BRANDI
RECHTSANWÄLTE

VERARBEITUNG VON GESUNDHEITSDATEN

Informationen zum Datenschutz I Dezember 2023

English version

Einleitung

Für die Verarbeitung von personenbezogenen Daten, die ihrem Wesen nach als besonders sensibel eingestuft werden, gelten aus datenschutzrechtlicher Perspektive besonders strenge Anforderungen und Maßstäbe. Da im Zusammenhang mit der Verarbeitung dieser Daten erhebliche Risiken für die Rechte der Betroffenen auftreten können, bedürfen die Daten eines besonderen Schutzes. Insbesondere dürfen entsprechende Daten nur auf Grundlage spezieller Rechtsgrundlagen verarbeitet werden und es sind besondere Schutzmaßnahmen zu ergreifen. Zu diesen sensiblen Daten gehören unter anderem auch Gesundheitsdaten, wie sich aus Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) ausdrücklich ergibt.

Aufgrund der besonders strengen Anforderungen an die Verarbeitung von Gesundheitsdaten und möglicher Bußgelder bei Nichtbeachtung der entsprechenden Vorgaben, sollten alle Datenverarbeitungsprozesse, die einen Bezug zu Gesundheitsdaten aufweisen, intensiv geprüft, abgesichert und dokumentiert werden, um den ordnungsgemäßen Umgang mit den besonders schutzwürdigen Daten sicherzustellen und nachweisen zu können.

Gesundheitsdaten

Gesundheitsdaten werden als alle personenbezogenen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen, in Art. 4 Nr. 15 DSGVO legal definiert. Aus Erwägungsgrund 35 ergibt sich weiter, dass zu den personenbezogenen Gesundheitsdaten alle Daten zählen sollen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen.

Beispielhaft werden insoweit insbesondere Informationen über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen und Behandlungen genannt. Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeordnet wurden, um sie für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen aus Untersuchungen des Körpers sowie genetische Daten und biologische Proben fallen ebenfalls unter den Begriff. Auf die Herkunft der Daten – ob sie von einem Arzt, einem Medizinprodukt oder dem Betroffenen selbst stammen – kommt es hingegen nicht an.

Es ist vom Grundsatz her auch ausreichend, wenn sich die Informationen über die gesundheitlichen Gegebenheiten lediglich mittelbar aus dem Gesamtzusammenhang ergeben. Die Feststellung, dass eine Person genesen oder gesund ist, einen Arzt besucht hat oder geimpft ist, ist insoweit ebenfalls als Gesundheitsdatum einzuordnen. Nach Auffassung des EuGH handelt es sich auch bei der Krankschreibung durch einen Arzt um ein Gesundheitsdatum (EuGH, Urt. v. 06.11.2003 - Az. C-101/01). Ebenso fallen auch physiologische Daten, die z. B. über Apps oder Smartwatches im Privat- aber auch im Arbeitsleben erfasst werden, unter den Begriff. Zu den Gesundheitsdaten gehören darüber hinaus auch Merkmale wie Gewicht und Größe.

Bei allgemeinen Daten, die Rückschlüsse auf sensible Informationen zulassen – wie etwa das Passbild eines Brillenträgers –, ist demgegenüber umstritten, inwieweit solche Daten als Gesundheitsdaten einzuordnen sind. Es wird insoweit vertreten, dass entsprechende Informationen nur dann als besonders zu schützendes Gesundheitsdatum einzuordnen sind, wenn eine Auswertungsabsicht oder ein Verwendungszusammenhang besteht (siehe etwa *Gola*, in Gola, DSGVO, 2. Aufl. 2018, Art. 4 Rn. 97 oder *Weichert,* in Kühling/Buchner, DSGVO-BDSG, 3. Auflage 2020, Art. 4 Nr. 15 Rn. 7). Dass eine Person krankenversichert ist, soll demgegenüber grundsätzlich kein Gesundheitsdatum sein.

Da die Auffassungen zu der Frage, welche Informationen als Gesundheitsdaten einzuordnen sind, mitunter auseinandergehen, empfiehlt sich grundsätzlich eine genaue Prüfung im Einzelfall. Dabei ist zu beachten, dass in der Regel eine weite Auslegung des Begriffs angezeigt ist, um dem besonderen Schutzbedarf Rechnung zu tragen und negative Konsequenzen aufgrund einer Datenschutzverletzung zu vermeiden.

Anforderungen an die Verarbeitung von Gesundheitsdaten

Aufgrund der besonderen Schutzbedürftigkeit von personenbezogenen Daten, die als besonders sensibel eingeordnet werden, enthält die DSGVO verschiedene Sonderregelungen, die bei der Verarbeitung von Gesundheitsdaten einzuhalten sind.

Rechtsgrundlage

Die Verarbeitung besonderer Kategorien personenbezogener Daten, darunter auch Gesundheitsdaten, ist nach Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Etwas anderes gilt nur dann, wenn einer der Ausnahmetatbestände des Art. 9 Abs. 2 DSGVO einschlägig ist. Der im Übrigen über Art. 6 DSGVO verankerte Grundsatz des Verbots mit Erlaubnisvorbehalt wird insoweit noch verschärft. Eine Verarbeitung von Gesundheitsdaten ist nach Art. 9 Abs. 2 DSGVO in den folgenden Fällen zulässig:

a. Die betroffene Person hat in die Datenverarbeitung für einen oder mehrere festgelegte Zwecke eingewilligt. Neben den allgemeinen Anforderungen an Einwilligungen ist zu beachten, dass grundsätzlich eine ausdrückliche Einwilligung des Betroffenen erforderlich ist, die sich explizit auch auf die Verarbeitung der sensiblen Daten bezieht. Für die Verarbeitung von Beschäftigtendaten ergibt sich dies explizit aus § 26 Abs. 3 BDSG.

b. Die Verarbeitung ist zur Ausübung bzw. Erfüllung von Rechten und Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich. Diese Rechtsgrundlage kommt in Verbindung mit § 26 Abs. 3 BDSG etwa für bestimmte Verarbeitungsprozesse im Rahmen des Betrieblichen Eingliederungsmanagements (BEM) in Betracht.

c. Die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben.

d. Die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

e. Die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat. Es fehlt insoweit an der besonderen Schutzbedürftigkeit.

f. Die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich. Ist die Verarbeitung von Gesundheitsdaten Vertragsgegenstand oder für ein Vertragsverhältnis zwingend erforderlich, kann eine Verarbeitung zulässig sein, was unter anderem für das Fragerecht des Arbeitgebers oder Gesundheitsapps von Relevanz ist.

g. Die Verarbeitung ist aus Gründen eines erheblichen öffentlichen Interesses erforderlich. Die rechtliche Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats 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. Die Verarbeitung ist dabei nach Art. 9 Abs. 3 DSGVO nur zulässig, soweit die Daten durch Fachpersonal oder unter dessen Verantwortung verarbeitet werden und das Fachpersonal einem Berufsgeheimnis oder einer Geheimhaltungspflicht unterliegt.

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, soweit die zuvor genannten Angemessenheitsvoraussetzungen erfüllt sind.

Darüber hinaus sieht Art. 9 Abs. 4 DSGVO eine Öffnungsklausel vor, nach der die Mitgliedstaaten zusätzliche Bedingungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten festlegen können. Der deutsche Gesetzgeber hat von dieser Möglichkeit in §§ 22, 26 ff. Bundesdatenschutzgesetz (BDSG) Gebrauch gemacht. Die Regelungen greifen unter anderem verschiedene Ausnahmetatbestände der DSGVO auf. Eine Verarbeitung besonderer Kategorien personenbezogener Daten ist nach den nationalen Vorschriften etwa zur Ausübung von Rechten und Pflichten des Sozialrechts, aus Gründen eines erheblichen öffentlichen Interesses oder zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit und erheblicher Nachteile für das Gemeinwohl sowie zu Forschungs- und Archivzwecken zulässig.

Liegt ein Fall vor, in dem die Verarbeitung von Gesundheitsdaten ausnahmsweise zulässig ist, müssen im Rahmen des Datenverarbeitungsprozesses auch die übrigen Grundsätze und Bestimmungen der DSGVO eingehalten werden. Hinsichtlich der Zweckbindung gelten nach Art. 6 Abs. 4 lit. c) DSGVO allerdings besonders strenge Maßstäbe.

Unternehmen, deren Kerntätigkeit in der umfangreichen Verarbeitung von besonders sensiblen Daten liegt, müssen nach Art. 37 Abs. 1 lit. c) DSGVO außerdem zwingend einen Datenschutzbeauftragten bestellen.

Sonderregelungen

Neben den Regelungen der DSGVO sind bei der Verarbeitung von Gesundheitsdaten auch verschiedene andere Regelungen aus anderen Rechtsbereichen einzuhalten. Werden Gesundheitsdaten etwa im Rahmen eines Behandlungsverhältnisses verarbeitet, ist zugleich die ärztliche Schweigepflicht zu beachten, deren Verletzung nach § 203 StGB auch strafrechtliche Konsequenzen haben kann. Vergleichbare Geheimnisschutzregelungen gelten etwa auch für Rechtsanwälte und Notare.

Die besonders sensiblen Daten i.S.v. Art. 9 Abs. 1 DSGVO unterfallen zudem den auf den Schutz vor Diskriminierung abzielenden Vorschriften des Allgemeinen Gleichbehandlungsgesetzes (AGG) sowie dem im Beschäftigungsverhältnis geltenden Benachteiligungsverbot des § 75 BetrVG.

Technische und organisatorische Maßnahmen

Verantwortliche Stellen müssen nach Art. 32 DSGVO grundsätzlich geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. An verschiedener Stelle ergibt sich auch aus Art. 9 Abs. 2 DSGVO das Erfordernis, spezifische Maßnahmen zur Wahrung der Rechte der Betroffenen zu ergreifen, das an dieser Stelle sogar eine Voraussetzung für die Rechtskonformität der Datenverarbeitung ist. Da

besonders sensible Daten, wie etwa Gesundheitsdaten, eines besonderen Schutzes bedürfen, sind die Absicherungsmaßnahmen entsprechend stark auszugestalten.

Dies ergibt sich zusätzlich auch aus § 22 Abs. 2 BDSG, der Verantwortliche ebenfalls zur Einhaltung spezifischer und angemessener Maßnahmen zur Wahrung der Interessen der betroffenen Personen verpflichtet. Hierunter fallen etwa Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem Daten eingegeben, verändert oder entfernt wurden, besondere Sensibilisierungsmaßnahmen der an der Datenverarbeitung Beteiligten, die Beschränkung des Zugangs sowie Verschlüsselungsmaßnahmen.

Erwähnenswert ist insoweit eine Entscheidung des SG Hamburg zur Übermittlung von Sozialdaten in barrierefreier Form – konkret per unverschlüsselter E-Mail – bei Vorliegen einer entsprechenden Einwilligung des Betroffenen (wir berichteten im Oktober 2023). In dem zugrundeliegenden Fall hatte die Behörde die seitens eines Blinden geforderte Übermittlung von Sozialdaten per unverschlüsselter E-Mail unter Hinweis auf datenschutzrechtliche Bedenken und die Vorschrift des Art. 32 DSGVO abgelehnt. Das Gericht führte hingegen aus, dass der Betroffene in die Datenverarbeitung eingewilligt habe und Art. 32 DSGVO keine Datensicherheit um jeden Preis fordere. Das Recht auf informationelle Selbstbestimmung und das Abwehrrecht des Klägers aus dem Benachteiligungsverbot seien im konkreten Fall gegeneinander abzuwägen. Es leuchte insoweit nicht ein, wieso der Schutz der Daten des Klägers dem Recht, nicht benachteiligt zu werden, in jedem Fall übergeordnet werden sollte.

Gleichwohl sollten Unternehmen, die Gesundheitsdaten verarbeiten, in jedem Fall darauf achten, ausreichende Maßnahmen i.S.v. Art. 32 DSGVO zu ergreifen, um die Datenverarbeitung genügend abzusichern.

Automatisierte Entscheidungsfindung
Sollen automatisierte Entscheidungen getroffen werden, die auch auf besonderen Kategorien personenbezogener Daten beruhen, ist dies nach Art. 22 Abs. 4 DSGVO nur zulässig, wenn für die Datenverarbeitung eine Einwilligung des Betroffenen vorliegt oder die Voraussetzungen von Art. 9 Abs. 2 lit. g) DSGVO erfüllt sind und zusätzlich einer der Ausnahmetatbestände des Art. 22 Abs. 2. DSGVO vorliegt. Hintergrund dieser Regelung ist das besondere Diskriminierungspotential der Daten. Beispiele für eine automatisierte Entscheidungsfindung wären etwa die automatische, mittels einer Software durchgeführte Auswertung von Gesundheitsdaten in Anträgen auf Leistungen einer Krankenversicherung zur Entscheidung über den Vertragsschluss oder die Berücksichtigung von Gesundheitsdaten durch eine Recruiting-Software.

Dokumentation

Verantwortliche Stellen unterliegen nach Art. 5 Abs. 2 DSGVO der sog. Rechenschaftspflicht. Das bedeutet, sie müssen mittels einer geeigneten Dokumentation positiv nachweisen, dass sie die datenschutzrechtlichen Vorschriften einhalten. Dies gilt insbesondere auch mit Blick auf die Verarbeitung besonders sensibler Daten wie Gesundheitsdaten.

Verfahrensverzeichnis
Wie jeder andere Prozess, bei dem personenbezogene Daten verarbeitet werden, ist auch die Verarbeitung von Gesundheitsdaten in das nach Art. 30 DSGVO verpflichtend zu führende Verzeichnis der Verarbeitungstätigkeiten aufzunehmen. Insbesondere die Einhaltung der strengen gesetzlichen Vorgaben sollte hierbei genau dokumentiert werden. Die Dokumentation sollte außerdem einer regelmäßigen Kontrolle unterzogen werden.

Datenschutz-Folgenabschätzung
Hat eine Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge, ist zusätzlich eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO durchzuführen. Eine Datenschutz-Folgenabschätzung ist nach Art. 35 Abs. 3 lit. b) DSGVO insbesondere auch bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO erforderlich. Erfolgt die Verarbeitung von Gesundheitsdaten durch einen einzelnen Arzt oder Rechtsanwalt, soll die Datenverarbeitung nach Erwägungsgrund 91 allerdings nicht als umfangreich anzusehen sein und eine Datenschutz-Folgenabschätzung nicht zwingend notwendig sein.

Werden besonders sensible Daten zum Zwecke der Übermittlung an Dritte anonymisiert, mittels Sensoren oder mobilen Anwendungen verarbeitet und von einer zentralen Stelle empfangen oder aufbereitet (z. B. Telemedizin-Lösungen) oder von Anbietern neuer Technologien verwendet, um die Leistungsfähigkeit von Personen zu bestimmen (z. B. Fitnessarmbänder, Apps, oder Smartphones), ist entsprechend der Muss-Liste der Datenschutzkonferenz ebenfalls eine Datenschutz-Folgenabschätzung durchzuführen.

Fazit

Bei der Verarbeitung von Gesundheitsdaten ist deren besonderer Schutzbedarf von besonderer Bedeutung. Angesichts der hohen Anforderungen, die bei der Verarbeitung entsprechender Daten zu erfüllen sind, sollten Unternehmen auf erster Stufe genau prüfen, ob eine Rechtsgrundlage für die Datenverarbeitung vorliegt. Auf zweiter Stufe sind sodann ausreichende Absicherungsmaßnahmen zum Schutz der Daten zu ergreifen. Es sollte außerdem auf eine genaue Dokumentation der Prozesse geachtet und gegebenenfalls auch eine Datenschutz-Folgenabschätzung erstellt werden. Außerdem muss überprüft werden, inwieweit neben den datenschutzrechtlichen Regelungen weitere Vorschriften, etwa aus dem Arbeitsrecht, beachtet werden müssen. In Zweifelsfällen empfiehlt sich ein Austausch mit dem Datenschutzbeauftragten des Unternehmens.

Christina Prowald

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net