und Verschwiegenheit verpflichtet ist, wie beispielsweise Ärzte, Apotheker, Psychotherapeuten, Rechtsanwälte, Steuerberater oder Wirtschaftsprüfer. Die Pflicht zur Geheimhaltung kann sich aus EU-Recht, nationalem Recht oder Vorschriften national zuständiger Stellen ergeben, in Deutschland beispielsweise aus § 203 Abs. 1 StGB oder den Berufsordnungen von Ärzten, Apothekern und Psychologen. Bei der Verarbeitung von Daten, die dem Berufsträgergeheimnis unterliegen, müssen sowohl die datenschutzrechtlichen als auch die straf- und berufsrechtlichen Anforderungen beachtet werden.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 B.)

## 4. Betroffenenrechte

In der DSGVO sind verschiedene gesetzliche Rechte und Ansprüche der von der Datenverarbeitung betroffenen Personen normiert (sogenannte **Betroffenenrechte**). Zu den Betroffenenrechten zählen z. B. das Auskunftsrecht, das Recht auf Berichtigung und Löschung und das Recht auf Datenportabilität.

Aus den Betroffenenrechten ergeben sich entsprechende gesetzliche Pflichten für das Unternehmen, das für die Datenverarbeitung verantwortlich ist. Teilweise müssen Unternehmen dabei von sich aus tätig werden (z. B. Erteilung von Informationen über die Datenverarbeitung, Löschung von Daten), teilweise (nur) auf Verlangen des Betroffenen (z. B. Recht auf Auskunft, Recht auf Datenübertragung).

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.III.)

## 5. Betroffener/betroffene Person

**Betroffener** oder **betroffene Person** ist die identifizierte oder identifizierbare natürliche Person, auf die sich die personenbezogenen Informationen bzw. Daten beziehen (Artikel 4 Nr. 1 DSGVO). Die bzw. der Betroffene ist somit die Person,

- um deren Daten es geht und

- die davor zu schützen ist, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird. Hierzu dienen ihr beispielsweise die Betroffenenrechte.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.III.)

## 6. Big Data

Unter **Big Data** ist eine Form der Datenanalyse zu verstehen, die es erlaubt, mit einer hohen Geschwindigkeit eine große Menge an Daten aus einer Vielzahl von Quellen zu kombinieren und hieraus wirtschaftlichen Nutzen zu erzeugen. Werden hierbei auch Gesundheitsdaten oder andere personenbezogene Daten verwendet, ist das Datenschutzrecht einzuhalten. Bestimmte Erleichterungen können im Rahmen von Forschungsvorhaben gelten.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 F.)

## 7. Datenpannen

**Datenpannen** sind Ereignisse, bei denen die Sicherheit personenbezogener Daten verletzt wird, beispielsweise weil Gesundheitsdaten fehlerhaft übermittelt oder gestohlen werden oder weil das verarbeitende Unternehmen „gehackt" wird. Im Falle einer Datenpanne bestehen für das verantwortliche Unternehmen und Auftragsverarbeiter umfassende Meldepflichten gegenüber der Datenschutzaufsicht und den von der Datenpanne betroffenen Personen.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.V.)

## 8. Datenschutz by design/by default

Das für eine Verwendung von (Gesundheits-)Daten verantwortliche Unternehmen ist verpflichtet, schon „**by design**", also z. B. bei Konzeptionierung einer App, durch geeignete (insbesondere technische) Maßnahmen, und „**by default**", also durch geeignete Voreinstellungen, zu gewährleisten, dass das Datenschutzrecht eingehalten wird. Hierdurch soll insbesondere gewährleistet werden, dass die Datenschutzgrundsätze Datenminimierung und Zweckbindung wirksam umgesetzt werden.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.X.)

## 9. Datenschutz-Folgenabschätzung

Sind mit einer geplanten Verwendung von (Gesundheits-) Daten hohe Risiken für die betroffene Person verbunden, muss das verantwortliche Unternehmen in bestimmten Fällen vorab eine sogenannte **Datenschutz-Folgenabschätzung** (DSFA) durchführen. So erfordert z. B. jede umfangreiche Verarbeitung von Gesundheitsdaten bereits eine DSFA. Die DSFA soll sicherstellen, dass das verantwortliche Unternehmen mögliche Folgen bestimmter kritischer Datenverarbeitungen vorab analysiert und Maßnahmen für den Schutz der betroffenen Personen festlegt, um so das Risiko auf ein angemessenes Maß zu reduzieren.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.VI.)

## 10. Datenschutzbeauftragter

Der **Datenschutzbeauftragte** soll als interne Kontrollinstanz Unternehmen bei der Einhaltung des Datenschutzrechts unterstützen. Die Bestellung eines Datenschutzbeauftragten ist unter der DSGVO für Unternehmen in der gesamten EU unter bestimmten Bedingungen verpflichtend.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.II.2.)

## 11. Datenschutzerklärung

Unternehmen müssen gegenüber den betroffenen Personen Transparenz darüber herstellen, wie sie personenbezogene Daten verarbeiten. Sie müssen daher Personen, deren (Gesundheits-)Daten sie verarbeiten, proaktiv bestimmte Informationen über die Datenverarbeitung zur Verfügung stellen. Unternehmen kommen ihren Informationspflichten häufig dadurch nach, dass sie eine **Datenschutzerklärung/Privacy Policy** zur Verfügung stellen und darin umfassend erläutern, wie und in welchem Umfang personenbezogene Daten verarbeitet werden.

Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.III.2.)

## 12. Datenschutzgrundverordnung (DSGVO)

Die europäische **Datenschutzgrundverordnung** (DSGVO) ist am 25. Mai 2018 nach einer Übergangsphase von zwei Jahren wirksam geworden und bildet seither den datenschutzrechtlichen Rahmen innerhalb der Europäischen Union. Unternehmen müssen ihre Geschäftsabläufe daher an die Rechtslage unter der DSGVO anpassen. Neben der DSGVO können weitere nationale datenschutzrechtliche Vorschriften, wie etwa in Deutschland die des Bundesdatenschutzgesetzes (BDSG), zu beachten sein.

Die DSGVO ist ein wichtiger Schritt zu einem harmonisierten europäischen Binnenmarkt. Ziel der Verordnung ist eine angemessene Balance zwischen Wirtschafts- und Verbraucherinteressen in Zeiten fortschreitender Digitalisierung. Sie stärkt das Grundrecht auf informationelle Selbstbestimmung durch höhere Transparenz und mehr Mitbestimmung der Bürgerinnen und Bürger mit Blick auf ihre Daten. Gleichzeitig schafft die Verordnung einen zukunftsorientierten und forschungsfreundlichen Rechtsrahmen für datenverarbeitende Unternehmen und innovative Geschäftsmodelle.

## 13. Einwilligung

Eine **Einwilligung** ist eine Willensbekundung der betroffenen Person, mit der Verarbeitung der sie betreffenden personenbezogenen Daten (z. B. Gesundheitsdaten) einverstanden zu sein. Die Willensbekundung kann in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung erfolgen. Sie muss freiwillig sein und in informierter und unmissverständlicher Weise abgegeben werden.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.I.3.1)

## 14. Gemeinsam Verantwortliche

Wenn zwei Unternehmen bei einer Verarbeitung von (Gesundheits-)Daten zusammenwirken und gemeinsam wesentliche Entscheidungen in Bezug auf die Zwecke und die Mittel der Verarbeitung treffen, sind beide Unternehmen **gemeinsam Verantwortliche** für die Datenverarbeitung. Das bedeutet, dass keines der Unternehmen privilegiert wird; eine Auftragsverarbeitung kommt nicht in Betracht. Ein Austausch von Daten zwischen zwei gemeinsam Verantwortlichen ist daher – wie jede andere Datenverarbeitung – rechtfertigungsbedürftig. Die beiden Unternehmen müssen eine die gemeinsame Verarbeitung regelnde Vereinbarung abschließen und besondere Informationspflichten beachten.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.VII.)

## 15. Gesundheitsdaten

**Gesundheitsdaten** sind alle personenbezogenen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Artikel 4 Nr. 15 DSGVO). Gesundheitsdaten stellen eine besondere Kategorie personenbezogener Daten dar und können als solche gesteigerten datenschutzrechtlichen Anforderungen unterliegen.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 1 I.1)

## 16. Personenbezogene Daten

Unter **personenbezogenen Daten** versteht man Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Artikel 4 Nr. 1 DSGVO). Das bedeutet:

- Es bedarf einer natürlichen Person,
- die natürliche Person muss mindestens identifizierbar sein und
- die Informationen müssen sich personenbezogen auf diese Person beziehen.

Es kann dabei auch ausreichen, dass die natürliche Person, auf die sich die Information bezieht, erst mit weiteren Hilfsmitteln identifizierbar ist, wie etwa bei Pseudonymen. Der Begriff ist daher sehr weit zu verstehen und kann neben persönlichen Angaben (z. B. Name, Alter, Fotos) oder sachlichen Angaben (z. B. Kreditwürdigkeit, Vertragsbeziehungen) auch etwa Geodaten oder Online-Kennungen (z. B. IP-Adressen, Cookies) umfassen. Das Gegenstück zum personenbezogenen Datum bildet das anonyme Datum.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 1 I.1.)

## 17. Profiling

Unter **Profiling** im Gesundheitsbereich ist jede automatisierte Verarbeitung personenbezogener Daten zu verstehen, die bestimmte persönliche Aspekte einer natürlichen Person bewertet, um etwa deren Gesundheit zu analysieren oder vorherzusagen (Artikel 4 Nr. 4 DSGVO). Im Allgemeinen geht es also darum, insbesondere durch Algorithmen Informationen über Personen automatisch zu sammeln und auszuwerten, um sie einer bestimmten Kategorie zuzuordnen.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 E. I.1.)

## 18. Pseudonymisierung

**Pseudonymisierung** ist die Verarbeitung personenbezogener Daten in einer Weise, dass eine Zuordnung der Daten zu einer spezifischen Person nur noch unter Hinzuziehung zusätzlicher Informationen möglich ist (Artikel 4 Nr. 5 DSGVO). Erforderlich ist dabei, dass die zusätzlichen Informationen technisch/räumlich getrennt aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten nicht einer bestimmten Person zugewiesen werden. Nach erfolgter Pseudonymisierung spricht man von pseudonymen Daten.

Charakteristisch für pseudonyme Daten ist somit – im Unterschied zu anonymen Daten – das Bestehen einer Zuordnungsregel wie z. B. einer Verschlüsselung, die den unter einem Pseudonym erfassten Daten ein Identifikationsmerkmal einer Person zuweist. Wurden personenbezogene Daten pseudonymisiert, so verlieren sie zwar dadurch nicht ihre Einstufung als personenbezogene Daten i. S. d. DSGVO und unterliegen daher – im Unterschied zu anonymen Daten – weiterhin sämtlichen Anforderungen des Datenschutzrechtes. Gleichwohl wird durch die Pseudonymisierung der Schutz der Betroffenen erhöht, so dass z. B. pseudonymisierte Daten eher für andere Zwecke genutzt werden können.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 1 I.1.)

## 19. TOM/Technische und organisatorische Maßnahmen

Unter **technischen Maßnahmen** versteht man Vorkehrungen, die sich auf den Vorgang der Verarbeitung von Daten erstrecken, wie z. B. bauliche Maßnahmen, die den Zutritt Unbefugter verhindern sollen, oder Steuerungen des Software- oder Hardwareprozesses der Verarbeitung, etwa durch Maßnahmen der Zugriffs- oder Weitergabekontrolle wie Verschlüsselung oder Passwortsicherung.

Organisatorische Maßnahmen beziehen sich insbesondere auf die äußeren Rahmenbedingungen zur Gestaltung des technischen Verarbeitungsprozesses, etwa die Einhaltung des Vieraugenprinzips, das Wegschließen von Datenträgern, Protokollierungen von Tätigkeiten und Stichprobenroutinen. Dazu können auch Schulungen der Mitarbeiter oder Verpflichtungserklärungen gehören.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A. IV. 2.2.1)

## 20. Verantwortlicher

Ein **Verantwortlicher** im Sinne der DSGVO ist eine natürliche oder juristische Person (z. B. eine GmbH oder AG) oder andere Stelle, die allein oder gemeinsam mit anderen über die wesentliche Entscheidungsbefugnis über Zwecke und Mittel der Datenverarbeitung verfügt (Artikel 4 Nr. 7 DSGVO). Der Begriff des Verantwortlichen dient somit dazu, die primäre Verantwortung für die Einhaltung des Datenschutzes zuzuweisen, etwa einem verantwortlichen Unternehmen.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A. II. 3.1)

## 21. Verarbeitungsverzeichnis

Das **Verarbeitungsverzeichnis** (oder auch Verzeichnis der Verarbeitungstätigkeiten) hat die Aufgabe, die wesentlichen Informationen einer Datenverarbeitung (Zweck, Kategorien, Empfänger, Löschfristen etc.) schriftlich oder in einem elektronischen Format zu dokumentieren (Artikel 30 DSGVO). Es umfasst alle Verarbeitungstätigkeiten, die (bei Verantwortlichen) in der Zuständigkeit des jeweiligen Unternehmens liegen bzw. (bei Auftragsverarbeitern) das Unternehmen im Auftrag eines Verantwortlichen durchführt.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A. II. 3.2.2)

## 22. Verarbeitung von Daten

Der Begriff **„Verarbeitung" von Daten** ist weit zu verstehen und erfasst grundsätzlich jeden Vorgang im Zusammenhang mit personenbezogenen Daten wie z. B. die Verwendung, das Erheben, das Erfassen, das Ordnen, die Speicherung, die Veränderung, das Abfragen, die Offenlegung durch Übermittlung, Bereitstellung, den Abgleich oder die Löschung von Daten (Artikel 4 Nr. 2 DSGVO).

## 23. Vertreter

Ein **Vertreter** im Sinne der DSGVO ist eine in der EU niedergelassene natürliche oder juristische Person, die von einem nicht in der EU niedergelassenen Unternehmen schriftlich gemäß Artikel 27 DSGVO bestellt wurde. Der Vertreter fungiert insbesondere als Anlaufstelle für Aufsichtsbehörden oder Betroffene bei Fragen im Zusammenhang mit der Einhaltung der DSGVO durch das nicht in der EU niedergelassene Unternehmen.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 2 A.II.4.)

## 24. Zertifizierung

Eine **Zertifizierung** ist eine Bewertung durch einen objektiven Dritten (sogenannte Zertifizierer), mit der bescheinigt wird, dass die geprüften datenschutzrechtlichen Kriterien eingehalten wurden. Nur akkreditierte Zertifizierungsstellen können Zertifizierungen im Sinne der DSGVO ausstellen. Die Zertifizierung kann dazu genutzt werden, die eigene Konformität mit dem Datenschutz zu demonstrieren. Sie ist nicht verpflichtend, sondern wird freiwillig von einem Unternehmen beantragt.

(Weitere Informationen finden Sie in der Orientierungshilfe in Teil 3)

www.bmwi.de