Neue EU-Datenschutz-Grundverordnung – bei Verstößen drohen hohe Geldstrafen

Ab dem 25. Mai 2018 gilt in der Europäischen Union eine neue Datenschutz-Grundverordnung. Sie ist für alle Unternehmen und somit auch für alle Arztpraxen verpflichtend und betrifft alle Daten der Patienten und Angestellten, die in der Praxis „verarbeitet" – also erhoben, abgefragt, geordnet, gespeichert, geändert, ausgelesen, weitergeleitet oder gelöscht – werden.
Auch wenn sich die neuen datenschutzrechtlichen Vorgaben nicht stark von den aktuell geltenden Vorgaben unterscheiden, so gibt es ab dem 25. Mai einige Änderungen der Dokumentations-, Informations- und Meldepflichten.
Kommt man diesen nicht nach, drohen hohe Geldstrafen: Je nachdem, wie schwer oder langfristig der Verstoß gegen die Datenschutz-Grundverordnung ist und je nachdem, wie stark die Auswirkung auf die Patienten ist, können im Einzelfall Geldbußen von bis zu 20 Millionen Euro bzw. bis zu 4 Prozent des Jahresumsatzes verhängt werden. Zudem sind Schadens- und Schmerzensgeldforderungen von Betroffenen – beispielsweise aufgrund einer Rufverletzung – möglich. Für leichtere Verstöße ist zunächst eine Beratung vorgesehen.
Die Kassenärztliche Bundesvereinigung (KBV) hat eine Übersicht erstellt, welche datenschutzrelevanten Vorgaben in den Arztpraxen verpflichtend umgesetzt werden müssen:

Datenschutzerklärung auf der Internet- oder Facebookseite anpassen

Praxen, die eine Internet- oder Facebook-Seite pflegen, sowie Praxen, die Patienten-Newsletter und Terminerinnerungen per SMS anbieten, sind verpflichtet, eine Datenschutzerklärung einzustellen, die alle nötigen Angaben enthält. So muss insbesondere auf folgende Punkte hingewiesen werden:

- Personenbezogene Daten werden nach dem geltenden Datenschutzrecht erhoben und genutzt.
- Eine Speicherung der Daten findet nur statt, wenn sie aktiv übermittelt werden.
- Eine Nutzung der Daten findet nur zur Beantwortung von Anfragen oder zur Zusendung von Informationsmaterial statt.
- Kontaktdaten werden ausschließlich zur Korrespondenz verwendet.
- E-Mail-Adressen für Newsletter werden nur zu diesem Verwendungszweck genutzt.

Es ist technisch sehr einfach, eine hohe Anzahl an Internetseiten in kürzester Zeit im Hinblick auf eine gültige Datenschutzerklärung zu durchforsten. Gerade in letzter Zeit kommt es gehäuft zu Anzeigen durch Abmahn-Anwälte – teils wegen Wettbewerbsgründen, teils wegen gezielter juristischer Abzocke. Daher empfiehlt sich eine sehr zügige Umsetzung aller relevanten Datenschutzmaßnahmen.

Verzeichnis von Verarbeitungstätigkeiten erstellen

Alle Praxen sind verpflichtet, ein Verzeichnis zu erstellen, das alle Informationen zu den anfallenden Verarbeitungstätigkeiten – beispielsweise erheben, speichern, bearbeiten oder weiterleiten – von personenbezogenen Daten enthält. Die Aufstellung muss auf Verlangen der Aufsichtsbehörde bereitgestellt werden.
Folgende Informationen müssen im Verzeichnis enthalten sein:

- Name und Adresse der Praxis sowie gegebenenfalls Name des Datenschutzbeauftragten
- Personengruppen, deren Daten verarbeitet werden, beispielsweise Patienten oder Angestellte
- Zweck der Verarbeitung, beispielsweise ärztliche Dokumentation oder Führen von Personalakten
- Kategorie der Daten, beispielsweise Adressdaten oder Gesundheitsdaten
- Interne und externe Empfängergruppen, beispielsweise Mitarbeiter oder Krankenkassen
- Fristen für die Löschung, beispielsweise zehn Jahre

Die KBV stellt auf ihrer Internetseite ein Muster sowie ein Ausfüllbeispiel bereit.

→

Aufstellung aller getroffenen Maßnahmen für den Datenschutz

Jede Praxis ist für den Schutz der personenbezogenen Daten verantwortlich und muss hierfür geeignete Maßnahmen ergreifen. Diese Maßnahmen müssen innerhalb eines Datenschutzplans dokumentiert werden und für alle Teammitglieder zugänglich gemacht werden. Zudem müssen sie im Fall einer externen Kontrolle oder Anfrage zur Verfügung gestellt werden.
Der Datenschutzplan sollte folgende Maßnahmen enthalten:

- Patientendaten werden nur verschlüsselt über Internet oder E-Mail versendet.
- Einzelne Mitarbeiter erhalten Zugriffsberechtigungen, die regeln, auf welche Dateien und Ordner zugegriffen werden darf.
- Es wird auf Diskretion geachtet, beispielsweise durch eine räumliche Trennung des Anmelde- und Wartebereiches oder eines Schildes mit dem Hinweis, Abstand zum Tresen zu halten.
- Patientenakten werden gesichert, indem die Computer mittels Passwort und automatischer Bildschirmsperre geschützt werden, Patientenunterlagen werden so positioniert, dass sie nicht durch Dritte einsehbar sind.
- Vertrauliche Arzt-Patienten-Gespräche finden in geschlossenen Räumen statt.
- Bei Telefonaten wird die Identität des Anrufers geschützt.
- Die fristgerechte Löschung der Daten wird durch einen namentlich dokumentierten Mitarbeiter gewährleistet.
- Daten werden nach DIN-Normen vernichtet.
- Es existiert ein Plan, der bei Datenpannen und Datenschutzverstößen in Kraft tritt und der Mitarbeiter, der die Meldung innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde weitergibt, ist namentlich festgelegt.
- Alle Praxismitarbeiter sind über die Einhaltung von Schweigepflicht und Datenschutz informiert.

Patienteninformation zum Datenschutz in der Arztpraxis

Die Arztpraxen müssen ihre Patienten zum Zeitpunkt der Datenerhebung über die Verwendung ihrer Daten informieren. Es empfiehlt sich, ein Aushang in der Praxis, der Angaben zum Zweck sowie zur Rechtsgrundlage der Datenverarbeitung sowie die Kontaktdaten der Praxis und gegebenenfalls des Datenschutzbeauftragten enthält. Zudem ist das Auslegen einer Wartezimmerinformation oder die Veröffentlichung einer Patienteninformation auf der Praxis-Webseite möglich. Eine persönliche Information, zum Beispiel bei der ersten Kontaktaufnahme am Telefon, ist nach Angabe der KBV explizit nicht erforderlich.
Muster für Patienteninformationen werden auf der Internetseite der KBV bereitgestellt.

Datenschutzverträge mit externen Dienstleistern

Für den Fall, dass externe Dienstleister auf Patienten- oder Mitarbeiterdaten zugreifen, ist der Abschluss eines Zusatzvertrages zur Auftragsverarbeitung erforderlich. Dies gilt beispielsweise für Firmen, die die Praxissoftware warten oder die Akten- und Datenträger nach Ablauf der Aufbewahrungsfrist vernichten. Zudem ist dies der Fall, wenn Cloud-Systeme genutzt werden und die Terminvergabe durch externe Stellen stattfindet.
Eine rein technische Wartung der IT-Infrastruktur, wie beispielsweise Arbeiten an Elektrik, Kühlung oder Heizung, stellt keine Auftragsverarbeitung dar. Auch bei der Beauftragung von Berufsgruppen, die als „Geheimnisträger“ gelten – beispielsweise bei Rechtsanwälten oder Steuerberatern – liegt keine Auftragsverarbeitung vor.
Der Vertrag muss folgende Punkte beinhalten:

- Gegenstand (Art der Leistung) und Dauer der Verarbeitung
- Art (Zweck der Leistung) und Zweck (Ziel der Leistung) der Verarbeitung
- Art der personenbezogenen Daten und Kategorie der betroffenen Personen
- Rechte, Pflichten und Weisungsbefugnisse des Auftraggebers
- Verpflichtung zur Vertraulichkeit aller zur Verarbeitung berechtigter Personen
- Benennung aller Maßnahmen, die das externe Unternehmen zum Datenschutz durchführt
- Verpflichtung des externen Unternehmens mit dem Auftraggeber zu kooperieren, falls
  - Anfragen oder Ansprüche von Personen, deren Daten verarbeitet werden, gestellt werden
  - Datenschutzverletzungen gemeldet werden müssen
  - Eine Datenschutz-Folgenabschätzung erforderlich ist
- Rückgabe bzw. Löschung der personenbezogenen Daten nach Abschluss der Auftragsverarbeitung

- Verpflichtung des externen Dienstleisters zur Bereitstellung aller Nachweise zur Einhaltung seiner datenschutzrechtlicher Pflichten

Die Praxen sind verpflichtet sicherzustellen, dass die externen Dienstleister alle Vorschriften und Maßnahmen des Datenschutzes einhalten. Dies ist an einem Datenschutzsiegel oder an einer Zertifizierung (ISO/IEC 27001) zu erkennen.

Datenschutzbeauftragten benennen

Praxen und Medizinische Versorgungszentren, in denen mindestens zehn Personen regelmäßig automatisiert mit der Verarbeitung von Daten beschäftigt sind, benötigen einen Datenschutzbeauftragten. Dies ist auch der Fall, wenn in kleineren Praxen eine sehr große Menge an personenbezogenen Daten verarbeitet wird, wenn eine Datenschutz-Folgenabschätzung notwendig ist oder wenn Praxisräume videoüberwacht werden.

Als Datenschutzbeauftragter kann ein fachlich qualifizierter Mitarbeiter oder ein externer Datenschützer fungieren, der Praxisinhaber hingegen kann diese Funktion nicht übernehmen. Name und Kontaktdaten des Datenschutzbeauftragten müssen an den Landesdatenschutzbeauftragten übermittelt werden. Der Datenschutzbeauftragte kontrolliert die Einhaltung von Datenschutz und Datensicherheit in der Praxis und legt geeignete Maßnahmen fest. Zudem informiert und berät er das Praxisteam über geltende Bestimmungen und dient als Ansprechpartner für die Aufsichtsbehörde.

Datenschutz-Folgenabschätzung

Für den Fall, dass sehr große Mengen an personenbezogenen Daten verarbeitet werden oder falls bei diesen Daten ein hohes Datenschutzrisiko besteht, ist eine Datenschutz-Folgenabschätzung erforderlich. Dies trifft auch zu, falls Praxisräume systematisch videoüberwacht werden. In diesen Fällen wird es empfohlen, eine externe Datenschutzprüfung durchführen zu lassen. Informationen zur Notwendigkeit kann beim Landesdatenschutzbeauftragten erfragt werden.

Einwilligungserklärung für Datenweitergabe an privatärztliche Verrechnungsstelle muss um Hinweis zur Widerrufbarkeit ergänzt werden

Werden Patientendaten weitergegeben, beispielsweise an eine privatärztliche Verrechnungsstelle, müssen die Patienten eine Einwilligungserklärung zur Datenverarbeitung unterschreiben. Diese muss einen Hinweis enthalten, dass das Einverständnis zur Weitergabe jederzeit durch den Patienten widerrufen werden kann.

Erforderliche Maßnahme:	Verpflichtend für	KBV-Hilfe	Check
Datenschutzerklärung auf der Homepage sowie auf Kontaktformularen und Newslettern	alle Praxen mit Internet- oder Facebookseite		✓
Verzeichnis von Verarbeitungstätigkeiten	alle Praxen		✓
Aufstellung der Datenschutzmaßnahmen	alle Praxen		✓
Patienteninformation Datenschutz	alle Praxen		✓
Datenschutzverträge mit externen Dienstleistern	Praxen, die Patienten- oder Personaldaten an externe Dienstleister geben		✓
Datenschutzbeauftragten benennen	Praxen ab zehn Mitarbeitern bzw. wenn eine sehr große Menge an personenbezogenen Daten verarbeitet wird / bei Videoüberwachung der Praxisräume		✓
Datenschutz-Folgenabschätzung	Praxen, die eine sehr große Menge an personenbezogenen Daten verarbeiten / Praxisräumen mit Videoüberwachen		✓
Hinweis zum Widerruf von Einwilligungserklärung bei Datenweitergabe	Praxen, die Daten an privatärztliche Verrechnungsstelle weitergeben		✓