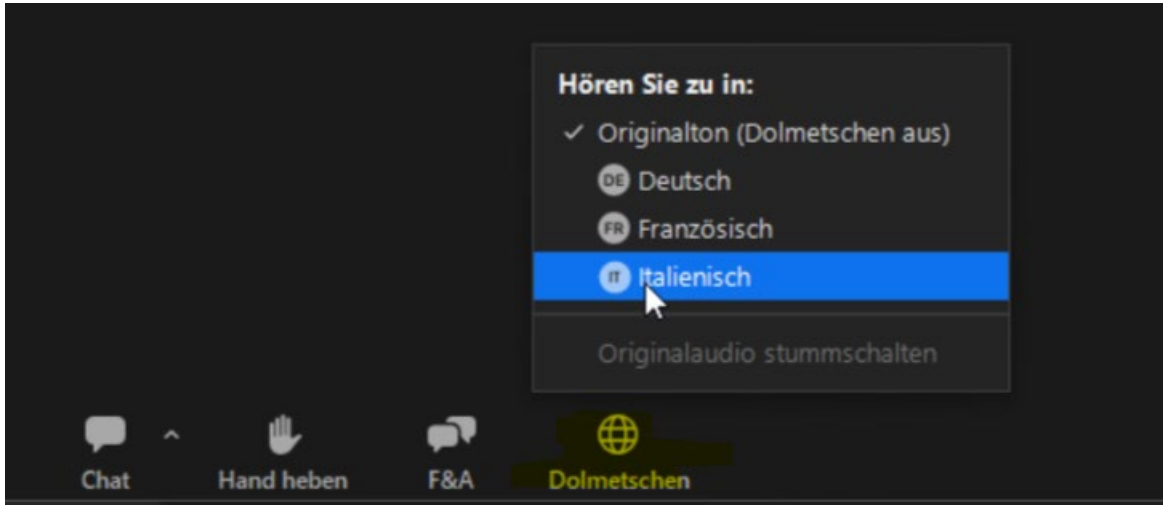
FMH Webinar: neues Datenschutzgesetz

Nouvelle loi sur la protection des données / nuova Legge sulla protezione dei dati

Übersetzung auf Französisch und Italienisch



Referentin und Referenten

Dr. iur. Bruno Baeriswyl
Externer Datenschutzberater der FMH

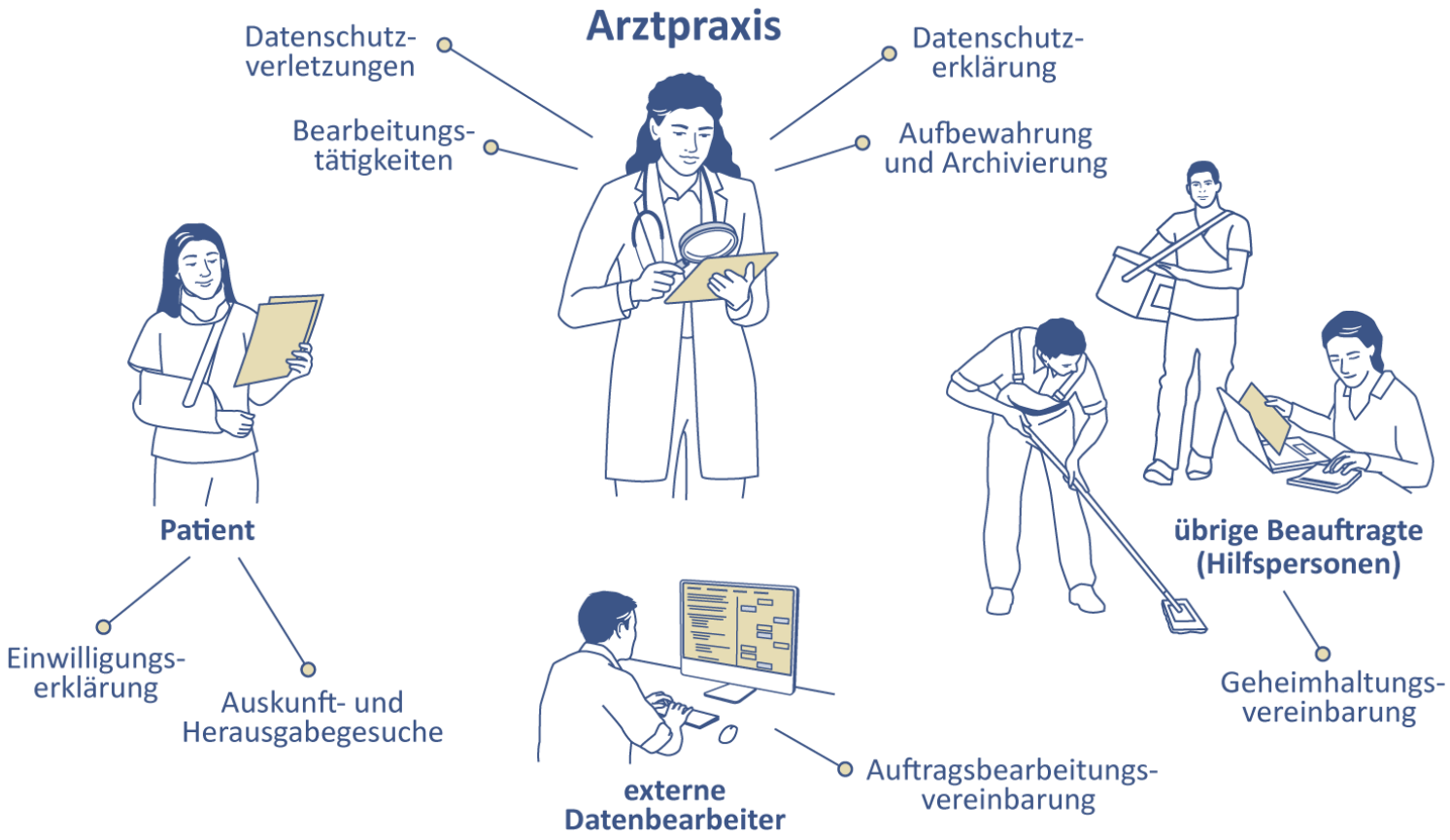
Dr. iur. Iris Herzog-Zwitter
Juristin FMH Rechtsdienst

Dr. rer. biol. hum. Reinhold Sojer
Abteilungsleiter Digitalisierung / eHealth FMH

Agenda

INHALT	WER	DAUER (MIN)
Begrüssung und Einleitung	R. Sojer	5
Zielsetzung zum revidierten DSG	B. Baeriswyl	5
Wesentliche Neuerungen	I. Herzog-Zwitter	5
Terminologie: Neue wichtige Begriffe im DSG	B. Baeriswyl	5
Einwilligungserklärung	I. Herzog-Zwitter	5
Strafbestimmungen	B. Baeriswyl	10
Auftragsbearbeitung	B. Baeriswyl	5
Haftungsrechtliche Aspekte	I. Herzog-Zwitter	5
3 wichtige Neuerungen	B. Baeriswyl	15
Datenschutz und Datensicherheit	R. Sojer	25
Roundtable	Alle	30
Abschluss	R. Sojer	5

Überblick Hilfsmittel



Zielsetzung zum revidierten DSG

Datenschutzgesetz (DSG) vom 25. September 2020

In Kraft ab 1. September 2023

Zielsetzung des (revidierten) Datenschutzgesetzes (1)

1993 → 2023

Technologische Entwicklung

- Datenbearbeitungen
  - Kein Internet
  - Kein Smartphone
  - Keine Cloud
  - Etc.

→ Anpassung an die technologischen Entwicklungen

Europäische Rechtsentwicklung

- Schutz des Menschen bei der automatischen Verarbeitung von Personendaten (Europaratskonvention 108+)
- Datenschutz im Bereich Polizei und Justiz (Richtlinie (EU) 2016/680)
- Allgemeines Datenschutzrecht der EU (Datenschutzgrundverordnung (DSGVO))

→ Anpassung an die rechtlichen Entwicklungen

Zielsetzung des (revidierten) Datenschutzgesetzes (2)

Themenschwerpunkte

Erhöhung der Transparenz der Datenbearbeitungen

Klare Festlegung der Verantwortlichkeiten («Accountability»)

Risikobasierte Massnahmen der Datensicherheit

Stärkung der Rechte der betroffenen Personen

Stärkere Überwachung durch Datenschutzbehörde (EDÖB) und strafrechtliche Sanktionen

→ Keine Änderung der Grundkonzeption

Wesentliche Neuerungen

In Kraft ab 1. September 2023

Die Basis, um sich datenschutzrechtlich zu schützen, ist der Überblick welche Daten bearbeitet werden!

Die Datenbearbeitungsgrundsätze sind im alten und im neuen Datenschutzgesetz deckungsgleich.

Datenbearbeitungsgrundsätze:
Rechtmässigkeit, Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein, Zweckbindung, Vernichtung oder Anonymisierung sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind, Richtigkeit, Einwilligung, Datensicherheit

Wesentliche Neuerungen

1	Die Definition der besonders schützenswerten Personendaten wird um genetische und biometrische Daten, sofern diese eine natürliche Person eindeutig identifizieren, erweitert. Ab dem 1. September 2023 sind nur noch die Personendaten natürlicher Personen betroffen.
2	Bei jeder Beschaffung von Personendaten muss die betroffene Person vorgängig informiert werden. Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten.
3	Nach dem DSG kann jede Person vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.
4	Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden.
5	Ebenso hat der Verantwortliche und der Auftragsbearbeiter eine dem Risiko angemessene Datensicherheit zu gewährleisten.

Wesentliche Neuerungen

6	Das Führen eines Verzeichnisses der Bearbeitungstätigkeiten unter bestimmten Voraussetzungen. Der Bundesrat sieht Ausnahmen für Unternehmen vor, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.
7	Die Durchführung einer Datenschutz-Folgenabschätzung (DSFA), wenn eine Bearbeitung geplant ist, welche voraussichtlich ein hohes Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person mit sich bringt. Diese DSFA ist nur durchzuführen, wenn die bisherigen Datenbearbeitungen nach dem 1. September 2023 geändert werden.
8	Meldepflichten bei Verletzung der Datensicherheit.
9	Verschärfung der Strafbestimmungen: Das neue Datenschutzgesetz sieht Bussen für private Personen bis zu CHF 250'000.- vor. Strafbar sind vorsätzliches Handeln und Unterlassen, aber nicht fahrlässiges Verhalten. Antragsdelikte!

Sofern Sie bis dato die datenschutzrechtlichen Vorgaben in der Praxis bereits umgesetzt haben, sind Sie aller Voraussicht datenschutzrechtlich geschützt. Es bedarf dann lediglich gemäss der wesentlichen Neuerungen Anpassungen.

Terminologie

Neue wichtige Begriffe im DSG

Begriffe

Verantwortlicher
- Entscheidet über Zweck und Mittel der Datenbearbeitung

Auftrags(daten)bearbeiter
- Bearbeitet Personendaten im Auftrag des Verantwortlichen

Besonders schützenswerte Personendaten
- u.a. Gesundheitsdaten, neu: genetische Daten, biometrische Daten

Verletzung der Datensicherheit
- Unbeabsichtigte oder widerrechtlicher Verlust, Löschung, Vernichtung und Veränderung von Personendaten oder Offenlegen oder Zugänglichmachen an Unbefugte

Einwilligung

Zentrales Element: Informationelle Selbstbestimmung

Einwilligung

- Dort wo gesetzliche Rahmenbedingungen wie zum Beispiel in der Invalidenversicherung, Unfallversicherung gegeben sind, bedarf es keiner ausdrücklichen Einwilligung, da mit der Unterschrift zum Beispiel des IV-Anmeldeformulars die Legitimation hiermit gegeben ist.

- Anders sieht es im Privatrecht (z. B. Behandlungsvertrag) und Privatversicherungsrecht aus. Hier bedarf es einer Entbindungserklärung bzw. Einwilligungserklärung.

Einwilligung

- Bei der Bearbeitung von besonders schützenswerten Personendaten muss die Einwilligung durch den Patienten ausdrücklich erfolgen, d.h. mündlich oder schriftlich. Das ist aber auch bereits gemäss geltendem Datenschutzgesetz so.

Einwilligung

- Die Einwilligung muss darüber hinaus eindeutig sein und aus der Erklärung der betroffenen Person muss deren Wille eindeutig hervorgehen.
- Gemäss dem Verhältnismässigkeitsgrundsatz muss die Einwilligung umso eindeutiger sein, je sensibler die fraglichen Personendaten sind.
- Die Einwilligung kann grundsätzlich formfrei erfolgen und ist nicht an die Schriftlichkeit gebunden.

Strafbestimmungen

Strafbestimmungen (1)

Vorbemerkungen

Die wichtigste Strafbestimmung:

→ Berufsgeheimnis; ärztliche Schweigepflicht (Art. 321 StGB)

Der falsche Vergleich:

→ In der EU (DSGVO) liegen umfassende Sanktionsmöglichkeiten bei der Datenschutzbehörde («Bussen»).
Die Schweiz hat nur wenige Strafbestimmungen.
(Bereits das bisherige Datenschutzgesetz kannte Strafbestimmungen. Verurteilungen aufgrund dieser Bestimmungen fehlen praktisch gänzlich.)

Strafbestimmungen (2)

Voraussetzungen der Strafbarkeit

Objektiver Tatbestand

- Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Art. 60 DSG)
- Verletzung von Sorgfaltspflichten (Art. 61 DSG)
- Verletzung der beruflichen Schweigepflicht (Art. 62 DSG)
- Missachtung von Verfügungen (Art. 63 DSG)

Subjektiver Tatbestand

- Vorsatz («mit Wissen und Willen»)

Strafantrag (ausser Art. 63 DSG)

- innert drei Monaten nach Kenntnis

Strafandrohung

- Busse (max. CHF 250 000) → Übertretung

Strafverfolgung

- Kantone

Auftragsbearbeitung

Auftragsbearbeitungs - Geheimhaltungsvereinbarung

Auftragsbearbeitungen

Verantwortlichkeiten

Bearbeitung durch Auftragsbearbeiter
→ z.B. Informatikauslagerung

Die datenschutzrechtliche Verantwortung bleibt beim *Verantwortlichen*!

- Auswahl, Instruktion und Überwachung des Auftragsbearbeiters
- Weisung in Bezug auf Datenbearbeitung an Auftragsbearbeiter
- Auftragsbearbeiter muss in der Lage sein, die Datensicherheit zu gewährleisten

→ **Auftragsbearbeitungsvereinbarung**

Datenbekanntgabe
→ z.B. Orthopädie-Techniker

Die datenschutzrechtliche Verantwortung geht an den Orthopädie-Techniker über.

- Der (ursprünglich) Verantwortliche ist für die sichere Übermittlung verantwortlich
- Sofern der Empfänger nicht unter dem Berufsgeheimnis steht, muss er für die angemessene Geheimhaltung sorgen

→ **Geheimhaltungsvereinbarung**

Haftungsrechtliche Aspekte

Haftungsrechtliche Aspekte

- Die Ärztin / der Arzt hat im Rahmen des Behandlungsvertrages für jede Sorgfaltspflichtverletzung einzustehen.
- Abzustellen ist somit auf eine berufsspezifische hinsichtlich jeder Handlung angepasste Sorgfaltsanwendung.
- Die geforderte Sorgfalt bei der vertraglichen Erfüllung bezieht sich auf die Auswahl (cura in eligendo), die Instruktion (cura in instruendo) und die Überwachung (cura in custodiendo).

Haftungsrechtliche Aspekte

- Die Sorgfaltspflicht der Ärztin bzw. des Arztes umfasst die sorgfältige Ausrüstung von Hilfspersonen mit tauglichem Material und Instrumenten, sowie die sorgfältige und zweckmässige Organisation der Arbeitsabläufe und des Unternehmens.

- Um einen sogenannten Schaden an Dritten zu verhindern, hat die Ärztin / der Arzt nötigenfalls eine Endkontrolle der Arbeitsabläufe durchzuführen.

- Der haftungsrechtliche Freibeweis erfolgt dann, wenn man nachweist, dass man alle nach den Umständen gebotene Sorgfalt angewendet hat, um einen Schaden dieser Art zu verhüten oder dass der Schaden ohnehin auch bei Anwendung dieser Sorgfalt eingetreten wäre.

Haftungsrechtliche Aspekte

Beispiele

- Fehlende Aufklärung und in der Folge mangelhafte Einwilligung
- Gesetzlich vorgeschriebene Datenverzeichnisse müssen aktuell und vollständig sein.
- Die Zuständigkeiten und die Abläufe in einer Arbeitspraxis müssen organisiert sein.
- Die Ausbildung und die Instruktion der MitarbeiterInnen muss sichergestellt sein.
- Haftungssubjekt ist die für die Verletzung des Datenschutzgesetzes verantwortliche Person. Gemäss Botschaft zum rev. Datenschutzgesetz wird nicht auf die Handlungsverantwortlichen abgestellt sondern auf die Organisationsverantwortlichen.

3 wichtige Neuerungen

Verzeichnis der Bearbeitungstätigkeiten
Meldung von Verletzungen der Datensicherheit
Datenschutz-Folgenabschätzung

Verzeichnis der Bearbeitungstätigkeiten

Dokumentation der Datenbearbeitungsprozesse
→ grosse Menge besonders schützenswerter Personendaten ((z.B. Gesundheitsdaten): keine Ausnahme

Inhalt («Mindestangaben»):

- die Identität des Verantwortlichen;
- den Bearbeitungszweck;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien

bearbeiteter Personendaten;

- die Kategorien der Empfängerinnen und Empfänger;
- wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
- wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit;
- falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien.

→ Vorlage Verzeichnis der Bearbeitungstätigkeiten

Meldung von Verletzungen der Datensicherheit

Meldepflicht bei «hohem Risiko»

- z.B. Verlust von Gesundheitsdaten oder unbefugter Zugang

Meldung an Eidgen. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)
- Online-Meldung: https://databreach.edoeb.admin.ch/report

Ev. Information der betroffenen Personen (→ wenn zu deren Schutz erforderlich)

→ Checkliste und Prozessablauf bei Datenschutzverletzungen

Datenschutz-Folgenabschätzung

Bei neuen Datenbearbeitungen
(Bestehende Datenbearbeitungen: zusätzliche Datenkategorien / weitere Zwecke)

Hohes Risiko für die Persönlichkeit oder Grundrechte betroffener Personen

- Verwendung neuer Technologien
- Umfangreiche Bearbeitung besonders schützenswerter Personendaten

→ Risikobeurteilung (und Planung der angemessenen technischen und organisatorischen Massnahmen)

Vorabkonsultation des EDÖB (Art. 23 DSG)

- hohes Risiko trotz vorgesehenen Massnahmen
- keine Vorabkonsultation, wenn Datenschutzberater/in

Aufbewahrungsfristen / Löschung

Personendaten sind zu vernichten oder zu anonymisieren

- sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind

Aufbewahrungsdauer festlegen resp. Kriterien

- Gesetzliche Bestimmungen

→ Leitfaden für die Aufbewahrung und Archivierung

Datenschutz und Datensicherheit

Technische und organisatorische Massnahmen

Datensicherheit

Art. 8 Datensicherheit

[1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

[2] Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

[3] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Datensicherheit

Datenschutz durch Technik

Art. 7 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

[1] Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung.

Datensicherheit

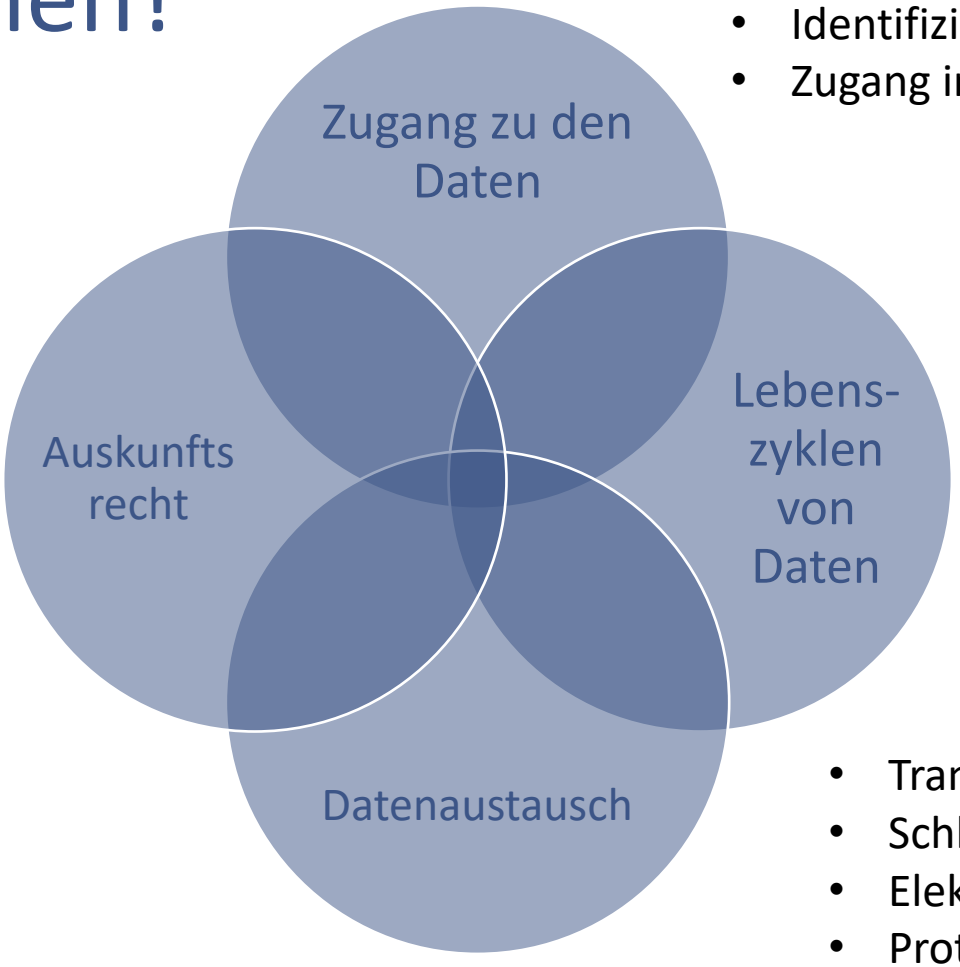
Art. 7 Abs. 1 begründet Sorgfaltspflicht für den Verantwortlichen
Art. 8 Abs. 1 nimmt beide, Verantwortlicher und Auftragsbearbeiter, in die Pflicht!

«Der Verantwortliche muss aktiv sicherstellen, dass der Auftragsbearbeiter das Gesetz im selben Umfang einhält, wie er selbst es tut.»

«Er ist daher verpflichtet, seinen Auftragsbearbeiter sorgfältig auszuwählen, ihn angemessen zu instruieren und soweit als nötig zu überwachen.»

Womit beginnen?

- Sicherheit der Räumlichkeiten, Serverräume,
- Arbeitsplätze
- Identifizierung und Authentifizierung
- Zugang innerhalb und ausserhalb der Arztpraxis



- Erfassung und Protokollierung
- Anonymisierung
- Verschlüsselung
- Datensicherung
- Auftragsbearbeitung (z. B. Cloud)
- Klassifizierung von Daten

- Prozess für Auskunftsgesuche
- Löschung von Daten
- Protokollierung

- Transport- und Inhaltsverschlüsselung
- Schlüsselmanagement
- Elektronische Identität
- Protokollierung

Empfehlungen

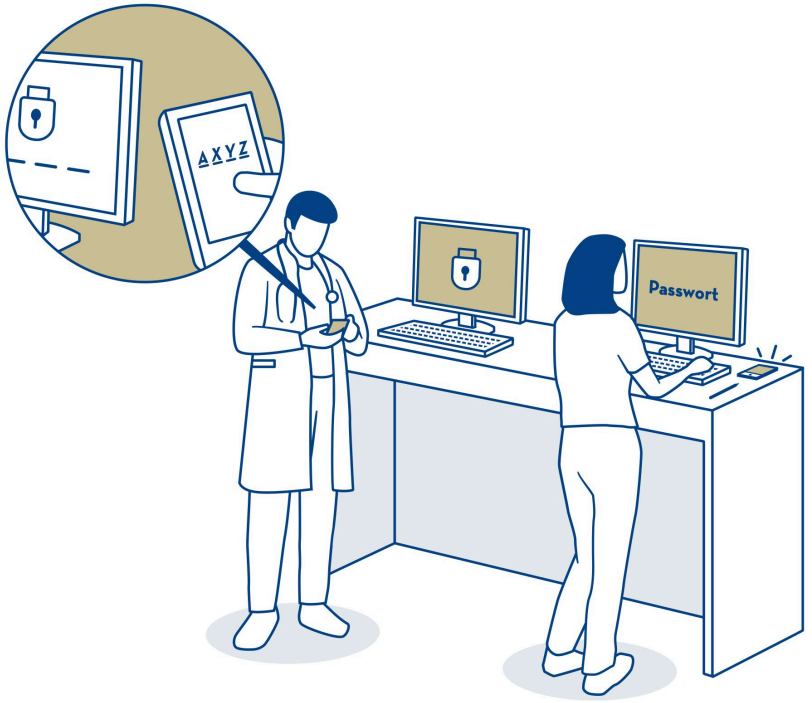
Empfehlungen EDÖB

Technische und organisatorische Anforderungen an Cloud-Dienste

Minimalanforderungen IT-Grundschutz

Beispiel «Zugriffschutz regulieren»

Die zentrale Verwaltung und strukturierte Vergabe der Zugriffs- und Benutzerrechte, beispielsweise mittels Active Directory oder alternativen Verzeichnisdiensten, minimiert die Risiken eines unbefugten Zugriffs auf sensiblen Daten durch interne oder externe Parteien. Die regelmässige Wartung der Zugriffs- und Benutzerrechte ermöglicht es, Änderungen durch Ein- und Austritte von Mitarbeitenden zu erfassen und nachzutragen.

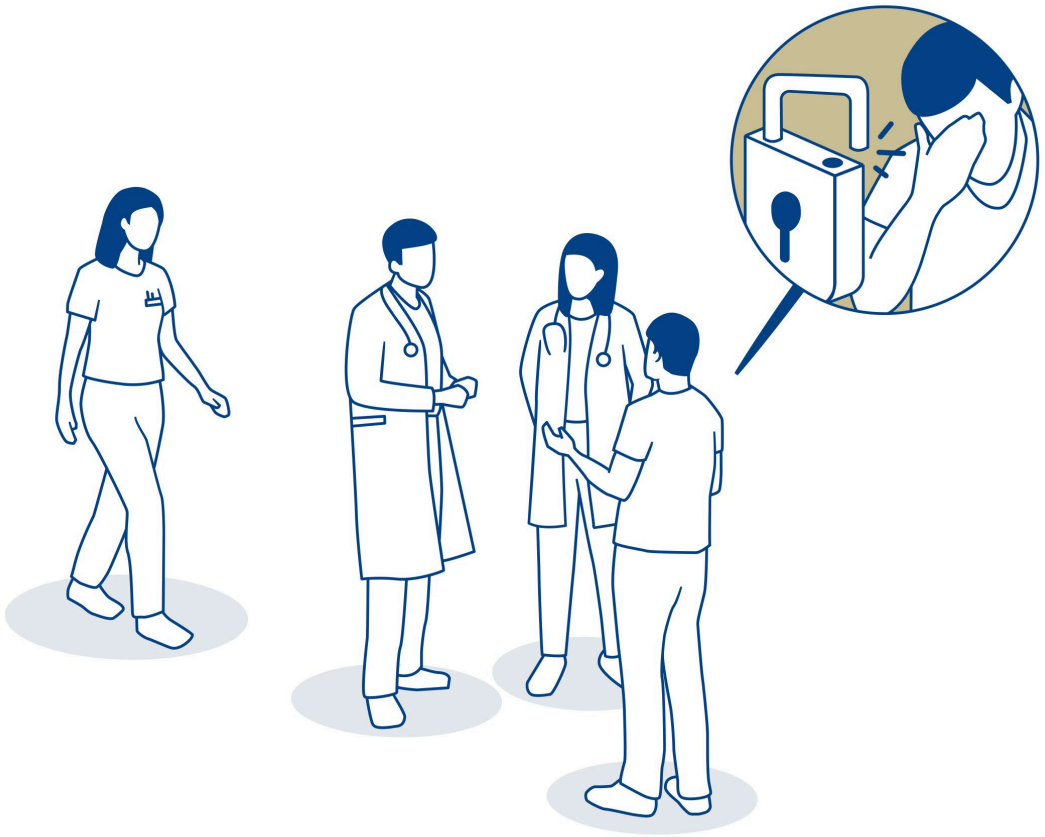


Massnahmen

- Persönliche Benutzerkonten für Mitarbeitende
- Einschränkung der Benutzerrechte («Need to know»)
- Zugriff auf das praxisinterne Netzwerk mit vorgängiger starker Authentifizierung
- Passwortwechsel

Beispiel «Praxismitarbeitende für Datensicherheit sensibilisieren»

Die Mitarbeitenden einer Arztpraxis sind ein beliebtes Angriffsziel für kriminelle Hacker, weshalb Angreifer oftmals versuchen, sich mittels Social-Engineering-Attacken Zugang zur ICT- Umgebung und zu Daten zu verschaffen. Um dies zu verhindern, ist die Sensibilisierung der Praxisverantwortlichen und der Praxismitarbeitenden zentraler Bedeutung.

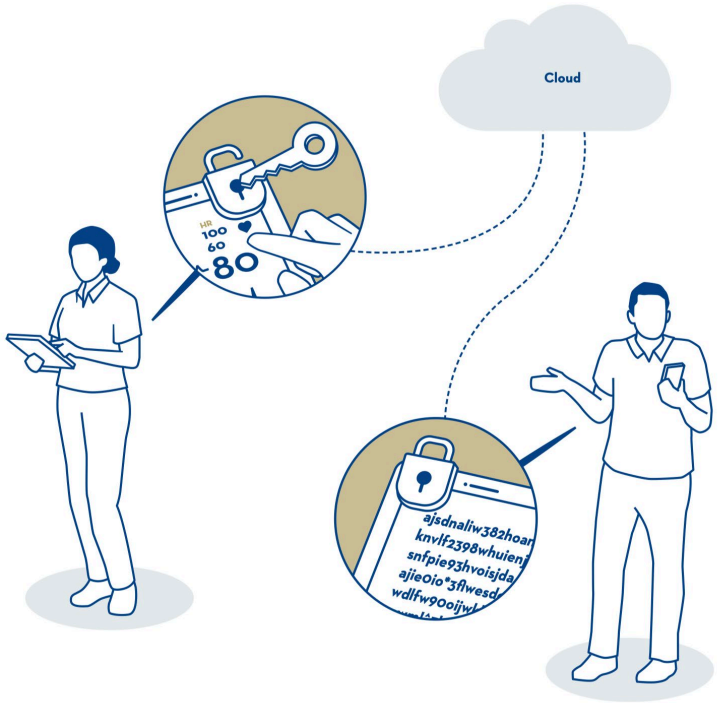


Massnahmen

- Themen in Teammeetings adressieren (Passwörter, Klassifizierung von Daten, Umgang mit ICT-Mitteln, Umgang und Austausch von Daten, Vorgehen bei Sicherheitsvorfällen)
- Neue Mitarbeiter/innen schulen, Merkblätter
- Private Nutzung von ICT-Mittel
- …

Beispiel «Verschlüsselung und Schlüsselmanagement (Cloud)»

Gespeicherte Daten (Data at Rest) wie auch die übertragenen Daten (Data in Transit) müssen mit kryptografischen Verfahren entsprechend geschützt werden. Ebenso muss die Kommunikation über alle ein- und ausgehenden Verbindungen zur und von der Cloud-Infrastruktur einschliesslich der Schnittstellen innerhalb der Cloud-Infrastruktur authentisiert und verschlüsselt erfolgen.



Massnahmen

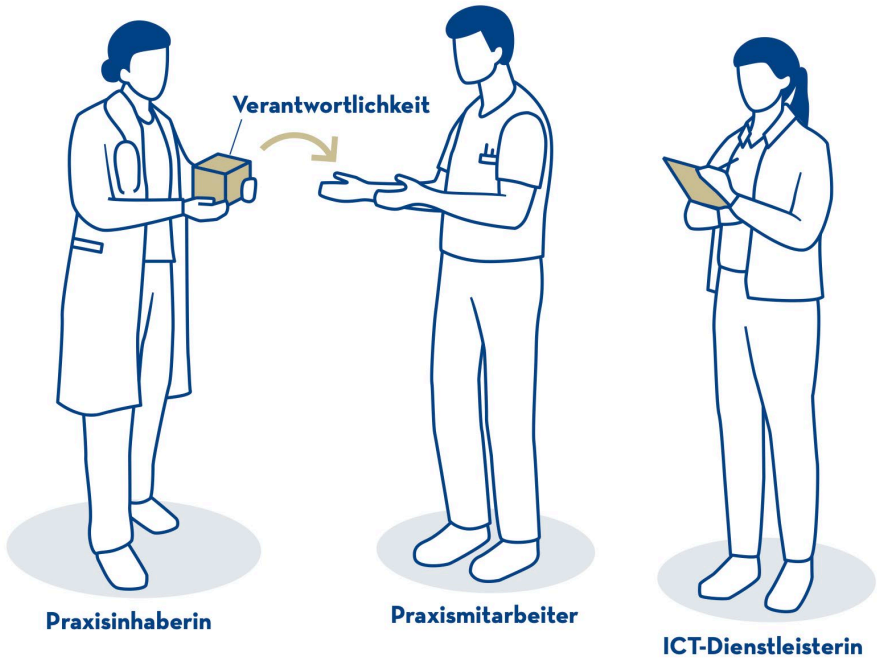
- Speicherverschlüsselung der Inhaltsdaten in allen Lebenszyklen
- Schlüsselmanagement (effektives Recovery-Management)
- Transportverschlüsselung

Verantwortlichkeiten bestimmen und Vorgaben erlassen

Verantwortliche erlässt Vorgaben, Prozesse und interne Kontrolle zur Validierung u. a. von:

- Zugriffskontrollen,
- Erfassen, Speichern und Löschen von Daten,
- Einhaltung regulatorischer Anforderungen,
- Risikomanagement
- weitere

Bei der Auslagerung der Datenbearbeitung in die Cloud verbleibt die Governance stets bei der Arztpraxis. Die Governance kann nicht ausgelagert werden, selbst wenn externe Anbieter einbezogen werden.



Roundtable

Roundtable

Auswahl an ausgewählten Fragen

Abschluss

Abschluss

- Webinar wird aufgezeichnet: Mail an alle Teilnehmerinnen und Teilnehmer mit Link zur Aufzeichnung des Webinars folgt nächste Woche
- Präsentationsfolien in den Sprachen Deutsch, Französisch und Italienisch werden zu einem späteren Zeitpunkt verfügbar sein (Information ebenfalls per Mail)

Vielen Dank für Ihre Aufmerksamkeit

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11
info@fmh.ch · www.fmh.ch