Gesundheitsdatenschutz unter der Datenschutzgrundverordnung (DSGVO)

Dr. Katharina Landes
Dr. Katja Kuck

Zum 25. Mai 2018 wird die bereits 2016 in Kraft getretene Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) wirksam. Zeitgleich löst das neue Bundesdatenschutzgesetz (BDSG n.F.) das bislang geltende Bundesdatenschutzgesetz ab.

Die Neuregelungen führen auch zu Änderungen im Gesundheitsdatenschutz und sind daher für Unternehmen und sonstige Stellen relevant, deren Geschäftszweck den Umgang mit Gesundheitsdaten mit sich bringt (Ärzte, Krankenhäuser, Medizinische Versorgungszentren, Heil- und Hilfsmittellieferanten, Labore etc.).

Aufgrund zahlreicher unbestimmter Rechtsbegriffe in der DSGVO, aber auch wegen des überwiegend noch ungeklärten Verhältnisses der DSGVO zu den bestehenden bereichsspezifischen Datenschutzvorschriften im Gesundheits- und Sozialsektor (z.B. Sozialgesetzbücher, Landeskrankenhausgesetze etc.) sind viele Fragen bei der praktischen Umsetzung der DSGVO noch ungeklärt. Eine vollständige Vereinheitlichung des europäischen Datenschutzrechts hat die DSGVO aufgrund der diversen Öffnungsklauseln für die nationalen Gesetzgeber zudem nicht erreicht.

Der Begriff der Gesundheitsdaten unter der DSGVO

Gesundheitsdaten werden unter der DSGVO definiert als „*personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen*“.

Erfasst werden vor allem solche personenbezogenen Daten, die unmittelbar Rückschlüsse auf den Gesundheitszustand einer Person zulassen (bspw. Informationen über medizinische Befunde, Diagnosen, Laborauswertungen etc.), und zwar unabhängig von der Herkunft der Daten, also egal, ob sie von einem Arzt, Apotheker oder einem sonstigen Angehörigen eines Gesundheitsberufes, von einem Krankenversicherungsträger oder auch von einer Health App erhoben wurden.

Zudem können auch solche Daten u.U. Gesundheitsbezug aufweisen, die nur mittelbar oder in der Gesamtschau mit anderen Daten Rückschlüsse auf den Gesundheitszustand einer Person zulassen (bspw. Informationen über Gewicht, Ernährungsgewohnheiten, Aufenthalte in gesundheitsrelevanten Einrichtungen, Arzneimitteleinnahmen etc.).

Voraussetzungen für die Verarbeitung von Gesundheitsdaten

Wie auch bereits unter dem bisherigen BDSG ist die Verarbeitung von besonderen Kategorien personenbezogener Daten, wozu auch Gesundheitsdaten zählen, nach der DSGVO nur aufgrund einer Einwilligung der betroffenen Person oder aufgrund eines der abschließend aufgezählten Erlaubnistatbestände des Art. 9 DSGVO zulässig (sog. Verbot mit Erlaubnisvorbehalt). Die Verarbeitung solcher besonders sensibler Daten unterliegt also weiterhin engen Grenzen (siehe hierzu weiter unten).

Anforderungen an die datenschutzrechtliche Einwilligung

Die Einwilligung des Betroffenen spielt im Umgang mit Gesundheitsdaten daher eine prominente Rolle. Nach den Regelungen der DSGVO werden an die Wirksamkeit einer Einwilligung jedoch hohe Anforderungen gestellt, insbesondere mit Blick auf die Freiwilligkeit und die Informiertheit der Einwilligung.

Unfreiwilligkeit bei Kopplung

Mit Art. 7 Abs. 4 DSGVO wird ein in dieser Form neues Kopplungsverbot eingeführt. Danach ist die Freiwilligkeit einer Einwilligung insbesondere dann zu hinterfragen, wenn der Abschluss eines Vertrags von der Einwilligung in die Verarbeitung solcher personenbezogener Daten abhängig gemacht wird, deren Verarbeitung zur Vertragserfüllung nicht erforderlich ist.

Ein weiteres Kopplungsverbot enthält Erwägungsgrund 43 der DSGVO, nach dem eine Einwilligung auch dann nicht als freiwillig gilt, wenn dem Betroffenen nicht die Möglichkeit gegeben wird, in verschiedene Verarbei-

tungsvorgänge gesondert einzuwilligen, obwohl dies im Einzelfall angebracht wäre. Was mit verschiedenen Verarbeitungsvorgängen genau gemeint ist (ob verschiedene Arten und/oder verschiedene Zwecke der Verarbeitung) und wann eine gesonderte Einwilligung *angebracht* wäre, beantwortet die DSGVO jedoch nicht.

Die Regelung kann durchaus so zu verstehen sein, dass das verantwortliche Unternehmen in einer Einwilligungserklärung nunmehr für verschiedene Verarbeitungen jeweils gesonderte Opt-in Felder vorsehen muss. Ob und in welchem Umfang Opt-in Felder vorzusehen sind, obliegt einer Einzelfallprüfung.

Informationspflichten

Gemäß Art. 13 und 14 DSGVO treffen das verantwortliche Unternehmen im Vorfeld der Datenverarbeitung wesentlich umfassendere Informationspflichten gegenüber dem Betroffenen als noch nach dem BDSG a.F. Neu ist z.B. die Angabe der Rechtsgrundlage der Verarbeitung und die Speicherdauer. Ob das Fehlen der Pflichtinformationen die Unwirksamkeit der Einwilligung zur Folge hat, ist in der DSGVO nicht eindeutig geregelt. Gemäß Erwägungsgrund 42 müssen „mindestens“ die Identität des Verarbeitungsverantwortlichen und die beabsichtigten Verarbeitungszwecke mitgeteilt werden. Dass auch das Fehlen anderer Informationen im Einzelfall zur Unwirksamkeit der Einwilligung führen kann, dürfte aber auf der Hand liegen.

Formerfordernisse

Ein Schriftformerfordernis für die Einwilligung, wie bislang von § 4a Abs.1 S.3 BDSG a.F. gefordert, besteht unter der DSGVO nicht mehr. Vielmehr sind grundsätzlich auch andere Formen der Einwilligung, solange sie eine eindeutige und bestätigende Handlung (kein Opt-out) darstellen, ausreichend. Bei besonderen Kategorien personenbezogener Daten - also auch bei Gesundheitsdaten - ist allerdings eine „ausdrückliche“ Einwilligung notwendig und daher die Möglichkeit der konkludenten Erteilung ausgeschlossen.

Da den Verantwortlichen jedoch eine Nachweispflicht hinsichtlich des Vorliegens der Einwilligung trifft, wird man in der Praxis aus Gründen der Rechtssicherheit um die Schriftform nicht herumkommen.

Der zentrale Erlaubnistatbestand des § 22 Abs. 1 Nr. 1 b) BDSG n.F. i.V.m. Art. 9 Abs. 2 h) DSGVO

Mit dem die Verarbeitung besonderer Kategorien personenbezogener Daten betreffenden § 22 Abs. 1 Nr. 1 b) BDSG n.F. hat der deutsche Gesetzgeber die in Art. 9 Abs. 2 h) DSGVO enthaltene Öffnungsklausel nahezu wortgleich übernommen, und so den bisher in § 28 Abs. 7 BDSG a.F. enthaltenen zentralen Erlaubnistatbestand zur Verarbeitung von Gesundheitsdaten weitestgehend erhalten.

Gemäß § 22 Abs. 1 Nr. 1 b) BDSG n.F. ist die Verarbeitung besonderer Kategorien von personenbezogenen Daten zulässig, wenn sie zu Zwecken

- der Gesundheitsvorsorge,
- der Beurteilung der Arbeitsfähigkeit von Beschäftigten,
- der medizinische Diagnostik,
- der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich,
- der Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich,
- oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs

erforderlich ist und die betreffenden Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden.

Die Erlaubnisnorm knüpft damit an eine Verarbeitung durch die in § 203 StGB genannten Berufsgeheimnisträger an. Am Rande sei erwähnt, dass auch der § 203 StGB kürzlich geändert wurde, insbesondere um Auftragsdatenverarbeitungen, die im Bereich des Datenschutzes bereits privilegiert sind, auch im Bereich des Berufsgeheimnisschutzes zu privilegieren.

Bereichsspezifische Sondernormen

In Deutschland existieren auf dem Gebiet des Gesundheits- und Sozialdatenschutzes zahlreiche bereichsspezifische Sondernormen (bspw. die Regelungen in den Sozialgesetzbüchern, den Landeskrankenhausgesetzen oder den Vorschriften kirchlicher Einrichtungen).

Wie das Verhältnis dieser bereichspezifischen Normen zur DSGVO zu bewerten ist, insbesondere ob diese Normen sämtlich unter eine der Öffnungsklauseln des Art. 9 DSGVO subsumiert werden können oder ob hier Anpassungsbedarf durch den deutschen Gesetzgeber besteht, kann derzeit noch nicht abschließend beantwortet werden. Jedenfalls zu den Sozialgesetzbüchern I bis III, VII, IX, X und XII existiert bereits ein Änderungsentwurf, das SGB V soll folgen.

Fazit

Mit Blick auf die nunmehr vorgesehenen empfindlich hohen Geldbußen bei Datenschutzverstößen (bis zu EUR 20 Mio. oder bis zu 4% des konzernweit (!) erzielten Jahresumsatzes) raten wir an, die Umsetzung der Vorgaben der DSGVO ernst zu nehmen und zu überprüfen, ob der Umgang mit Gesundheitsdaten in Ihrem Unternehmen den (neuen) Anforderungen genügt. Dies gilt insbesondere vor dem Hintergrund der im Bereich des Gesundheitsdatenschutzes bestehenden Unsicherheiten und des in Deutschland vorhandenen Flickenteppichs an bereichsspezifischen Sondernormen.

Hinweis

Dieser Überblick dient ausschließlich der allgemeinen Information und kann konkreten Rechtsrat im einzelnen Fall nicht ersetzen. Sprechen Sie bei Fragen bitte Ihren gewohnten Ansprechpartner bei GÖRG bzw. die Autorin Dr. Katharina Landes unter klandes@goerg.de oder Dr. Katja Kuck unter kkuck@goerg.de an. Informationen zu den Autoren finden Sie auf unserer Homepage www.goerg.de.

Unsere Standorte

GÖRG Partnerschaft von Rechtsanwälten mbB

BERLIN
Kantstraße 164, 10623 Berlin
Tel. +49 30 884503-0, Fax +49 30 882715-0

KÖLN
Kennedyplatz 2, 50679 Köln
Tel. +49 221 33660-0, Fax +49 221 33660-80

FRANKFURT AM MAIN
Neue Mainzer Straße 69 – 75, 60311 Frankfurt am Main
Tel. +49 69 170000-17, Fax +49 69 170000-27

MÜNCHEN
Prinzregentenstraße 22, 80538 München
Tel. +49 89 3090667-0, Fax +49 89 3090667-90

HAMBURG
Dammtorstraße 12, 20354 Hamburg
Tel. +49 40 500360-0, Fax +49 40 500360-99