JAHRESSTART-CHECKLISTE

Datenschutz & IT-Sicherheit: zehn Punkte für den Jahresbeginn

Zehn Punkte, die Sie zu Jahresbeginn prüfen sollten.

Ein neues Jahr ist ein guter Anlass, Datenschutz und IT-Sicherheit einmal durchzugehen. Nicht als Großprojekt, sondern als feste Routine: zehn Punkte, die sich in wenigen Stunden prüfen lassen und viel Ärger ersparen. Die Liste passt für Praxen, MVZ, Labore und Pflegedienste gleichermaßen. Auf Seite 3 finden Sie die Checkliste zum Abhaken.

1 Verzeichnis der Verarbeitungstätigkeiten aktualisieren

Neue Software, ein neuer Dienstleister, eine zusätzliche Online-Terminbuchung? Alles, womit Sie personenbezogene Daten verarbeiten, gehört ins Verarbeitungsverzeichnis (Art. 30 DSGVO). Prüfen Sie, ob es noch zum tatsächlichen Alltag passt.

2 Verträge mit Dienstleistern prüfen

Für jeden Dienstleister, der in Ihrem Auftrag mit Patientendaten arbeitet, brauchen Sie einen Vertrag zur Auftragsverarbeitung (Art. 28 DSGVO). Typische Kandidaten sind IT-Betreuung, Praxissoftware, Cloud-Speicher, Abrechnung und Aktenvernichtung. Fehlt ein Vertrag, holen Sie ihn jetzt nach.

3 Zugänge und Berechtigungen aufräumen

Haben ausgeschiedene Mitarbeitende noch Zugänge? Gibt es gemeinsam genutzte Konten? Jede Person sollte nur die Rechte haben, die sie für ihre Arbeit braucht. Entfernen Sie alles, was nicht mehr benötigt wird.

4 Passwörter und Anmeldung absichern

Ersetzen Sie Standardpasswörter, etwa bei Routern und Geräten, und schalten Sie die Zwei-Faktor-Anmeldung überall dort ein, wo sie angeboten wird: E-Mail, Fernzugriff, Cloud-Dienste. Ein Passwortmanager hilft dem Team, sichere Passwörter zu nutzen, ohne sie aufzuschreiben.

5 Updates und veraltete Geräte prüfen

Sind Betriebssysteme, Programme und Router auf dem aktuellen Stand? Geräte, für die es keine Sicherheitsupdates mehr gibt, sollten ersetzt werden. Arztpraxen gleichen bei dieser Gelegenheit den Stand mit der IT-Sicherheitsrichtlinie der KBV ab.

6 Datensicherung testen

Eine Sicherung ist nur so gut wie die erfolgreiche Wiederherstellung. Lassen Sie testweise einige Dateien zurückspielen. Prüfen Sie auch, ob eine Kopie getrennt vom Praxisnetz aufbewahrt wird, damit sie bei einem Angriff nicht mitverschlüsselt wird.

7 Notfallplan aktualisieren

Stimmen die Telefonnummern von IT-Dienstleister, Datenschutzbeauftragtem und Versicherung noch? Weiß jede Person im Team, was bei einem Verdacht auf einen Cyberangriff zu tun ist? Unsere Notfallkarte dazu finden Sie unter privalexis.de/wissen.

8 Schulungen planen

Legen Sie die Termine für das Jahr fest: Datenschutzschulung, Hinweise zu Phishing-Mails und, wenn Sie KI nutzen, die Schulung zur KI-Kompetenz. Neue Mitarbeitende werden bei der Einarbeitung geschult. Dokumentieren Sie Datum, Inhalte und Teilnehmende.

9 Informationen für Patienten und Website prüfen

Sind Datenschutzhinweise in der Praxis, im Anmeldebogen und auf Ihrer Website noch aktuell? Neue Dienste wie eine Online-Terminbuchung oder ein Kontaktformular müssen dort beschrieben sein.

10 Löschfristen umsetzen

Unterlagen dürfen nicht unbegrenzt aufbewahrt werden. Behandlungsunterlagen sind in der Regel zehn Jahre nach Abschluss der Behandlung aufzubewahren (§ 630f BGB), soweit keine längeren Fristen gelten. Was abgelaufen ist, wird datenschutzgerecht vernichtet: Papier über einen zertifizierten Aktenvernichter, Datenträger durch sichere Löschung.

+ Bonus: Das Vorjahr auswerten

Gab es Datenpannen, Beschwerden oder Auskunftsanfragen? Was ist gut gelaufen, was nicht? Ein kurzer Rückblick mit Ihrem Datenschutzbeauftragten zeigt, wo Sie im neuen Jahr nachsteuern sollten.

Lieber prüfen lassen? Unser Datenschutz-Quick-Check zum Festpreis ist eine kompakte Bestandsaufnahme mit klarer Liste, was zu tun ist. Kostenloses Erstgespräch: 06124 607962-0 oder kontakt@privalexis.de

PrivaLexis
CONSULTING&SOLUTIONS

Praxis / Einrichtung _____ Jahr _____

CHECKLISTE

Jahresstart: Datenschutz & IT-Sicherheit

Abhaken, Datum und Kürzel eintragen, zu den Unterlagen legen. Erklärungen zu jedem Punkt auf Seite 1 und 2.

ERL.	PRÜFPUNKT	ERLEDIGT AM	KÜRZEL
☐	**1 Verarbeitungsverzeichnis aktualisieren** Neue Software, Dienstleister oder Abläufe ergänzt? (Art. 30 DSGVO)		
☐	**2 Verträge mit Dienstleistern prüfen** Auftragsverarbeitungsvertrag für IT, Software, Cloud, Abrechnung vorhanden? (Art. 28 DSGVO)		
☐	**3 Zugänge und Berechtigungen aufräumen** Zugänge Ausgeschiedener gesperrt, keine gemeinsamen Konten, nur nötige Rechte		
☐	**4 Passwörter und Anmeldung absichern** Standardpasswörter ersetzt, Zwei-Faktor-Anmeldung für E-Mail, Fernzugriff, Cloud		
☐	**5 Updates und veraltete Geräte prüfen** Systeme aktuell, Geräte ohne Sicherheitsupdates ersetzt, ggf. KBV-Richtlinie abgeglichen		
☐	**6 Datensicherung testen** Wiederherstellung erfolgreich getestet, Kopie getrennt vom Praxisnetz		
☐	**7 Notfallplan aktualisieren** Telefonnummern aktuell, Team kennt die Sofortmaßnahmen bei einem Cyberangriff		
☐	**8 Schulungen planen** Termine für Datenschutz, Phishing und ggf. KI-Kompetenz festgelegt und dokumentiert		
☐	**9 Patienteninformationen und Website prüfen** Datenschutzhinweise in Praxis, Anmeldebogen und auf der Website aktuell		
☐	**10 Löschfristen umsetzen** Abgelaufene Unterlagen datenschutzgerecht vernichtet (Behandlungsunterlagen i. d. R. 10 Jahre, § 630f BGB)		

ⓘ **Bonus: Das Vorjahr auswerten.** Gab es Datenpannen, Beschwerden oder Auskunftsanfragen? Ein kurzer Rückblick mit Ihrem Datenschutzbeauftragten zeigt, wo Sie nachsteuern sollten.