Schutz von Gesundheitsdaten

Einleitung

Personenbezogene Daten, die ihrem Wesen nach besonders sensibel sind, verdienen einen besonderen Schutz und dürfen nur auf Basis spezieller Rechtsgrundlagen verarbeitet werden. In der Datenschutz-Grundverordnung (DSGVO) finden sich Ausführungen zur besonderen Schutzbedürftigkeit unter anderem in den Erwägungsgründen 51 bis 54. Zu diesen sensiblen Daten gehören unter anderem Gesundheitsdaten, die in Art. 9 Abs. 1 DSGVO explizit genannt werden. Für einen Verstoß gegen die Vorgaben zur Verarbeitung von Gesundheitsdaten sieht Art. 83 Abs. 5 DSGVO einen Bußgeldrahmen bis zu 20 Mio. Euro oder 4 % des weltweit erzielten Jahresumsatzes eines Unternehmens vor.

Aufgrund der besonders strengen Anforderungen an die Verarbeitung von Gesundheitsdaten und der drohenden Bußgelder bei einer fehlenden Beachtung dieser Vorgaben ist es ratsam, alle Datenverarbeitungsvorgänge intensiv zu prüfen, wenn sich Berührungspunkte zu Gesundheitsdaten ergeben können.

Nachfolgend ist zunächst erläutert, wie Gesundheitsdaten überhaupt definiert sind, unter welchen Voraussetzungen ihre Verarbeitung erlaubt ist und welche weiteren Beschränkungen besonders zu beachten sind. Zur Veranschaulichung haben wir außerdem an geeigneter Stelle Beispiele und Hinweise für die praktische Umsetzung der Vorgaben aufgeführt.

Was sind Gesundheitsdaten?

Gesundheitsdaten werden in Art. 4 Nr. 15 DSGVO definiert als personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Nach Erwägungsgrund 35 fallen unter die Definition Angaben zu dem früheren, gegenwärtigen und künftigen Gesundheitszustand einer Person, unabhängig von der Herkunft der Daten, die zum Beispiel von einem Arzt, einem Medizinprodukt oder dem Betroffenen selbst stammen können.

Beispielhaft werden in dem Erwägungsgrund als Gesundheitsdaten Informationen über Krankheiten, Behinderungen, Krankheitsrisiken und klinische Behandlungen sowie Untersuchungsergebnisse genannt. Auch Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt werden, um sie für gesundheitliche Zwecke eindeutig zu identifizieren, fallen unter den Begriff. Die Feststellung, dass eine Person genesen oder gesund ist, kann ebenfalls bereits dazu zählen. Bei der Krankschreibung durch einen Arzt handelt es sich nach einem Urteil des EuGH, das sich auf die Datenschutzrichtlinie (Richtlinie 95/46/EG) als Vorläufer der DSGVO bezog, um ein Gesundheitsdatum (Urt. v. 06.11.2003 – C-101/01, Rn. 49-51).

Bei Daten, aus denen nur mittelbar Rückschlüsse auf den Gesundheitszustand möglich sind, ist umstritten, ob zusätzliche Anforderungen an die Qualifikation als Gesundheitsdatum zu stellen sind. Es wird beispielsweise vertreten, dass zusätzlich eine Absicht der Auswertung (Gola, in: Gola, DSGVO, 2. Aufl. 2018, Art. 4 Rn. 97) oder ein Verwendungszusammenhang (Weichert, in Kühling/Buchner, DS-GVO-BDSG, Art. 4 Nr. 15 Rn. 7) bezüglich der Daten erforderlich ist. Das Passbild eines Brillenträgers soll danach zum Beispiel kein Gesundheitsdatum sein. Das Bundesministerium für Wirtschaft und Energie, das eine Orientierungshilfe zum Datenschutz für Gesundheitsdaten herausgebracht hat, zählt dagegen grundsätzlich auch indirekte Informationen dazu, soweit Rückschlüsse auf den gesundheitlichen Zustand des Betroffenen möglich sind. Danach könne auch das Lichtbild einer Person ein Gesundheitsdatum sein, beispielsweise wenn daraus hervorgehe, dass der Betroffene eine Brille trägt.

Letztendlich ist für jeden Einzelfall konkret zu prüfen, ob Gesundheitsdaten vorliegen. Um der besonderen Schutzbedürftigkeit von Gesundheitsdaten Rechung zu tragen, ist vorsorglich eine weite Auslegung des Begriffs zu empfehlen, sodass bereits Daten, die nur mittelbar Rückschlüsse auf die Gesundheit einer Person zulassen, Gesundheitsdaten sein können, soweit sie den Schluss auf den Gesundheitszustand nahelegen.

Grundsätzliches Verbot der Verarbeitung von Gesundheitsdaten

Die Verarbeitung von Gesundheitsdaten ist nach Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. In Erwägungsgrund 51 ist dazu beschrieben, dass derartige sensible personenbezogene Daten nicht verarbeitet werden sollen, soweit die Verarbeitung in den in der DSGVO dargelegten besonderen Fällen nicht explizit zugelassen ist. Der allgemein in der DSGVO geltende Grundsatz des Verbots mit Erlaubnisvorbehalt ist damit gegenüber der Verarbeitung von personenbezogenen Daten, die nicht besonders sensibel sind, nochmals deutlich strenger ausgestaltet.

Erlaubnistatbestände des Art. 9 Abs. 2 DSGVO

Die besonderen Fälle, in denen die Verarbeitung ausnahmsweise zulässig ist, sind in Art. 9 Abs. 2 DSGVO abschließend aufgeführt. Die speziellen Anforderungen des Art. 9 Abs. 2 DSGVO gelten

zusätzlich zu den allgemeinen Grundsätzen der Datenverarbeitung. Zu beachten ist auch, dass nach Art. 9 Abs. 4 DSGVO und Erwägungsgrund 51 S. 4 in dem Recht der Mitgliedstaaten zusätzliche Bedingungen festgelegt sein können. Für Deutschland gibt es unter Nutzung dieser Öffnungsklausel besondere Vorgaben in §§ 22, 27 f. BDSG, die bei bestimmten Konstellationen wie Forschungsvorhaben Privilegierungen vorsehen.

Das grundsätzliche Verarbeitungsverbot gilt nach Art. 9 Abs. 2 DSGVO nur dann nicht, wenn eine der folgenden Voraussetzungen erfüllt ist.

a. Die betroffene Person hat in die Datenverarbeitung für einen oder mehrere festgelegte Zwecke eingewilligt. Es gelten dabei erhöhte Anforderungen an die Bestimmtheit der Einwilligung und die Informiertheit des Betroffenen.

b. Die Verarbeitung ist für die Ausübung bzw. Erfüllung von Rechten und Pflichten aus dem Arbeits- oder Sozialrecht erforderlich.

c. Die Verarbeitung ist zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben. Diese Rechtsgrundlage soll nach Erwägungsgrund 46 S. 2 nur dann greifen, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann.

d. Die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten. Die Verarbeitung darf sich ausschließlich auf aktuelle oder ehemalige Mitglieder der Organisation oder auf Personen beziehen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit der Organisation unterhalten. Die personenbezogenen Daten dürfen außerdem nicht ohne Einwiligung des Betroffenen nach außen offengelegt werden.

e. Die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat.

f. Die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich.

g. Die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats aus Gründen eines erheblichen öffentlichen Interesses erforderlich. Die rechtliche Grundlage muss dabei in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen.

h. Die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs erforderlich. Eine solche Verarbeitung darf nach Art. 9 Abs. 3 DSGVO nur durch Fachpersonal oder unter dessen Verantwortung stattfinden. Die verarbeitende Person muss dem Berufsgeheimnis oder einer sonstigen Geheimhaltungspflicht unterliegen.

i. Die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats erforderlich. Die rechtliche Grundlage muss dabei angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsehen. Beispielhaft werden der Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und die Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei Arzneimitteln, Medizinprodukten und der Gesundheitsversorgung genannt.

j. Die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO erforderlich.

Sonderregelungen für kirchliche Stellen und Berufsgeheimnisträger

Zu beachten ist, dass für Verantwortliche, die in den Anwendungsbereich von kirchlichen Datenschutzregelungen fallen, Sonderbestimmungen gelten können. Relevant ist dies beispielsweise für katholische oder evangelische Krankenhäuser. Für sie gelten das Gesetz über den kirchlichen Datenschutz (KDG) beziehungsweise das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD).

Auch für Berufsgeheimnisträger existieren Sonderregelungen. Ärzte müssen beispielsweise zusätzlich zu den datenschutzrechtlichen Bestimmungen auch die besonderen Vorgaben berücksichtigen, die sich aus § 203 StGB ergeben. Danach kann die Verletzung von Privatgeheimnissen sogar einen Straftatbestand erfüllen.

Anforderungen an technische und organisatorische Maßnahmen

Verantwortliche Stellen und ihre Auftragsverarbeiter haben nach Art. 32 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Da Gesundheitsdaten besonders sensibel und schützenswert sind, sind die diesbezüglichen technischen und organisatorischen Maßnahmen gegenüber dem allgemeinen Standard entsprechend zu erhöhen. Erwähnenswert ist an dieser Stelle ein Bescheid der österreichischen Datenschutzbehörde, über den wir in unserem Newsletter im Mai 2019 berichtet haben. Die Einholung einer Einwilligung in die unverschlüsselte Übermittlung von Gesundheitsdaten sei danach prinzipiell nicht datenschutzkonform möglich, da die Pflicht aus Art. 32 DSGVO nicht durch eine Einwilligung abbedungen werden könne.

Allen Unternehmen, die maßgeblich mit Gesundheitsdaten arbeiten, ist zu raten, bei der Datenverarbeitung geeignete Sicherheitsmaßnahmen gemäß Art. 32 DSGVO, beispielsweise Verschlüsselungen bei Datenübermittlungen, zu treffen.

Automatisierte Entscheidungsfindungen

Nach Art. 22 Abs. 4 DSGVO dürfen automatisierte Entscheidungsfindungen, die auf besonderen Kategorien personenbezogener Daten beruhen, nur mit Einwilligung des Betroffenen oder auf Grundlage des Art. 9 Abs. 2 lit. g) DSGVO stattfinden. Eine solche automatisierte Entscheidungsfindung wäre beispielsweise die automatische, durch einen Computer stattfindende Auswertung von Gesundheitsdaten in Anträgen auf Leistungen einer Krankenversicherung zur Entscheidung über den Vertragsschluss oder die Gewährung von Prämienzahlungen.

Datenschutzfolgenabschätzung

Hat eine Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, führt der Verantwortliche nach Art. 35 Abs. 1 S. 1 DSGVO vorab eine Abschätzung der Folgen der Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Eine Datenschutz-Folgenabschätzung ist nach Art. 35 Abs. 3 lit. b) DSGVO insbesondere auch bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO erforderlich. Eine umfangreiche Verarbeitung von Gesundheitsdaten erfordert demnach regelmäßig eine Datenschutz-Folgenabschätzung. Nicht zwingend vorgeschrieben ist eine Datenschutz-Folgenabschätzung nach Erwägungsgrund 91 allerdings für die Verarbeitung personenbezogener Daten von Patienten oder Mandanten durch einen einzelnen Arzt, sonstige Angehörige eines Gesundheitsberufes oder einen Rechtsanwalt.

Unternehmen, die Gesundheitsdaten verarbeiten, ist zu empfehlen, für jeden Verarbeitungsvorgang zu prüfen, ob eine Datenschutz-Folgenabschätzung notwendig ist. Hilfreich ist dabei auch ein Blick in die von der Datenschutzkonferenz („DSK"), dem Zusammenschluss der Datenschutzbehörden der Länder und des Bundes, veröffentlichten Listen von Verarbeitungsvorgängen, die eine Datenschutz-Folgenabschätzung erfordern (abrufbar auf der Internetseite der DSK).

Fazit

Gesundheitsdaten erfordern einen besonderen Schutz. Unternehmen sollten insbesondere genau prüfen, ob einer der Ausnahmetatbestände des Art. 9 Abs. 2 DSGVO greift und somit eine Rechtsgrundlage für die Datenverarbeitung besteht. Ist dies der Fall, ist darauf zu achten, dass ausreichende technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau der Daten zu gewährleisten. Gegebenenfalls ist eine Datenschutz-Folgenabschätzung durchzuführen. Bei Zweifeln empfiehlt es sich, Rücksprache mit dem Datenschutzbeauftragten des Unternehmens zu halten.

Johanna Schmale

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Wissenschaftliche Mitarbeiterin
T +49 521 96535 - 890
F +49 521 96535 - 114
M johanna.schmale@brandi.net
www.brandi.net