

NOTFALLBLATT: SICHERHEITSVORFALL

Zahnarztpraxis | Notfallverfahren | Bei jedem Arbeitsplatz aushängen

Art. 24 DSGVO. Meldepflicht bei Verletzungen der Datensicherheit

Verdacht auf einen Angriff? Diese 6 Schritte der Reihe nach befolgen. Keine Panik.

1 ISOLIEREN

- Netzkabel (Ethernet) sofort ausstecken
- WLAN am betroffenen Computer deaktivieren
- Computer NICHT AUSSCHALTEN; das zerstört die Beweise

2 IHREN IT-DIENSTLEISTER ANRUFEN

- Zuerst Ihren IT-Dienstleister kontaktieren
- Falls nicht erreichbar: BACS über report.ncsc.admin.ch oder incidents@ncsc.ch
- Die beobachteten Symptome schildern

3 DOKUMENTIEREN

- Fehler- oder Lösegeldmeldungen fotografieren
- Genaue Uhrzeit der Entdeckung des Vorfalls notieren
- Möglicherweise betroffene Computer und Daten auflisten

4 KEIN LÖSEGELD BEZAHLEN

- Offizielle Empfehlung des Bundes
- Eine Zahlung garantiert nicht, dass die Daten zurückkommen
- Sie finanziert kriminelle Netzwerke

5 BEURTEILEN: hohes Risiko für die Patienten?

- Röntgenbilder, Akten, Diagnosen, AHV-Nummern, Rechnungen betroffen?
- Falls JA oder nicht auszuschliessen: Meldung an den EDÖB obligatorisch
- Meldung nicht bis zum Ende der Abklärung aufschieben

6 DEM EDÖB MELDEN

- Portal: databreach.edoeb.admin.ch
- Telefon EDÖB: +41 58 462 43 95
- Frist: so rasch als möglich (Art. 24 DSGVO)

NOTFALLKONTAKTE UND REFERENZEN

Bei jedem Arbeitsplatz der Praxis aufbewahren

BACS: Bundesamt für Cybersicherheit

Laufender Angriff, Ransomware, Eindringen

incidents@ncsc.ch

Online-Formular: **report.ncsc.admin.ch**

EDÖB: Meldung einer Verletzung der Datensicherheit

Gesetzliche Pflicht nach Art. 24 DSG. Mo–Fr 10–12 Uhr

+41 58 462 43 95

Portal: **databreach.edoeb.admin.ch**

Kantonspolizei
117

No More Ransom (Entschlüsselung)

www.nomoreransom.org

SZENARIO B: VERSEHENTLICHER VERLUST ODER ABFLUSS VON DATEN

- Verlust eines Datenträgers (USB-Stick, Festplatte, gestohlener Laptop)
- Versand von Patientendaten per E-Mail an den falschen Empfänger
- Versehentliches Löschen von Patientenakten ohne Datensicherung
- Unberechtigter Zugriff entdeckt (ehemalige Mitarbeitende, kompromittiertes Konto)

Vorgehen: dokumentieren, Risiko beurteilen, bei hohem Risiko dem EDÖB melden, Patientinnen und Patienten nötigenfalls informieren

RECHTSGRUNDLAGEN: DSG (SR 235.1)

Art. 5 Bst. h	Begriff der Verletzung der Datensicherheit
Art. 8	Pflicht zur Datensicherheit (technische und organisatorische Massnahmen)
Art. 9	Auftragsbearbeitung: Vertrag mit Ihrem IT-Dienstleister obligatorisch
Art. 24	Meldung von Verletzungen an den EDÖB so rasch als möglich
Art. 60-61	Strafbestimmungen: bis CHF 250'000 (persönliche Haftung)
Art. 66	Verjährung der Strafverfolgung: 5 Jahre

PRÄVENTION: DIE WICHTIGSTEN KONTROLLEN

☐ Sicheres E-Mail (HIN Mail / ProtonMail)	☐ Alle Computer mit aktuellem Windows 11 / macOS
☐ 3-2-1-Backups mindestens einmal pro Jahr getestet	☐ Patienten-WLAN vom Praxisnetz getrennt
☐ Festplattenverschlüsselung (BitLocker / FileVault)	☐ Sicherer Fernzugriff (nie Gratis-TeamViewer)
☐ Passwörter mit 12+ Zeichen + Passwort-Manager	☐ Auftragsbearbeitungsvertrag signiert (Art. 9 DSG)
☐ Zwei-Faktor-Authentifizierung für kritische Zugänge	☐ Notfallplan dokumentiert und zugänglich

Der EDÖB macht keine Razzia in Ihrer Praxis.

Er liest Ihre Meldung, prüft, ob Sie richtig reagiert haben, und kann Präzisierungen verlangen.

Die goldene Regel: Lieber früh melden als gar nicht.

Rechtliche Hinweise und Nutzungsbedingungen

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

Bei rechtlichen Fragen zum DSG, zur DSGVO oder zum Datenschutz im medizinischen Umfeld wenden Sie sich an eine spezialisierte Juristin oder einen spezialisierten Juristen.

Geistiges Eigentum

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

Erlaubte Nutzung

Dieses Dokument wird kostenlos zur Verfügung gestellt. Es darf innerhalb einer Zahnarztpraxis oder einer medizinischen Einrichtung frei heruntergeladen, ausgedruckt und verbreitet werden, unverändert und mit Nennung der Urheberin (DentalSystems Sàrl).

Verbotene Nutzung

Ohne vorgängige schriftliche Zustimmung der DentalSystems Sàrl ist Folgendes verboten:

- Der Verkauf dieses Dokuments, auch in geänderter Form.
- Das Anbieten zum Herunterladen für Dritte (Download-Websites, Austauschplattformen, Wiederverkäufer).
- Das Entfernen oder Ändern der Nennung der Urheberin oder dieses Hinweises.

Es gelten die auf www.dentalsystems.ch veröffentlichten Nutzungsbedingungen; bei Abweichungen gehen sie diesem Hinweis vor.

Haftungsbeschränkung

Dieses Dokument wird kostenlos und zu Informationszwecken zur Verfügung gestellt. Soweit nach schweizerischem Recht zulässig, haftet die DentalSystems Sàrl nicht für die Folgen seiner Verwendung; diese Beschränkung gilt nicht bei Vorsatz oder grober Fahrlässigkeit. Die Nutzerin oder der Nutzer bleibt dafür verantwortlich, es an die eigene Situation anzupassen. Es 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.