ERSTE 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 Angehörigen des zahnärztlichen Berufs, da von diesen personenbezogene sensible Daten (Gesundheitsdaten der Patienten) verarbeitet werden und sie damit als „Verantwortliche" im Sinne der Verordnung gelten. Sowohl die EDV-unterstützte als auch die nicht automatisierte Verarbeitung der Daten ist davon betroffen. Durch passende **technische und organisatorische Maßnahmen**, die in der Datenschutz-Grundverordnung geregelt sind, sollen die Rechte der betroffenen Personen bzw. die Verarbeitung ihrer Daten geschützt werden. Diese Maßnahmen und die Einhaltung der Grundsätze der Datenverarbeitung sollten **gut dokumentiert** werden. Um die Einhaltung der neuen Bestimmungen zu gewährleisten, werden Verstöße nämlich mit besonders hohen Geldstrafen (weniger schwere Verstöße bis zu **€ 10 Mio**. bzw. 2 % vom Vorjahresumsatz, schwere Verstöße bis zu **€ 20 Mio.** bzw. 4 % vom Vorjahresumsatz) sanktioniert.

Folgende Aspekte und Neuerungen stehen dabei im Vordergrund:

Ad Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO):

Auch Angehörige des zahnärztlichen Berufs 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 im Anhang)*:

- den Namen des Angehörigen des zahnärztlichen Berufs
- die Kontaktdaten (Ordinationsadresse, Telefonnummer, allfällige E-Mail-Adresse)
- die Daten eines allfälligen Vertreters
- die Zwecke der Verarbeitung und Rechtmäßigkeit (Verweis aufs Zahnärztegesetz, insb. § 19 ZÄG – Dokumentationspflicht, Einwilligung der Patienten im Rahmen des Behandlungsvertrages)
- 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: Löschungsfristen, Speicherbegrenzung, Beschreibung technischer und organisatorischer Maßnahmen betreffend z.B. Zweckbindung, Datenminimierung, Richtigkeit der Daten, Vertraulichkeit durch angemessene Sicherheit.

Am Besten sollte das Verzeichnis von Verarbeitungstätigkeiten, die EDV-unterstützt erfolgen, 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. 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.

Allgemein muss weiters der **Serverraum** versperrbar bzw. versperrt sein! Außerdem müssen die „Datenverarbeitungen" dokumentiert werden, insbesondere wer worauf Zugriff hat.

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.

Ad 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-Folgeabschätzung ist festgehalten, dass die Verarbeitung von sensiblen Daten bei einem einzelnen (Zahn-)Arzt nicht als „umfangreich" angesehen wird und damit **keine Datenschutz-Folgeabschätzung für Einzelordinationen** notwendig ist. Eine zusätzliche Absicherung durch den österreichischen Verfassungsdienst ist im Laufen.

Ad 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 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-Folgeabschätzung und betreffend Benennung 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 im Anhang)*.

Ad 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.) an die Datenschutzbehörde in Österreich zu erstatten.

Notwendige Änderungen in den gesetzlichen Regelungen werden mit dem zuständigen BMG und BMJ noch ausverhandelt, z.B. betreffend Aufbewahrungsfristen der Dokumentation, Schadenersatzansprüche, Umgang mit dem Recht auf Löschung der Daten, Recht auf Datenübertragbarkeit etc.

Da noch einige Unklarheiten auch auf Seiten der vollziehenden Behörden bestehen, werden wir Sie über die Entwicklungen auf dem Laufenden halten.