5 Jahre DSGVO

# Die Datenschutz-Grundverordnung *im Gesundheitswesen*

Autorin: C. Czeschik

## Was war vor der DSGVO?

Ein kleiner Rückblick: In Deutschland wurde der Datenschutz schon lange vergleichsweise wichtig genommen. Seit 1977 gibt es das Bundesdatenschutzgesetz. 1983 wurde im sogenannten Volkszählungsurteil das Recht auf Informationelle Selbstbestimmung in der Rechtsprechung verankert. Hier hatten Bürgerrechtlerinnen und Bürgerrechtler dagegen geklagt, dass bei der Volkszählung detaillierte Informationen über die Lebensverhältnisse der Deutschen erhoben und verarbeitet werden sollten.

Bis 2018 wurde der Datenschutz in Deutschland vor allem durch das bereits erwähnte Bundesdatenschutzgesetz (BDSG) sowie die Datenschutzgesetze der Länder geregelt. Relevant für das Gesundheitswesen waren und sind außerdem die Datenschutzgesetze der beiden großen Kirchen in Deutschland, da diese als Träger von Krankenhäusern fungieren und deren Patientinnen und Patienten wie auch Mitarbeitende somit unter diese Datenschutzgesetze fallen. Zudem gab und gibt es zahlreiche andere Gesetze, die den Datenschutz im Gesundheitswesen berühren, etwa das Strafgesetzbuch (StGB), in dem beispielsweise im § 203 die ärztliche Schweigepflicht und die Schweigepflicht anderer Berufsgruppen verankert sind.

## DSGVO: unmittelbar gültig

Am 25.05.2018 kam dann die Datenschutz-Grundverordnung (DSGVO) hinzu. Diese wurde in Deutschland und den anderen Mitgliedsstaaten der EU unmittelbar gültig, weil es sich um eine Verordnung handelt. Anders ist es etwa bei EU-Richtlinien: Diese müssen erst in nationales Recht umgesetzt werden. Nicht so die DSGVO – ihre Vorschriften sind seit 2018 direkt anwendbar. Das bedeutet allerdings nicht, dass das BDSG und andere nationale Gesetze überflüssig geworden sind. Diese gelten weiterhin und sind dort notwendig, wo die DSGVO keine konkreten Regelungen enthält oder sogar sogenannte Öffnungsklauseln: Dies sind festgelegte Bereiche, in denen die Mitgliedsstaaten der EU ihre eigenen gesetzlichen Regelungen treffen sollen.

Ein Beispiel einer solchen Regelung infolge einer Öffnungsklausel: In Deutschland müssen nach § 28 BDSG solche Unternehmen einen Datenschutzbeauftragten stellen, in denen „in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt" sind. Diese Regelung fällt in anderen Mitgliedsstaaten anders aus.

Auch, dass der Datenschutz in kirchlichen Krankenhäusern und anderen kirchlichen Organisationen weiterhin von den Kirchen selbst geregelt werden darf, ist Folge einer DSGVO-Öffnungsklausel, und zwar des Artikels 91 DSGVO. Dieser besagt, dass kirchliche Datenschutzgesetze weiter angewandt werden dürfen, wenn sie beim Inkrafttreten der DSGVO schon bestanden. Diese Gesetze sind das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) sowie das Gesetz über den Kirchlichen Datenschutz (KDG) der katholischen Kirche.

>> Für eilige Leser

Vor nun etwas über fünf Jahren ist sie in Kraft getreten: die europäische Datenschutz-Grundverordnung (DSGVO). Grund genug, sie noch einmal anzuschauen: Was steht eigentlich drin – und was davon ist Realität geworden? Welche Hoffnungen und Befürchtungen der verschiedenen Stakeholder haben sich erfüllt und welche nicht?

## Identifizierte oder identifizierbare natürliche Personen

In der DSGVO geht es stets um den Schutz von personenbezogenen Daten – nicht von Geschäftsgeheimnissen oder anderen vertraulichen Daten, die sich nicht auf Personen beziehen. Diese sind an anderen Stellen gesetzlich geregelt.

Die DSGVO definiert auch, was genau unter „personenbezogenen" Daten zu verstehen ist, und zwar – nach Art. 4 Nr. 1 DSGVO – Daten, die sich auf eine „identifizierte oder identifizierbare natürliche Person" beziehen. Mit dieser Formulierung weist die DSGVO darauf hin, dass die Pseudonymisierung von Daten kein Freifahrtschein ist. Auch personenbezogene Daten, die pseudonymisiert sind, können gegebenenfalls auf eine bestimmte Person zurückgeführt werden, indem das Pseudonym aufgelöst wird oder Informationen aus verschiedenen Quellen zusammengeführt werden. Dagegen können Daten, die zuverlässig anonymisiert sind, ohne die in der DSGVO festgelegten Beschränkungen verarbeitet werden. Was tatsächlich eine zuverlässige Anonymisierung darstellt, ohne Gefahr der Re-Identifizierung von natürlichen Personen, ist auch abhängig vom Stand der Technik.

## Grundsätze des Datenschutzes nach DSGVO

Die DSGVO hat zwar keine besondere Detailtiefe und lässt viele Zweifelsfragen offen, auch außerhalb der Öffnungsklauseln.

Dafür zeichnet sie sich aber durch klare Formulierungen und nachvollziehbare Begründungen aus, letztere in den sogenannten Erwägungsgründen, die ein Anhang zur eigentlichen DSGVO sind. In diesen wird häufig der Sinn von Regelungen näher erläutert und so eine Hilfestellung zur Auslegung der DSGVO gegeben.

Die DSGVO legt in Art. 5 die Grundsätze der Datenverarbeitung fest:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz: Die Datenverarbeitung muss in einer rechtmäßigen und für die betroffene Person nachvollziehbaren Art und Weise erfolgen.
- Zweckbindung: Die Erhebung der Daten muss für festgelegte, eindeutige und legitime Zwecke erfolgen. Eine Weiterverarbeitung darf nicht zu Zwecken erfolgen, die von diesen legitimierten Zwecken abweichen.
- Datenminimierung, Datensparsamkeit: Die erhobenen Daten müssen dem jeweiligen Zweck angemessen sein. Es dürfen nur solche Daten erhoben werden, die für die Zweckerfüllung notwendig sind.
- Richtigkeit: Die erhobenen Daten müssen sachlich richtig sein. Es müssen angemessene Maßnahmen getroffen werden, damit falsche Daten erkannt und berichtigt werden können.
- Speicherbegrenzung: Die erhobenen Daten dürfen nur so lange gespeichert werden, wie der Zweck es erforderlich macht und die gesetzliche Grundlage es erlaubt. In diesem Zusammenhang ist auch manchmal vom „Recht auf Vergessen" die Rede – das aber so nicht in der DSGVO festgeschrieben ist.
- Integrität und Vertraulichkeit: Die erhobenen Daten müssen sicher verarbeitet werden, also so, dass unbefugter Zugriff, Zerstörung oder andere Eingriffe mit angemessener Sicherheit verhindert werden.

Diese Grundsätze können auch unabhängig von konkreten gesetzlichen Regelungen als vernünftige Maßstäbe für den Umgang mit personenbezogenen Daten, auch in einer digitalisierten Welt, gelten.

## Besondere Kategorien von personenbezogenen Daten

Die DSGVO definiert in Artikel 9 sogenannte „besondere Kategorien" von personenbezogenen Daten. Besondere Kategorien sind nach Art. 9 DSGVO:

- Daten, aus denen ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit hervorgehen
- genetische Daten
- biometrische Daten
- Daten zum Sexualleben oder der sexuellen Orientierung
- Gesundheitsdaten

Hier wird klar, dass im Gesundheitswesen nicht nur Gesundheitsdaten als besondere Kategorie verarbeitet werden, sondern auch andere aus dieser Auflistung. Die Verarbeitung von Daten aus besonderen Kategorien ist zwar prinzipiell verboten – es werden aber im selben Artikel direkt zahlreiche Ausnahmen und Öffnungsklauseln formuliert. Unter anderem zählt dazu natürlich die Möglichkeit der Einwilligung des Betroffenen in die Verarbeitung.

Die anderen Erlaubnistatbestände werden aber in der Praxis oft zu wenig beachtet. So besagt Art. 9 unter anderem, dass „die Verarbeitung […] 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" auch für besondere Kategorien erlaubt ist – also auch ohne explizite vorherige Einwilligung. Voraussetzung ist lediglich, dass die Verarbeitung durch Fachpersonal erfolgt, das einem Berufsgeheimnis unterliegt.

## TOM dürfen wirtschaftlich sinnvoll bleiben

Ein weiterer wichtiger Begriff der DSGVO (und der früheren Datenschutz-Gesetzgebung): die technischen und organisatorischen Maßnahmen, kurz TOM. Diese bezeichnen die konkreten Maßnahmen, mit denen die Informationssicherheit gewährleistet wird – von der verschlossenen Tür über die Firewall bis hin zum Berechtigungsmanagement im IT-System.

TOM sind in Art. 25 der DSGVO geregelt und in Erwägungsgrund 78 näher erläutert. Insbesondere regt die DSGVO an, schon beim Entwurf eines Systems den Datenschutz zu berücksichtigen statt hinterher nur nachzurüsten, also „data protection by design" und datenschutzfreundliche Voreinstellungen, „data protection by default", anzustreben.

Ausdrücklich dürfen bei der Planung und Umsetzung von TOM aber auch die Implementierungskosten mit berücksichtigt werden und ob diese in einem sinnvollen Verhältnis zur „unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen" stehen. Mit anderen Worten müssen TOM nicht unendlich aufwendig werden, sondern dürfen wirtschaftlich angemessen bleiben. Zertifizierungen (geregelt in Art. 42) sind sinnvoll, um die Einhaltung des Art. 25 zu belegen.

## Welche Bußgelder gab es bisher?

Große Wellen geschlagen hat zur Einführung der DSGVO vor fünf Jahren der im Vergleich zum alten BDSG deutlich erhöhte Bußgeldrahmen für Verstöße. Und zwar beträgt dieser bis zu 20 Millionen Euro oder bis zu 4% des Jahresumsatzes des Unternehmens – je nachdem, welcher Betrag höher ist.

Und tatsächlich sind Bußgelder in der ganzen EU verhängt worden. Auch in schmerzhafter Höhe, auch im Gesundheitswesen. Konkret gibt es verschiedene Online-Quellen, in denen man nach bisher verhängten Bußgeldern recherchieren kann, beispielsweise: https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank. Hier zeigt sich, dass das höchste bisher im deutschen Gesundheitswesen verhängte Bußgeld, 1.240.000 EUR, die AOK Baden-Württemberg betraf, und zwar wegen der unrechtmäßigen Verwendung der Daten von Gewinnspiel-Teilnehmenden zu Werbezwecken. Das war im Jahr 2020.

## Bußgelder bei mangelndem Schutz von Patientendaten

Die Mainzer Universitätsmedizin wurde 2019 wegen einer Patientenverwechslung zu einem Bußgeld von knapp über 100.000 EUR verurteilt, ein anderer, nicht näher bezeichneter Betrieb im Gesundheitswesen im Jahr 2022 zu ebenfalls knapp über 105.000 EUR wegen wiederholten Falschversandes von

Arztbriefen und fehlender Protokollierung des Zugriffs auf Patientendaten. Ansonsten blieben die wenigen Fälle von Bußgeldern im deutschen Gesundheitswesen unter 100.000 EUR – darunter auch der Fall, in dem sensible Gesundheitsdaten im Internet veröffentlicht wurden und die zuständige Datenschutzbehörde nicht preisgeben wollte, um welches Unternehmen es sich handelte, um die Betroffenen so weit wie möglich zu schützen.

In anderen EU-Ländern wurden Krankenhäuser schon zu beträchtlichen Bußgeldern von mehreren 100.000 EUR verurteilt, unter anderem in Schweden, Norwegen und den Niederlanden. Ursache dieser hohen Bußgelder waren häufig Mängel im Berechtigungsmanagement und andere Versäumnisse beim Schutz von Patientendaten in der Krankenhaus-IT.

Im Bereich der Gesundheitsapps kam es bisher nicht zu aufsehenerregenden Bußgeldern, wobei allerdings Behörden nicht in allen Fällen von Bußgeldern das betroffene Unternehmen offenlegen, wie im oben genannten Beispiel. Bekannt wurde aber, dass 2022 ein italienisches Gesundheitsapp-Unternehmen zu einem Bußgeld von 45.000 EUR verurteilt wurde. Der Grund war allerdings fast altmodisch: Man hatte versehentlich eine E-Mail an einen offenen Verteilerkreis von 2000 Kunden versandt.

Auch Schadensersatz kann bei DSGVO-Verstößen fällig werden. Allerdings wurde in einem EuGH-Urteil vom 4. Mai 2023 festgelegt, dass Schadensersatz in Zukunft nur dann gezahlt werden muss, wenn tatsächlich ein Schaden für den Betroffenen eingetreten ist. „Unwohlsein" angesichts eines Datenschutzverstoßes genügt nicht mehr als Grundlage, um ein Unternehmen zur Zahlung von Schadensersatz zu verpflichten.

**Dokumentation:** C. Czeschik. Die Datenschutz-Grundverordnung im Gesundheitswesen. mt | medizintechnik 143 (2023), Nr. 6, S. 7

**Schlagwörter:** Datenschutz, Datenschutz-Grundverordnung (DSGVO), personenbezogene Daten, Technische und organisatorische Maßnahmen (TOM), Bußgeld

**Autorin**

Dr. med.
Christina Czeschik

Ärztin und Medizininformatikerin
E-Mail: czeschik@serapion.de
Web: www.serapion.de