Checkliste: Cybersecurity in der Tierarztpraxis

Damit die Daten Ihrer Kund*innen und Patienten, Laborberichte sowie die Praxissoftware sicher bleiben.

Grundschutz & Verantwortlichkeiten

- [ ] Verantwortliche Person für IT und Datenschutz im Team festlegen
- [ ] IT-Sicherheitskonzept erstellen (inkl. Notfallsplan)
- [ ] Auftragsverarbeitungsverträge mit Software- und Cloudanbietern prüfen (DSGVO-Konformität, Serverstandort in der EU)
- [ ] Mitarbeitende regelmäßig über Datenschutz und IT-Sicherheit informieren (mind. 1x jährlich)

Passwörter & Zugriffsrechte

- [ ] Starke Passwörter (mind. 12 Zeichen, Kombination aus Klein-, Großbuchstaben, Ziffern und Sonderzeichen)
- [ ] Kein gemeinsames Login im Team – jede Person hat eigene Zugangsdaten
- [ ] Passwortmanager einsetzen
- [ ] Zwei-Faktor-Authentifizierung (2FA) bei Praxissoftware und Cloudsystemen aktivieren
- [ ] Zugriffsrechte regelmäßig überprüfen (z. B. bei Personalwechsel)

Software & Geräte

- [ ] Betriebssysteme, Praxissoftware und Antivirenprogramme aktuell halten
- [ ] Automatische Updates aktivieren
- [ ] Geräte (PCs, Laptops, etc.) mit Passwort oder PIN sperren
- [ ] Mobile Geräte (Praxis-Smartphones, Tablets, etc.) verschlüsseln
- [ ] Alle Geräte vor Entsorgung sicher löschen (Datenträger vernichten oder professionell löschen lassen)

Daten & Backups

- [ ] Regelmäßig Backups durchführen (täglich oder wöchentlich)
- [ ] 3-2-1-Regel umsetzen:
  3 Kopien der Daten
  auf 2 verschiedenen Speichermedien
  1 Kopie extern speichern (Cloud oder Offsite)
- [ ] Wiederherstellung von Daten regelmäßig testen
- [ ] Backups verschlüsselt speichern
- [ ] Zugriff auf Backups nur für autorisierte Personen

TIERÄRZTE VERLAG

Checkliste: Cybersecurity in der Tierarztpraxis

E-Mail & Internetnutzung

- [ ] Verdächtige Anhänge oder Links nicht öffnen
- [ ] E-Mail-Verschlüsselung bei sensiblen Daten aktivieren
- [ ] Download-Quellen prüfen (keine „kostenlosen" Tools von unbekannten Seiten)
- [ ] WLAN passwortschützen, Gäste erhalten eigenes Netz

DSGVO & Dokumentation

- [ ] Verzeichnis der Verarbeitungstätigkeiten
- [ ] Datenschutz-Information für Tierhalter*innen aktuell halten und leicht zugänglich machen
- [ ] Datenspeicherungs- und Löschungsfristen dokumentieren
- [ ] Externe Dienstleister*innen (z. B. Labor, Buchhaltung, etc.) auf Datenschutz prüfen
- [ ] Zugriffe auf sensible Daten regelmäßig kontrollieren und protokollieren

Bonus-Tipps für den Praxisalltag

- [ ] PC-Monitor nach Inaktivität automatisch sperren
- [ ] Passwörter nicht auf Zetteln oder unter der Tastatur aufbewahren
- [ ] Externe USB-Sticks nur nach Virenprüfung anschließen
- [ ] Bei Softwarewechsel: sichere Datenmigration planen
- [ ] Regelmäßig einen Security-Check mit IT-Partner durchführen

Verhalten im Notfall: Keine Panik!

- [ ] Infizierte Geräte sofort vom Netzwerk trennen
- [ ] Bereits im Vorfeld einen Notfallplan für Cyberangriff oder Datenverlust anlegen
- [ ] Wichtige Kontakte griffbereit halten (IT-Dienstleister, Datenschutzbehörde, Software-Support)
- [ ] Vorfall dokumentieren (Zeitpunkt, betroffene Systeme, Maßnahmen)
- [ ] Bei Datenschutzverletzung: Meldung an die Datenschutzbehörde (dsb.gv.at) innerhalb von 72 Stunden prüfen

TIERÄRZTE VERLAG