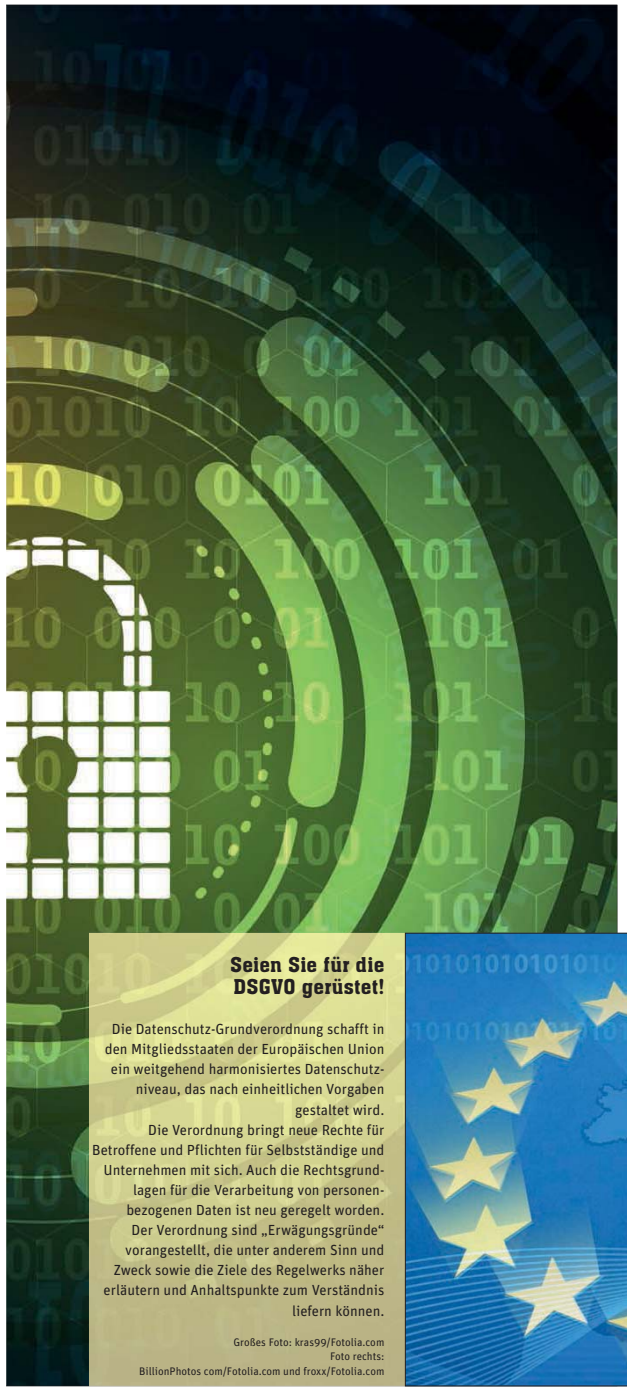

Der Datenschutz wird europäisch

Am Freitag, 25. Mai 2018 ist es soweit: Die Datenschutz-Grundverordnung der Europäischen Union wird scharf geschaltet. Die Verordnung bringt für Unternehmen, wie auch für Arztpraxen und Kliniken, die personenbezogene Daten verarbeiten, einige Neuerungen mit sich. Bei Nichteinhaltung der Vorgaben drohen empfindliche Bußen.

von Jürgen Brenn

Weihnachten kommt jedes Jahr plötzlich und unerwartet. Das behaupten zumindest viele Spötter. Das Gleiche wird derzeit der *Datenschutz-Grundverordnung der Europäischen Union* (2016/679), kurz *DSGVO*, nachgesagt. Die Verordnung, die nicht wie eine EU-Richtlinie in nationales Gesetz gegossen werden muss, wurde am 4. Mai 2016 im Amtsblatt der EU veröffentlicht, trat am 25. Mai 2016 in Kraft und gilt verbindlich und „unmittelbar in jedem Mitgliedstaat“ ab dem 25. Mai 2018.

Seien Sie für die DSGVO gerüstet!

Die Datenschutz-Grundverordnung schafft in den Mitgliedsstaaten der Europäischen Union ein weitgehend harmonisiertes Datenschutzniveau, das nach einheitlichen Vorgaben gestaltet wird.
Die Verordnung bringt neue Rechte für Betroffene und Pflichten für Selbstständige und Unternehmen mit sich. Auch die Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten ist neu geregelt worden. Der Verordnung sind „Erwägungsgründe“ vorangestellt, die unter anderem Sinn und Zweck sowie die Ziele des Regelwerks näher erläutern und Anhaltspunkte zum Verständnis liefern können.

Großes Foto: kras99/Fotolia.com
Foto rechts:
BillionPhotos com/Fotolia.com und froxx/Fotolia.com

Die Verordnung setzt den unterschiedlichen staatlichen Datenschutzbestimmungen in den einzelnen EU-Mitgliedstaaten ein Ende. Sie formuliert einheitliche Spielregeln „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“, wie es in *Artikel 2* heißt. Der Kreis der Selbstständigen und Unternehmen, die von den Regelungen erfasst werden, ist bewusst weit gehalten. Die Verordnung wird angewendet auf die Verarbeitung personenbezogener Daten, „soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet“ *(Artikel 3 DSGVO)*. Damit müssen sich auch Unternehmen wie etwa Google oder Facebook sowie Dienstleister, die ihre Server außerhalb der EU betreiben, an die Vorgaben der *DSGVO* halten.

Arztpraxen und Kliniken sind gleichermaßen betroffen

Die Frage, ob niedergelassene Ärztinnen und Ärzte von den neuen Regeln betroffen sind, kann folglich mit Ja beantwortet werden. Denn es fallen an vielen Stellen personenbezogene Daten an, von den Patientendaten über Ausbildungs- oder Arbeitsverträge bis zur Lohnabrechnung aller Beschäftigten etwa durch einen Dienstleister (Auftragsverarbeitung). Auch Betreiber von Homepages, die ein Statistik-Tool nutzen (Nutzertracking), einen Newsletter anbieten oder eine elektronische Terminvergabe über ihre Webseite anbieten, haben sich an die neuen Spielregeln zu halten. Auch die Datenschutzerklärung auf der Praxis-Homepage muss angepasst werden *(siehe Interview auf S. 20)*.

Da das *Bundesdatenschutzgesetz* schon bisher strenge Vorgaben beinhaltete, krempelt die EU-Verordnung den Umgang mit Daten in Deutschland nicht komplett um. Dennoch sind zahlreiche Punkte zu beachten. Die *DSGVO* hat der deutsche Gesetzgeber mit dem neuen *Bundesdatenschutzgesetz (BDSG neu)* ergänzt. Das Hauptaugenmerk liegt allerdings auf der *DSGVO*. Da hohe Bußgelder bei Nichtbeachtung der Verordnung drohen, sollten Ärztinnen und Ärzte die Umsetzung der neuen Maßgaben nicht auf die lange Bank schieben, sondern die neuen Regeln bis zum Stichtag zumindest auf der Praxishomepage implementiert haben.

Folgende Themen können unterschieden werden: Die *DSGVO* regelt die Rechtsgrundlagen der Datenverarbeitung, die Rechte Betroffener und die Pflichten der Verantwortlichen.

Rechtsgrundlagen der Datenverarbeitung

Hier ändert sich in Deutschland nicht sehr viel. Bereits jetzt gilt bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten das Verbot mit Erlaubnisvorbehalt. Das besagt, dass die Daten verarbeitet werden dürfen, wenn die betroffene Person ausdrücklich eingewilligt hat oder eine gesetzliche Grundlage besteht. Auch die Grundsätze der Datensparsamkeit, der Zweckbindung und der Datenrichtigkeit kannte das bisherige Recht bereits. Ausdrücklich erwähnt werden Gesundheitsdaten, die verarbeitet werden dürfen „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“. Diese Daten dürfen von Fachpersonal oder anderen Personen unter dessen Verantwortung verarbeitet werden, wenn diese dem Berufsgeheimnis (Schweigepflicht) unterliegen *(Artikel 9 DSGVO)*.

Neu führt die *DSGVO* in *Artikel 32* den Grundsatz der Datensicherheit ein: „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Das bedeutet, welche Maßnahmen konkret an welcher Stelle ergriffen werden müssen, orientiert sich an der Schutzbedürftigkeit der Daten, dem Stand der Technik, den Kosten und den weiteren Umständen. Die Schutzbedürftigkeit von Gesundheitsdaten ist gewiss höher anzusehen als beispielsweise eine E-Mail-Adresse für einen Newsletter-Bezug.

Die Rechte Betroffener

Ebenfalls neu ist für Verbraucher und Internetnutzer das „Recht auf Vergessenwerden“. Insbesondere gegenüber Suchmaschinen ist ein solches Recht vom Europäischen Gerichtshof bereits in der Vergangenheit bestätigt worden. Die Verordnung schreibt dieses Recht nun in *Artikel 17* fest. Die Daten sind auf Verlangen der betroffenen Person zu löschen, wenn der Zweck, für den die Daten erhoben wurden, erfüllt ist und die Daten nicht mehr notwendig sind, der Betroffene seine Einwilligung widerruft oder die Daten unrechtmäßig verarbeitet wurden. Das Recht auf Vergessenwerden spielt insbesondere im Internet und speziell in sozialen Netzwerken und Suchmaschinen eine wichtige Rolle.

Ebenfalls neu ist das Recht auf Datenübertragbarkeit (Datenportabilität), das *Artikel 20* regelt. Danach haben Betroffene das Recht, ihre Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“, von einem Datenverarbeiter zu einem anderen zu übermitteln oder direkt übermitteln zu lassen. Dieses Recht beschränkt sich auf Daten, die nach Einwilligung oder Vertrag erhoben wurden und

deren Verarbeitung automatisiert erfolgt. Als Beispiel wäre etwa der Umzug von einem sozialen Netzwerk zu einem anderen zu nennen.

Fühlt sich eine Person bezüglich der Verarbeitung ihrer personenbezogenen Daten falsch behandelt, kann Beschwerde eingelegt werden. Betroffene wenden sich stets an die Datenschutzbehörde des eigenen Landes, unabhängig davon, wo der Datenschutzverstoß begangen worden sein soll *(Artikel 77)*.

Pflichten der Verantwortlichen

Unternehmer wie Ärztinnen und Ärzte in eigener Praxis oder als Teil einer anderen Praxisform sind gut beraten, die aus der *DSGVO* erwachsenen Pflichten zügig umzusetzen, denn es drohen nicht nur Schadenersatzansprüche der betroffenen Personen, sondern auch empfindliche Bußgelder. Diese können bis zu 20 Millionen Euro betragen oder vier Prozent des weltweiten Jahresumsatzes des Unternehmens, das gegen die Vorschriften der *DSGVO* verstoßen hat. Denn die Buße soll ausdrücklich „wirksam, verhältnismäßig und abschreckend" sein *(Artikel 82 und 83)*.

Die Verordnung verpflichtet diejenigen, die personenbezogene Daten erheben und verarbeiten, nicht nur dazu, nach den oben beschriebenen Grundsätzen zu handeln, sondern auch dazu, die Einhaltung der Prinzipien auf Aufforderung nachzuweisen. *Artikel 5 DSGVO* spricht von „Rechenschaftspflicht". Dies bedeutet, dass sich in Zukunft ein effektives Datenschutzmanagement empfiehlt, das der Nachweis- und Dokumentationspflicht genügt.

Zur Rechenschaftspflicht gehört auch, dass ein „Verzeichnis von Verarbeitungstätigkeiten" geführt werden muss *(Artikel 30 DSGVO)*. Der Artikel listet genau die Angaben auf, die dieses Verzeichnis zu enthalten hat. Zwar sieht der Artikel Ausnahmen für Unternehmen mit weniger als 250 Beschäftigte vor, allerdings nur, wenn beispielsweise keine besonders sensiblen Daten verarbeitet werden, worunter allerdings Gesundheitsdaten fallen. Darüber hinaus verpflichtet die Verordnung nun auch sogenannte Auftragsverarbeiter, ein entsprechendes Verzeichnis zu führen. Auftragsverarbeiter kann zum Beispiel der Dienstleister sein, der die Lohnabrechnung für die Mitarbeiter der Praxis erledigt, Rechnungen im Auftrag des Arztes erstellt oder die Praxishomepage pflegt. Gegebenenfalls müssen bestehende Verträge an die neuen Erfordernisse angepasst werden.

Neuerungen für Homepagebetreiber

Wer eine Praxishomepage betreibt, sollte sich *Artikel 13 DSGVO* näher ansehen. Darin werden die Angaben aufgelistet, die eine Datenschutzerklärung zukünftig zu beinhalten hat, wenn personenbezogene Daten erhoben werden, was bereits dann der Fall ist, wenn ein Statistik-Tool eingesetzt wird. Zu den Angaben gehören unter anderem die Kontaktdaten des Verantwortlichen und – falls vorhanden – des Datenschutzbeauftragen, Zweck der Datenerhebung und ebenfalls neu, die Rechtsgrundlagen dafür. Zusätzlich werden neue Informationspflichten eingeführt wie etwa die Unterrichtung über das Recht auf Auskunft über die betreffenden personenbezogenen Daten sowie das Recht auf Löschung oder Einschränkung der Verarbeitung sowie das Recht auf Widerruf einer bereits gegebenen Einwilligung. Diese Informationen sind nach *Artikel 12 DSGVO* „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln".

Die *Datenschutz-Grundverordnung* sowie das flankierende *Bundesdatenschutzgesetz neu* bergen für Unternehmen, und damit auch für Arztpraxen und Kliniken, die mit personenbezogenen Daten arbeiten, einen nicht zu unterschätzenden Regelungsbedarf auf verschiedenen Ebenen. Deshalb sollten unter anderem die Prozesse der Datenverarbeitung genau unter die Lupe genommen und gegebenenfalls angepasst werden.

Für die geforderten Dokumentations- und Nachweispflichten sind entsprechende Verzeichnisse anzulegen und nicht zuletzt die Homepage an die neuen Erfordernisse anzupassen. Hierbei kann es hilfreich sein, sich von Experten mit Erfahrungen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis beraten zu lassen. Die Wettbewerbszentrale schreibt auf ihrer Homepage dazu: „*Die Datenschutz-Grundverordnung* lässt nicht alleine aufgrund ihrer zahlreichen Öffnungsklauseln noch viele Fragen für die Unternehmen offen. Es empfiehlt sich, das Thema in den kommenden Monaten im Auge zu behalten und sich selbst und seine Mitarbeiter in Bezug auf die DSGVO fortzubilden." RÄ

Weitere Informationen im Internet

- **Datenschutzgrundverordnung – Verordnungstext und Erwägungsgründe:** *http://eur-lex.europa.eu/* Suchbegriff: *Datenschutz-Grundverordnung*
- **Wettbewerbszentrale:** *www.wettbewerbszentrale.de/de/aktuelles* *Mitteilung vom 25.1.2018:* „EU-Kommission veröffentlicht Leitfaden zur *Datenschutz-Grund VO*" (Darin enthalten sind Links zu Hilfen der EU-Kommission) *Mitteilung vom 24.11.2017:* „6 Monate bis zur *EU-Datenschutz-Grundverordnung* – Die wichtigsten Regelungen im Überblick"
- **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit:** *www.bfdi.bund.de*
- **Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen:** *www.ldi.nrw.de* Dort findet sich unter „Aktuelles" auch eine Checkliste für kleine und mittlere Unternehmen.
- Die **Bundesärztekammer** hat angekündigt, in Kürze „Hinweise und Erläuterungen zur Schweigepflicht und zum Datenschutz in der Arztpraxis" zu veröffentlichen.
- Einige Rechtsportale im Internet beschäftigen sich ebenfalls mit der DSGVO.