

REFERENZLEITFADEN

Cybersicherheit & DSG

Die Daten Ihrer Patientinnen und Patienten schützen.

Ihre IT-Infrastruktur absichern.

Ihre rechtlichen Pflichten verstehen.

DentalSystems Sàrl

Thomas Alvino, IT-Techniker

www.dentalsystems.ch | talvino@dentalsystems.ch | +41 77 245 48 44

Oktober 2026. Konform mit dem DSG (SR 235.1)

INHALTSVERZEICHNIS

Einleitung	7
Kapitel 1. Der rechtliche Rahmen: das DSGVO	8
1.1 Was ist das DSGVO?	8
1.2 Welche Daten sind betroffen?	8
1.3 Die drei Grundpflichten	10
1.4 Meldung von Verletzungen der Datensicherheit (Art. 24 DSGVO)	11
1.5 Rechte der Patientinnen und Patienten (Art. 25 DSGVO)	12
Mitteilung von Gesundheitsdaten (Art. 25 Abs. 3)	12
Verantwortung bei Auftragsbearbeitung (Art. 25 Abs. 4)	12
Zwingender Charakter des Auskunftsrechts (Art. 25 Abs. 5)	12
Kostenlosigkeit und Frist (Art. 25 Abs. 6 und 7)	12
Rechtsbehelfe der Patientinnen und Patienten bei Nichteinhaltung	12
1.6 Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSGVO)	14
1.7 Sanktionen (Art. 60 bis 66 DSGVO)	14
1.8 Die wichtigsten Unterschiede zum alten Recht (DSG von 1992)	16
1.9 Privacy by Design und Privacy by Default (Art. 7 DSGVO)	16
1.10 Datenschutz-Folgenabschätzung (Art. 22 DSGVO)	17
Beispiele, die eine DSFA erfordern	17
Inhalt der Folgenabschätzung	17
1.11 Neuere Rechtsprechung	17
Statthalteramt Bezirk Zürich, März 2025 (ST.2024.1046/ZM)	17
1.12 Bewährtes Vorgehen bei Auskunftsbegehren	18
Kapitel 2. Sichere E-Mail	19
2.1 Das Problem	19
2.2 Konforme Lösungen	19
Kapitel 3. Updates	21
3.1 Betriebssystem	21

3.2 Anwendungen und Branchensoftware	21
Kapitel 4. Datensicherung	22
4.1 Die 3-2-1-Regel	22
4.2 Warum die unveränderbare Kopie entscheidend ist	23
4.3 Die Wiederherstellung testen	23
Kapitel 5. Passwörter und Zwei-Faktor-Authentifizierung	24
5.1 Das Problem schwacher Passwörter	24
5.2 Ein starkes Passwort erstellen	24
5.3 Einen Passwortmanager verwenden	24
5.4 Zwei-Faktor-Authentifizierung (2FA)	24
Kapitel 6. Verschlüsselung von Festplatten und Archiven	25
6.1 Verschlüsselung der Arbeitsplätze	25
6.2 Verschlüsselte Container für sensible Archive	25
Kapitel 7. WLAN	26
7.1 Die empfohlene Konfiguration: drei getrennte Netze	26
Kapitel 8. Sicherer Fernzugriff	27
8.1 Das Risiko dauerhaft aktiver Gratisversionen	27
8.2 Empfohlene Lösungen	27
Kapitel 9. Phishing	28
9.1 Eine Phishing-E-Mail erkennen	28
9.2 Erweiterter Schutz: Filtern nach Label	28
Kapitel 10. Verwaltung der Benutzerzugriffe	29
10.1 Prinzip der minimalen Rechte	29
10.2 Regeln für die Kontoverwaltung	29
10.3 Eintritte und Austritte verwalten	29
10.4 Regelmässige Überprüfung der Zugriffsrechte	31
10.5 Hilfsmittel für die Zugriffsverwaltung	31
Kapitel 11. Polymorphe Malware und EDR-Schutz	32
11.1 Warum ein klassisches Antivirenprogramm nicht mehr genügt	32

11.2 Die Lösung: EDR (Endpoint Detection and Response).....	32
11.3 EDR, EPP, Antivirus: die Unterschiede verstehen	34
11.4 Die Rolle des IT-Dienstleisters	34
Kapitel 12. Modernisierung der IT-Ausstattung.....	35
12.1 Warum ein veralteter Computer gefährlich ist	35
12.2 Empfohlener Erneuerungszyklus	35
12.3 Sonderfall: iMacs mit Boot Camp	36
12.4 Die Migration planen	37
12.5 Sichere Vernichtung alter Geräte	37
Kapitel 13. Der Auftragsbearbeitungsvertrag (Art. 9 DSGVO)	38
13.1 Voraussetzungen für jede Auftragsbearbeitung	38
13.2 Wen betrifft der Auftragsbearbeitungsvertrag?	38
13.3 Was der Vertrag enthalten muss.....	40
13.4 Die Tools Ihres Dienstleisters prüfen	42
13.5 Verantwortung gegenüber den Patientinnen und Patienten (Art. 25 Abs. 4)	42
13.6 Mein aktueller Dienstleister hat keinen Vertrag: Was tun?.....	42
Kapitel 14. Schulung des Personals	43
14.1 Eine implizite Pflicht aus dem DSGVO	43
14.2 Empfohlene Schulungsinhalte.....	43
14.3 Private Geräte und BYOD	46
14.4 Temporäres Personal und Dritte	46
14.5 Die schriftliche interne Sicherheitsrichtlinie	47
14.6 Häufigkeit, Format und Evaluation	47
14.7 Geteilte Verantwortung.....	47
Kapitel 15. Cyberversicherungen.....	49
15.1 Was eine Cyberversicherung abdeckt.....	49
15.2 Wichtigste Versicherer in der Schweiz	49
15.3 Worauf zu achten ist.....	49
Kapitel 16. Was tun bei einem Vorfall	51

16.1 Szenario A: aktiver Angriff (Ransomware, Eindringen)	51
16.2 Szenario B: versehentlicher Verlust oder Datenabfluss	51
16.3 Was der EDÖB konkret tut	51
Kapitel 17. Reale Fälle in der Westschweiz	52
Groupe 3R, Réseau Radiologique Romand (April 2025 und April 2026)	52
Vidymed, Lausanne (Dezember 2024)	52
Die Schweiz in Zahlen	52
Typische Angriffsszenarien im medizinischen Bereich	53
Ransomware über ungesicherten Fernzugriff	53
Phishing mit gefälschter Rechnung eines Telekomanbieters	53
Falscher IT-Dienstleister	53
Infizierter USB-Stick	53
Was ein Angriff kostet	53
Konformitäts-Checkliste	54
Kommunikation	54
Infrastruktur	54
Datensicherung	54
Zugriff und Authentifizierung	54
DSG-Konformität	55
Schutz und Überwachung	55
Glossar zur Checkliste	56
Nützliche Kontakte und Ressourcen	58
Notfallkontakte	58
Gesetzestexte	58
Weitere Ressourcen	58
Häufige Fragen	59
Ist ein versehentlicher Datenverlust eine Verletzung der Datensicherheit im Sinne des DSG?	59
Mein IT-Dienstleister hat Daten gelöscht. Wer ist verantwortlich?	59

Ich bin seit 3 Jahren pensioniert, und ein 4 Jahre zurückliegender Datenabfluss wird entdeckt. Bin ich noch betroffen?	59
Meine iMacs laufen mit Windows 10 über Boot Camp: Können wir zu macOS zurückwechseln?	59
Welche Dentalsoftware soll ich wählen?	60
Eine Dentalassistentin verschickt ein Röntgenbild über WhatsApp. Wer ist verantwortlich?	60
Führt der EDÖB Kontrollen in Praxen durch?	60
Schreibt das DSG wie die DSGVO eine Frist von 72 Stunden vor?	60
Glossar.....	61
Impressum und Nutzungsbedingungen	64
Geistiges Eigentum	64
Erlaubte Nutzung	64
Untersagte Nutzung	64
Haftungsbeschränkung	64

Einleitung

Dieser Leitfaden richtet sich an Zahnärztinnen und Zahnärzte, an Praxisverantwortliche und an ihre Teams. Er entstand im Anschluss an die Konferenz der Schweizerischen Zahnärzte-Gesellschaft SSO, Sektion Neuenburg (SSO-NE), vom 12. März 2026 zur Cybersicherheit und zur Einhaltung des neuen Bundesgesetzes über den Datenschutz (revidiertes Datenschutzgesetz, DSG).

Das DSG, in Kraft seit dem 1. September 2023, auferlegt Zahnarztpraxen konkrete Pflichten beim Schutz von Patientendaten. Gesundheitsdaten (Röntgenbilder, Diagnosen, Behandlungspläne) sind besonders schützenswerte Personendaten im Sinne des Gesetzes und unterliegen strengeren Regeln.

Dieses Dokument behandelt alle an der Konferenz angesprochenen Themen, vertieft und ergänzt um zwei weitere: die Schulung des Personals und die Cyberversicherungen. Es ist als dauerhaftes Nachschlagewerk gedacht, zum Aufbewahren und für den täglichen Gebrauch.

Über diesen Leitfaden

Dieses Dokument dient der Information und der Weiterbildung. Es stellt keine Rechtsberatung dar. Für Fragen zu Ihrer konkreten Situation wenden Sie sich an eine auf Datenschutz spezialisierte Rechtsfachperson. Diese deutsche Fassung ist eine Übersetzung; massgebend ist die französische Fassung.

Kapitel 1. Der rechtliche Rahmen: das DSG

1.1 Was ist das DSG?

Das neue Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG, SR 235.1) ist am 1. September 2023 in Kraft getreten. Es ersetzt vollständig das alte Gesetz von 1992, aus einer Zeit, als Patientendossiers noch auf Papier geführt wurden und es in Arztpraxen noch kein Internet gab.

Das DSG modernisiert den Schweizer Rechtsrahmen und passt ihn an die heutige digitale Realität an. Es orientiert sich an den europäischen Standards der DSGVO, behält aber Schweizer Besonderheiten bei, namentlich bei den Sanktionen und den Meldefristen.

Kernpunkt: Für den Schutz der Daten der Patientinnen und Patienten ist die Praxisinhaberin oder der Praxisinhaber (die Zahnärztin oder der Zahnarzt) persönlich verantwortlich. Nicht der IT-Dienstleister, nicht die Praxisverwaltungssoftware, nicht der Cloud-Anbieter.

1.2 Welche Daten sind betroffen?

Eine Zahnarztpraxis bearbeitet täglich Personendaten, von denen viele besonders schützenswerte Personendaten im Sinne von Art. 5 Bst. c DSG sind:

- Gesundheitsdaten: Panoramaröntgenbilder, Einzelzahnaufnahmen, DVT (CBCT) / 3D-Scans, intra- und extraorale Fotos, Diagnosen, Behandlungspläne, Verordnungen, medizinische Vorgeschichte (Allergien, chronische Krankheiten, laufende Behandlungen), Operationsberichte, klinische Notizen, vollständige Behandlungshistorie, medizinische Korrespondenz mit anderen Behandelnden, Labors oder Fachpersonen
- Digitale Abdrücke und Modelle: digitale Zahnabdrücke, optische Abformungen aus Intraoralscannern, digitale 3D-Modelle (Gesundheitsdaten)
- Genetische Daten: Ergebnisse genetischer Untersuchungen, falls das Dossier solche enthält (Art. 5 Bst. c Ziff. 3 DSG)
- Administrative Daten: AHV-Nummern, Geburtsdaten, Kontaktangaben, unterzeichnete Einwilligungen, Versicherungsdaten (Grundversicherung nach KVG, Zusatzversicherungen); Anamnesebögen hingegen sind Gesundheitsdaten
- Finanzdaten: Rechnungen, Versicherungsabrechnungen, Zahlungsarten, Rechnungshistorie
- Korrespondenz: Austausch mit Patientinnen und Patienten per E-Mail oder Messenger, Austausch mit Versicherern, Auftragsformulare an Dentallabors mit Patientendaten

Besonders schützenswerte Personendaten unterliegen strengeren Regeln und erfordern verstärkte Sicherheitsmassnahmen; die Praxis und ihr Personal unterstehen zudem dem Berufsgeheimnis (Art. 321 StGB).

1.3 Die drei Grundpflichten

1. Wissen, wo Ihre Daten liegen und wie sie geschützt sind. Auf dem Praxisserver, auf einem Laptop, der abends mit nach Hause geht, in einer Cloud-Software, von der Sie nicht wissen, wo ihre Server stehen, in Ihrem unverschlüsselten E-Mail-Postfach, auf einem USB-Stick in einer Schublade, auf einer alten, nie gelöschten Festplatte, auf dem privaten Telefon einer Dentalassistentin, in E-Mails, die über Gmail an ein Labor geschickt wurden, in Datensicherungen, die seit Monaten niemand überprüft hat. Oft sind diese Daten durch ein Windows-Passwort «1234», ein veraltetes Gratis-Antivirenprogramm oder überhaupt nicht geschützt.
2. Den EDÖB bei einem Vorfall benachrichtigen. Art. 24 DSGVO verpflichtet den Verantwortlichen, so rasch als möglich jede Verletzung der Datensicherheit zu melden, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. Die Meldung muss mindestens die Art der Verletzung, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen nennen (Art. 24 Abs. 2). Der Auftragsbearbeiter (zum Beispiel Ihr IT-Dienstleister) muss Ihnen so rasch als möglich jede Verletzung melden, unabhängig von ihrer Schwere (Art. 24 Abs. 3). Wenn es zum Schutz der Patientinnen und Patienten erforderlich ist oder der EDÖB es verlangt, müssen Sie die betroffenen Personen zudem direkt informieren (Art. 24 Abs. 4).
3. Ihre Konformität nachweisen können. Im Rahmen einer Untersuchung kann der EDÖB verlangen, dass Sie die erforderlichen technischen und organisatorischen Massnahmen belegen (Art. 8 und 49 Abs. 3 DSGVO). Konkret heisst das, über eine aktuelle Dokumentation zu verfügen: Verzeichnis der Bearbeitungstätigkeiten, unterzeichneter Auftragsbearbeitungsvertrag mit Ihrem IT-Dienstleister, interne Sicherheitsrichtlinie, Nachweis der Schulung des Personals, Verfahren zur Reaktion auf Vorfälle, Protokoll der Datensicherungen und ihrer Wiederherstellungstests.

Fehlende Dokumentation bedeutet nicht zwingend eine Sanktion, macht Ihre Position bei einem Vorfall aber unhaltbar.

1.4 Meldung von Verletzungen der Datensicherheit (Art. 24 DSG)

Das Schweizer Recht verlangt eine Meldung «so rasch als möglich», eine bewusst offene Formulierung, im Gegensatz zur europäischen DSGVO, die eine strikte Frist von 72 Stunden festlegt. Der EDÖB empfiehlt, nach der Entdeckung der Verletzung so schnell wie möglich zu handeln.

Das offizielle Meldeportal ist unter databreach.edoeb.admin.ch erreichbar. Mit Zustimmung des Verantwortlichen kann der EDÖB die Meldung zur Analyse des Vorfalls an das Bundesamt für Cybersicherheit (BACS) weiterleiten.

Wichtig

Eine Meldung nach Art. 24 darf in einem Strafverfahren gegen die meldende Person nur mit deren Einverständnis verwendet werden (Art. 24 Abs. 6 DSG). Melden schadet Ihnen nicht. Nicht zu melden hingegen schon.

1.5 Rechte der Patientinnen und Patienten (Art. 25 DSG)

Jede Patientin und jeder Patient kann von der Praxis Auskunft darüber verlangen, ob Personendaten über sie oder ihn bearbeitet werden. Die Praxis muss dann innert 30 Tagen und kostenlos Folgendes mitteilen:

- Die Identität und die Kontaktdaten des Verantwortlichen
- Die bearbeiteten Personendaten als solche
- Den Bearbeitungszweck
- Die Aufbewahrungsdauer oder die Kriterien zu deren Festlegung
- Die Herkunft der Daten, soweit sie nicht bei der Patientin oder beim Patienten beschafft wurden
- Gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie deren Logik
- Die Empfänger, denen Daten bekanntgegeben werden, auch im Ausland

Mitteilung von Gesundheitsdaten (Art. 25 Abs. 3)

Gesundheitsdaten können Patientinnen und Patienten mit ihrer Einwilligung über eine von ihnen bezeichnete Gesundheitsfachperson mitgeteilt werden. Diese Bestimmung schützt sie vor medizinischen Informationen, die ohne Begleitung schwer zu deuten sind.

Verantwortung bei Auftragsbearbeitung (Art. 25 Abs. 4)

Setzt die Praxis einen Auftragsbearbeiter ein (Datenhoster, IT-Dienstleister), bleibt sie dafür verantwortlich, der Patientin oder dem Patienten Auskunft zu erteilen. Sie können Patienten nicht an Ihren IT-Dienstleister verweisen.

Zwingender Charakter des Auskunftsrechts (Art. 25 Abs. 5)

Keine Patientin und kein Patient kann im Voraus auf das Auskunftsrecht verzichten. Jede Vertragsklausel in diesem Sinn ist nichtig.

Kostenlosigkeit und Frist (Art. 25 Abs. 6 und 7)

Die Auskunft wird kostenlos und innert 30 Tagen erteilt. Kann diese Frist nicht eingehalten werden (Komplexität, Datenmenge), muss der Verantwortliche die Patientin oder den Patienten darüber informieren und die Verlängerung begründen.

Rechtsbehelfe der Patientinnen und Patienten bei Nichteinhaltung

Verweigert die Praxis die Antwort oder hält sie die Fristen nicht ein, stehen der Patientin oder dem Patienten mehrere Wege offen:

- Mahnung an die Praxis per eingeschriebenem Brief
- Anzeige beim EDÖB
- Zivilklage vor Gericht (Art. 32 DSG)
- Strafantrag, wenn die erteilten Auskünfte vorsätzlich falsch sind (Art. 60 DSG)

Vorsicht bei missverständlichen Formulierungen

Ein Unternehmensjurist wurde im März 2025 mit einer Busse von CHF 600 bestraft (Statthalteramt Bezirk Zürich, Entscheid ST.2024.1046/ZM), weil er geantwortet hatte, ein Unternehmen habe «keine Daten gefunden», obwohl es solche besass. Die irreführende Formulierung genügte, um den Tatbestand zu erfüllen. Selbst eine teilweise zutreffende Antwort, die einen falschen Eindruck von Vollständigkeit erweckt, kann bestraft werden.

1.6 Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG)

Grundsätzlich führt jeder Verantwortliche ein Verzeichnis seiner Bearbeitungstätigkeiten (Art. 12 Abs. 1 DSG). Unternehmen mit weniger als 250 Mitarbeitenden sind davon befreit, doch diese Ausnahme entfällt, wenn sie umfangreich besonders schützenswerte Personendaten bearbeiten oder ein Profiling mit hohem Risiko durchführen (Art. 12 Abs. 5 DSG und Art. 24 DSV). Eine Zahnarztpraxis bearbeitet naturgemäss Gesundheitsdaten, also besonders schützenswerte Personendaten: Je nach Anzahl Patientinnen und Patienten und Datenmenge greift die Ausnahme daher möglicherweise nicht. In jedem Fall wird dringend empfohlen, ein Verzeichnis zu führen, auch in kleinen Strukturen.

Das Verzeichnis muss mindestens enthalten: die Identität des Verantwortlichen, den Bearbeitungszweck, die Kategorien betroffener Personen und bearbeiteter Personendaten, die Empfänger, die Aufbewahrungsdauer und eine Beschreibung der getroffenen Sicherheitsmassnahmen.

1.7 Sanktionen (Art. 60 bis 66 DSG)

Vorsätzliche Verstösse gegen das DSG können mit Bussen bis zu CHF 250'000 bestraft werden. Diese Sanktionen richten sich gegen die verantwortlichen natürlichen Personen, nicht gegen das Unternehmen. In einer Zahnarztpraxis ist die Praxisinhaberin oder der Praxisinhaber direkt betroffen.

Verstoss	Höchstbusse	Voraussetzung
Vorsätzlich falsche oder unvollständige Auskünfte	CHF 250'000	Auf Antrag
Vorsätzliches Unterlassen der Information der betroffenen Person	CHF 250'000	Auf Antrag
Auftragsbearbeitung ohne Vertrag oder ohne Prüfung der Datensicherheit (Art. 9)	CHF 250'000	Auf Antrag
Bekanntgabe von Daten ins Ausland ohne Garantien	CHF 250'000	Auf Antrag
Falsche Auskünfte an den EDÖB in einer Untersuchung	CHF 250'000	Von Amtes wegen
Verweigerung der Mitwirkung gegenüber dem EDÖB	CHF 250'000	Von Amtes wegen

Verjährungsfrist: 5 Jahre (Art. 66 DSG). Pensionierung oder Aufgabe der Berufstätigkeit heben die Verantwortung für Taten, die während der Berufsausübung begangen wurden, nicht auf.

Nur vorsätzliche Verstösse sind strafbar

Fahrlässigkeit ist nach dem DSG nicht strafbar, kann aber zivilrechtliche Ansprüche geschädigter Patientinnen und Patienten nach sich ziehen. Guter Glaube und rasches Handeln wirken sich immer mildernd aus.

1.8 Die wichtigsten Unterschiede zum alten Recht (DSG von 1992)

Das revidierte DSG von 2023 ist eine Totalrevision des Gesetzes von 1992. Die wichtigsten Unterschiede:

Altes DSG (1992)	Revidiertes DSG (2023)
Schützt natürliche und juristische Personen	Schützt nur natürliche Personen
Keine Meldepflicht	Meldepflicht gegenüber dem EDÖB bei Verletzungen mit hohem Risiko
Begrenzte und seltene Bussen	Bussen bis CHF 250'000 (persönliche Haftung)
Keine Pflicht zur Folgenabschätzung	Folgenabschätzung bei hohem Risiko obligatorisch
Verzeichnis der Bearbeitungen freiwillig	Verzeichnis obligatorisch (mit begrenzten Ausnahmen)
Kein Privacy by Design	Privacy by Design und Privacy by Default obligatorisch (Art. 7)
Biometrische Daten nicht besonders geschützt	Biometrische und genetische Daten gelten als besonders schützenswert

1.9 Privacy by Design und Privacy by Default (Art. 7 DSG)

Art. 7 verankert zwei Grundprinzipien, die jeden IT-Entscheid in der Praxis leiten müssen:

Privacy by Design (Datenschutz durch Technik): Datenschutzmassnahmen müssen bereits bei der Wahl einer Software, eines Geräts oder eines Prozesses eingeplant werden. Es geht nicht darum, nachträglich zu korrigieren, sondern die Sicherheit von Anfang an vorzusehen.

Privacy by Default (datenschutzfreundliche Voreinstellungen): Die Standardeinstellungen jedes Systems müssen die Datenbearbeitung auf das absolut Notwendige beschränken. Eine Dentalsoftware sollte Patientendaten standardmässig weder mit Dritten teilen noch mehr Informationen speichern als nötig.

Konkret gelten diese Grundsätze bei der Wahl einer Praxisverwaltungssoftware, bei der Konfiguration eines Netzwerks, bei der Einrichtung eines neuen Arbeitsplatzes oder bei der Einführung eines Cloud-Tools. Jeder Entscheid muss die Frage einschliessen: «Schützt diese Lösung die Patientendaten standardmässig?»

1.10 Datenschutz-Folgenabschätzung (Art. 22 DSG)

Eine Datenschutz-Folgenabschätzung (DSFA) ist obligatorisch, wenn eine geplante Bearbeitung voraussichtlich ein hohes Risiko für die Rechte der betroffenen Personen mit sich bringt. Ob ein hohes Risiko besteht, hängt von der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ab.

Beispiele, die eine DSFA erfordern

- Einführung eines Gesichtserkennungssystems in der Praxis
- Umfangreiches Profiling von Patientinnen und Patienten
- Massenhafte Bearbeitung von Gesundheitsdaten mit künstlicher Intelligenz
- Umfassende Videoüberwachung der Praxis

Inhalt der Folgenabschätzung

Die DSFA muss eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Rechte der betroffenen Personen und die zum Schutz dieser Rechte vorgesehenen Massnahmen enthalten. Bleibt das Risiko trotz der vorgesehenen Massnahmen hoch, muss der Verantwortliche vor der Bearbeitung den EDÖB konsultieren (Art. 23 DSG).

Konkret für eine Zahnarztpraxis

Die meisten Zahnarztpraxen werden im Praxisalltag keine DSFA durchführen müssen. Hingegen könnte die Einführung einer neuen Software, die Patientendaten in grossem Umfang bearbeitet, eines KI-Tools zur Analyse von Röntgenbildern oder eines biometrischen Zutrittssystems diese Pflicht auslösen.

1.11 Neuere Rechtsprechung

Obwohl das DSG noch jung ist, zeichnen die ersten Entscheide bereits die Konturen seiner praktischen Anwendung.

Statthalteramt Bezirk Zürich, März 2025 (ST.2024.1046/ZM)

Ein Unternehmensjurist wurde mit einer Busse von CHF 600 bestraft, weil er auf ein Auskunftsbegehren geantwortet hatte, ein Unternehmen habe «keine Daten gefunden», obwohl es solche besass. Die irreführende Formulierung genügte, um den Tatbestand von Art. 60 Abs. 1 Bst. a DSG zu erfüllen.

Dieser Fall zeigt, dass selbst eine teilweise zutreffende Antwort, die einen falschen Eindruck von Vollständigkeit erweckt, bestraft werden kann. Für eine Zahnarztpraxis bedeutet das: Ein

Auskunftsbegehren einer Patientin oder eines Patienten muss innert 30 Tagen vollständig, präzise und überprüfbar beantwortet werden.

1.12 Bewährtes Vorgehen bei Auskunftsbegehren

- Immer innert 30 Tagen antworten
- Gleich beim ersten Mal vollständig antworten
- Missverständliche Formulierungen vermeiden (nie «wir haben nichts gefunden» antworten, wenn Daten vorhanden sind)
- Jedes Begehren und jede Antwort in einem internen Register dokumentieren
- Das Personal schulen, damit es diese Begehren korrekt behandelt
- Eine verantwortliche Person für Auskunftsbegehren bestimmen
- Vor jeder Bekanntgabe von Daten die Identität der anfragenden Person prüfen

Kapitel 2. Sichere E-Mail

Das Versenden von Patientendaten per E-Mail gehört zu den häufigsten und zugleich riskantesten Praktiken in Zahnarztpraxen. Ein Röntgenbild, das über Gmail, Bluewin oder Hotmail verschickt wird, läuft ohne Ende-zu-Ende-Verschlüsselung über Server, die oft ausserhalb der Schweiz stehen.

2.1 Das Problem

E-Mail-Dienste für Privatkunden sind nicht für medizinische Daten ausgelegt:

- **Gmail / Hotmail / Yahoo:** Server ausserhalb der Schweiz, keine Ende-zu-Ende-Verschlüsselung. Doppelt nicht konform.
- **Bluewin:** Server in der Schweiz, aber keine Ende-zu-Ende-Verschlüsselung. Swisscom kann technisch auf die Inhalte zugreifen. Für medizinische Daten ungenügend.
- **Infomaniak Mail:** besser geschützt als Gmail, aber keine native Ende-zu-Ende-Verschlüsselung. Geeignet für nicht sensible interne Kommunikation, nicht für Patientendaten.

2.2 Konforme Lösungen

- **HIN Mail:** die Referenz im Schweizer Gesundheitswesen. Sichere Kommunikation zwischen Gesundheitsfachpersonen, kompatibel mit dem nationalen HIN-Netzwerk. Die ideale Lösung für den Austausch mit Ärztinnen und Ärzten, Labors und Fachpersonen.
- **Proton:** 2014 am CERN in Genf von Wissenschaftlern und Ingenieuren gegründet, die über die von Edward Snowden aufgedeckte Massenüberwachung besorgt waren. Das Gründungsziel war, Kommunikationswerkzeuge zu schaffen, die niemand lesen kann, nicht einmal Proton selbst. Das Unternehmen hat seinen Sitz in Genf und untersteht dem Schweizer Recht, einer der strengsten Datenschutzgesetzgebungen der Welt. Gemäss seiner Datenschutzerklärung werden die Daten ausschliesslich auf Servern in der Schweiz, in Deutschland oder in Norwegen gespeichert; Deutschland

und Norwegen sind vom Bundesrat als Staaten mit angemessenem Schutzniveau anerkannt (Anhang 1 DSV).

Proton beschränkt sich nicht auf E-Mail. Das gesamte Ökosystem umfasst **ProtonMail** (verschlüsselte E-Mail, Ende-zu-Ende zwischen Proton-Nutzern), **Proton Drive** (verschlüsselter Cloud-Speicher, eine konforme Alternative zu Google Drive oder Dropbox), **Proton Pass** (verschlüsselter Passwortmanager), **Proton VPN** (virtuelles privates Netzwerk zur Absicherung von Fernverbindungen) und **Proton Calendar** (verschlüsselter Kalender). Für eine Zahnarztpraxis deckt dieses Ökosystem mehrere Bedürfnisse mit einer einzigen Lösung ab: sichere E-Mail für den Austausch mit Patientinnen und Patienten sowie Lieferanten ausserhalb des HIN-Netzwerks, Cloud-Speicher für sensible administrative Dokumente, ein Passwortmanager für das Team und ein VPN. Die Ende-zu-Ende-Verschlüsselung erfolgt nur zwischen Proton-Nutzern automatisch: An eine Adresse ausserhalb von Proton (ein Labor, eine Patientin) ist die Nachricht nur dann Ende-zu-Ende verschlüsselt, wenn man die passwortgeschützte E-Mail wählt; die Empfängerin oder der Empfänger muss dieses Passwort eingeben, um sie zu öffnen (die Nachricht läuft spätestens nach 28 Tagen ab). Proton verfolgt eine Zero-Access-Politik: Es kann Ende-zu-Ende verschlüsselte Inhalte nicht entschlüsseln, auch nicht auf Verlangen einer Behörde. Es kann jedoch von den zuständigen Schweizer Behörden verpflichtet werden, die Daten herauszugeben, über die es verfügt, insbesondere Metadaten: Adressen von Absender und Empfängern, Betreff der Nachrichten, Datum und Uhrzeit von Versand und Empfang.

Faustregel

Enthält eine E-Mail ein Röntgenbild, eine Diagnose, eine AHV-Nummer oder andere identifizierbare Patientendaten, muss sie über einen Ende-zu-Ende-verschlüsselten E-Mail-Dienst laufen. Ohne Ausnahme.

Kapitel 3. Updates

Updates schliessen Sicherheitslücken und verhindern die meisten der häufigsten Angriffe. Ein System ohne Updates ist ein verwundbares System. Jeder Tag ohne Sicherheitsupdate ist eine weitere offene Tür für Angreifer.

3.1 Betriebssystem

Windows und macOS müssen unbedingt aktuell gehalten werden. Der Support für Windows 10 endete im Oktober 2025: Nach diesem Datum entdeckte Lücken werden von Microsoft nicht mehr behoben, ausser auf Geräten, die im kostenpflichtigen Programm für erweiterte Sicherheitsupdates (ESU) registriert sind.

Für einen Arbeitsplatz ist Windows 11 heute die einzige Windows-Version, die ohne besondere Vorkehrungen noch Sicherheitsupdates erhält. Die Ausnahmen sind begrenzt: Das ESU-Programm verlängert Windows 10 für Unternehmen um höchstens drei Jahre (bis Oktober 2028), zu einem Preis, der sich jedes Jahr verdoppelt; bestimmte spezialisierte Editionen von Windows 10 LTSC, die Unternehmen und dedizierten Geräten vorbehalten sind, werden je nach Edition bis 2027, 2029 oder 2032 unterstützt; Server folgen ihrem eigenen Zeitplan (Windows Server). Das sind Übergangslösungen, keine dauerhafte Alternative: Jeder Computer mit Windows 7, 8 oder 10 muss ersetzt oder migriert werden.

3.2 Anwendungen und Branchensoftware

Dentalsoftware muss regelmässig aktualisiert werden, unabhängig davon, welche Lösung in Ihrer Praxis eingesetzt wird. Eine alte Version kann ausnutzbare Lücken enthalten oder Datenbeschädigungen verursachen. Das betrifft Praxisverwaltungssoftware ebenso wie Bildgebungs- und Röntgensoftware.

Auch Webbrowser, PDF-Reader und Office-Pakete müssen aktuell gehalten werden. Sie sind häufige und oft vernachlässigte Angriffswege.

Klären Sie mit Ihrem Softwareanbieter, ob die installierte Version noch unterstützt wird und Sicherheitsupdates erhält. Ist das nicht mehr der Fall, planen Sie die Migration auf eine aktuelle Version oder eine alternative Lösung.

Empfehlung

Aktivieren Sie die automatischen Updates auf allen Geräten. Planen Sie einen wöchentlichen Neustart ein, damit ausstehende Sicherheitsupdates installiert werden können. Ein Computer, der nie neu gestartet wird, sammelt ungeschlossene Sicherheitslücken an.

Kapitel 4. Datensicherung

Die Datensicherung ist Ihre letzte Verteidigungslinie. Bei Ransomware, menschlichem Versagen oder Hardwaredefekt entscheidet sie darüber, ob Sie alles verlieren oder den Betrieb innert weniger Stunden wieder aufnehmen.

4.1 Die 3-2-1-Regel

3 Kopien Ihrer Daten (das Original und zwei Sicherungen), auf 2 verschiedenen Datenträgern, davon 1 ausserhalb der Praxis an einem anderen Ort aufbewahrt, damit ein Brand, ein Wasserschaden oder ein Diebstahl nicht alle Kopien gleichzeitig zerstört. Diese Regel empfiehlt das Bundesamt für Cybersicherheit (BACS). Zudem wird empfohlen, dass eine der Kopien getrennt oder unveränderbar ist: eine Version, die niemand ändern oder löschen kann, nicht einmal eine Ransomware (Variante 3-2-1-1-0, siehe unten).

Eine unveränderbare Kopie bedeutet nicht zwingend eine Festplatte, die jeden Abend ausgesteckt wird. Technologien wie automatische Snapshots, Cloud-Speicher mit unveränderbarer Aufbewahrung oder versionierte Sicherungen schützen die Daten ohne tägliches menschliches Eingreifen. Ihr IT-Dienstleister muss Ihnen ein auf Ihre Praxis zugeschnittenes Sicherungssystem vorschlagen und einrichten können, das der 3-2-1-Regel entspricht und schriftlich dokumentiert ist. Es ist nicht Aufgabe der Praxisinhaberin oder des Praxisinhabers, die Sicherungsarchitektur zu entwerfen; sie oder er muss jedoch sicherstellen, dass sie existiert, funktioniert und getestet wird.

Ein konkretes Umsetzungsbeispiel: Der Praxisserver hält die Arbeitsdaten (Kopie 1), eine automatische Sicherung wird auf ein NAS oder eine dedizierte Festplatte in der Praxis repliziert (Kopie 2), und eine dritte Kopie wird jede Nacht in einen sicheren Cloud-Speicher in der Schweiz mit unveränderbarer Aufbewahrung übertragen (Kopie 3). Verschlüsselt eine Ransomware die ersten beiden Kopien, bleibt die dritte unversehrt und ermöglicht eine vollständige Wiederherstellung.

Die Lösung lässt sich an die Grösse der Praxis und an die Datenmenge anpassen. Manche Dienstleister wenden die 3-2-1-1-0-Regel an, die der Grundregel eine Offline- oder unveränderbare Kopie hinzufügt (die zweite «1») und bei den Wiederherstellungstests null Fehler anstrebt (die «0»). Entscheidend ist nicht die Komplexität des Systems, sondern die Gewissheit, dass Ihre Patientendaten im Schadenfall wiederhergestellt werden können, und zwar innert einer Frist, die mit der Fortführung Ihrer Tätigkeit vereinbar ist.

Kann Ihr aktueller IT-Dienstleister Ihnen nicht klar erklären, wie Ihre Sicherungsstrategie aussieht, wo sich Ihre Kopien befinden, ob eine davon ausserhalb der Praxis aufbewahrt wird,

ob eine Kopie getrennt oder unveränderbar ist und wann sie zuletzt getestet wurden, ist das ein Warnsignal.

4.2 Warum die unveränderbare Kopie entscheidend ist

Moderne Ransomware erkennt und verschlüsselt alle mit dem Netzwerk verbundenen Sicherungen. Eine dauerhaft angeschlossene externe Festplatte wird beim Angriff ebenfalls verschlüsselt. Nur eine physisch getrennte oder logisch isolierte Kopie (unveränderbare Versionierung) bleibt unversehrt.

4.3 Die Wiederherstellung testen

Eine ungetestete Datensicherung ist eine Scheinsicherheit

Testen Sie regelmässig die tatsächliche Wiederherstellung einer Stichprobe von Daten, zum Beispiel einiger Patientendossiers oder einiger Röntgenbilder. Die Empfehlungen der SSO und der FMH verlangen mindestens einen Test pro Jahr; ein monatlicher Test ist empfehlenswert und deckt ein Problem früher auf. Prüfen Sie, ob sich die Dateien korrekt öffnen lassen und die Daten verwendbar sind. Ohne regelmässige Tests stellen Sie zu spät fest, dass Ihre Sicherungen beschädigt oder unvollständig sind.

Kapitel 5. Passwörter und Zwei-Faktor-Authentifizierung

5.1 Das Problem schwacher Passwörter

Ein Passwort wie «1234», der Name der Praxis oder ein Geburtsdatum ist in Sekunden erraten. Ein Konto, das das ganze Team teilt, verunmöglicht bei einem Vorfall jede Nachvollziehbarkeit. Ohne Zwei-Faktor-Authentifizierung ist ein einziges Passwort die einzige Hürde zwischen einem Angreifer und Ihren Patientendaten.

5.2 Ein starkes Passwort erstellen

Mindestens 12 Zeichen, mit Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen. Eine konkrete Methode: Wählen Sie zwei Wörter ohne logischen Zusammenhang und fügen Sie eine einprägsame Zahl sowie Sonderzeichen hinzu, die auf der Tastatur nebeneinanderliegen.

Beispiel

CarmolTropfen91()=. Leicht zu merken, kein Bezug zu Ihrer Praxis oder zu Ihnen selbst.

5.3 Einen Passwortmanager verwenden

Ein Passwortmanager speichert alle Ihre Zugangsdaten verschlüsselt. Sie müssen sich nur ein einziges Master-Passwort merken.

- Proton Pass: Ende-zu-Ende verschlüsselt, Server in der Schweiz, in Deutschland oder in Norwegen
- Bitwarden: Open Source, selbst hostbar
- KeePass: lokale Speicherung, keine Cloud

5.4 Zwei-Faktor-Authentifizierung (2FA)

Die 2FA fügt nach dem Passwort eine zweite Prüfung hinzu: einen temporären Code auf Ihrem Telefon, eine Push-Benachrichtigung oder einen physischen Schlüssel. Selbst wenn Ihr Passwort kompromittiert ist, kann ein Angreifer ohne diesen zweiten Faktor nicht auf das Konto zugreifen.

Zu aktivieren für: geschäftliche E-Mail, Dentalsoftware (falls verfügbar), Cloud-Sicherungen, Fernzugriff, Bankkonten.

Kapitel 6. Verschlüsselung von Festplatten und Archiven

6.1 Verschlüsselung der Arbeitsplätze

Ein aus einem Auto gestohlener Laptop oder ein bei einem Einbruch entwendeter Server gibt sofortigen Zugriff auf alle Daten, wenn die Festplatte nicht verschlüsselt ist. Die Verschlüsselung macht die Daten ohne den Entschlüsselungsschlüssel völlig unlesbar.

- **Windows:** BitLocker, in Windows Pro und Enterprise integriert, kostenlos. Auf allen Geräten zu aktivieren.
- **macOS:** FileVault, integriert, kostenlos. In den Systemeinstellungen zu aktivieren.
- **Server:** Hardwareverschlüsselung (TPM), BitLocker oder Softwareverschlüsselung je nach Infrastruktur.

6.2 Verschlüsselte Container für sensible Archive

Für externe Festplatten mit Patientenarchiven, Buchhaltung oder alten Sicherungen funktioniert ein verschlüsselter Container wie ein digitaler Tresor: nur mit einem starken Passwort zugänglich.

- **Windows:** BitLocker To Go (externe Festplatten), VeraCrypt (verschlüsselte Container)
- **macOS:** FileVault für externe Festplatten
- **Plattformübergreifend:** VeraCrypt: Open Source, robust, kostenlos

Kapitel 7. WLAN

Ein einziges WLAN, das sich Personal, medizinische Geräte und Patienten teilen, ist eine grosse Sicherheitslücke. Ohne Trennung kann ein infiziertes Telefon im Gästernetz den Praxisserver erreichen.

7.1 Die empfohlene Konfiguration: drei getrennte Netze

- **Hauptnetz:** Arbeitsplätze, Server, Drucker, isoliert und geschützt.
- **Medizinisches Netz:** Röntgengeräte, Sensoren, vernetzte Geräte, falls je nach Infrastruktur nötig.
- **Gästernetz:** Patientinnen und Patienten. Nur Internetzugang, keine Sicht auf das interne Netz der Praxis.

Die Trennung der Netze ist das digitale Gegenstück zur Wand zwischen Wartezimmer und Behandlungszimmer. Empfohlen wird das Protokoll WPA3, sofern die Hardware es unterstützt; WPA2 ist das akzeptable Minimum.

WLAN-Passwort

Das Passwort des Hauptnetzes nie im Wartezimmer aushängen. Das Gästernetz kann ein Captive Portal mit einem Tagescode oder einem Einmalcode nutzen, der auf Anfrage abgegeben wird.

Kapitel 8. Sicherer Fernzugriff

Fernzugriffs-Tools sind für die IT-Fernwartung unverzichtbar, doch schlecht konfiguriert sind sie ein bevorzugtes Einfallstor für Angreifer.

8.1 Das Risiko dauerhaft aktiver Gratisversionen

Typisches Szenario: Ein Fernsteuerungstool, das mit einem schwachen Passwort dauerhaft in Bereitschaft bleibt, ermöglicht es einem Angreifer, nachts in die Praxis einzudringen und dort eine Ransomware einzuschleusen. Die Praxis verliert mehrere Arbeitstage, und nur die ausser Reichweite gesicherten Daten können wiederhergestellt werden.

TeamViewer, AnyDesk oder ein anderes Fernzugriffs-Tool rund um die Uhr ohne verstärkte Sicherheit aktiv zu lassen, ist, als würde man eine Tür zu Ihrer Praxis dauerhaft offen lassen.

8.2 Empfohlene Lösungen

Lösung	Einsatz	Sicherheit	Empfehlung
TeamViewer / AnyDesk gratis	Gelegentlich	Gering	Für medizinische Daten vermeiden
TeamViewer Pro + 2FA	Punktuell	Angemessen	Akzeptabel, wenn gut konfiguriert
Professionelles VPN	Dauerhaft	Hoch	WireGuard oder OpenVPN empfohlen
RMM für Unternehmen	Fernwartung	Sehr hoch	NinjaOne, Datto, Atera

Goldene Regel

Kein Fernzugriff darf als dauerhaft offener Zugang konfiguriert sein. Jede Verbindung muss protokolliert, authentifiziert und zeitlich begrenzt sein. Je höher die Berechtigungsstufe (Serverzugriff, Patientendaten), desto sicherer muss die Lösung sein.

Kapitel 9. Phishing

Phishing bleibt der häufigste Angriffsweg gegen Arztpraxen. Der Angreifer gibt sich als vertrauenswürdiger Kontakt aus (Swisscom, Ihre Bank, Ihr IT-Dienstleister), um Zugangsdaten zu erhalten oder jemanden dazu zu bringen, eine infizierte Datei zu öffnen.

9.1 Eine Phishing-E-Mail erkennen

- Verdächtige Absenderadresse (ungewöhnliche Domain, Tippfehler)
- Künstliche Dringlichkeit: «Ihr Konto wird in 24 Stunden gesperrt»
- Aufforderung, auf einen Link zu klicken oder einen unerwarteten Anhang zu öffnen
- Rechtschreibfehler oder ungewöhnliche Formulierungen
- Aufforderung zur Angabe von Zugangsdaten, Passwörtern oder Bankdaten

9.2 Erweiterter Schutz: Filtern nach Label

E-Mails von regelmässigen, vertrauenswürdigen Absendern können automatisch gefiltert und mit einem Label versehen werden. Jede E-Mail, die angeblich von einem dieser Kontakte stammt, vom Filter aber nicht erkannt wird, muss sofort Verdacht wecken.

Diese Konfiguration ist über die integrierten Filterregeln Ihres E-Mail-Dienstes oder über professionelle Anti-Phishing-Lösungen möglich. Entscheiden Sie sich für ein Filtertool eines Drittanbieters, prüfen Sie unbedingt, wo die Server stehen, die den Inhalt Ihrer Nachrichten analysieren.

Eine Lösung, die Ihre E-Mails über Server ausserhalb der Schweiz leitet, kann im Hinblick auf Art. 16 DSGVO problematisch sein, insbesondere wenn diese E-Mails Patientendaten enthalten. Bevorzugen Sie Lösungen, deren Datenbearbeitung in der Schweiz erfolgt oder, falls das nicht möglich ist, in einem Staat, den der Bundesrat als Staat mit angemessenem Schutzniveau anerkannt hat. Ihr IT-Dienstleister muss Ihnen den Standort der Server und die anwendbaren Schutzgarantien bestätigen können.

Kapitel 10. Verwaltung der Benutzerzugriffe

Festzulegen, wer worauf zugreifen darf, senkt die internen Risiken erheblich und begrenzt den Schaden, wenn ein Konto kompromittiert wird.

10.1 Prinzip der minimalen Rechte

Alle Benutzerinnen und Benutzer dürfen nur auf die Daten zugreifen, die für ihre Funktion unbedingt nötig sind. Dieses in der IT-Sicherheit weithin anerkannte Prinzip hängt direkt mit Art. 8 DSGVO zusammen, der angemessene organisatorische Massnahmen zur Gewährleistung der Datensicherheit verlangt.

In einer Zahnarztpraxis sind die Rollen klar getrennt, und die Zugriffe müssen diese Realität abbilden. Eine Dentalassistentin muss Patientendossiers einsehen und Termine vergeben können, braucht aber keinen Zugriff auf die Buchhaltung der Praxis, auf Personaldaten oder auf die Administrationseinstellungen des Servers. Eine Dentalhygienikerin braucht die Behandlungshistorie ihrer Patientinnen und Patienten, nicht die unbezahlten Rechnungen. Ein externer Buchhalter braucht die Finanzdaten, nicht die Röntgenbilder.

Wird ein Konto kompromittiert (erfolgreiches Phishing, gestohlenen Passwort), begrenzt das Prinzip der minimalen Rechte den Schaden: Der Angreifer kann nur auf die für dieses Konto freigegebenen Daten zugreifen. Teilen alle dasselbe Login mit Vollzugriff, legt eine einzige Kompromittierung die gesamte Praxis offen.

10.2 Regeln für die Kontoverwaltung

Ein Konto pro Person, nie ein geteiltes Konto. Generische Konten wie «praxis», «admin», «empfang» oder «buchhaltung» verunmöglichen jede Nachvollziehbarkeit. Bei einem Vorfall lässt sich nicht feststellen, wer was wann getan hat. Alle Mitarbeitenden müssen über ein eigenes Login verfügen, mit einem persönlichen Passwort, das sie mit niemandem teilen.

Administratorkonten sind technischen Arbeiten vorbehalten (Installation von Software, Netzwerkkonfiguration, Wartung) und dürfen nie für die tägliche Arbeit verwendet werden. Nutzt Ihr IT-Dienstleister ein Administratorkonto, muss dieses von den Konten des Personals getrennt, mit einer Zwei-Faktor-Authentifizierung geschützt und einer Protokollierung der Anmeldungen unterstellt sein.

10.3 Eintritte und Austritte verwalten

Der Eintritt einer neuen Mitarbeiterin oder eines neuen Mitarbeiters muss die Einrichtung eines persönlichen Kontos auslösen, dessen Rechte genau der Funktion entsprechen. Die neue Person muss eine Schulung zu den Regeln für die Nutzung der IT-Systeme der Praxis erhalten, einschliesslich der Passwortrichtlinie und der Verbote (WhatsApp, private USB-Sticks, Übertragung von Daten auf nicht autorisierte Geräte).

Der Austritt einer Mitarbeiterin oder eines Mitarbeiters, ob freiwillig oder nicht, muss die sofortige Deaktivierung aller Zugänge nach sich ziehen: Benutzerkonto, E-Mail, Praxisverwaltungssoftware, Fernzugriff, Cloud-Speicher. Nicht auf den nächsten Tag verschieben, nicht auf Ende Monat aufschieben. Unzufriedene ehemalige Mitarbeitende, die noch über ihre Zugänge verfügen, sind ein reales Risiko, sowohl für die Datensicherheit als auch für die Verantwortung der Praxis nach dem DSGVO.

10.4 Regelmässige Überprüfung der Zugriffsrechte

Zugriffsrechte sind nicht in Stein gemeisselt. Mitarbeitende wechseln die Funktion, ein Praktikum geht zu Ende, ein externer Dienstleister wird nicht mehr beigezogen. Ohne regelmässige Kontrolle häufen sich veraltete Zugänge an und schaffen unsichtbare Lücken. Planen Sie eine vierteljährliche Überprüfung: Gehen Sie die Liste der aktiven Konten durch und prüfen Sie, ob jedes Konto einer Person entspricht, die noch in der Praxis tätig ist, ob die vergebenen Rechte der aktuellen Funktion entsprechen und ob alle unbenutzten Konten deaktiviert sind. Dokumentieren Sie diese Überprüfung schriftlich: Sie gehört zu den organisatorischen Massnahmen, deren Vorlage der EDÖB verlangen kann.

10.5 Hilfsmittel für die Zugriffsverwaltung

Bestimmte Geräte und Technologien ermöglichen es, die Verwaltung von Konten und Zugriffsrechten in einer Praxis zu zentralisieren und zu vereinfachen. Ein professioneller NAS-Server (zum Beispiel ein Gerät von Synology) bietet eine Verwaltung von Benutzern und freigegebenen Ordnern mit feingranularen Berechtigungen: Alle Mitarbeitenden greifen nur auf die für ihre Funktion freigegebenen Verzeichnisse zu, und Anmeldungen sowie Änderungen werden protokolliert. Diese Lösung eignet sich für kleine und mittlere Praxen ohne eigenen Server.

Für Praxen mit einer fortgeschritteneren Windows-Infrastruktur ermöglicht ein zentraler Verzeichnisdienst wie Active Directory, alle Konten, Passwörter, Sicherheitsgruppen und Zugriffsrichtlinien an einer einzigen Stelle zu verwalten. Er erleichtert das Anlegen und Löschen von Konten, die automatische Anwendung von Sicherheitsregeln (Passwortkomplexität, Sperrung nach Fehlversuchen, Ablauf von Sitzungen) und die Einschränkung der Zugriffe nach Funktionsgruppen (Zahnärztinnen und Zahnärzte, Dentalassistentinnen, Buchhaltung, Administration). Ihr IT-Dienstleister muss Sie beraten können, welche Lösung am besten zur Grösse und zur Organisation Ihrer Praxis passt.

Kapitel 11. Polymorphe Malware und EDR-Schutz

Polymorphe Malware ist ein Schadprogramm, das seinen eigenen Code bei jeder Infektion verändern kann, um von klassischen Antivirenprogrammen nicht erkannt zu werden. Das ist keine neue Bedrohung; diese Techniken gibt es seit den 1990er-Jahren, doch die künstliche Intelligenz hat ihre Verfeinerung stark beschleunigt. Was einen Angreifer früher Wochen an Entwicklung kostete, entsteht heute in wenigen Minuten.

11.1 Warum ein klassisches Antivirenprogramm nicht mehr genügt

Ein herkömmliches Antivirenprogramm arbeitet mit Signaturen: Es vergleicht jede Datei mit einer Datenbank bekannter Bedrohungen. Ändert die Malware bei jeder Infektion ihre Form, wird sie nie erkannt. Das ist wie ein Wachmann, der nur polizeilich erfasste Kriminelle erkennt. Ändert der Kriminelle sein Gesicht, bleibt er unbemerkt.

Dieses Erkennungsmodell bleibt gegen bekannte und weit verbreitete Bedrohungen nützlich, genügt aber nicht gegen gezielte Angriffe oder neue Malware, die noch nie katalogisiert wurde. Genau diese Art von Angriff trifft jedoch Arztpraxen: massgeschneiderte Ransomware, oft nach einer Phase der Auskundschaftung des Netzwerks des Opfers.

11.2 Die Lösung: EDR (Endpoint Detection and Response)

Ein EDR sucht kein bekanntes Gesicht, es beobachtet ein Verhalten. Beginnt ein Programm, massenhaft Patientendateien zu öffnen und eine nach der anderen zu verschlüsseln, erkennt das EDR dies, stoppt das Programm und stellt es in Echtzeit unter Quarantäne, bevor es fertig ist. Es spielt keine Rolle, wie das Programm aussieht oder ob es bereits erfasst wurde.

Über die Verhaltenserkennung hinaus bietet ein EDR Funktionen, die ein klassisches Antivirenprogramm nicht hat: automatische Isolierung des kompromittierten Geräts, um eine Ausbreitung im übrigen Netzwerk zu verhindern, vollständige Protokollierung des Vorfalls (welche Dateien betroffen waren, zu welcher Uhrzeit, durch welchen Prozess), Möglichkeit zur Wiederherstellung veränderter Dateien (Rollback) sowie Echtzeitwarnungen an Ihren IT-Dienstleister.

Zu den anerkannten EDR-Lösungen auf dem Markt gehören SentinelOne, CrowdStrike, Sophos Intercept X, Microsoft Defender for Endpoint und ESET Inspect. Sie unterscheiden

sich in Funktionsumfang und Preis; die Wahl sollte gemeinsam mit Ihrem IT-Dienstleister getroffen werden, abhängig von der Grösse Ihrer Praxis und Ihrer bestehenden Infrastruktur.

11.3 EDR, EPP, Antivirus: die Unterschiede verstehen

Ein klassisches Antivirenprogramm erkennt bekannte Bedrohungen anhand von Signaturen. Eine EPP (Endpoint Protection Platform) kombiniert das Antivirenprogramm mit zusätzlichen Schichten: lokale Firewall, Kontrolle von USB-Geräten, Webfilter. Ein EDR geht weiter und ergänzt Verhaltensanalyse, automatisierte Reaktion und vollständige Sicht auf das, was auf jedem Gerät geschieht. Für eine Zahnarztpraxis, die besonders schützenswerte Personendaten bearbeitet, ist ein von Ihrem IT-Dienstleister verwaltetes EDR das empfohlene Schutzniveau.

Zum Beispiel bietet ein klassisches Antivirenprogramm wie Windows Defender (kostenlos in Windows enthalten) einen Basisschutz auf Signaturbasis. Eine EPP wie Bitdefender GravityZone oder ESET Protect fügt zusätzliche Präventionsschichten hinzu. Ein EDR wie SentinelOne oder CrowdStrike Falcon ergänzt die Verhaltenserkennung und die automatisierte Reaktion. Die Kosten steigen mit dem Schutzniveau, doch die finanziellen Folgen eines erfolgreichen Angriffs übersteigen die Investition in eine geeignete Lösung bei Weitem.

11.4 Die Rolle des IT-Dienstleisters

Ein EDR konfiguriert sich nicht von selbst. Es erfordert eine an Ihre Umgebung angepasste Einrichtung (Ausnahmen für legitime Dentalsoftware, Alarmschwellen, Richtlinie für automatische Reaktionen) und eine regelmässige Überwachung der erzeugten Alarme.

Ihr IT-Dienstleister muss diese Lösung einführen, konfigurieren und überwachen können. Fragen Sie ihn, ob er auf den von ihm betreuten Geräten ein EDR einsetzt, ob er die Alarme in Echtzeit erhält und wie schnell er reagiert, wenn eine aktive Bedrohung erkannt wird. Begnügt sich Ihr Dienstleister damit, ein Gratis-Antivirenprogramm ohne Überwachung zu installieren, ist das Schutzniveau für medizinische Daten, die dem DSGVO unterstehen, ungenügend.

Kapitel 12. Modernisierung der IT-Ausstattung

Lassen Sie in einer modernen Praxis nie einen oder zwei alte Arbeitsplätze stehen. Ein einziger veralteter oder nicht aktualisierter Computer genügt, um das gesamte Netzwerk zu kompromittieren. In einer Zahnarztpraxis bedeutet das ein reales Risiko eines Datenabflusses oder einer Lösegeldforderung, die Röntgenbilder, Diagnosen, administrative oder buchhalterische Daten betrifft. Ein einziges schwaches Glied genügt, um die gesamte Praxis zu gefährden.

12.1 Warum ein veralteter Computer gefährlich ist

Ein veralteter oder nie neu gestarteter Windows-Computer sammelt bekannte und öffentlich dokumentierte Sicherheitslücken an. Angreifer verfügen über Datenbanken, in denen diese Lücken verzeichnet sind, und über automatisierte Werkzeuge, um sie auszunutzen. Wird eine davon ausgenutzt, ist die Angriffskette vorhersehbar: über den verwundbaren Computer einen ersten Zugang zum lokalen Netzwerk erlangen, die Schutzmassnahmen der neueren Computer umgehen, indem man sich lateral im Netzwerk bewegt, den Speicherserver erreichen, auf die Branchensoftware oder die Sicherungen zugreifen und dann die sensiblen Daten stehlen oder verschlüsseln. All das kann innert weniger Stunden geschehen, oft nachts oder am Wochenende, wenn niemand hinschaut.

Das Problem betrifft nicht nur die sichtbaren Arbeitsplätze. Oft vergessene Geräte sind ebenso kritisch: ein alter Server, der «übergangsweise» noch läuft, ein Netzwerkdrucker, dessen Firmware nie aktualisiert wurde, ein WLAN-Router älterer Generation, ein NAS mit veraltetem Betriebssystem. Jedes dieser Geräte ist ein potenzieller Einstiegspunkt.

12.2 Empfohlener Erneuerungszyklus

Als Faustregel gilt: Arbeitsplätze spätestens alle 5 Jahre erneuern. Diese Frist ist nicht willkürlich: Sie entspricht der durchschnittlichen Dauer, während der ein Hersteller die Kompatibilität mit den Sicherheitsupdates des Betriebssystems und der Hardwarekomponenten (Treiber, Firmware, TPM-Modul) gewährleistet.

Entscheidend ist nicht das Alter des Computers an sich, sondern seine Fähigkeit, die neuesten Sicherheitsupdates zu erhalten. Ein 4 Jahre alter, Windows-11-kompatibler Computer mit TPM-2.0-Modul ist sicherheitstechnisch in besserem Zustand als ein 2 Jahre alter Computer, der auf einem System am Ende des Supports festsetzt.

Für einen Arbeitsplatz ist Windows 11 heute die einzige Windows-Version, die der Hersteller ohne besondere Vorkehrungen unterstützt. Ein Computer mit Windows 7 oder 8 erhält keinerlei Sicherheitsupdates mehr; ein Computer mit Windows 10 erhält sie nur noch, wenn

er im kostenpflichtigen ESU-Programm registriert ist (höchstens drei Jahre für Unternehmen, bis Oktober 2028) oder eine spezialisierte LTSC-Edition nutzt (siehe Kapitel 3). Diese Lösungen schieben die Frist nur hinaus. Einen Computer, der keine Sicherheitsupdates mehr erhält, im Praxisnetzwerk zu belassen, heisst, eine Tür dauerhaft offen zu lassen, unabhängig vom Schutzniveau der übrigen Geräte.

12.3 Sonderfall: iMacs mit Boot Camp

Manche Praxen nutzen noch Intel-iMacs, auf denen Windows über Boot Camp installiert ist. Diese Konfiguration bringt ein doppeltes Problem mit sich: Diese iMacs lassen sich oft weder auf Windows 11 (mangels TPM-2.0-Modul) noch auf die neuesten macOS-Versionen aktualisieren (Apple hat den Support für die ältesten Intel-Modelle eingestellt). Diese Geräte erreichen auf beiden Seiten gleichzeitig das Ende ihrer Lebensdauer.

Die Lösung besteht darin, sie durch dedizierte PCs mit Windows 11 zu ersetzen. Die Praxisverwaltungs- und Bildgebungssoftware für Zahnarztpraxen läuft ausschliesslich unter Windows; ein Mac bringt in diesem Umfeld daher keinen funktionalen Vorteil und erschwert Wartung, Updates und Hardwarekompatibilität.

12.4 Die Migration planen

Die Erneuerung der IT-Ausstattung darf nicht überstürzt an dem Tag erfolgen, an dem ein Computer ausfällt oder Ziel eines Angriffs wird. Sie muss vorausschauend geplant werden, gemeinsam mit Ihrem IT-Dienstleister. Die empfohlenen Schritte:

Beginnen Sie mit einer vollständigen Bestandsaufnahme: jeder Arbeitsplatz, jeder Server, jedes Netzwerkgerät, mit dem installierten Betriebssystem, dem Kauf- oder Inbetriebnahmedatum und der Kompatibilität mit den aktuellen Updates. Ermitteln Sie die Geräte, die das Ende ihrer Lebensdauer oder ihres Supports erreicht haben. Erstellen Sie einen realistischen Erneuerungsplan, nötigenfalls über mehrere Monate verteilt, um die Investition zu staffeln. Planen Sie die Migration der Daten und der Branchensoftware, die Neukonfiguration der Netzwerkzugänge und die Funktionsprüfung jedes Geräts vor der Inbetriebnahme.

Dokumentieren Sie diese Bestandsaufnahme und diesen Zeitplan schriftlich. Sie gehören zu den organisatorischen Massnahmen, die Ihre Konformität mit Art. 8 DSGVO belegen.

12.5 Sichere Vernichtung alter Geräte

Mit der Installation des neuen Computers ist die Erneuerung nicht abgeschlossen. Das alte Gerät enthält möglicherweise noch Patientendaten auf seiner Festplatte, selbst wenn Sie glauben, alles gelöscht zu haben. Eine einfache Formatierung genügt nicht: Mit Wiederherstellungsprogrammen lassen sich auf herkömmliche Weise gelöschte Daten zurückholen.

Zwei Möglichkeiten sind DSGVO-konform: das sichere Löschen mit spezialisierter Software (mehrfaches Überschreiben der Daten, das jede Wiederherstellung unmöglich macht) oder die physische Vernichtung des Datenträgers (Schreddern, Entmagnetisieren). Verlangen Sie in beiden Fällen von Ihrem IT-Dienstleister ein Vernichtungszertifikat und bewahren Sie es in Ihrer Konformitätsdokumentation auf. Dieses Zertifikat belegt, dass Patientendaten nicht auf einem ungesicherten Datenträger zurückgelassen wurden.

Kapitel 13. Der Auftragsbearbeitungsvertrag (Art. 9 DSG)

Art. 9 DSG regelt die Bearbeitung von Personendaten durch Auftragsbearbeiter streng. Konkret betrifft das direkt die Beziehung zwischen einer Zahnarztpraxis und allen Dritten, die in Ihrem Auftrag auf Personendaten Ihrer Patientinnen und Patienten zugreifen, sie speichern, bearbeiten oder übermitteln.

Ohne konformen Auftragsbearbeitungsvertrag bleiben Ansprüche gegen den Dienstleister nach Obligationenrecht möglich, sind aber viel schwieriger durchzusetzen. Und bei einem Vorfall stehen Sie als Praxisinhaberin oder Praxisinhaber gegenüber dem EDÖB und Ihren Patientinnen und Patienten in der Verantwortung. Wer vorsätzlich Daten einem Dienstleister ohne Vertrag oder ohne Prüfung der Datensicherheit anvertraut, wird auf Antrag mit Busse bis zu CHF 250'000 bestraft (Art. 61 Bst. b DSG).

13.1 Voraussetzungen für jede Auftragsbearbeitung

Noch bevor ein Vertrag aufgesetzt wird, nennt Art. 9 Abs. 1 zwei Voraussetzungen, die der Verantwortliche prüfen muss. Erstens darf der Auftragsbearbeiter nur Bearbeitungen vornehmen, welche die Praxis selbst vornehmen dürfte. Ist Ihnen eine Bearbeitung untersagt, können Sie sie nicht einem Dritten übertragen, um das Verbot zu umgehen. Zweitens darf keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbieten. Im medizinischen Umfeld verlangt das Berufsgeheimnis (Art. 321 StGB) besondere Wachsamkeit bei den Daten, auf die der Auftragsbearbeiter tatsächlich zugreifen kann.

Art. 9 Abs. 2 fügt eine aktive Prüfpflicht hinzu: Der Verantwortliche muss sich vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Das ist keine Formalität. Sie müssen nachweisen können, dass Sie die Kompetenzen, Werkzeuge und Sicherheitspraktiken Ihres Dienstleisters geprüft haben, bevor Sie ihm Zugang zu Ihrer Infrastruktur gewährt haben.

13.2 Wen betrifft der Auftragsbearbeitungsvertrag?

Der Auftragsbearbeitungsvertrag betrifft nicht nur Ihren IT-Dienstleister. Alle Personen und Unternehmen, die in Ihrem Auftrag auf Personendaten Ihrer Patientinnen und Patienten zugreifen, sind Auftragsbearbeiter im Sinne des DSG. Die häufigsten Fälle in einer Zahnarztpraxis:

Ihr IT-Dienstleister, der bei Wartungsarbeiten auf Computer, Server, Sicherungen und möglicherweise auf Patientendaten zugreift. Ihr Cloud-Anbieter, wenn Ihre Daten oder Sicherungen bei einem externen Anbieter gespeichert sind. Ein Dentallabor, wenn es digitale

Dateien mit identifizierbaren Patientendaten erhält (optische Abformungen, Röntgenbilder mit dem Namen der Patientin oder des Patienten). Ein externer Buchhalter oder Treuhänder, wenn er auf Abrechnungsdaten mit Patienteninformationen zugreift. Ein Anbieter von Dentalsoftware, wenn die Software in der Cloud läuft und die Daten auf den Servern des Anbieters gespeichert sind.

Mit jedem dieser Auftragsbearbeiter muss ein Vertrag nach Art. 9 DSG bestehen.

13.3 Was der Vertrag enthalten muss

Der Vertrag muss klar festlegen, in welchem Rahmen der Auftragsbearbeiter Daten bearbeiten darf:

- Die Art der Daten, auf die der Auftragsbearbeiter zugreifen kann, und die Kategorien betroffener Personen (Patientinnen und Patienten, Personal, Lieferanten).
- Den Bearbeitungszweck, beschränkt auf die Weisungen der Praxis. Der Auftragsbearbeiter darf die Daten ohne vorgängige Weisung des Verantwortlichen weder für andere Zwecke verwenden noch verkaufen oder Dritten bekanntgeben.
- Die Liste der eingesetzten Tools und den Standort der Server. Dieser Punkt hängt direkt mit Art. 16 DSGVO zusammen: Speichern die Tools des Dienstleisters Daten auf Servern ausserhalb der Schweiz oder leiten sie Daten über solche Server, müssen die Garantien für einen angemessenen Schutz im Vertrag dokumentiert sein.
- Die technischen und organisatorischen Sicherheitsmassnahmen des Auftragsbearbeiters (Verschlüsselung, Zugriffskontrolle, Protokollierung, Antivirenprogramm oder EDR).
- Das Verfahren zur Meldung von Vorfällen mit einer festgelegten Frist. Art. 24 Abs. 3 DSGVO verpflichtet den Auftragsbearbeiter, den Verantwortlichen bei einer Verletzung der Datensicherheit so rasch als möglich zu informieren. Der Vertrag muss eine konkrete Frist festlegen, zum Beispiel 24 Stunden nach der Entdeckung.
- Das Verfahren bei Vertragsende: Entzug aller Zugänge, Rückgabe oder Löschung der vorhandenen Daten, schriftliche Bestätigung der Umsetzung dieser Massnahmen.
- Das Verbot, die Bearbeitung ohne vorgängige Genehmigung der Praxis an Dritte zu übertragen (Art. 9 Abs. 3 DSGVO), idealerweise schriftlich erteilt. Setzt Ihr IT-Dienstleister seinerseits Unterauftragsbearbeiter ein (zum Beispiel einen Cloud-Anbieter für Ihre Sicherungen), muss dies offengelegt und vertraglich geregelt sein.

- Eine zeitlich unbefristete Vertraulichkeitsklausel, auch über das Vertragsende hinaus.

Das ist kein 40-seitiges Dokument. Ein gut formulierter Vertrag umfasst 9 Artikel, ist in 5 Minuten gelesen und in 2 unterschrieben.

13.4 Die Tools Ihres Dienstleisters prüfen

Der Vertrag muss eine Tabelle oder einen Anhang enthalten, der die Tools auflistet, die der Dienstleister bei seinen Einsätzen verwendet, jeweils mit Zweck und Speicherort der Daten. Zum Beispiel: das eingesetzte Fernwartungstool, die Monitoring-Lösung, der Passwortmanager, die Sicherungslösung, die geschäftliche E-Mail. Prüfen Sie bei jedem Tool mit Servern ausserhalb der Schweiz, ob der betreffende Staat vom Bundesrat als Staat mit angemessenem Schutzniveau anerkannt ist (Art. 16 Abs. 1 DSG) oder ob zusätzliche vertragliche Garantien bestehen (Art. 16 Abs. 2).

13.5 Verantwortung gegenüber den Patientinnen und Patienten (Art. 25 Abs. 4)

Auch wenn ein Auftragsbearbeiter Daten in Ihrem Auftrag bearbeitet, bleiben Sie die einzige Ansprechstelle Ihrer Patientinnen und Patienten. Art. 25 Abs. 4 DSG ist eindeutig: Der Verantwortliche, der Personendaten von einem Auftragsbearbeiter bearbeiten lässt, bleibt zur Auskunft verpflichtet. Verlangt eine Patientin oder ein Patient Auskunft über die eigenen Daten, können Sie sie oder ihn nicht an Ihren IT-Dienstleister verweisen. Sie müssen innert 30 Tagen antworten, auch wenn Sie dafür Ihren Auftragsbearbeiter um die Informationen bitten müssen.

13.6 Mein aktueller Dienstleister hat keinen Vertrag: Was tun?

Besteht mit Ihrem IT-Dienstleister oder Ihren anderen Auftragsbearbeitern derzeit kein Auftragsbearbeitungsvertrag, ist das Vorgehen einfach. Kontaktieren Sie Ihren Dienstleister und fragen Sie, ob er über einen Vertrag nach Art. 9 DSG verfügt. Schlägt er einen vor, lesen Sie ihn aufmerksam und prüfen Sie, ob er die oben aufgeführten Punkte abdeckt. Schlägt er keinen vor, ist das ein Warnsignal für seinen Reifegrad im Datenschutz. Sie können ihm eine Vertragsvorlage zur Verfügung stellen oder einen Vertrag von einer spezialisierten Rechtsfachperson aufsetzen lassen.

Fehlt ein Vertrag, muss die Zusammenarbeit nicht sofort beendet werden, doch die Bereinigung der Situation muss Priorität haben. Tritt ein Vorfall ein, ohne dass ein Vertrag besteht, ist Ihre Position sowohl gegenüber dem EDÖB als auch gegenüber Ihren Patientinnen und Patienten erheblich geschwächt.

Sie delegieren die Technik. Niemals die Verantwortung.

Kapitel 14. Schulung des Personals

Technologie genügt nicht, wenn die Menschen, die sie nutzen, nicht geschult sind.

Menschliche Fehler (eine geöffnete Phishing-E-Mail, ein nicht gesperrter Bildschirm, ein am Empfang liegengelassenes Patientendossier, ein per WhatsApp verschicktes Röntgenbild) machen einen erheblichen Teil der Verletzungen der Datensicherheit aus. Die meisten dieser Vorfälle entstehen nicht aus böser Absicht, sondern aus mangelnder Sensibilisierung und fehlenden klaren Regeln.

14.1 Eine implizite Pflicht aus dem DSGVO

Art. 8 DSGVO verpflichtet den Verantwortlichen, angemessene organisatorische und technische Massnahmen zur Gewährleistung der Datensicherheit zu treffen. Die Schulung des Personals gehört zu diesen organisatorischen Massnahmen. Der Bundesrat hält in seinem vom Bundesamt für Justiz veröffentlichten erläuternden Bericht zum DSGVO ausdrücklich fest, dass die wirksame Umsetzung der Datensicherheit von der korrekten Schulung der beteiligten Personen abhängt. Mangelnde Schulung könnte zu Verletzungen der Datensicherheit führen, zum Beispiel wenn eine Mitarbeiterin oder ein Mitarbeiter eine E-Mail mit Schadsoftware öffnet.

Nach Schweizer Arbeitsrecht kann der Arbeitgeber Weisungen erteilen, welche die Mitarbeitenden befolgen müssen (Art. 321d OR). Schulen Sie sie und übergeben Sie ihnen die Regeln schriftlich: Sonst lässt sich ihnen ein Sicherheitsfehler kaum vorwerfen, und eine Kündigung aus diesem Grund, besonders eine fristlose, könnte angefochten werden.

14.2 Empfohlene Schulungsinhalte

Die Schulung muss die realen Situationen abdecken, mit denen das Personal im Alltag konfrontiert ist.

Betrugsversuche erkennen. Phishing per E-Mail ist der häufigste Angriffsweg, aber nicht das einzige Risiko. Die Schulung muss auch betrügerische Telefonanrufe behandeln (jemand gibt sich als IT-Dienstleister aus und verlangt ein Passwort, ein angeblicher Mitarbeiter des Dentalsoftware-Anbieters verlangt einen Fernzugriff, eine unbekannte Person gibt sich als Patientin oder Patient aus und verlangt am Telefon medizinische Auskünfte), betrügerische SMS und Nachrichten sowie unbekannte USB-Sticks, die in oder in der Nähe der Praxis gefunden werden. Konkrete Beispiele und praktische Übungen helfen, das Gelernte zu verankern.

Regeln zum Sperren der Geräte. Den Bildschirm bei jedem Verlassen des Arbeitsplatzes sperren, auch nur für wenige Sekunden. Die Tastenkombination Windows+L unter Windows oder Ctrl+Cmd+Q unter macOS muss zum Reflex werden. Ein nicht gesperrter Bildschirm in einem für Patientinnen und Patienten zugänglichen Raum ist eine mögliche Verletzung der Vertraulichkeit.

Passwortrichtlinie. Obligatorische Nutzung des Passwortmanagers der Praxis, Aktivierung der Zwei-Faktor-Authentifizierung für alle kritischen Zugänge, Verbot, Passwörter auf Haftnotizen oder in unverschlüsselten Dateien zu notieren.

Nutzung der sicheren E-Mail. Wissen, wann die verschlüsselte E-Mail zu verwenden ist (jeder Inhalt mit identifizierbaren Patientendaten) und wann die normale E-Mail genügt (interner Austausch ohne sensible Daten, Materialbestellungen). Striktes Verbot, Messaging-Dienste für Privatkunden (Gmail, Hotmail, WhatsApp) für Mitteilungen mit Patientendaten zu nutzen.

Vorgehen bei einem Vorfall

Alle Mitarbeitenden müssen wissen, was bei Verdacht auf einen Angriff oder einen Datenabfluss zu tun ist: wen sie zuerst anrufen (die verantwortliche Zahnärztin oder den verantwortlichen Zahnarzt, dann den IT-Dienstleister), was sofort zu tun ist (Netzwerkkabel ausstecken, Computer nicht ausschalten), was zu unterlassen ist (nicht versuchen, das Problem selbst zu lösen, kein Lösegeld bezahlen, verdächtige Nachrichten nicht löschen, bevor sie dokumentiert sind).

Umgang mit Patientendaten. Nie Patientendaten über WhatsApp, SMS oder private E-Mail verschicken. Keine Daten auf private USB-Sticks, private Festplatten oder nicht autorisierte Cloud-Dienste kopieren. Keine Patientendateien auf einen privaten Computer übertragen, auch nicht, um «von zu Hause aus zu arbeiten».

Physische Sicherheit und Clean-Desk-Richtlinie. Nie Patientendossiers, ausgedruckte Röntgenbilder oder administrative Dokumente mit Personendaten sichtbar auf einer Theke, einem Schreibtisch oder in der Nähe des Empfangs liegen lassen.

Papierdokumente mit Patientendaten müssen mit einem Aktenvernichter vernichtet und dürfen nie in den Abfall geworfen werden. Bildschirme, die vom Wartezimmer oder von Durchgangsbereichen aus sichtbar sind, müssen entsprechend ausgerichtet oder mit Blickschutzfiltern ausgestattet sein.

Berufsgeheimnis. Erinnerung an die strafrechtlichen Pflichten: Art. 321 StGB bestraft die Offenbarung von Geheimnissen, die im Rahmen der Berufsausübung anvertraut wurden. Diese Pflicht gilt für das gesamte Praxispersonal, nicht nur für die Zahnärztin oder den Zahnarzt.

14.3 Private Geräte und BYOD

Die Nutzung privater Geräte (Telefone, Tablets, Laptops, USB-Sticks) für den Zugriff auf Daten der Praxis muss entweder verboten oder durch eine schriftliche Regel streng geregelt sein. Liest eine Mitarbeiterin oder ein Mitarbeiter geschäftliche E-Mails auf dem privaten Telefon, landen die darin enthaltenen Patientendaten auf einem Gerät, das die Praxis nicht kontrolliert, das möglicherweise unverschlüsselt ist und verloren gehen, gestohlen oder kompromittiert werden kann. Die Richtlinie der Praxis muss klar festlegen, welche Geräte zugelassen sind, welche Anwendungen genutzt werden dürfen und welche Daten darüber laufen dürfen.

14.4 Temporäres Personal und Dritte

Praktikantinnen und Praktikanten, Stellvertretungen, Reinigungspersonal, externe Techniker und alle anderen Personen mit physischem Zugang zu den Räumlichkeiten der Praxis müssen in der Sicherheitsrichtlinie berücksichtigt werden. Wer zwei Wochen lang ein Praktikum macht, kann dieselben Bildschirme sehen wie fest angestellte Mitarbeitende. Das Reinigungspersonal, das ausserhalb der Öffnungszeiten arbeitet, hat Zugang zu Büros, Druckern und möglicherweise zu sichtbar liegengelassenen Dokumenten. Externe Techniker (Lieferanten medizinischer Geräte, Installateure) brauchen unter Umständen vorübergehend Zugang zum Netzwerk.

Jede Person mit physischem oder digitalem Zugang, auch vorübergehend, muss ein Minimum an Informationen über die Vertraulichkeitsregeln der Praxis erhalten. Für temporäres Personal genügt ein einseitiges Merkblatt mit den wesentlichen Regeln, das beim Eintritt unterschrieben wird.

14.5 Die schriftliche interne Sicherheitsrichtlinie

Mündliche Schulung genügt nicht. Die Praxis muss über eine schriftlich festgehaltene interne IT-Sicherheitsrichtlinie verfügen, die allen Mitarbeitenden beim Eintritt abgegeben und mindestens einmal pro Jahr aktualisiert wird. Dieses Dokument ist die Referenz bei Streitigkeiten und schützt die Praxisinhaberin oder den Praxisinhaber bei einem Vorfall: Es belegt, dass Regeln bestanden, dass sie kommuniziert wurden und dass die Mitarbeitenden davon Kenntnis genommen haben.

Die Richtlinie muss mindestens Folgendes abdecken: die Regeln für die Nutzung der Arbeitsplätze, die Passwortrichtlinie, die Regeln zu E-Mail und Kommunikation, das Verbot oder die Regelung privater Geräte, das Vorgehen bei einem Vorfall und die internen Sanktionen bei Nichteinhaltung. Alle Mitarbeitenden unterschreiben ein Exemplar und bestätigen damit, dass sie die Regeln gelesen, verstanden und akzeptiert haben. Diese Unterschrift wird im Personaldossier aufbewahrt.

14.6 Häufigkeit, Format und Evaluation

Die Schulung muss mindestens einmal pro Jahr für das gesamte Personal stattfinden, mit einer eigenen Sitzung beim Eintritt jeder neuen Mitarbeiterin und jedes neuen Mitarbeiters, einschliesslich Praktikantinnen, Praktikanten und Stellvertretungen. Das Format kann eine interne Präsentation von 30 bis 60 Minuten sein, ergänzt durch die Abgabe der internen Richtlinie.

Um die Wirksamkeit der Schulung zu beurteilen, werden praktische Übungen empfohlen: Phishing-Simulationen (Versand einer gefälschten betrügerischen E-Mail, um die Reaktion des Personals zu prüfen), kurze Quiz zu bewährten Praktiken, Rollenspiele (eine Mitarbeiterin erhält einen Anruf, in dem nach einem Passwort gefragt wird). Diese Übungen sollen das Personal nicht hereinlegen, sondern Schwachstellen erkennen und die nächste Schulung entsprechend anpassen.

Dokumentieren Sie jede Sitzung: Datum, Teilnehmende, behandelte Themen, gegebenenfalls Ergebnisse der Übungen. Diese Dokumentation gehört zu den organisatorischen Massnahmen, die der EDÖB bei einer Kontrolle einsehen kann.

14.7 Geteilte Verantwortung

Verschickt eine Dentalassistentin ein Röntgenbild über WhatsApp, kann sie sich persönlich strafbar machen, wenn dieser Versand eine vorsätzliche Offenbarung geheimer Daten

darstellt (Art. 62 DSG zur Verletzung der beruflichen Schweigepflicht und Art. 321 StGB zum Berufsgeheimnis, der auch die Hilfspersonen der Zahnärztinnen und Zahnärzte erfasst; Antragsdelikte). Blosser Fahrlässigkeit ist nach diesen beiden Artikeln nicht strafbar. Doch die Praxisleitung, also die Zahnärztin oder der Zahnarzt, benachrichtigt den EDÖB und muss sich gegenüber den Patientinnen und Patienten verantworten. Ihr eigenes Risiko hängt von den Massnahmen ab, die sie getroffen hat: schriftliche und unterzeichnete interne Richtlinie, erteilte und dokumentierte Schulung, angemessene Zugriffsverwaltung. War nichts davon vorhanden, trägt sie eine Mitverantwortung, weil sie dem Risiko nicht vorgebeugt hat. War alles vorhanden und dokumentiert, ist ihre Position erheblich gestärkt.

Kapitel 15. Cyberversicherungen

Selbst bei einem ausgezeichneten IT-Sicherheitsniveau gibt es kein Nullrisiko. Eine Cyberversicherung ermöglicht es, einen Teil des finanziellen Risikos auf einen Versicherer zu übertragen und in einer Krise professionelle Hilfe zu erhalten.

15.1 Was eine Cyberversicherung abdeckt

Die in der Schweiz angebotenen Cyberversicherungen decken in der Regel:

- Die Kosten für IT-Notfalleinsätze (Forensik, Wiederherstellung)
- Den Umsatzausfall infolge Betriebsunterbruchs
- Die Kosten der obligatorischen Meldung (EDÖB, betroffene Patientinnen und Patienten)
- Die Haftpflicht bei Schäden an Daten Dritter
- Die Kosten für Krisenmanagement und Kommunikation
- Die Rechtskosten im Zusammenhang mit dem Vorfall

15.2 Wichtigste Versicherer in der Schweiz

Mehrere Schweizer Versicherer bieten speziell für KMU konzipierte Lösungen an:

- **Zurich:** modulare Lösung in 4 Varianten, einschliesslich einer kostenlosen Cybersicherheitsschulung für Versicherte.
- **Helvetia:** Cyberversicherung mit 24-Stunden-Hotline und einem Netzwerk spezialisierter Partner, Label cyber-safe für 20% Rabatt.
- **AXA:** Schutz auf drei Ebenen: Prävention, Notfallhilfe, Schadenbehebung.
- **Baloise:** drei Lösungen (ECO, SMART, TOP) mit Deckung des Lösegelds unter bestimmten Bedingungen.
- **Allianz:** Cyber Risk mit Deckung von Betriebsunterbrüchen über 24 Monate.

15.3 Worauf zu achten ist

Prüfen Sie vor dem Abschluss sorgfältig:

- Die Ausschlüsse (manche Policen schliessen Angriffe aus, wenn die Updates nicht auf dem neuesten Stand waren)
- Die Höhe des Selbstbehalts, bei KMU teilweise hoch
- Die vom Versicherer verlangten Sicherheitsvoraussetzungen
- Die Deckungssumme und ob sie Ihrem tatsächlichen Risiko entspricht
- Ob die Zahlung eines Lösegelds gedeckt ist (je nach Versicherer unterschiedlich)

Tipp

Die Cyberversicherung ersetzt die Sicherheitsmassnahmen nicht, sie ergänzt sie. Ein Versicherer verlangt ein Mindestmass an Schutz (Antivirenprogramm, Datensicherungen, Passwörter), bevor er Sie versichert. Das ist ein positiver Kreislauf: Je besser Sie geschützt sind, desto tiefer die Prämie.

Kapitel 16. Was tun bei einem Vorfall

Wenn es passiert (und statistisch gesehen wird es manche Praxen treffen), sind die ersten Minuten entscheidend.

16.1 Szenario A: aktiver Angriff (Ransomware, Eindringen)

Schritt 1. ISOLIEREN: Netzkabel ausstecken, WLAN deaktivieren. Den Computer nicht ausschalten; das vernichtet Spuren, die für die Analyse nützlich sind.

Schritt 2. IT ANRUFEN: zuerst Ihren IT-Dienstleister. Ist er nicht erreichbar, das BACS über incidents@ncsc.ch oder das Formular auf report.ncsc.admin.ch.

Schritt 3. NICHT BEZAHLEN: offizielle Empfehlung des Bundes. Bezahlen garantiert nicht, dass die Daten wiederhergestellt werden, und finanziert kriminelle Netzwerke.

Schritt 4. DOKUMENTIEREN: Fehlermeldungen fotografieren, den genauen Zeitpunkt der Entdeckung notieren, alles aufbewahren. Diese Informationen werden für die Versicherung, die Polizei und die gesetzliche Meldung benötigt.

Schritt 5. BEURTEILEN: Führt die Verletzung voraussichtlich zu einem hohen Risiko für die Patientinnen und Patienten (z. B. Gesundheitsdaten gestohlen, offengelegt oder durch Ransomware verschlüsselt)? Falls ja oder wenn Sie es nicht rasch ausschliessen können, ist die Meldung an den EDÖB obligatorisch (Art. 24 Abs. 1 DSGVO).

Schritt 6. MELDEN: databreach.edoeb.admin.ch, so rasch als möglich.

16.2 Szenario B: versehentlicher Verlust oder Datenabfluss

Verlust eines Datenträgers, Versand an den falschen Empfänger, versehentliches Löschen, entdeckter unbefugter Zugriff: Das Vorgehen ist ähnlich: dokumentieren, das Risiko für die Patientinnen und Patienten beurteilen, den EDÖB bei hohem Risiko benachrichtigen, die Patientinnen und Patienten bei Bedarf informieren.

16.3 Was der EDÖB konkret tut

Es ist keine Razzia in Ihrer Praxis. Der EDÖB liest Ihre Meldung, prüft, ob Sie richtig reagiert haben, und kann Präzisierungen verlangen oder Ratschläge erteilen.

Der EDÖB kann keine Bussen direkt verhängen. Strafrechtliche Sanktionen laufen über die kantonalen Behörden und richten sich gegen vorsätzliche Verstösse, nicht gegen Praxen, die in gutem Glauben gemeldet haben.

Die goldene Regel: Früh melden ist besser als nicht melden.

Kapitel 17. Reale Fälle in der Westschweiz

Diese Angriffe sind nicht theoretisch. Sie haben medizinische Einrichtungen in der Westschweiz getroffen, in einem Umfeld, das mit einer Zahnarztpraxis vergleichbar ist.

Groupe 3R, Réseau Radiologique Romand (April 2025 und April 2026)

Zwanzig Zentren für medizinische Bildgebung in sieben Kantonen. Ransomware, Diebstahl medizinischer und administrativer Daten, Erpressungsversuch. Die Zahlung des Lösegelds wurde verweigert. Der Vorfall wurde dem BACS gemeldet. Die Gruppe erlitt im April 2026 einen zweiten Ransomware-Angriff; sie weigerte sich erneut zu bezahlen, und gestohlene Daten wurden im Internet veröffentlicht.

Vidymed, Lausanne (Dezember 2024)

Ein am 7. Dezember 2024 entdecktes Eindringen in die IT-Systeme von vier medizinischen Zentren in Lausanne und Épalinges: Die gesamte IT wurde stillgelegt, und das Personal kehrte zu Papier zurück. Der Grossteil der Daten wurde erst fünf Wochen später wiederhergestellt. Eine Situation, die jede Zahnarztpraxis lahmlegen würde.

Die Schweiz in Zahlen

2025 gingen beim Bundesamt für Cybersicherheit (BACS) 64'733 freiwillige Meldungen zu Cybervorfällen ein (Jahresbericht 2025 des BACS).

Typische Angriffsszenarien im medizinischen Bereich

Über die oben genannten realen Fälle hinaus folgen hier vier typische Szenarien, die auf den häufigsten Angriffen gegen Praxen beruhen. Sie zeigen, wie ein Angriff meistens beginnt:

Ransomware über ungesicherten Fernzugriff

Ein Fernsteuerungstool bleibt dauerhaft offen, geschützt durch ein kurzes Passwort, um die Einsätze des Dienstleisters zu erleichtern. Ein Angreifer errät es durch automatisierte Versuche und übernimmt nachts die Kontrolle über den Server. Die Ransomware breitet sich im gesamten Netzwerk aus: Die Praxis bleibt mehrere Tage geschlossen, und nur die ausser Reichweite gesicherten Daten können wiederhergestellt werden.

Phishing mit gefälschter Rechnung eines Telekomanbieters

Eine E-Mail imitiert die Rechnung eines Telekomanbieters, mit dem Betreff «Ihre unbezahlte Rechnung». Sobald der Anhang geöffnet ist, verschlüsselt eine Ransomware das Netzwerk, einschliesslich der dauerhaft angeschlossenen Sicherungen. Ohne eine Kopie ausser Reichweite verfügt die Praxis über keine verwendbare Kopie ihrer Daten mehr.

Falscher IT-Dienstleister

Ein Angreifer gibt sich als IT-Dienstleister der Praxis aus und verlangt die Zugangsdaten «für ein dringendes Update». Eine Dentalassistentin gibt sie in gutem Glauben weiter. Der Angreifer greift auf den Server zu und kopiert Patientendossiers, bevor er entdeckt wird.

Infizierter USB-Stick

Ein auf dem Parkplatz der Praxis «vergessener» USB-Stick trägt die Aufschrift «Löhne». Sobald er an einem Computer eingesteckt ist, installiert er eine Spyware, die die über die Tastatur eingegebenen Passwörter aufzeichnet: Jene für die Dentalsoftware, die E-Mail und das Online-Banking sind kompromittiert.

Was ein Angriff kostet

Tage, manchmal Wochen mit eingeschränktem Betrieb: Bei Vidymed dauerte es fünf Wochen, bis der Grossteil der Daten wiederhergestellt war. Hinzu kommen die Instandsetzung, der Einsatz von Fachleuten, die Information der Patientinnen und Patienten und der Verlust ihres Vertrauens.

Konformitäts-Checkliste

Verwenden Sie diese Liste, um Ihren aktuellen Konformitätsstand zu beurteilen und zu verbessern, was in Ihrer bestehenden Infrastruktur fehlt. Jeder nicht abgehakte Punkt ist ein Risiko, das angegangen werden muss. Ein Glossar der Fachbegriffe finden Sie am Ende der Liste.

Kommunikation

- Verschlüsselte E-Mail für alle Patientendaten im Einsatz (HIN Mail, ProtonMail oder gleichwertig)
- Keine Patientendaten über Gmail, Hotmail, Bluewin, WhatsApp oder SMS versandt
- Papierdokumente mit Patientendaten werden im Aktenvernichter vernichtet

Infrastruktur

- Alle Computer mit Windows 11 oder aktuellem macOS
- Kein Computer mit Windows 7, 8 oder 10 im Netzwerk
- Automatische Updates auf allen Computern, Servern und Anwendungen aktiviert
- Festplattenverschlüsselung auf allen Computern und Servern aktiviert (BitLocker / FileVault)
- Patienten-WLAN vom Praxisnetz getrennt

Datensicherung

- 3-2-1-Strategie umgesetzt (3 Kopien, 2 Datenträger, 1 ausserhalb der Praxis), mit einer getrennten oder unveränderbaren Kopie
- Wiederherstellung regelmässig getestet (mindestens einmal pro Jahr, idealerweise monatlich)

Zugriff und Authentifizierung

- Ein persönliches Konto pro Person, keine geteilten Konten
- Passwörter mit 12+ Zeichen, in einem sicheren Passwortmanager gespeichert
- 2FA für E-Mail, Praxisverwaltungssoftware und Fernzugriff aktiviert
- Konten ehemaliger Mitarbeitender deaktiviert

- Fernzugriff nur über VPN oder professionelles RMM

DSG-Konformität

- Auftragsbearbeitungsvertrag nach Art. 9 mit dem IT-Dienstleister unterzeichnet
- Auftragsbearbeitungsvertrag mit allen Dritten, die auf Patientendaten zugreifen
- Interne Sicherheitsrichtlinie erstellt und von allen Mitarbeitenden unterzeichnet
- Schulung des Personals in den letzten 12 Monaten durchgeführt
- Notfallplan für Vorfälle dokumentiert und zugänglich
- Notfallkontakte ausgehängt (IT-Dienstleister, BACS, EDÖB)

Schutz und Überwachung

- EDR-Lösung eingeführt und überwacht
- Jährliches Sicherheitsaudit durchgeführt
- Cyberversicherung abgeschlossen und Bedingungen geprüft

Glossar zur Checkliste

Verschlüsselte E-Mail: E-Mail-Dienst, dessen Inhalt beim Versand verriegelt wird und nur von der Empfängerin oder dem Empfänger gelesen werden kann. Weder der Anbieter noch ein Hacker, der die Nachricht abfängt, kann darauf zugreifen. Beispiele: HIN Mail, ProtonMail.

3-2-1-Datensicherung: 3 Kopien Ihrer Daten, auf 2 verschiedenen Datenträgern, davon 1 ausserhalb der Praxis aufbewahrt. Empfohlen wird, dass eine der Kopien zusätzlich getrennt oder unveränderbar ist (geschützt vor jeder Änderung oder Löschung, selbst durch ein Virus): Das ist die Variante 3-2-1-1-0.

BitLocker / FileVault: kostenlos in Windows (BitLocker) und macOS (FileVault) integrierte Verschlüsselungswerkzeuge. Sie machen den Inhalt der Festplatte bei einem Diebstahl des Computers völlig unlesbar.

2FA (Zwei-Faktor-Authentifizierung): zweite Prüfung nach dem Passwort, meist ein temporärer Code, der auf dem Telefon angezeigt wird. Dasselbe Prinzip wie bei der Bankkarte: Die Nummer allein genügt nicht, es braucht auch den Code.

VPN: verschlüsselte Verbindung zwischen einem entfernten Gerät und dem Netzwerk der Praxis. Schützt die übertragenen Daten wie ein privater Tunnel.

RMM: professionelle Fernwartungssoftware, die jede Verbindung protokolliert, Updates einspielt und die Geräte laufend überwacht. Sichere Alternative zu Gratis-Tools wie TeamViewer.

EDR: fortgeschrittener Schutz, der das Verhalten von Programmen in Echtzeit analysiert und verdächtige Aktionen blockiert, auch unbekannte. Geht über das klassische Antivirenprogramm hinaus, das nur bereits erfasste Bedrohungen erkennt.

Art. 9 DSGVO: Gesetzesartikel zur Auftragsbearbeitung. Ein Dritter darf Patientendaten für die Praxis (IT-Dienstleister, Cloud-Anbieter, Labor, Buchhalter) nur bearbeiten, wenn ein Vertrag oder das Gesetz es vorsieht, und die Praxis muss sich vergewissern, dass er die

Datensicherheit gewährleisten kann. Die Schriftform ist nicht vorgeschrieben, aber der sicherste Nachweis des Vertrags. Wer vorsätzlich Daten anvertraut, ohne diese Voraussetzungen einzuhalten, wird auf Antrag mit Busse bis zu CHF 250'000 bestraft (Art. 61 Bst. b).

BACS: Bundesamt für Cybersicherheit. Anlaufstelle bei einem Cyberangriff. Kontakt: incidents@ncsc.ch oder report.ncsc.admin.ch.

EDÖB: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. Behörde, der eine Verletzung der Datensicherheit mit hohem Risiko zu melden ist (Art. 24 DSG). Kontakt: +41 58 462 43 95 oder databreach.edoeb.admin.ch.

Nützliche Kontakte und Ressourcen

Notfallkontakte

- **BACS:** Bundesamt für Cybersicherheit: incidents@ncsc.ch / report.ncsc.admin.ch
- **EDÖB:** Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter: +41 58 462 43 95 (Mo–Fr 10–12 Uhr) / databreach.edoeb.admin.ch
- **Kantonspolizei:** 117

Gesetzestexte

- **DSG (SR 235.1):** www.fedlex.admin.ch
- **Datenschutzverordnung (DSV):** www.fedlex.admin.ch
- **Leitfaden des EDÖB zu Verletzungen der Datensicherheit:** www.edoeb.admin.ch
- **KMU-Leitfaden Datenschutz:** www.kmu.admin.ch

Weitere Ressourcen

- **FMH:** Werkzeuge und Vorlagen für Arztpraxen: www.fmh.ch
- **HIN:** Informationssicherheit für das Gesundheitswesen: www.hin.ch
- **No More Ransom (Hilfe beim Entschlüsseln):** www.nomoreransom.org

Häufige Fragen

Die folgenden Fragen stellen Zahnärztinnen und Zahnärzte am häufigsten. Sie stammen aus realen Situationen in Zahnarztpraxen der Westschweiz.

Ist ein versehentlicher Datenverlust eine Verletzung der Datensicherheit im Sinne des DSGVO?

Ja. Art. 5 Bst. h DSGVO definiert die Verletzung der Datensicherheit als jeden Verlust, jede Veränderung, Löschung oder Vernichtung von Personendaten, ob versehentlich oder widerrechtlich. Patientendossiers irrtümlich löschen, eine Festplatte verlieren oder einen Serverausfall ohne Datensicherung erleiden: All das fällt unter diese Definition. Ist das Risiko für die Patientinnen und Patienten hoch, ist die Meldung an den EDÖB obligatorisch.

Mein IT-Dienstleister hat Daten gelöscht. Wer ist verantwortlich?

Sie, als Zahnärztin oder Zahnarzt und damit als Verantwortlicher im Sinne des DSGVO (Art. 9 und Art. 25 Abs. 4 DSGVO). Sie können die Patientin oder den Patienten nicht an Ihren Informatiker verweisen. Ihr Rückgriff auf den Dienstleister ist mit einem konformen Auftragsbearbeitungsvertrag viel stärker; ohne Vertrag bleibt er nach Obligationenrecht möglich, ist aber schwieriger durchzusetzen. Sie delegieren die Technik, niemals die Verantwortung.

Ich bin seit 3 Jahren pensioniert, und ein 4 Jahre zurückliegender Datenabfluss wird entdeckt. Bin ich noch betroffen?

Ja. Art. 66 DSGVO legt die Verjährungsfrist für die Strafverfolgung auf 5 Jahre fest. Pensionierung oder Aufgabe der Berufstätigkeit heben die Verantwortung für Taten, die während der Berufsausübung begangen wurden, nicht auf. Der genaue Beginn der Frist (Zeitpunkt des Datenabflusses oder der Entdeckung) erfordert die Einschätzung einer Rechtsfachperson, doch die Frist von 5 Jahren ist gesetzlich festgelegt.

Meine iMacs laufen mit Windows 10 über Boot Camp: Können wir zu macOS zurückwechseln?

Nein, und das würde nichts lösen. Die Dentalsoftware (Sidexis, Romexis, DBSWin, Cliniview, DTX Studio) läuft ausschliesslich unter Windows. Zudem lassen sich diese Intel-iMacs oft weder auf Windows 11 noch auf die neuesten macOS-Versionen aktualisieren. Sie sind auf beiden Seiten am Ende ihrer Lebensdauer. Die Lösung: sie durch dedizierte PCs mit Windows 11 ersetzen.

Welche Dentalsoftware soll ich wählen?

Dieser Leitfaden empfiehlt keine bestimmte Software öffentlich und rät auch von keiner ab. Prüfen Sie jedoch die folgenden Sicherheitskriterien: Bietet die Software die Zwei-Faktor-Authentifizierung (2FA) nativ an? Veröffentlicht der Anbieter regelmässig Sicherheitsupdates? Wo werden die Daten gespeichert? Verfügt das Entwicklungsteam über dokumentierte Sicherheitskompetenzen? Eine kritische medizinische Software ist ein IT-Produkt: Fragen Sie sich, ob der Anbieter die Mittel hat, sie langfristig weiterzuentwickeln.

Eine Dentalassistentin verschickt ein Röntgenbild über WhatsApp. Wer ist verantwortlich?

Beide, aber nicht aus denselben Gründen. Die Dentalassistentin kann sich persönlich strafbar machen, wenn der Versand eine vorsätzliche Offenbarung geheimer Daten darstellt: Art. 62 DSG (Verletzung der beruflichen Schweigepflicht) und Art. 321 StGB (Berufsgeheimnis, das auch die Hilfspersonen der Zahnärztinnen und Zahnärzte erfasst), auf Antrag. Ein Fehler aus blosser Fahrlässigkeit ist nach diesen Artikeln nicht strafbar. Die Praxisleitung, also die Zahnärztin oder der Zahnarzt, benachrichtigt ihrerseits den EDÖB und muss sich gegenüber den Patientinnen und Patienten verantworten. Ihr eigenes Risiko hängt von den Massnahmen ab, die sie getroffen hat: schriftliche interne Richtlinie, erteilte Schulung, Zugriffsverwaltung. Bestand nichts davon, trägt sie eine Mitverantwortung, weil sie dem Risiko nicht vorgebeugt hat.

Führt der EDÖB Kontrollen in Praxen durch?

Der EDÖB kann von Amtes wegen oder auf Anzeige hin eine Untersuchung eröffnen, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen Datenschutzvorschriften verstossen könnte (Art. 49 DSG). Die realen Risikoquellen für eine Zahnärztin oder einen Zahnarzt sind unzufriedene Patientinnen und Patienten, ein Vorfall, der öffentlich wird, oder eine Anzeige ehemaliger Mitarbeitender.

Schreibt das DSG wie die DSGVO eine Frist von 72 Stunden vor?

Nein. Das Schweizer Recht verlangt eine Meldung «so rasch als möglich», eine bewusst offenere Formulierung als die europäische DSGVO, die eine strikte Frist von 72 Stunden festlegt. Der EDÖB empfiehlt, «so schnell wie möglich» zu handeln. Konkret heisst das: sofort handeln, sobald man von der Verletzung Kenntnis hat, und die Dokumentation bei Bedarf danach ergänzen. Für eine Verspätung gibt es keine spezifische Sanktion, doch rasches Handeln wird bei der Beurteilung des guten Glaubens berücksichtigt.

Glossar

Die folgenden Begriffe werden in diesem Leitfaden und im DSGVO verwendet. Dieses Glossar erklärt sie in einer auch für Laien verständlichen Sprache.

Begriff	Definition
DSG	Neues Bundesgesetz über den Datenschutz (SR 235.1), in Kraft seit dem 1. September 2023.
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. Unabhängige Aufsichtsbehörde, die über die Einhaltung des Gesetzes wacht.
BACS	Bundesamt für Cybersicherheit (früher NCSC/MELANI). Kompetenzzentrum des Bundes für Cyberbedrohungen.
Personendaten	Alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Art. 5 Bst. a).
Besonders schützenswerte Personendaten	Kategorie mit verstärktem Schutz: Daten über die Gesundheit, religiöse oder politische Ansichten, genetische und biometrische Daten, strafrechtliche Verfolgungen, Massnahmen der sozialen Hilfe (Art. 5 Bst. c).
Verantwortlicher	Die Person, die über Zweck und Mittel der Bearbeitung entscheidet. In einer Zahnarztpraxis: die Praxisinhaberin oder der Praxisinhaber (Art. 5 Bst. j).
Auftragsbearbeiter	Die Person, die im Auftrag des Verantwortlichen Personendaten bearbeitet. Beispiel: der IT-Dienstleister der Praxis (Art. 5 Bst. k).
Verletzung der Datensicherheit	Jeder Verlust, jede Veränderung, Löschung, Vernichtung oder Offenlegung von Personendaten und jeder unbefugte Zugriff darauf, ob versehentlich oder widerrechtlich (Art. 5 Bst. h).

Privacy by Design	Pflicht, den Datenschutz bereits bei der Konzeption eines Systems oder Prozesses einzubauen (Art. 7 Abs. 1).
Privacy by Default	Pflicht, die Bearbeitung standardmässig auf das absolut Notwendige zu beschränken (Art. 7 Abs. 3).
DSFA	Datenschutz-Folgenabschätzung. Obligatorisch, wenn eine Bearbeitung ein hohes Risiko mit sich bringt (Art. 22).
2FA / MFA	Zwei-Faktor-Authentifizierung / Multi-Faktor-Authentifizierung. Zweite Prüfung nach dem Passwort (SMS-Code, App, physischer Schlüssel).
EDR	Endpoint Detection and Response. Sicherheitslösung, die Bedrohungen durch Verhaltensanalyse in Echtzeit erkennt und nicht anhand von Signaturen.
Ransomware	Schadsoftware, die Daten verschlüsselt und für deren Freigabe ein Lösegeld verlangt.
Phishing	Betrugstechnik per E-Mail, SMS oder Telefon, mit der Zugangsdaten erlangt oder Personen zum Öffnen einer infizierten Datei verleitet werden sollen.
BitLocker	In Windows Pro/Enterprise integriertes Verschlüsselungswerkzeug. Macht die Daten ohne Entschlüsselungsschlüssel unlesbar.
FileVault	Das Gegenstück zu BitLocker unter macOS. Integrierte Verschlüsselung des Systemlaufwerks.
VPN	Virtual Private Network. Verschlüsselter Tunnel für einen sicheren Fernzugriff auf das Netzwerk der Praxis.
RMM	Remote Monitoring and Management. Professionelle Fernwartungslösung mit Nachvollziehbarkeit (NinjaOne, Datto, Atera).

3-2-1-Regel	Vom BACS empfohlene Sicherungsstrategie: 3 Kopien der Daten, auf 2 verschiedenen Datenträgern, davon 1 ausserhalb der Praxis. Die Variante 3-2-1-1-0 fügt eine Offline- oder unveränderbare Kopie hinzu (vor Veränderung geschützt) und strebt bei den Wiederherstellungstests null Fehler an.
WPA3 / WPA2	WLAN-Sicherheitsprotokolle. WPA3 ist die neueste und sicherste Version; WPA2 ist das akzeptable Minimum.
HIN	Health Info Net. Sicheres Schweizer Netzwerk für den Austausch zwischen Gesundheitsfachpersonen.
DSV	Datenschutzverordnung. Ausführungserlass zum DSG, der die technischen und organisatorischen Einzelheiten regelt.

Impressum und Nutzungsbedingungen

Dieses Dokument wurde von **DentalSystems Sàrl** zu Informations- und Sensibilisierungszwecken verfasst. Es stellt keine Rechtsberatung dar. Die Informationen in diesem Dokument entsprechen dem Stand von Oktober 2026 und können sich mit Gesetzes- und Verordnungsänderungen weiterentwickeln. Diese deutsche Fassung ist eine Übersetzung; massgebend ist die französische Fassung.

Wenden Sie sich bei allen Rechtsfragen zum DSGVO, zur DSGVO oder zum Datenschutz im medizinischen Umfeld an eine spezialisierte Rechtsfachperson.

Geistiges Eigentum

Dieses Dokument ist ausschliessliches Eigentum der DentalSystems Sàrl. Sein gesamter Inhalt (Texte, Struktur, Layout und grafische Elemente) ist urheberrechtlich geschützt gemäss dem Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG, SR 231.1).

Erlaubte Nutzung

Dieser Leitfaden (DS1) und das Notfallblatt (DS2) werden kostenlos zur Verfügung gestellt. Sie dürfen innerhalb einer Zahnarztpraxis oder einer medizinischen Einrichtung frei heruntergeladen, ausgedruckt und verbreitet werden, unverändert und unter Nennung ihres Urhebers (DentalSystems Sàrl). Die Vorlagen des Kits (DS3 bis DS11) dürfen angepasst und unter dem Namen der Praxis verwendet werden, auch gegenüber ihren Patientinnen und Patienten, Mitarbeitenden und Dienstleistern, ohne die Hinweise auf DentalSystems Sàrl beizubehalten.

Untersagte Nutzung

Ohne vorgängige schriftliche Zustimmung der DentalSystems Sàrl ist Folgendes strikt untersagt:

- Der Verkauf oder die Vermarktung dieser Dokumente in jeglicher Form, auch in veränderter Fassung.
- Die Verbreitung einer veränderten Fassung des Leitfadens oder des Notfallblatts oder deren Ausgabe als Werk eines anderen Urhebers.
- Das Entfernen, Verändern oder Verbergen der Urheberangaben, des Logos oder der Kontaktdaten der DentalSystems Sàrl im Leitfaden und im Notfallblatt.
- Das Bereitstellen dieser Dokumente zum Herunterladen für Dritte (Download-Websites, Austauschplattformen, Wiederverkäufer).

Jede nicht autorisierte kommerzielle Nutzung stellt eine Urheberrechtsverletzung dar und kann rechtlich verfolgt werden. Bei Abweichungen gehen die auf www.dentalsystems.ch veröffentlichten Nutzungsbedingungen vor.

Haftungsbeschränkung

Dieses Dokument wird kostenlos und zu Informationszwecken zur Verfügung gestellt. Soweit nach Schweizer Recht zulässig, haftet DentalSystems Sàrl nicht für direkte oder indirekte Folgen seiner Nutzung; diese Beschränkung gilt nicht bei Vorsatz oder grober Fahrlässigkeit (Art. 100 OR). Die Nutzerinnen und Nutzer sind allein dafür verantwortlich, diese Informationen an ihre konkrete Situation anzupassen. Dieses Dokument ersetzt weder ein professionelles Audit noch eine Rechtsberatung.

DentalSystems Sàrl

Thomas Alvino, IT-Techniker

www.dentalsystems.ch | talvino@dentalsystems.ch | +41 77 245 48 44

© 2026 DentalSystems Sàrl. Alle Rechte vorbehalten.