Die Datenschutz-Grundverordnung in Krankenanstalten

Die fortschreitende Digitalisierung und Vernetzung erleichtert die Verarbeitung von Gesundheitsdaten nicht nur, sie geht auch mit zahlreichen Pflichten einher, die durch die Europäische Datenschutz-Grundverordnung („DSGVO") weitere Verschärfungen erfahren.

Gerald Ganzger, Amra Bajraktarevic

Im Gesundheitsbereich herrschte aufgrund des nationalen Datenschutzgesetzes sowie zahlreicher Nebengesetze, wie etwa des Gesundheitstelematikgesetzes, schon bisher ein sehr hohes Datenschutzniveau. Diese Bestimmungen werden durch die DSGVO nicht nur verschärft. Die DSGVO stärkt auch Betroffenenrechte und überbindet damit Verantwortlichen eine ganze Reihe von neuen Pflichten, die ab ihrem Inkrafttreten am 25. Mai 2018 einzuhalten sind. Jeder Verantwortliche, der personenbezogene Daten verarbeiten will, hat sich daher zwingend die Frage zu stellen, welche Anforderungen er zu erfüllen hat, um die Datenverarbeitung rechtskonform durchzuführen.

Was sind personenbezogene Daten?

Nach der Definition der DSGVO handelt es sich bei personenbezogenen Daten um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Es werden daher nicht nur Daten mit einem offensichtlichen Personenbezug geschützt, sondern insbesondere auch solche, bei denen eine Person mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer oder einem oder mehreren besonderen Merkmalen identifiziert werden kann. Daraus folgt, dass auch Kundennummern, Patientennummern, KFZ-Kennzeichen, aber auch die Sozialversicherungsnummer dem Regime der DSGVO unterliegen. Anders als das nationale Datenschutzgesetz, das aufgrund einer Verfassungsbestimmung nach wie vor auch die Daten juristischer Personen schützt, unterwirft die DSGVO nur Daten natürlicher Personen ihrem Anwendungsbereich. Ob der nationale Gesetzgeber diesen Widerspruch bis zum 25. Mai 2018 saniert, bleibt abzuwarten.

Unter welchen Voraussetzungen dürfen personenbezogene Daten verarbeitet werden?

Die DSGVO setzt bei jeder Datenverarbeitung die Einhaltung der nachstehenden Grundsätze voraus:

1. Die Datenverarbeitung erfolgt auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise (Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz).
2. Die Daten werden für festgelegte, eindeutige und legitime Zwecke erhoben und dürfen nur in einer mit dem Zweck vereinbarenden Weise weiterverarbeitet werden (Grundsatz der Zweckbindung).
3. Die Verarbeitung ist angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt (Grundsatz der Datenminimierung).
4. Sie ist sachlich richtig und erforderlichenfalls auf dem neuesten Stand (Grundsatz der Richtigkeit).
5. Die Daten werden in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Verarbeitungszwecke erforderlich ist (Grundsatz der Speicherbegrenzung).
6. Die Daten werden in einer Weise verarbeitet, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet (Grundsatz der Integrität und Vertraulichkeit).

Nach dem Grundsatz der Rechtmäßigkeit ist sohin jegliche Verarbeitung personenbezogener Daten grundsätzlich unzulässig, es sei denn, es liegt einer der in der DSGVO abschließend geregelten Ausnahmetatbestände vor („Verbot mit Ausnahmen"). Welche Rechtsgrundlage im konkreten Fall herangezogen werden kann, hängt von der Art der Daten ab. So gilt im Zusammenhang mit der Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten anderes, als bei der Verarbeitung sogenannter „sensibler" Daten, also genetischer und biometrischer Daten sowie solcher betreffend die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, das Sexualleben, die sexuelle Orientierung und von Gesundheitsdaten. Gerade letztere fallen im Gesundheitsbereich schon aufgrund der gesetzlichen Vorschriften zur Führung einer Krankengeschichte regelmäßig an, dürfen aber nur unter den ganz eingeschränkten Voraussetzungen des Art 9 DSGVO verarbeitet werden.

Verarbeitung von Gesundheitsdaten: Als Rechtsgrundlage bietet sich hier zunächst die ausdrückliche Einwilligung der betroffenen Person an. Diese ist jedoch in jeder Hinsicht an strenge Voraussetzungen geknüpft. Insbesondere muss diese freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich erfolgen und klar erkennen lassen, welche personenbezogenen Daten zu welchem Zweck verarbeitet werden, an

wen die Daten weitergegeben werden dürfen und wie lange die Nutzung andauert. Zur Erfüllung der geforderten Transparenz und Informiertheit des Patienten muss die Einwilligungserklärung daher verständlich und möglichst ohne technisches oder fremdsprachliches Fachvokabular abgefasst sein, da sie sonst unwirksam ist. Zudem muss der betroffenen Person auch eine jederzeitige Widerrufsmöglichkeit eingeräumt werden. Das Risiko, diesen Voraussetzungen nicht zu genügen, ist umso höher, je unklarer und unkonkreter die Einwilligungserklärung formuliert ist. Rechtliche Folge desselben ist, dass die Zustimmung den Bedingungen der DSGVO nicht standhält.

Da eine Einholung einer Einwilligung in bestimmten Fällen nicht möglich ist, ist die Verarbeitung auch dann gestattet, wenn dies dem Schutz lebenswichtiger Interessen des Betroffenen dient. Dies setzt jedoch voraus, dass es dem Patienten aus körperlichen oder rechtlichen Gründen, wie etwa bei einer Bewusstlosigkeit, nicht möglich ist, seine Einwilligung zu erteilen.

Am praktisch relevantesten ist die Ausnahmebestimmung des Art 9 Abs 2 lit h DSGVO. Demnach ist die Verarbeitung von sensiblen Daten dann zulässig, wenn dies 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 erforderlich ist und auf einer nationalen oder unionsrechtlichen Bestimmung basiert oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs notwendig ist. In jedem Fall darf die Verarbeitung der Daten nur von Fachpersonal oder unter dessen Verantwortung erfolgen, welches einem Berufsgeheimnis bzw. einer gesetzlichen Geheimhaltungspflicht unterliegt. Damit ist nicht nur der ärztliche Behandlungsvertrag privilegiert. Auch die landesrechtlichen Krankenanstaltengesetze ermöglichen die Verarbeitung.

Welche neuen Pflichten treffen den Verantwortlichen?

Eigenverantwortlichkeit: Eine ganz wesentliche Neuerung der DSGVO ist, dass sie dem Verantwortlichen ein hohes Maß an Eigenverantwortlichkeit abverlangt. Der Verantwortliche muss künftig daher nicht nur selbst einschätzen, ob die Verarbeitung der Daten rechtskonform ist. Es treffen ihn auch zahlreiche Informations- und Dokumentationspflichten, die der Verantwortliche in Eigenregie zu erfüllen hat.

Transparenz: Um dem Transparenzgebot genüge zu tun, muss der Verantwortliche die betroffene Person schon bei der Erhebung der Daten umfänglich über die Datenverarbeitungsvorgänge informieren. Dabei reicht es nicht nur aufzuzählen, welche Daten verarbeitet werden. Es sind auch die Zwecke der Datenverarbeitung sowie die entsprechende Rechtsgrundlage zu nennen. Darüber hinaus muss die betroffene Person auch über ihre Rechte informiert werden.

Diese wurden durch die DSGVO ausgeweitet und gestärkt. Nach der aktuellen Rechtslage hatten Betroffene zwar schon ein Auskunfts-, Berichtigungs- und Löschungsrecht sowie ein Widerspruchsrecht, allerdings war die Ausübung dieser Rechte bislang an diverse Voraussetzungen geknüpft und der Verantwortliche hatte in der Regel acht Wochen Zeit, diese zu erfüllen. Die DSGVO lockert diese Voraussetzungen und verkürzt die Reaktionszeiten erheblich. Mit Inkrafttreten der DSGVO können Betroffene nämlich formfrei, also auch mündlich, ein Auskunfts- bzw Berichtigungsbegehren stellen. Ihre Identität müssen sie dabei nicht mehr aktiv, sondern nur in Zweifelsfällen nachweisen. Zumal dies im Gesundheitsbereich das Risiko eröffnet, dass Dritte unbefugt Auskunft über sensible Daten einer betroffenen Person erhalten könnten, erscheint die Einholung eines Identitätsnachweises jedenfalls gerechtfertigt, wenn nicht sogar erforderlich.

Liegt ein entsprechender Betroffenenantrag vor, hat der Verantwortliche unverzüglich bzw. binnen eines Monats Auskunft zu erteilen. Zusätzlich muss er über die schon bisher zu erteilenden Informationen hinaus insbesondere auch über den Zweck der Verarbeitung, die Speicherdauer der Daten und die weiteren Betroffenenrechte Auskunft erteilen. Dem nicht genug, führt die DSGVO auch folgende neue Rechte ein:

- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht bei einwilligungsloser Verarbeitung zur Wahrung berechtigter Interessen
- Recht auf Unbetroffenheit von rechtsverbindlichen Entscheidungen mit Grundlage in automatisierten Datenprozessen

Das Recht auf Einschränkung der Verarbeitung trägt dabei dem Gedanken Rechnung, dass eine sofortige Löschung von Daten nicht immer umsetzbar ist, weil sie etwa Interessen des Betroffenen selbst zuwiderlaufen würde. Dies ist etwa dann der Fall, wenn der Zweck der Datenverarbeitung erreicht wurde und der Verantwortliche die personenbezogenen Daten nicht mehr benötigt, der Betroffene sie jedoch für die Geltendmachung von Rechten braucht. Künftig kann der Betroffene daher unter bestimmten Voraussetzungen verlangen, dass sämtliche erhobene personenbezogene Daten fortan nur mit individueller Einwilligung verarbeitet werden dürfen. Liegt diese nicht vor, dann wäre die Verarbeitung nur zur Ausübung, Verteidigung oder Geltendmachung von Rechtsansprüchen, zum Schutz der Rechte einer anderen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Europäischen Union oder eines Mitglieds-

staates zulässig. Fehlt es an einer derartigen Ausnahme, dann darf der Verantwortliche die Daten zwar weiterhin speichern, aber nicht wie bisher verwenden.

Mit dem Recht auf Datenübertragbarkeit erhält die betroffene Person erstmals die Möglichkeit, ihre personenbezogenen Daten von einem Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese, ohne Behinderung durch den Verantwortlichen, an einen anderen Verantwortlichen übertragen zu können. Durch dieses Recht soll einerseits eine bessere persönliche Überwachung und Kontrolle gewährleistet werden. Andererseits soll die Weiterleitung von einmal erhobenen Daten an einen Dritten vereinfacht werden. Für einen Verantwortlichen bedeutet dies in erster Linie, dass er Daten in ein Format bringen muss, das eine reibungslose Datenübertragbarkeit ermöglicht.

Zu beachten ist jedoch, dass das Recht auf Datenübertragbarkeit nur dann zusteht, wenn die Verarbeitung mithilfe automatisierter Verfahren erfolgt und auf einer Einwilligung oder einer Vertragsbeziehung nach Art 6 Abs 1 DSGVO beruht. In Bezug auf sensible Daten kommt daher nur die Einwilligung in Frage, da der Behandlungsvertrag des Art 9 DSGVO nicht in der Aufzählung des Art 20 Abs 1 DSGVO enthalten ist.

Abgesehen von der Informationspflicht muss der Verantwortliche auch ein Verzeichnis der Verarbeitungstätigkeiten führen, in dem er nicht nur die Zwecke der Verarbeitung dokumentiert, sondern insbesondere auch die Kategorien der betroffenen Personen, der personenbezogenen Daten sowie deren Empfänger dokumentiert. Wiewohl die DSGVO im Zusammenhang mit dieser Verpflichtung kleinere Unternehmen mit weniger als 250 Mitarbeitern privilegiert, kommt diese Ausnahmebestimmung aufgrund der Gegenausnahme des Art 30 Abs 5 DSGVO dann nicht zur Anwendung, wenn sensible Daten verarbeitet werden. Gesundheitsbetriebe sind unabhängig von ihrer Größe jedenfalls zur Führung dieses Verzeichnisses verpflichtet und haben dieses der Behörde auf Anfrage zur Verfügung zu stellen.

Datenschutz-Folgenabschätzung: Eine weitere Pflicht bürdet der Art 35 DSGVO auf: Nach dieser Bestimmung haben Verantwortliche, insbesondere bei der umfangreichen Verarbeitung sensibler Daten, eine Datenschutz-Folgenabschätzung durchzuführen und darin im Wesentlichen die geplanten Verarbeitungsvorgänge und die Zwecke der Verarbeitung zu beschreiben, die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck sowie die Risiken für die Rechte und Freiheiten der betroffenen Personen zu bewerten und die geplanten Abhilfemaßnahmen zur Bewältigung der Risiken darzustellen. Bei diesem Vorhaben kann sich der Verantwortliche durch einen Datenschutzbeauftragten („DSB“) beraten lassen.

Datenschutzbeauftragter: Dieser ist nach Art 37 Z 1 lit c DSGVO insbesondere dann obligatorisch, wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung sensibler Daten besteht. Wiewohl die Kerntätigkeit einer Krankenanstalt regelmäßig nicht in der Datenverarbeitung liegt, werden dennoch sämtliche Tätigkeiten hinzugezählt, bei denen die Verarbeitung von Daten einen untrennbaren Bestandteil der Tätigkeit des Verantwortlichen darstellt. Die Verarbeitung von gesundheitsbezogenen Daten, wie z.B. von Krankenakten von Patienten, wird daher als Kerntätigkeit jedes Krankenhauses angesehen. Nach herrschender Ansicht ist bei Krankenhäusern auch die weitere Voraussetzung der umfangreichen Verarbeitung erfüllt, während dies bei der Verarbeitung durch einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufes nicht der Fall sein soll. Im Ergebnis stellt die Verarbeitung von Patientendaten im gewöhnlichen Geschäftsbetrieb eines Krankenhauses daher umfangreiche Verarbeitungen iSd Art 37 DSGVO dar und Krankenhäuser haben zwingend einen DSB zu bestellen, um ihren aus der DSGVO erfließenden Verpflichtungen nachkommen zu können. ::

Dr. Gerald Ganzger
Rechtsanwalt und Managing Partner bei Lansky, Ganzger + partner, Wien
office@lansky.at

Mag. Ing.
Amra Bajraktarevic
Rechtsanwalts-anwärterin bei Lansky, Ganzger + partner, Wien
bajraktarevic@lansky.at