Dr. Werner Pilgermair
Datenschutzexperte

Auswirkungen der Datenschutz-Grundverordnung auf den Gesundheits- und Sozialbereich (Teil 1)

Einführung. Ab 25. 5. 2018 gilt die neue Rechtslage im Datenschutz. Die Datenschutz-Grundverordnung der EU wird massive Auswirkungen auf die Heim- und Pflegepraxis und den gesamten Gesundheits- und Sozialbereich haben. Im Rahmen dieses Beitrags wird ein Überblick über die neue Rechtslage verschafft. Während im Teil 1 allgemeine Informationen und Regelungsinhalte den Einstieg in die Datenschutz-Grundverordnung erleichtern sollen, wird der Fokus in Teil 2 und 3[1] auf konkrete Pflichten und Betroffenenrechte gerichtet, die künftig von jeder Einrichtung im Gesundheits- und Sozialbereich zu beachten sind.

Die Datenschutz-Grundverordnung (DSGVO)

Derzeit gilt auf europäischer Ebene die Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995, die in Österreich durch das Datenschutzgesetz 2000 (DSG 2000) umgesetzt wird. Im Laufe der Jahre wurde die Kritik an der Datenschutzrichtlinie zunehmend lauter:

- Die Richtlinie stellt nur den kleinsten gemeinsamen Nenner der Mitgliedstaaten dar und lässt unterschiedliche Datenschutzniveaus zu, was zu Rechtsunsicherheit und Wettbewerbsverzerrungen („Datenschutz-Hopping") führt.
- Internetnutzer (speziell Kinder und Jugendliche) sind immer größeren Risiken ausgesetzt.
- Das bestehende Datenschutzsystem ist veraltet und muss an die technologische Entwicklung und globalisierte Datenverwendung (explosionsartige Zunahme des Datenaustauschs) angepasst werden.

Aus diesen und weiteren Gründen wurde nach vier Jahren Diskussion und Verhandlung im April 2016 die finale Textierung der DSGVO beschlossen. Die Verordnung ist am 25. 5. 2016 in Kraft getreten und wird ab 25. 5. 2018 unmittelbar anwendbar sein. Gleichzeitig wird die Datenschutzrichtlinie außer Kraft treten. Daraus ergibt sich eine **zweijährige Übergangsphase**, in der Einrichtungen im Gesundheits- und Sozialbereich bis zum Stichtag die neuen Datenschutzvorschriften umzusetzen haben. Die damit einhergehenden Adaptierungs- und Compliance-Maßnahmen sind komplex und vielfältig.[2] Der Zeitaufwand, der sich daraus zwangsläufig ergeben wird, darf nicht unterschätzt werden.

Für Einrichtungen im Gesundheits- und Sozialbereich, die noch keine Maßnahmen zur Vorbereitung auf die DSGVO gesetzt haben, empfiehlt es sich, notwendige Schritte spätestens im Herbst 2017 einzuleiten.

Neue Begriffe

Durch die unmittelbare Anwendbarkeit der DSGVO werden künftig andere datenschutzrechtliche Begriffe verwendet, so wird insbesondere

- der *„Auftraggeber"* zum *„Verantwortlichen"* (controller),
- der *„Dienstleister"* zum *„Auftragsverarbeiter"* (processor),
- die *„Datei"* zum *„Dateisystem"* (filing system),
- die *„Verwendung"* von Daten zur *„Verarbeitung"* von Daten (processing),
- die *„Datenanwendung"* zur *„Verarbeitungstätigkeit"* (processing activity),
- die *„Zustimmung"* zur *„Einwilligung"* (consent),
- die *„sensiblen"* Daten zu *„besonderen Kategorien personenbezogener Daten"* (special categories of personal data).[3]

Mit der DSGVO werden auch bestehende Begriffe erstmals näher bestimmt. So werden zB **„Gesundheitsdaten"**, die bislang weder in der Datenschutzrichtlinie noch im DSG 2000 definiert werden, in Art 4 Z 15 DSGVO wie folgt beschrieben: *„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"*. Nach den Erwägungen zur DSGVO sind darunter auch Nummern, Symbole oder Kennzeichen zu verstehen, die einer natürlichen Person zugeteilt wurden, um sie für gesundheitliche Zwecke eindeutig zu identifizieren. Damit gilt künftig auch die Sozialversicherungsnummer als sensible Information.

Schließlich werden mit der DSGVO auch gänzlich neue Begriffe eingeführt, die wichtigsten aus Sicht des Gesundheits- und Sozialbereichs sind

- **„genetische Daten"** (Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über ihre Physiologie oder Gesundheit liefern; vgl im Detail Art 4 Z 13),
- **„biometrische Daten"** (mit speziellen technischen Verfahren gewonnene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die ihre eindeutige Identifizierung ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten; vgl Art 4 Z 14),
- **„Profiling"** (jede Art der automatisierten Verarbeitung personenbezogener Daten, die zum Zweck der Bewertung persönlicher Aspekte durchgeführt wird, insbesondere in Bezug auf die Arbeitsleistung, die wirtschaftliche Lage, die **Gesundheit**, die persönlichen Vor-

[1] Teil 2 (Neue Pflichten) und Teil 3 (Neue Betroffenenrechte) dieser Beitragsserie werden jeweils in einer der nächsten Ausgaben der ÖZPR erscheinen. [2] Vgl Teil 2 und 3 dieser Beitragsserie (FN 1). [3] In diesem Beitrag wird das neue Datenschutzvokabular verwendet. Nur am Begriff der „sensiblen Daten" wird aus Vereinfachungsgründen festgehalten.

lieben und Interessen, die Zuverlässigkeit, das Verhalten sowie den Aufenthaltsort oder Ortswechsel einer natürlichen Person; vgl im Detail Art 4 Z 4).

Neben sprachlichen Änderungen werden mit der DSGVO bestehende Begriffe näher bestimmt und neue Begriffe eingeführt. Zu den sensiblen Gesundheitsdaten zählt künftig auch die Sozialversicherungsnummer.

Verarbeitung nicht-sensibler Daten

Bei der Verarbeitung nicht-sensibler („**normaler**") Daten muss sich die Einrichtung im Gesundheits- und Sozialbereich auf einen der im Art 6 Abs 1 DSGVO aufgezählten Tatbestände stützen können. Die wichtigsten sind:

- **Einwilligung** der betroffenen Person (Art 6 Abs 1 lit a)

> Beispiel 1
> In einem Altenheim wird eine Liste mit den Geburtstagen der Bewohner ausgehängt und aus gegebenem Anlass ein Foto mit Gratulationstext in der monatlich erscheinenden Heimzeitung abgedruckt. Von den Bewohnern wird im Vorfeld die schriftliche Einwilligung dafür eingeholt.[4]

- Notwendigkeit der Verarbeitung zur Erfüllung einer **vertraglichen Verpflichtung** (Art 6 Abs 1 lit b)

> Beispiel 2
> In einem Pflegeheim werden dem Bewohner zusätzliche, individuell vereinbarte Sachmittel gewährt, die direkt mit ihm verrechnet werden. Zur Abwicklung kann das Pflegeheim die dafür benötigten Daten verarbeiten.

Verarbeitung sensibler Daten

Sensible Daten dürfen nur verarbeitet werden, wenn einer der im Art 9 Abs 2 DSGVO aufgezählten Tatbestände erfüllt ist. Die wichtigsten sind:

- Erforderlichkeit der Verarbeitung zur **Verteidigung von Rechtsansprüchen** (Art 9 Abs 2 lit f)

> Beispiel 3
> Ein behindertes Kind, das sich in ständiger Betreuung einer Rehabilitationseinrichtung befindet, verletzt sich schwer. Die Eltern begehren von der Einrichtung Schadenersatz wegen Vernachlässigung von Sorgfalts- und Betreuungspflichten. Zu ihrer Verteidigung kann die Einrichtung sensible Gesundheitsdaten aus der Betreuungsdokumentation verwenden (etwa zur Einholung eines externen Fachgutachtens oder im Rahmen einer außergerichtlichen Streitbeilegung).

- Erforderlichkeit der Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses und auf Grundlage einer **gesetzlichen Regelung** (Art 9 Abs 2 lit g)

> Beispiel 4
> In einer Krankenanstalt ergibt sich der begründete Verdacht der Misshandlung eines Minderjährigen. Bei Vorliegen der sonstigen Voraussetzungen hat die Anstalt eine schriftliche Mitteilung nach § 37 Bundes-Kinder- und Jugendhilfegesetz 2013 an den zuständigen Kinder- und Jugendhilfeträger zu erstatten. Diese Mitteilungspflicht durchbricht auch berufsrechtliche Verschwiegenheitspflichten (zB der Ärzte und Psychologen) und liegt zweifellos im hohen öffentlichen Interesse.

> Beispiel 5
> Ein anderes Beispiel ist die Auskunftspflicht in § 11 Abs 2 Tiroler Heimgesetz, wonach den Angehörigen von Gesundheits- und Sozialberufen, die einen Heimbewohner behandeln oder betreuen, die für diese Tätigkeiten erforderlichen Auskünfte zu erteilen sind.

- Erforderlichkeit der Verarbeitung ua für Zwecke der **Gesundheitsvorsorge**, der medizinischen **Diagnostik** oder der Versorgung oder Behandlung im **Gesundheits- oder Sozialbereich** auf der Grundlage einer **gesetzlichen Regelung** oder aufgrund eines **Vertrags** mit einem Angehörigen eines **Gesundheitsberufs** (Art 9 Abs 2 lit h)

Eine solche Eingriffsgrundlage stellt zB § 51 Ärztegesetz 1998 dar, der den Arzt zur umfassenden Dokumentation seiner Leistungen verpflichtet und zur automationsunterstützten Verarbeitung der im Rahmen dieser Dokumentation anfallenden Daten berechtigt.

- **Einwilligung** der betroffenen Person (Art 9 Abs 2 lit a)

> Beispiel 6
> In einer privaten Rehabilitationseinrichtung werden für einen öffentlichen Auftraggeber Klienten betreut. Liegen keine spezifischen landesgesetzlichen Regelungen über die Datenverarbeitung vor und wird die Betreuung von Mitarbeitern der Einrichtung durchgeführt, die keinem Gesundheitsberuf angehören, wird für die Verarbeitung sensibler Gesundheitsdaten die Einwilligung der betroffenen Klienten benötigt. Der zivilrechtliche Vertrag zwischen der Einrichtung und dem Klienten reicht dafür ebenso wenig aus wie der Kooperationsvertrag zwischen der Einrichtung und dem öffentlichen Auftraggeber, weil die Datenverarbeitung zur Erfüllung vertraglicher Pflichten nur bei nichtsensiblen Daten eine taugliche Eingriffsgrundlage darstellt.

Bei der Verarbeitung nichtsensibler Daten muss einer der im Art 6 Abs 1 DSGVO beschriebenen Tatbestände und bei der Verarbeitung sensibler Daten einer der im Art 9 Abs 2 DSGVO beschriebenen Tatbestände erfüllt sein.

[4] Fotos einer Person (Bilddaten) gelten per se noch nicht als sensible Daten (so auch EuGH 11. 12. 2014, C-212/13). Anderes würde nur gelten, wenn die fotografierte Person anhand von sensiblen Daten (zB offenkundige Verletzungen oder Behinderungen) als Auswahlkriterium bestimmt werden soll.

HINWEIS

Wird die Datenverarbeitung auf spezifische bundes- oder landesgesetzliche Normen gestützt, sollte der jeweilige Regelungsumfang genau beachtet werden. Umso mehr gilt dies bei der Verarbeitung sensibler Gesundheitsdaten.

Der neue Kinderschutz

Kinder und Jugendliche werden im Datenschutzrecht bislang nicht anders behandelt als erwachsene Personen, von denen Daten verarbeitet werden.[5] Künftig werden sie aber vor der Verarbeitung ihrer Daten durch Dienste der Informationsgesellschaft (zB Online-Shops, On-demand-Dienste und Social-Network-Services) geschützt, indem sie erst ab dem vollendeten 14. Lebensjahr rechtswirksam in entsprechende Angebote einwilligen können. Bei jüngeren Kindern muss die Einwilligung durch den Obsorgeberechtigten oder mit dessen Zustimmung erteilt werden (Art 8 DSGVO).[6]

Weitere Maßnahmen zum Schutz von Kindern betreffen auch Einrichtungen im Gesundheits- und Sozialbereich. So müssen nach Art 12 DSGVO alle verpflichtenden Mitteilungen und Informationen, die künftig an betroffene Kinder ergehen, in einer besonders **„klaren und einfachen Sprache"** formuliert sein.[7] Eine Kombination aus Text und Bildsymbolen kann hier hilfreich sein. Es ist davon auszugehen, dass die Europäische Kommission mittelfristig standardisierte Bildsymbole einführen wird. Bis dahin können eigene Symbole verwendet werden, die in Bezug auf die beabsichtigte Datenverarbeitung aussagekräftig sind.

Verpflichtende Informationen und Mitteilungen an Kinder müssen besonders einfach und verständlich formuliert sein. Die Kombination aus Text und Bildsymbolen kann hier hilfreich sein.

Die neuen Geldbußen

Als zentrale Sanktion bei Verstößen gegen die DSGVO sind **Geldbußen** vorgesehen, die bis zur Maximalhöhe von 20 Mio Euro oder 4% des Jahresumsatzes im vergangenen Geschäftsjahr (je nachdem, welcher der Beträge höher ist) verhängt werden können.

Bei der Bemessung der Geldbuße sind im Einzelfall insbesondere folgende Faktoren zu berücksichtigen (vgl im Detail Art 83 Abs 2 DSGVO):

- Art, Schwere und Dauer des Verstoßes,
- Verschuldensgrad (Vorsatz oder Fahrlässigkeit),
- getroffene Maßnahmen zur Minderung des Schadens,
- Grad der Verantwortung unter Berücksichtigung der implementierten organisatorischen und technischen Schutzmaßnahmen,
- Kategorien der Daten, die vom Verstoß betroffen sind,
- Umfang der Zusammenarbeit mit der Datenschutzbehörde.

Einrichtungen im Gesundheits- und Sozialbereich können das Geldbußenrisiko deutlich reduzieren, wenn sie die Erfordernisse der DSGVO vollständig umsetzen.[8]

Das geänderte österreichische Datenschutzgesetz stellt in § 30 klar, dass Geldbußen auch gegen juristische Personen (somit gegen den **Rechtsträger** der Einrichtung) verhängt werden können, und zwar dann, wenn die Verstöße von Personen begangen werden, die

- zur Vertretung der juristischen Person befugt sind oder dazu befugt sind, Entscheidungen im Namen der juristischen Person zu treffen, oder
- eine Kontrollbefugnis innerhalb der juristischen Person innehaben.

Weiters wird klargestellt, dass gegen Behörden und öffentliche Stellen keine Geldbußen verhängt werden können. Wer als **„öffentliche Stelle"** gilt, bleibt allerdings unklar und wird auch in der DSGVO nicht näher geregelt. Vorstellbar ist, dass darunter „öffentliche Stellen" im Sinne des Informationsweiterverwendungsrecht oder **„öffentliche Auftraggeber"** im Sinn des Vergaberechts zu verstehen sind.

Im Vergleich zur bestehenden Rechtslage stellt das neue Geldbußensystem eine deutliche Verschärfung dar. Ausgenommen sind nur Behörden und öffentliche Stellen.

Änderungen im Datenschutzgesetz

Ursprünglich war in Österreich geplant, ein gänzlich neues Datenschutzgesetz zu erlassen. Letztlich hat sich der Nationalrat aber nur auf eine umfassende Novellierung des bestehenden DSG 2000 (nunmehr mit Beschluss vom 29. 6. 2017 „DSG") geeinigt.

Im DSG werden nur jene Bereiche geregelt, die entweder außerhalb des Geltungsbereichs der DSGVO liegen (zB Datenverarbeitung für Zwecke der Sicherheitspolizei) oder Gegenstand sog **Öffnungsklauseln** sind. Dabei handelt es sich um Regelungsspielräume, die den Mitgliedstaaten von der DSGVO eröffnet werden. Im DSG wird von diesen Spielräumen nur vereinzelt Gebrauch gemacht, so zB mit der oben beschriebenen Klarstellung, dass Geldbußen auch gegen juristische Personen verhängt werden können. Die anderen Öffnungsklauseln sollen nach den Erläuternden Bemerkungen zum DSG – soweit erforderlich – in den spezifischen Materiengesetzen geregelt werden.

Das DSG wird für den Gesundheits- und Sozialbereich nur eine begleitende Rolle spielen. Entscheidende Bedeutung kommt der unmittelbar anwendbaren DSGVO zu.

Abgesehen von der Klarstellung zu Geldbußen dürften die Regelungen im DSG für die Heim- und Pflegepraxis von untergeordneter Bedeutung sein bzw sind diese im Kern unverändert geblieben (etwa in Bezug auf die Datenverarbeitung zum Zweck der wissenschaftlichen Forschung und Statistik, hinsichtlich der Verarbeitung strafrelevanter Daten oder in Bezug auf die Videoüberwachung).

ÖZPR 2017/59

[5] Dazu auch *Pilgermair*, Kinder im Spannungsfeld des Grundrechts auf Datenschutz, in *Loderbauer* (Hrsg), Kinder- und Jugendrecht[5] (2016) 451 ff. [6] Die DSGVO sieht die Grenze bei 16 Jahren, überlässt es aber den Mitgliedstaaten, eine niedrigere Grenze festzulegen. Österreich hat davon Gebrauch gemacht und die Grenze an die mündigen Minderjährigen im Sinne des ABGB angepasst. Vgl dazu auch *Pilgermair*, Datenschutz-Grundverordnung: Der neue Kinderschutz, Dako 2017, 7. [7] Zu diesen neuen Mitteilungs- und Informationspflichten siehe Teil 2 und 3 dieser Beitragsserie (FN 1). [8] Zu Compliance-Maßnahmen siehe Teil 2 und 3 dieser Beitragsserie (FN 1).