EMPFEHLUNGEN

betreffend
Umsetzung der Regelungen der Datenschutz-Grundverordnung in der zahnärztlichen Ordination

Am **25. Mai 2018** wird die **Datenschutz-Grundverordnung (DSGVO)**, die in Österreich durch das Datenschutz-Anpassungsgesetz 2018 umgesetzt wurde, Geltung erlangen. Betroffen von der EU-Verordnung sind auch alle Zahnärztinnen und Zahnärzte, da von diesen **regelmäßig personenbezogene, sensible Daten** (Gesundheitsdaten der Patienten) eigenverantwortlich verarbeitet werden und sie damit als „Verantwortliche" im Sinne der Verordnung gelten. Sowohl die EDV-unterstützte als auch die nicht automatisierte Verarbeitung der Daten (z.B. Papierkartei) ist davon betroffen. Durch passende **technische und organisatorische Maßnahmen**, wie von der Datenschutz-Grundverordnung vorgeschrieben, sollen die Rechte der betroffenen Personen bzw. die Verarbeitung ihrer Daten geschützt werden. Diese Maßnahmen und die Einhaltung der **Grundsätze der Datenverarbeitung** (Rechtmäßigkeit der Verarbeitung, Zweckbindung, Datenminimierung, Datenrichtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) sollten **gut dokumentiert** werden. Um die Einhaltung der neuen Bestimmungen zu gewährleisten, werden Verstöße nämlich mit besonders hohen Geldstrafen (bis zu **€ 10 Mio**. bzw. 2 % vom Vorjahresumsatz bei Verstoß gegen die Pflichten als Verantwortlicher, bis zu **€ 20 Mio.** bzw. 4 % vom Vorjahresumsatz bei Verstoß gegen die Grundsätze oder Rechte der Betroffenen) sanktioniert. Außerdem besteht gegenüber der Datenschutzbehörde eine Rechenschaftspflicht.

Folgende Aspekte und Neuerungen stehen dabei im Vordergrund:

1) Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO):

Auch Zahnärztinnen und Zahnärzte trifft als Verantwortliche die Verpflichtung, **schriftlich** ein Verzeichnis aller Verarbeitungstätigkeiten (Datenanwendungen) zu führen. Das Verzeichnis hat laut Datenschutzbehörde jedenfalls zu enthalten *(siehe auch Vorlage 1)*:

- den Namen der Zahnärztin und des Zahnarztes
- die Kontaktdaten (Ordinationsadresse, Telefonnummer, allfällige E-Mail-Adresse)
- die Zwecke der Verarbeitung und Rechtmäßigkeit (Verweis aufs Zahnärztegesetz (ZÄG), insb. §§ 19-21 ZÄG – Dokumentationspflicht und Honorarabrechnung; Behandlungsvertrag)
- die Beschreibung der Kategorie betroffener Personen (Patienten)
- die Beschreibung der Kategorien personenbezogener Daten (= betroffene Personenkreise und Datenarten –> insb. Gesundheitsdaten) und
- die Kategorien von Empfängern der Daten (Versicherungsträger, Gebietskrankenkassen, Abrechnungsstelle, Zahntechniker etc.).

Wenn möglich auch noch: Beschreibung technischer und organisatorischer Maßnahmen betreffend Zweckbindung, Datenminimierung/ Speicherbegrenzung, Richtigkeit der Daten, Vertraulichkeit durch angemessene Sicherheit u.a..

Am Besten sollte das Verzeichnis von Verarbeitungstätigkeiten, die EDV-unterstützt erfolgen, insb. bezüglich der technischen Maßnahmen mit der jeweiligen Ordinationssoftwarefirma erstellt werden. Da die Inhalte des Verzeichnisses wesentlich vom Tätigkeitsspektrum und Organisation der jeweiligen Ordination abhängig sind, ist die *Vorlage 1* lediglich als Minimalgerüst anzusehen, für das von Seiten der Österreichischen Zahnärztekammer keine Haftung übernommen wird. Das Verzeichnis ist **auf Anfrage** der Datenschutzbehörde zu übermitteln (NICHT an LZÄK/ÖZÄK). Außerdem sollte die „Datenverarbeitungen" dokumentiert werden, insbesondere wer worauf Zugriff hat bzw. wer welche Daten verarbeitet.

Auch die Datenschutzbehörde hält fest, dass jedem Verantwortlichen die inhaltliche Gestaltung selbst überlassen bleibt und gibt dazu keine Vorlagen heraus, sodass sich wohl erst durch Anwendung der DSGVO und entsprechende Judikatur eindeutige Vorgaben ergeben werden.

Mit 25. Mai 2018 **entfällt** die Meldepflicht an das Datenverarbeitungsregister (DVR-Meldungen). Die alten DVR-Meldungen können als Vorlage für ein Verzeichnis herangezogen werden.

2) Auftragsverarbeiter:

WICHTIG: Bei Daten, die an sogenannte **„Auftragsverarbeiter"** weitergeleitet werden (z.B. Abrechnungsstelle, Zahntechniker), um die Gesundheitsdaten weiterzuverarbeiten, muss die Verarbeitung ebenfalls im Einklang mit der DSGVO erfolgen und der Schutz der betroffenen Personen gewährleistet werden. Es ist ein **schriftlicher Vertrag** mit dem Auftragsverarbeiter abzuschließen, der **gemäß Art. 28 DSGVO** Folgendes zu beinhalten hat: Bindung an den Verantwortlichen, Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorie der betroffenen Personen und Rechte und Pflichten des Verantwortlichen.

3) Datenschutz-Folgenabschätzung (Art. 35 DSGVO):

Eine **Datenschutz-Folgenabschätzung** ist laut Datenschutz-Grundverordnung erforderlich bei der „umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten".

In den Leitlinien der Artikel-29-Datenschutzgruppe (= ein unabhängiges Gremium, das die EU-Kommission in Datenschutzfragen berät und sich aus Vertretern der in jedem Mitgliedstaat des EWR bestehenden unabhängigen Datenschutz-Kontrollstellen zusammensetzt) betreffend Datenschutz-Folgenabschätzung ist festgehalten, dass die Verarbeitung von sensiblen Daten bei einem einzelnen

(Zahn-)Arzt nicht als „umfangreich" angesehen wird und damit **keine Datenschutz-Folgenabschätzung für Einzelordinationen** notwendig ist.

4) Datenschutzbeauftragter (Art. 37 DSGVO):

Die zahnärztliche Kerntätigkeit besteht nicht in einer „umfangreichen" Datenverarbeitung, sondern in der Behandlung von Patienten. Es ist damit aus heutiger Sicht **kein Datenschutzbeauftragter für Einzelordinationen** notwendig, wie auch von der Artikel-29-Datenschutzgruppe, im Leitfaden der Datenschutzbehörde der Republik Österreich und dem Bundesministerium für Gesundheit bestätigt wird.

Daher empfehlen wir, keine diesbezüglichen Angebote anzunehmen oder Verträge über die Beauftragung abzuschließen.

Jedenfalls notwendig ist, dass jeder Angehörige des zahnärztlichen Berufs für sich die Entscheidung fällt, dass ihn **keine Verpflichtung** zur Datenschutz-Folgenabschätzung und betreffend Bestellung eines Datenschutzbeauftragten trifft. Diese Entscheidung sollte jedenfalls **vor dem 25. Mai 2018 schriftlich festgehalten** werden, um einen Nachweis auf Anfrage der Aufsichtsbehörde (Datenschutzbehörde) vorlegen zu können *(siehe Vorlage 2)*.

5) Meldung einer Datenschutzverletzung (Art. 33 DSGVO):

Im Falle einer Verletzung des Schutzes von personenbezogenen Daten hat der Verantwortliche unverzüglich und möglichst **binnen 72 Stunden** ab Kenntnis derselben eine Meldung mit den notwendigen Informationen (Beschreibung der Verletzung, Anzahl der Betroffenen, Maßnahmen, wahrscheinliche Folgen, Dokumentation etc. – *Vorlage 3*) an die Datenschutzbehörde der Republik Österreich zu erstatten. Darüber hinaus können betroffene Personen unter Umständen auch einen allfällig entstandenen materiellen oder immateriellen Schaden geltend machen. Halten Sie diesbezüglich Rücksprache mit Ihrer Haftpflichtversicherung.

6) Angestellte – Zahnärztliche AssistentInnen

Die Grundsätze, Rechte der Betroffenen und Pflichten des Verantwortlichen gemäß der DSGVO sind auch bei der Verarbeitung von Daten der Angestellten der zahnärztlichen Ordination anzuwenden d.h. auch für die Personalverwaltung ist getrennt ein Verarbeitungsverzeichnis zu erstellen. Die Grundlage bzw. Rechtmäßigkeit der Verarbeitung, Speicherfristen etc. ergeben sich hier v.a. aus arbeitsrechtlichen Verpflichtungen und dem Dienstvertrag.

Als organisatorische Maßnahme ist jedenfalls eine Unterweisung der ZAss in Hinblick auf den sicheren Umgang mit Patientendaten unter besonderem Hinweis auf die gesetzliche Verschwiegenheitspflicht vorzunehmen und zu dokumentieren (*siehe Vorlage 4*).

Notwendige Änderungen und Anpassungen in den gesetzlichen Bestimmungen des Zahnärzte- und Zahnärztekammergesetzes vom zuständigen Bundesministerium insbesondere betreffend Rechte der Patienten werden noch erwartet.

Da noch einige Unklarheiten auch auf Seiten der vollziehenden Behörden bestehen, werden wir Sie über die Entwicklungen auf dem Laufenden halten. Für Informationen und Vorlagen wird keine Haftung übernommen.