BLZK

Die EU-Datenschutz-Grundverordnung

Was jetzt zu tun ist – Teil 1

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 behandelt die Themen „Benennung eines Datenschutzbeauftragten" und „Dokumentations- und Informationspflichten". Im zweiten Teil geht es um den Anpassungsbedarf bei Einwilligungsformularen und Auftragsdatenverarbeitungsverträgen sowie die Betroffenenrechte.

Benennung eines Datenschutzbeauftragten

Bereits nach der bisherigen Rechtslage war die Bestellung eines Datenschutzbeauftragten in bestimmten Zahnarztpraxen verpflichtend. Die aktuell noch geltende Fassung des Bundesdatenschutzgesetzes (BDSG) regelt in § 4f, dass Stellen, die personenbezogene Daten automatisiert verarbeiten, einen Beauftragten für den Datenschutz bestellen müssen. Das betrifft alle Zahnarztpraxen, in denen mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst sind.

Was ändert sich nach der Einführung der neuen DS-GVO und der Neufassung des BDSG? Gemäß Art. 37 Abs. 1 Buchst. c) DS-GVO muss ein Datenschutzbeauftragter benannt werden, wenn „die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 besteht". Besondere Kategorien von Daten im Sinne von Art. 9 DS-GVO sind insbesondere Gesundheitsdaten. Zwar werden in einer Zahnarztpraxis Gesundheitsdaten verarbeitet, dabei handelt sich in der Regel jedoch nicht um eine „umfangreiche Verarbeitung".

Die Frage, wann eine „umfangreiche Verarbeitung" gegeben ist, wird von Datenschutzaufsichtsbehörden derzeit nicht allgemeingültig beantwortet. Als Entscheidungskriterien werden bislang unter anderem die Anzahl der von der Datenverarbeitung betroffenen Personen, die Menge der verarbeiteten Daten, die Dauer der Verarbeitungstätigkeit und die geografische Ausdehnung der Verarbeitung herangezogen. Als Beispiel für eine umfangreiche Verarbeitung von Gesundheitsdaten wird in den Erwägungsgründen der DS-GVO die Verarbeitung von Patientendaten im Geschäftsbetrieb eines Krankenhauses genannt.

Keine „umfangreiche Datenverarbeitung"

Daher vertritt die Bayerische Landeszahnärztekammer die Auffassung, dass bei Einzelpraxen und kleinen Berufsausübungsgemeinschaften keine umfangreiche Verarbeitung von Patientendaten vorliegt. Damit in Einklang stehen auch erste, allerdings noch vorläufige Bewertungen vonseiten der Datenschutzbehörden.

In Grenzfällen ist die Diskussion, ob eine Bestellpflicht nach Art. 37 Abs. 1 Buchst. c) DS-GVO wegen einer umfangreichen Verarbeitung besonderer Kategorien von Daten besteht, häufig nur rein akademisch, weil die Bestellpflicht schon durch die „Zehn-Personen-Regel" ausgelöst wird. Der Gesetzesformulierung ist zu entnehmen, dass auch der Praxisinhaber selbst mitzuzählen ist. Nur wenn einschließlich des Praxisinhabers mindestens zehn Personen ständig mit der automatisierten Verarbeitung von Daten beschäftigt sind, muss ein Datenschutzbeauftragter benannt werden. Wenn eine Praxis nach der internen Analyse zum Ergebnis kommt, dass sie keinen Datenschutzbeauftragten benennen muss, sollte dies begründet und dokumentiert werden.

Liegt die Zahl der ständig mit der Verarbeitung von Patientendaten betrauten Personen über neun, wird ein Datenschutzbeauftragter auf Grundlage seiner beruflichen Qualifikation und seines Fachwissens auf dem Gebiet des Datenschutzrechts benannt. Zum Datenschutzbeauftragten kann also weiterhin sowohl ein Mitarbeiter der Zahnarztpraxis als auch ein externer Dienstleister benannt werden. Die nach der bisherigen Rechtslage unterzeichneten Bestellungsurkunden gelten fort. Die Urkunden müssen jedoch dahingehend überprüft werden, ob sie den Vorgaben der DS-GVO entsprechen.

Neu ist, dass die Kontaktdaten des Datenschutzbeauftragten veröffentlicht werden müssen. Nach derzeitigem Kenntnisstand reicht dafür die Be-

kanntgabe der Funktion und Erreichbarkeit des Datenschutzbeauftragten mittels einer Funktions-E-Mail-Adresse und Telefonnummer, beispielsweise auf der Website der Praxis. Daneben muss der Datenschutzbeauftragte namentlich und unter Angabe seiner Kontaktdaten an das Bayerische Landesamt für Datenschutzaufsicht als zuständige Datenschutzaufsichtsbehörde in Bayern gemeldet werden.

Aufgaben und Stellung des Datenschutzbeauftragten

Der Datenschutzbeauftragte ist nicht „Verantwortlicher" im Sinne des Gesetzes. Verantwortlicher für die Einhaltung der datenschutzrechtlichen Bestimmungen bleibt der Praxisinhaber. Der Datenschutzbeauftragte hat den Praxisinhaber zu beraten und ihm Hilfestellung bei der Umsetzung der datenschutzrechtlichen Vorgaben zu geben. Dabei unterrichtet und berät er den Praxisinhaber sowie die Beschäftigten über die Datenschutzvorschriften und überwacht die Einhaltung der DS-GVO und anderer Datenschutzvorschriften. Er unterstützt den Praxisinhaber bei der Erstellung und Führung des verpflichtenden Verzeichnisses aller Verarbeitungstätigkeiten und anderer erforderlicher Dokumentationen. Der Datenschutzbeauftragte muss frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Angelegenheiten eingebunden werden. Er ist Ansprechpartner für das Bayerische Landesamt für Datenschutzaufsicht und in seiner Funktion direkt dem Praxisinhaber unterstellt. Bei der Erfüllung seiner Aufgaben ist er weisungsfrei und darf vom Praxisinhaber wegen der Erfüllung seiner Aufgaben als Datenschutzbeauftragter nicht benachteiligt werden.

Dokumentationspflichten

Nach der DS-GVO unterliegt der Praxisinhaber als Verantwortlicher für den Datenschutz einer gewissen Rechenschaftspflicht. Er muss jederzeit die Einhaltung der Datenschutzgrundsätze gegenüber der Datenschutzaufsichtsbehörde nachweisen können. Dies gelingt durch eine ausführliche datenschutzrechtliche Dokumentation. Wie bereits dargestellt, muss die Benennung des Datenschutzbeauftragten dokumentiert werden. Daneben sind im Zusammenhang mit den Dokumentationspflichten vor allem das Verzeichnis der Verarbeitungstätigkeiten und die Datenschutz-Folgenabschätzung zu nennen.

Verzeichnis der Verarbeitungstätigkeiten

Bereits nach der alten Rechtslage musste eine Zahnarztpraxis dem Beauftragten für den Datenschutz eine Übersicht über die Verfahren automatisierter Datenverarbeitung übergeben. Gemäß Art. 30 DS-GVO muss ein Verzeichnis aller Verarbeitungstätigkeiten geführt werden. In das Verzeichnis aufzunehmen sind alle Verarbeitungen personenbezogener Daten. In einer Zahnarztpraxis fallen darunter beispielsweise die elektronische Patientenkartei, die Buchhaltungsdatenverarbeitung, Adressdatenbanken, die elektronische Terminverwaltung und die Personaldatenverarbeitung. Die Vorschrift richtet sich in Absatz 1 an den Verantwortlichen, also den Praxisinhaber, und bestimmt, welche Angaben dieses Verzeichnis enthalten muss:

- den Namen und die Kontaktdaten der Zahnarztpraxis sowie des Datenschutzbeauftragten,
- die Zwecke der Datenverarbeitung,
- die Kategorien der betroffenen Personen und die Kategorien der personenbezogenen Daten,
- die Kategorien der Empfänger der personenbezogenen Daten,
- die Übermittlung von Daten an ein Drittland,
- die vorgesehenen Löschfristen,
- die Beschreibung der verpflichtend vorgegebenen technischen und organisatorischen Maßnahmen zur Datensicherheit.

Das Verzeichnis muss schriftlich geführt werden, wobei auch die elektronische Form zulässig ist. Weitere Vorgaben macht das Gesetz dazu nicht, sodass eine Word- oder Excel-Datei als Verzeichnis ausreicht. Das bestehende Verfahrensverzeichnis muss auf Vereinbarkeit mit den Vorgaben der DS-GVO geprüft und angepasst werden.

Sinnvolle Bestandsaufnahme

Das Verzeichnis dient zum einen der Bestandsaufnahme. Es soll der Praxis helfen, die Übersicht zu behalten, welche Verfahren elektronischer Datenverarbeitung genutzt werden. Zum anderen werden in diesem Verzeichnis sämtliche Informationen gebündelt, die die Aufsichtsbehörde für die Prüfung der Einhaltung von Datenschutzstandards benötigt. Auf Anfrage ist das Verzeichnis der Aufsichtsbehörde zur Verfügung zu stellen.

Datenschutz-Folgenabschätzung nur im Einzelfall

Ein wichtiges Instrument des Datenschutzes ist die zu dokumentierende Datenschutz-Folgenabschätzung. Sie beschreibt die Verarbeitung personenbezogener Daten, bewertet die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung sowie die Risiken und Folgen für die Rechte und Freiheiten der betroffenen

Personen. Durch eine Risikoabschätzung und die Festlegung von Gegenmaßnahmen soll die Beeinträchtigung der Betroffenen kontrolliert werden. Geregelt ist die Datenschutz-Folgenabschätzung in Art. 35 DS-GVO. Die Durchführung einer Datenschutz-Folgenabschätzung ist nur dann erforderlich, wenn ein konkreter Datenverarbeitungsvorgang „wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt". Da in der Zahnarztpraxis in der Regel keine „umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten" erfolgt, erscheint eine Datenschutz-Folgenabschätzung bei Einzelpraxen sowie kleinen Berufsausübungsgemeinschaften nicht erforderlich.
Auch wenn in einer Praxis keine „umfangreiche Verarbeitung" von Gesundheitsdaten erfolgt, muss der Praxisinhaber als Verantwortlicher nach der DS-GVO weiter prüfen, ob durch die Verarbeitungsvorgänge in seiner Praxis dennoch ein „voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen" vorliegt. Kommt er dabei zu dem Ergebnis, dass ein hohes Risiko wahrscheinlich nicht gegeben ist, muss dieses Ergebnis begründet und dokumentiert werden. Bei einer Überprüfung durch die Datenschutzaufsichtsbehörde ist diese Abwägung vorzulegen.

Informationspflichten der Praxis

Die Informationspflichten dienen der Transparenz der Datenverarbeitungsvorgänge. Die Betroffenen sollen zu jeder Zeit darüber informiert sein, welche Daten von der Praxis erhoben werden und was ihre Rechte sind. Die Information über die Erhebung von personenbezogenen Daten muss zum Zeitpunkt der Datenerhebung in verständlicher Sprache und in leicht zugänglicher Form schriftlich oder elektronisch übermittelt werden. Hinter dieser Regelung verbirgt sich ein umfangreiches Geflecht an Informationspflichten, die die Praxis gegenüber Patienten, Mitarbeitern, Lieferanten und anderen einhalten muss. Art. 13 DS-GVO verpflichtet bei der Erhebung personenbezogener Daten insbesondere zur Information über die folgenden Punkte:

- Namen und Kontaktdaten der Zahnarztpraxis sowie des Datenschutzbeauftragten,
- die Zwecke der Datenverarbeitung und Angabe der Rechtsgrundlage,
- die Kategorien der betroffenen Personen und die Kategorien der personenbezogenen Daten,
- Empfänger der personenbezogenen Daten,
- die Absicht der Übermittlung von Daten an ein Drittland,
- die geplante Speicherdauer,
- die Betroffenenrechte (Auskunft, Berichtigung, Löschung etc.),
- das Recht zum Widerruf einer erteilten Einwilligung.

Im Internet können diese Informationen durch das Bereithalten der Informationen auf der öffentlich zugänglichen Website erfolgen. Sie müssen leicht auffindbar gekennzeichnet sein, zum Beispiel als „Informationen zum Datenschutz". Bereits nach derzeitiger Rechtslage sind auf einer Website in bestimmten Fällen sogenannte „Datenschutzerklärungen" verpflichtend. Diese müssen vom Verantwortlichen auf die Vereinbarkeit mit den Vorgaben der DS-GVO geprüft und angepasst werden. Werden die Daten in der Praxis direkt erhoben, reicht es nicht aus, auf die Website zu verweisen. Um die Informationen bei der Erhebung der Daten an den Betroffenen zu geben, sind „Allgemeine Hinweise zur Datenverarbeitung" in Papierform empfehlenswert.

Zusammenfassung

Auch bislang galten für die Berufsausübung bereits Datenschutzbestimmungen. Diese werden durch die DS-GVO ergänzt und gelten ab Mai 2018. Handlungsbedarf besteht bei der Umsetzung von Informations- und Dokumentationspflichten. Hier wird die BLZK im Rahmen ihres Qualitätsmanagement-Systems QM Online weitere Informationen und Musterformulare zur Verfügung stellen. Auch die Hinweise auf den Websites der Praxen müssen angepasst werden, um kostenträchtige Abmahnungen zu vermeiden. Ein Datenschutzbeauftragter ist dann zu bestellen, wenn mehr als neun Personen dauerhaft mit der Datenverarbeitung befasst sind. Auch eine Datenschutz-Folgenabschätzung erscheint in der Zahnarztpraxis in der Regel nicht nötig.

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

Informationen im Netz

Weitere Informationen und Tipps zur Umsetzung der Datenschutz-Grundverordnung enthält das Rundschreiben 1/2018 der BLZK und KZVB vom 20. März:
https://qm.blzk.de/1801rs-blzk-kzvb

In ihrem Qualitätsmanagement-System QM Online wird die BLZK zeitnah entsprechende Informationen und Musterformulare bereitstellen:
https://qm.blzk.de