Dental Branche auf EU-DSGVO nicht vorbereitet

Was Sie jetzt dazu wissen müssen

Die Dental Branche in der Schweiz ist auf die Europäische Datenschutz Grundverordnung (EU-DSGVO), die am 25.Mai 2018 in Kraft tritt, nicht vorbereitet. Die Auswirkungen, die dabei eintreten können, wenn die Compliance nicht hergestellt ist, kann teuer werden.

Einführung

Datenschutz ist mehr als eine Pflichtnummer: Die neu EU-Datenschutz-Grundverordnung gibt eine scharfe Marschrichtung vor. Zahnärzte müssen sich an die neue Rechtslage anpassen und die Daten ihrer Kunden effektiv zu schützen. Die Strafen für das Nichteinhalten der neuen Verordnung sind empfindlich und der Handlungsbedarf ist entsprechend akut. Mitarbeiter müssen informiert und Workflows und Tools überprüft werden, um sicherzustellen, dass Kundendaten gesetzestreu verarbeitet werden. Auch im Bereich IT fällt hier eine beträchtliche Anzahl an Massnahmen an. In diesem Archiv Beitrag finden Sie die wichtigsten Anforderungen der neuen Datenschutz-Grundverordnung und erfahren, wie eine ganzheitliche IT-Sicherheitslösung Sie bei der Einhaltung unterstützen kann.

Was ist die EU-Datenschutz-Grundverordnung?

Die EU-Datenschutz-Grundverordnung wurde im April 2016 vom europäischen Parlament verabschiedet und regelt die europaweite Modernisierung und Vereinheitlichung von Datenschutzgesetzen. Das Ziel ist das Garantieren des Schutzes von personenbezogenen Daten im Hinblick auf folgende Grundsätze:

- Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Die Verordnung ersetzt die in die Jahre gekommene Data Protection Directive (DPD) von 1995. Anders als die DPD ist die EU-DSGVO nicht „nur“ eine Richtlinie, sondern tatsächlich ein Gesetz. Dies bedeutet, dass die Verordnung nicht separat von den EU-Mitgliedsstaaten implementiert werden muss. Das Datum des Inkrafttretens war deshalb schon der 24. Mai 2016. Um Unternehmen die Zeit zu geben, sich an die neue Gesetzeslage anzupassen, wurde eine Übergangsfrist bis zum 25. Mai 2018 eingeräumt. Bis zu diesem Datum hat die Dentalbranche Zeit, die Vorgaben der EU-DSGVO umzusetzen. Bleibt dies aus, können bei einer Datenschutzpanne hohe Bussgelder verhängt werden.

Bitte beachten Sie, dass dieses Whitepaper als Denkanstoss zu den möglichen Auswirkungen der EU-DSGVO gedacht ist und eine umfassende rechtliche Beratung nicht ersetzen kann.

Warum ist die Dentalbranche besonders von der neuen EU-DSGVO betroffen?

Die EU Datenschutz-Grundverordnung regelt den Schutz von personenbezogenen Daten. Deshalb ist die Dental Branche, die personenbezogene Daten von Privatpersonen in der europäischen Union verarbeiten, besonders betroffen. Um deutlich zu machen, auf was für Daten das Gesetz sich bezieht, findet sich im Gesetzestext im Artikel 4 folgende Definition:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann."

Welche Rechte haben Kunden in der EU-DSGVO?

Die EU-DSGVO beschreibt die Vorgaben, die die Dental Branche umsetzen muss, wenn sie personenbezogene Daten verarbeiten. Obwohl viele Massnahmen schon in der Data Protection Directive definiert wurden, gibt es ein paar neue Anordnungen, die selbst für den Zahnarzt, die bis jetzt immer scheinbar „compliant" waren, eine sportliche Herausforderung darstellen werden. Ein kurzer Überblick:

- Recht auf Vergessenwerden: Kunden haben „das Recht zu verlangen, dass seine personenbezogenen Daten gelöscht werden" (Artikel 17)
- Zweckbindung und das Recht auf Zustimmung: Teilweise ist diese bereits im Datenschutzgesetz von 1995 festgeschrieben, wird aber in der EU-DSGVO konkretisiert. Jeder Kunde muss „umfassend und in einfacher Sprache" über den Verwendungszweck von Daten, die er preisgibt, informiert werden. Die Einwilligung zur Nutzung muss freiwillig erfolgen – sie darf also nicht an andere Bedingungen geknüpft sein (z. B. das Einwilligen zur werblichen Verwendung der Daten, um eine Bestellung abschließen zu können); dies ist im Erwägungsgrund Nr. 42 sowie 43 zur EU-DSGVO festgeschrieben.
- Zügige Meldung an die Aufsichtsbehörde: „Im Fall einer Verletzung des Schutzes meldet der Datenschutzverantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der Aufsichtsbehörde" (Artikel 33). Recht auf Datenübertragbarkeit: Kunden haben das Recht, die über sie gespeicherten Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten" (Artikel 20).

Was passiert bei Verstössen gegen die EU-DSGVO?

Nicht nur die in der EU-DSGVO beschriebenen Massnahmen sind neu: Auch die Bussgelder für die Dentalbranche, die diese entweder nicht oder nur mangelhaft umsetzen, wurden neu definiert. Wenn eine Datenschutzbehörde einen Verstoss feststellt, können – je nach Schwere eines Falls – folgende Bussgeld Beträge fällig werden:

- Bis zu € 20 Million Euro oder 4 % des weltweiten Firmenjahresumsatzes (der jeweils höhere Betrag wird angesetzt)
- Bis zu € 10 Million Euro oder 2 % des weltweiten Firmenjahresumsatzes (der jeweils höhere Betrag wird angesetzt)

Der Countdown läuft: Worauf kommt es an?

Trotz möglicher hoher Geldstrafen und der schnell ablaufenden Übergangsfrist hat die Dentalbranche noch keine Vorkehrungen getroffen. Mit so vielen möglichen Auswirkungen ist es wichtig, einen Überblick über die Implementierungsschwerpunkte zu bekommen.

Datenschutzbeauftragten benennen

Der erste Schritt ist die Benennung oder Bestellung eines Datenschutzbeauftragten. Dies gilt gemäß Artikel 37 für Behörden, öffentliche Stellen und Unternehmen, die personenbezogene Daten verarbeiten; also auch insbesondere für die Dentalbranche.

Brennpunkte und Sicherheitsdefizite identifizieren

- Welche von der EU-DSGVO betroffenen Daten werden im Unternehmen gesammelt oder verarbeitet?
- Werden die Daten ausreichend geschützt?
- Entspricht die eingesetzte Technologie dem Stand der Technik und ist diese entsprechend gesichert?
- Kann im Fall einer Datenschutzverletzung eine Meldung an die Datenschutzbehörde innerhalb 72 Stunden verschickt werden?
- Können Kunden Auskunft über die über sie gespeicherten Daten bekommen resp. kann die Löschung der Daten durchgeführt werden?
- Werden Daten zur Speicherung oder Verarbeitung an andere Unternehmen übermittelt? wer korrespondiert mit wem?
- Müssen hier gegebenenfalls Anpassungen in den Verträgen zur Auftrags-Datenverarbeitung vorgenommen werden? Wichtig hier: es gibt keinen „Bestandsschutz“ für Altverträge.

Workflows und Tools überprüfen

Dabei gilt es, sowohl die Mitarbeiter für das Thema zu sensibilisieren als auch die Workflows und Tools zu überprüfen und auf einen gesetzeskonformen Stand zu bringen. Die Erstellung von Compliance-Regeln, die den Umgang mit Informationen festlegen, ist hier ein wichtiger Schritt. Solche Regeln stellen eine Kombination aus technischen und organisatorischen Maßnahmen dar. So kann z. B. auf der Technologieebene ein Policy Management dafür sorgen, dass nur die für die Datenverarbeitung notwendigen Tools verwendet werden dürfen – und Anwendungen wie z. B. private Cloud-Speicherdienste nicht. Auch die Benutzung von externen Geräten soll unterbunden werden, damit Mitarbeiter die personenbezogenen Daten nicht auf z. B. USB-Sticks abspeichern können / dürfen.

IT-Infrastruktur überprüfen und absichern

Ein weiterer wichtiger Baustein ist die umfassende Absicherung der IT-Systeme. Bestehende Systeme müssen überprüft und neue Systeme eingeplant und ausgerollt werden. Der Schutz fängt schon auf der Netzwerk- und Kommunikationsebene an. Um unerlaubte Verbindungen zu unterbinden, soll eine Firewall verwendet werden. Web-Verkehr und andere Kommunikationswege aus dem Internet sollten gründlich überprüft werden, z. B. von einer Web-Schutz-Komponente oder auch einem E-Mail-Scan. Schutz gegen bösartige Malware kann mit Hilfe einer proaktiven Dateisystem- und Prozessüberwachung sichergestellt werden. Um dafür zu sorgen, dass das Betriebssystem und die Anwendungen auf dem aktuellsten Stand sind und Schwachstellen rechtzeitig behoben werden, kann ein Patch-Management-System dabei helfen, den Überblick über die Patchverteilung zu behalten. Nicht zuletzt ist die Datensicherung sehr relevant: Um dafür zu sorgen, dass Daten nicht verloren gehen können, muss ein Backup- und Wiederherstellungskonzept, sowie Notfallmanagement erarbeitet werden.

IT-Consulting Ebikon unterstützt Sie bei der Einhaltung der EU-DSGVO

Um die technischen und organisatorischen Anforderungen der EU-DSGVO erfüllen zu können, müssen die Schutzkomponente für die IT-Infrastruktur und Prozesse optimal aufeinander abgestimmt sein. Ein einheitliches Konzept für die Überwachung der Netzwerkinfrastruktur und die Benachrichtigung des Datenschutzbeauftragten im Fall eines möglichen Datenschutzvorfalles ist essenziell. Wir bieten ihnen mit unserem Fachwissen aus dem Bereichen ISO / IEC 2700x, ISO / IEC 31010, sowie der BestPractics, OWASP und ITIL einen umfassenden Schutz für eine komplette Lösung ihrer Praxis oder Depot an, die einen ausgefeilten proaktiven Schutz, mit effizienten und akkuraten Möglichkeiten für ein regelmässiges Reporting und Vorfallbenachrichtigung kombiniert. Zudem bieten wir Herstellerunabhängige Beratung an.

Ihr Kontakt

IT-Security & Cyber-Security Consulting

Security Engineering

Telefon: 079 267 40 41
Sagenhofstrasse 6
6030 Ebikon (LU)
E-Mail: support (@) it-consulting-ebikon.ch

IT-Security SSCP / CISSP
Wirtschaftsinformatik

<u>Hinweis:</u> Die EU-DSGVO erlangt Gültigkeit, ab 25. Mai 2018 für die gesamte Schweiz

Bitte beachten Sie, dass dieses Whitepaper als Denkanstoss zu den möglichen Auswirkungen der EU-DSGVO gedacht ist und eine umfassende rechtliche Beratung nicht ersetzen kann.