Die EU-Datenschutz-Grundverordnung

Was jetzt zu tun ist – Teil 2

Datenschutz spielt in der Zahnarztpraxis eine wichtige Rolle. Am 25. Mai tritt die EU-Datenschutz-Grundverordnung (DS-GVO) in Kraft. Als EU-Verordnung gilt sie in allen Mitgliedsstaaten der Europäischen Union. Gleichzeitig löst das neue Bundesdatenschutzgesetz (BDSG-neu) die bisherigen deutschen Rechtsnormen ab.

Das BZB stellt in einer zweiteiligen Serie die wichtigsten Änderungen vor und klärt über die Rechtslage auf. Der erste Teil behandelte die Themen „Benennung eines Datenschutzbeauftragten“ und „Dokumentations- und Informationspflichten“ (siehe BZB 4/2018, S. 28 ff.). Im zweiten Teil geht es um Regelungen zur Auftragsverarbeitung und zu den Einwilligungserklärungen, die richtige Vorgehensweise bei Datenschutzverletzungen und um die Betroffenenrechte.

Auftragsverarbeitung

Unter einer Auftragsverarbeitung versteht man die Verarbeitung personenbezogener Daten durch einen Dienstleister im Auftrag der verantwortlichen Stelle, zum Beispiel die Datenverarbeitung durch eine externe Lohnabrechnungs- oder Patientenabrechnungsstelle. Auch eine externe Wartung und Betreuung von IT-Systemen, bei der nicht ausgeschlossen werden kann, dass personenbezogene Daten zur Kenntnis gelangen, stellt eine Auftragsverarbeitung dar. Schon nach der bis zum 24. Mai noch geltenden alten Rechtslage muss bei einer Auftragsdatenverarbeitung ein schriftlicher Vertrag mit den im Bundesdatenschutzgesetz vorgegebenen Inhalten zwischen der Praxis und dem Auftragnehmer geschlossen werden.

Auch nach den neuen Regelungen ist ein schriftlicher Vertrag für die Auftragsverarbeitung erforderlich. Der Vertrag legt den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Datenverarbeitung, die Art der personenbezogenen Daten, den Kreis der betroffenen Personen sowie die Rechte und Pflichten des Verantwortlichen fest. Für die konkrete Ausgestaltung des Vertrags zur Auftragsverarbeitung regelt nun Art. 28 Abs. 3 DS-GVO die erforderlichen Inhalte. Im Wesentlichen entsprechen die Vorgaben zur Auftragsverarbeitung der bisherigen Rechtslage. Dennoch sollten Zahnarztpraxen bestehende Verträge zur Auftragsdatenverarbeitung dahingehend überprüfen, ob diese allen Vorgaben der DS-GVO entsprechen. Insbesondere ist zu prüfen, ob der Auftragsverarbeitungsvertrag die Einhaltung der nach der DS-GVO erforderlichen technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung vorsieht. Für den Fall, dass es noch keine schriftlichen Verträge gibt, sollte dies schnellstmöglich nachgeholt werden.

Auf seiner Website hat das Bayerische Landesamt für Datenschutzaufsicht ein Vertragsmuster für die Auftragsverarbeitung bereitgestellt:
www.lda.bayern.de/de/datenschutz_eu.html

Foto: fotolia.com/coldwaterman

Der Schutz der Patientendaten spielt in Zahnarztpraxen künftig eine noch wichtigere Rolle. Dafür sorgt die neue EU-Datenschutz-Grundverordnung, die ab 25. Mai gilt.

Verbot mit Erlaubnisvorbehalt

Auch nach der DS-GVO gilt der Grundsatz, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist – es sei denn, die DS-GVO oder andere Rechtsvorschriften erlauben dies ausdrücklich. Ferner kann der Erlaubnis zur Datenverarbeitung auch eine individuell erteilte Einwilligung des Betroffenen zugrunde liegen. Eine Einwilligung des Betroffenen ist bereits nach bestehender Rechtslage beispielsweise dann einzuholen, wenn Patientendaten an einen Abrechnungsdienstleister weitergegeben werden sollen oder wenn geplant ist, Fotos von Praxismitarbeitern zu veröffentlichen.

Wie eine Einwilligungserklärung ausgestaltet sein muss, regeln nun Art. 6 Abs. 1 Buchst. a) und Art. 4 Nr. 11 DS-GVO. Die Einwilligung in die Verarbeitung von personenbezogenen Daten muss für einen bestimmten Zweck gegeben werden. Sie muss freiwillig, in informierter Weise und unmissverständlich abgegeben werden. Dies setzt voraus, dass der Betroffene zunächst vom Verantwortlichen ausführlich informiert und darüber aufgeklärt wird, für welche Zwecke die Einwilligung erfolgt. Anschließend erhält der Betroffene eine Einwilligungserklärung, die in verständlicher Form und einfacher Sprache sowie getrennt von anderen Inhalten verfasst ist. Es muss klargestellt werden, dass die Abgabe der Einwilligung freiwillig erfolgt und jederzeit widerruflich ist.

Die in der Praxis bereits vorliegenden Einwilligungserklärungen müssen dahingehend überprüft werden, ob diese den Vorgaben nach der DS-GVO entsprechen. Gegebenenfalls sind die Einwilligungserklärungen zu aktualisieren und neu einzuholen. Einen Bestandsschutz für bereits vorliegende Einwilligungserklärungen gibt es nicht.

Grundprinzipien bei der Verarbeitung personenbezogener Daten

Die DS-GVO beinhaltet eine Reihe von Grundprinzipien, die bei der Verarbeitung von personenbezogenen Daten zu beachten sind. Diese sind im Grunde nicht neu und bereits jetzt einzuhalten. Dennoch sollten bestehende Datenschutzkonzepte der Zahnarztpraxis im Hinblick auf die Grundprinzipien überprüft werden.

- *Grundprinzip der Zweckbindung und Datensparsamkeit*
  Die Verarbeitung personenbezogener Daten muss auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden. Personenbezogene Daten dürfen nur für den festgelegten Zweck erhoben und nur in einer mit diesem Zweck zu vereinbarenden Weise weiterverarbeitet werden. Sofern die Speicherung von Daten nicht mehr erforderlich ist, weil beispielsweise das Arbeits- oder Patientenverhältnis beendet ist und keine gesetzlichen Aufbewahrungspflichten beziehungsweise etwaige längere Verjährungsfristen mehr bestehen, müssen diese Daten gelöscht werden.

- *„Recht auf Vergessenwerden“*
  Das sogenannte „Recht auf Vergessenwerden“ ist in der DS-GVO konkreter als bisher ausgestaltet. Es beschreibt das Recht des Betroffenen, die Löschung seiner Daten in bestimmten Fallgruppen zu verlangen. Vom Löschungsverlangen umfasst sind auch sämtliche Querverweise und Kopien der Daten. Sofern also im Rahmen eines Back-ups Daten gespeichert werden, muss sichergestellt sein, dass bei einer endgültigen Datenlöschung auch dieses Back-up entsprechend gelöscht wird.
  Die EU-Verordnung sieht in Art. 17 eine Reihe von Fallkonstellationen vor, in denen der Betroffene die Datenlöschung verlangen kann. Dies ist zum Beispiel dann der Fall, wenn die Notwendigkeit der Verarbeitung der Daten durch Zweckerreichung entfallen ist oder die Einwilligung zur Datenerhebung widerrufen wird. Für die Löschung der Daten ist der Zahnarzt selbst verantwortlich.
  Zu beachten sind in diesem Zusammenhang jedoch gesetzliche Aufbewahrungspflichten: zum Beispiel die Aufbewahrungspflicht gemäß § 630 f Abs. 3 BGB, wonach die Patientenakte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren ist, sowie möglicherweise längere Verjährungsfristen in bestimmten Fällen.
  Die Löschfristen müssen in einem Löschkonzept festgelegt werden, das Teil der datenschutzrechtlichen Dokumentation des Zahnarztes ist.

Meldepflicht bei Datenschutzverletzungen

Kommt es zu einer Datenpanne und dadurch zu einer Verletzung des Schutzes personenbezogener Daten, muss der Zahnarzt diesen Vorfall als Verantwortlicher an das Bayerische Landesamt für Datenschutzaufsicht als zuständige Aufsichtsbehörde melden, selbst wenn er alle erforderlichen Maßnahmen zum Schutz personenbezogener Daten ergriffen hat. Die Meldung der Datenschutzverletzung muss innerhalb von 72 Stunden, nachdem die Verletzung bekannt geworden ist, erfolgen. Sie muss eine Beschreibung der Art der Verletzung und zumindest eine ungefähre Zahl der betroffenen Personen be-

inhalten, den Namen und die Kontaktdaten des Datenschutzbeauftragten sowie eine Beschreibung der Folgen der Datenschutzverletzung. Die ergriffenen Maßnahmen sind ebenfalls dem Bayerischen Landesamt für Datenschutzaufsicht mitzuteilen. Bringt die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen mit sich, muss der Verantwortliche auch die betroffenen Personen informieren.
Da im Fall einer Datenschutzverletzung nur eine sehr kurze Zeitspanne von 72 Stunden zur Meldung vorgesehen ist, empfiehlt es sich, ein entsprechendes Meldekonzept zu erstellen und es in die Datenschutzdokumentation aufzunehmen.

Bußgelder bei Datenschutzverstößen

Die DS-GVO sieht für Verstöße gegen ihre Regelungen Bußgelder vor, deren Höchstsätze im Vergleich zum bisher geltenden BDSG deutlich angehoben wurden. Aber auch nach den Bestimmungen der DS-GVO sind Bußgelder einzelfallbezogen festzulegen, wobei es detaillierte Ermessensgrundsätze zu beachten gilt.

Zusammenfassung

Das Datenschutzmanagement rückt mit dem Inkrafttreten der DS-GVO deutlich in den Fokus. Zahnarztpraxen sollten deshalb dem Thema Datenschutz unter den individuellen Gegebenheiten der Praxis die nötige Aufmerksamkeit schenken, das vorhandene Datenschutzkonzept überprüfen und die erforderlichen Maßnahmen ergreifen und dokumentieren. Im Falle einer Datenschutzprüfung durch die Aufsichtsbehörde muss ein Datenschutzkonzept vorgelegt werden, um nachweisen zu können, dass alle erforderlichen Maßnahmen zum Datenschutz umgesetzt wurden.

Ass. jur. Sarah Winter
Geschäftsbereich Recht und Praxis der BLZK

Informationen im Netz

In ihrem Qualitätsmanagement-System QM Online hat die BLZK Informationen und Musterformulare bereitgestellt, die fortlaufend ergänzt werden:
https://qm.blzk.de

Weitere Informationen und Tipps zur Umsetzung der Datenschutz-Grundverordnung enthält der „Datenschutz- und Datensicherheitsleitfaden für die Zahnarztpraxis-EDV“:
www.bzaek.de/dsl