DOMENIG PARTNER

RECHTSANWÄLTE AG

Das neue Datenschutzgesetz

Umsetzung in der Zahnarztpraxis

Chantal Lutz
Senior Associate

St. Gallen, Schweiz

31. August 2023

Agenda

I. Warum ist Datenschutz in der Zahnarztpraxis wichtig?

II. Was ist Datenschutz – und welche Pflichten haben Sie?

III. Wie setzen Sie Datenschutz in ihrer Praxis um?

IV. Key Takeaways

I. Warum ist Datenschutz in der Zahnarztpraxis wichtig?

Warum ist Datenschutz an Ihrer Praxis wichtig?

- **Patientendaten sind besonders sensibel**
- **Rechtssicherheit für Personal schaffen**
- **Haftungsrisiken minimieren**

(Organ- bzw. Mitarbeiterhaftung oder Bussen möglich)

- **Reputation wahren**

✓ **Sie können alle gut schlafen**

Was sind Ihre Risiken?

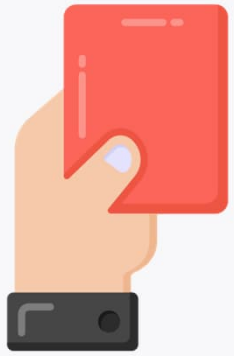
REPUTATION / ZIVILKLAGEN

Security-Flop bei Viseca machte Kreditkartendaten einsehbar

Von Reto Vogt, 20. März 2023 um 11:37

SECURITY DATENSCHUTZ VISECA

Quelle: https://www.inside-it.ch/security-flop-bei-viseca-machte-kreditkartendaten-einsehbar-20230320



Was sind Ihre Risiken?

KOSTEN

Datenbearbeitungen können **vom EDÖB künftig untersagt oder ausgesetzt** werden

- Anpassung Produkte / Geschäftsprozesse nötig

BUSSEN

Strafverfahren (Bussen bis max. CHF 250'000):

- Unvollständige oder falsche Auskunft
- Unvollständige oder falsche Information an betroffenen Personen
- Verletzung von Sorgfaltspflichten (Datensicherheit, Auftragsdatenbearbeitung, Übertragung von Daten in Drittstaaten)
- Verletzung des Berufsgeheimnisses

➢ **In den meisten Fällen werden Entscheidungsträger*innen in Unternehmen die Busse tragen müssen.**

➢ **Das strafrechtliche Risiko kann nicht an den Datenschutzberater delegiert werden!**

II. Was ist Datenschutz – und welche Pflichten haben Sie?

Was ist Datenschutz?

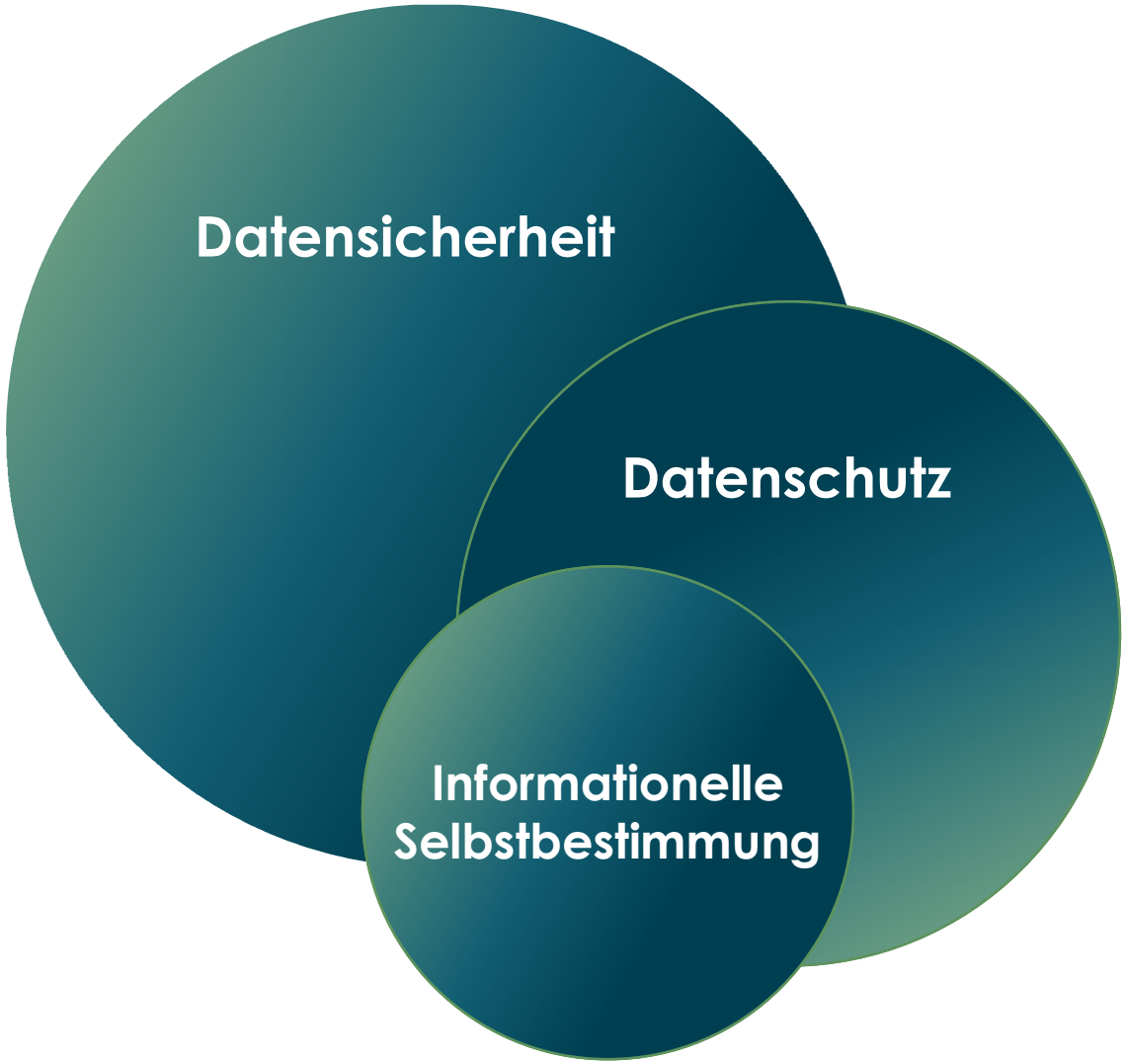
Datenschutz ist die Verwirklichung des Grundrechts auf informationelle Selbstbestimmung.

Aus der Bundesverfassung:

Art. 13 Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.



DAS NEUE DSG

Pflichten des Verantwortlichen

- Führung eines **Datenbearbeitungsverzeichnisses**
- Einhaltung der **Bearbeitungsgrundsätze** (ggf. Einwilligung einholen)
- **Sorgfältige Auswahl, Instruktion und Kontrolle** von Auftragsbearbeitern
- **Risikoabwägung** und Massnahmen bei Datenübermittlung an Drittstaaten
- Ergreifen von **technischen und organisatorischen Massnahmen** (TOM)
- **Informationspflicht** gegenüber betroffenen Personen
- Wahrung der **Rechten der betroffenen Personen**
- **Cybervorfälle: Meldepflichten** einhalten, **Notfall- und Kommunikationskonzept** erstellen
- Erstellung einer **Datenschutz-Folgeabschätzung** bei Cloudvorhaben und anderen risikoreichen Vorhaben (bspw. KI-Einführung)

Bearbeitungsverzeichnis

Pflicht?

Ausnahme für Unternehmen mit weniger als 250 Mitarbeiter und wenn Bearbeitung ein geringes Risiko für die Betroffenen mit sich bringt

- Hohes Risiko bei besonders umfangreicher Bearbeitung besonders schützenswerter Personendaten
- **Klar Ja!**

- Gesetz gibt Mindestinhalt vor
- Mind. 1x pro Jahr nachführen

Bearbeitungsverzeichnis

Vorgang	Rolle	Zweck	Kategorien betroffener Personen	Kategorien bearbeiteter Daten	Kategorien der Empfänger	Dauer der Aufbe-wahrung	Datensicher-heitsmass-nahmen
Patienten-registrierung / Behandlung	Verant-wortlich	Vertrags-abwicklung	Patienten	Personenstamm-, Kontakt-, Adress- und Gesundheitsdaten (Historie, Diagnose, Medikamente, Therapie etc.), Versichertennummer, **genetische Daten?**	IT- und Cloud-provider	Gemäss den gesetzlichen Aufbewahrungs- und Verjährungs-fristen	Massnahmen des Providers (Verweis), Datenklassi-fizierung, Berechtigungs konzept, etc.
Einholung Labor-berichte	…						
Etc.	…						

= Besonders schützenswert
oder
= besonderes Risiko

Was sind Personendaten?

Personenstammdaten, Kontaktdaten, Finanzdaten

Name, Geburtsdatum, Adresse, Zivilstand, Telefon, AHV-Nummer, IBAN-Nummer etc.

Massnahmen und Sanktionen

Informationen über verwaltungs- und strafrechtliche Verfolgung und Sanktionen, Daten über Sozialhilfemassnahmen

Bewegungsdaten

Überwachung, Standort, Tracking (physisch oder online)

Profile

Auswertungen über persönliche Interessen, Vorlieben, Leistung

Aussehen, Identität, Köper und Gesundheit

Ethnie, **Gesundheitsdaten**, Intimsphäre, genetische und biometrische Daten

Weltanschauung

Politische und gewerkschaftliche Tätigkeit und Überzeugung, Religion

Gesundheitsdaten

Gesundheitsdaten liegen vor wenn die Personendaten **Aufschluss über den Körper, die Psyche, das Verhalten oder die (Leistungs-)Fähigkeiten** eines Menschen geben.

Zusätzlich ist ein **klarer Bezug zur Gesundheit** vorausgesetzt. Dieser Bezug ist gegeben, wenn bereits eine **Bewertung des Wohlergehens eines Menschen** erfolgt ist, oder diese Informationen als entsprechende Bewertungsgrundlage dienen können.

Was sind Personendaten?

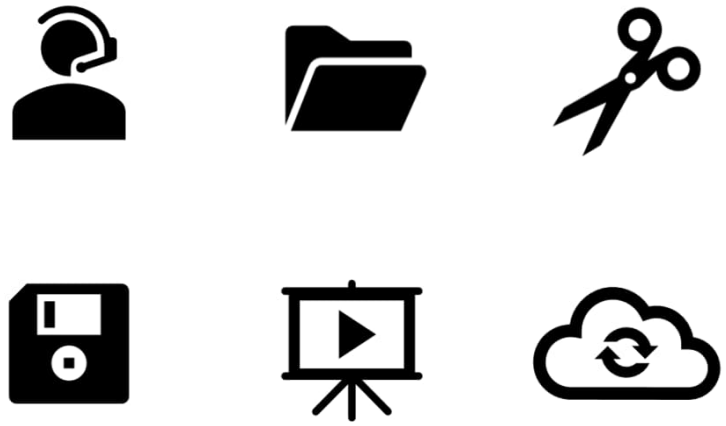
Personendaten:

alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen

Betroffene Person:

natürliche Person, über die Personendaten bearbeitet werden

Was ist das Bearbeiten?



Bearbeiten:

jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren

z.B.: Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, **Bekanntgeben**, Archivieren, Löschen oder Vernichten von Daten

Umgang mit Personendaten

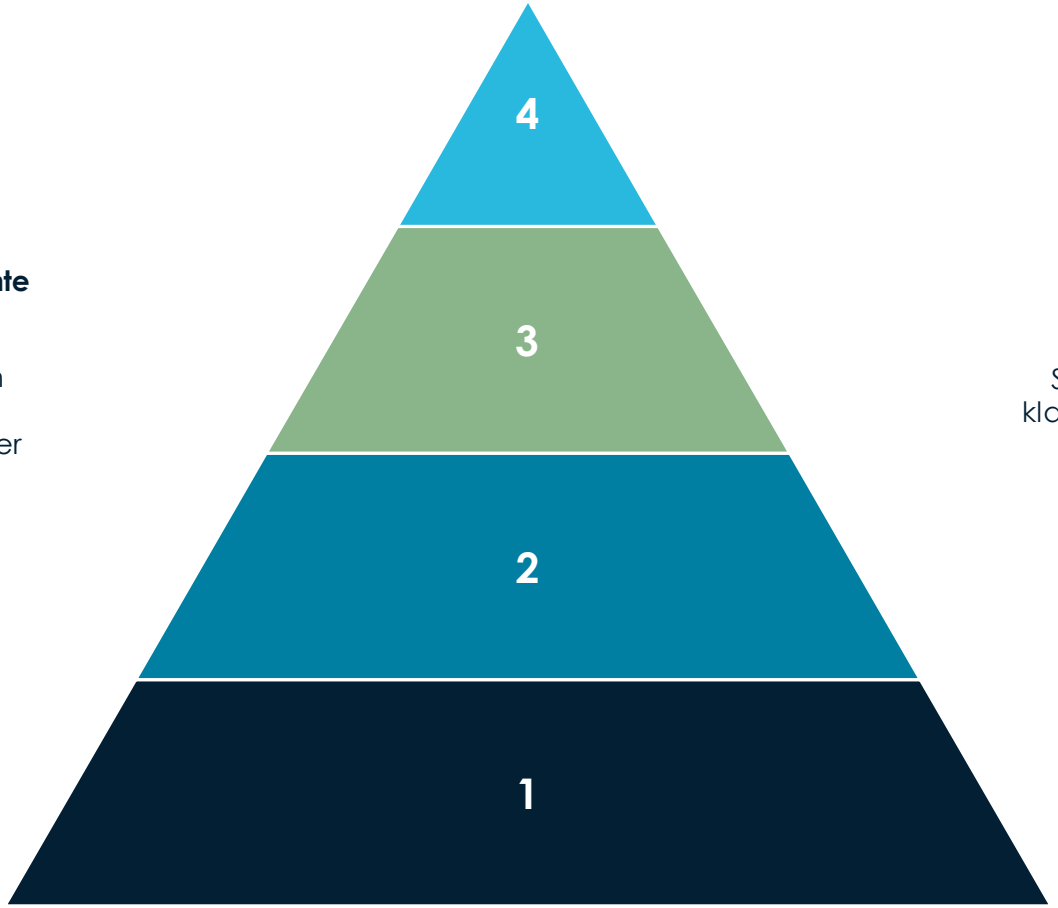
1 **Öffentlich bekanntgemachte Personendaten**

Öffentliche Personendaten dürfen verwendet werden, sofern betroffene Person der Verwendung nicht widersprochen hat.

➢ DSGVO: strenger!

2 **Personendaten**

Sollten mind. als intern qualifiziert werden. Schutzmassnahmen ergreifen.



Besonders schützenswerte Personendaten **3**

Sollten mind. als vertraulich klassifiziert werden, brauchen mehr Schutzmassnahmen. Ggf. Datenschutzfolgen-abschätzung nötig

Profiling mit hohem Risiko **4**

Datenschutzfolgen-abschätzung und ggf. Rücksprache mit EDÖB notwendig, Profiling ggf. nicht zulässig

Datenschutzrechtliche Rollen

Verantwortliche (Zahnarztpraxis)	Auftragsdatenbearbeiter (IT-Provider etc.)
• Entscheidet über die Zwecke und Mittel der Bearbeitung • Tragt Hauptverantwortung und Konsequenzen für Datenbearbeitung	• Darf keine eigenen Zwecke verfolgen • Hauptpflicht ist die Datensicherheit • Auftragsdatenbearbeitungsvertrag (ADV)

Prüft und überwacht Provider!

Auslagerung Daten oder Erteilen eines Zugriffs auf eigene Systeme (Support, Wartung etc.)

Erlaubte Bearbeitung (inkl. Bekanntgabe)

Grundsatz

Datenbearbeitung ist erlaubt.

Aber

Bearbeitungsgrundsätze müssen eingehalten werden.

- Wird einer dieser Grundsätze verletzt, liegt eine Persönlichkeitsverletzung vor!

TRANSPARENZ

ZWECKBINDUNG

DATENMINIMIERUNG

Bekanntgabe von Patientendaten

Berufsgeheimnis und Datenschutz

Berufsgeheimnis ist strafgeschützt (Art. 321 StGB).

Für die Bekanntgabe an Dritte bedarf es **immer einer Einwilligung**.

Die Einwilligung kann auf folgende Arten erfolgen:

- *Ausdrücklich*
- *Stillschweigend*
- *Konkludent*

Die Bekanntgabe von besonders schützenswerten Daten **muss stets rechtmässig erfolgen**.

Als Grundlagen für eine Bekanntgabe kommen in Frage:

- *Einwilligung (muss **ausdrücklich** und freiwillig sein!)*
- *Überwiegende Interessen*
- *Gesetz*

Bekanntgabe von Patientendaten: Beispiel 1

Ein Patient kommt zum Zahnarzt für eine Behandlung. Bei der Behandlung merkt der Zahnarzt, dass er eine **Mundprobe an ein Laboratorium schicken** muss. Nur so erhält er die nötigen Informationen, um die angezeigte Behandlung bestimmen zu können.

Berufsgeheimnis: Der Zahnarzt sagt, dem Patienten, dass er die Probe dem Laboratorium schickt. Da der Patient nicht widerspricht, liegt eine **stillschweigende Einwilligung** vor.

Datenschutz: Der Beizug des Labors ist notwendig, um die Behandlung durchzuführen und die vertraglichen Pflichten zu erfüllen. Der Zahnarzt kann somit **überwiegende Interessen als Rechtfertigungsgrund** für die Datenbekanntgabe geltend machen.

Bekanntgabe von Patientendaten: Beispiel 2

Ein Patient kommt zur Zahnärztin für eine Behandlung. Die Zahnärztin schickt **Patientendaten an ein Forschungsinstitut** weiter, da dieses Forschungszentrum genau solche Fälle benötigt. Hierdurch möchte die Zahnärztin die wichtige Forschung in diesem Gebiet unterstützen.

Berufsgeheimnis: Die Zahnärztin sagt, dem Patienten, dass sie die Probe dem Institut schickt. Da der Patient nicht widerspricht, liegt eine **stillschweigende Einwilligung** vor.

Datenschutz: Sofern die Patientendaten nicht anonymisiert oder pseudonymisiert sind, kann die Zahnärztin keine überwiegenden Interessen geltend machen. Sie braucht folglich eine Einwilligung. Bei Gesundheitsdaten muss diese Einwilligung **ausdrücklich** erfolgen. Der Patient muss also zumindest ausdrücklich sagen, dass er mit der Weitersendung einverstanden ist. Zu Beweiszwecken sollte diese **Einwilligung in Textform** erfolgen.

➢ **Würde die Zahnärztin eigene Forschung betreiben, wäre diese Bearbeitung nach Art. 31 Abs. 2 Bst. e DSG zulässig.**

Betroffenenrechte

Welche Betroffenenrechte gibt es?

- Auskunft
- Herausgabe und Übermittlung
- Berichtigung
- Löschung bzw. Anonymisierung
- Widerspruch
- Widerruf einer Einwilligung

Müssen diese Rechte immer gewährt werden?

- Nein, Betroffenenrechte können unter Umständen aufgeschoben, eingeschränkt oder verweigert werden.
- Bei Auskunft und Datenherausgabe darf bei grossem Aufwand eine max. Kostenbeteiligung von CHF 300.00 verlangt werden.

Auslandsübermittlung

- Bundesrat entscheidet, welche Länder ein **angemessenes Datenschutzniveau** haben.
- Gesetz schreibt gewisse **vertragliche Garantien** vor, mit denen der angemessene Datenschutz gewährleistet wird.
- Ggf. braucht es eine **Risikoprüfung** und der Form eines Transfer Impact Assessment (TIA).
  - Die **Liste der Staaten** mit einem angemessenen Datenschutzniveau kann auf der Webseite des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten abgerufen werden: **www.edoeb.ch**

Datensicherheit

*«Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete **technische** und **organisatorische Massnahmen** eine **dem Risiko angemessene** Datensicherheit.»* Art. 8 Abs. 1 DSG

Schutzziele («CIA»)

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- *Nachvollziehbarkeit*

Meldepflichten?

Europäischer Wirtschaftsraum

Schweiz

Meldung an Aufsichts-behörden innert 72 Stunden

Meldung an EDÖB bei hohem Risiko so bald wie möglich

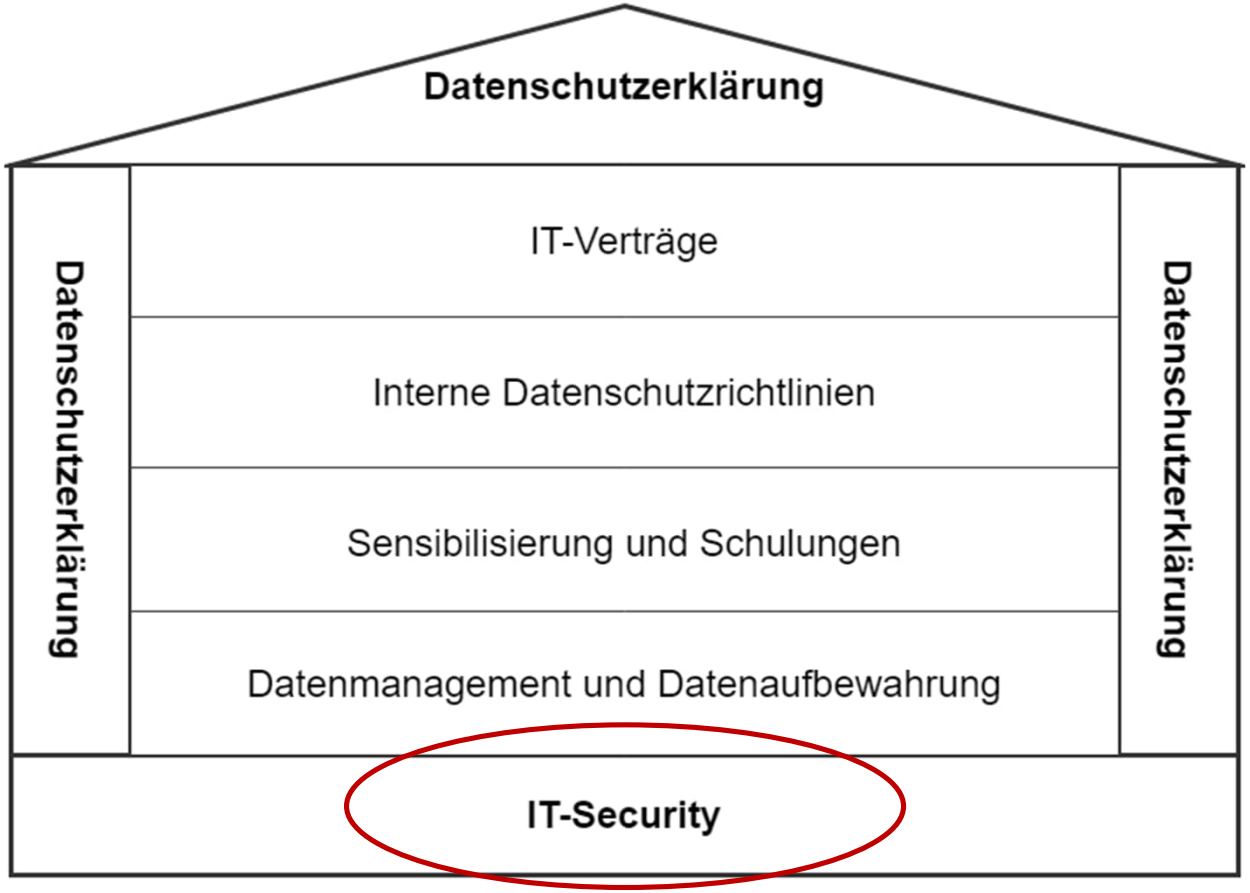
2024: Meldung an NCSC? Cyberangriff auf kritische Infrastrukturen

Meldung an Betroffene, wenn zu deren Schutz notwendig

III. Wie setzen Sie Datenschutz in Ihrer Praxis um?

Meilensteine

Datenschutz Haus



Informations- und Datensicherheit

Bei der Abwägung ist wie folgt vorzugehen:

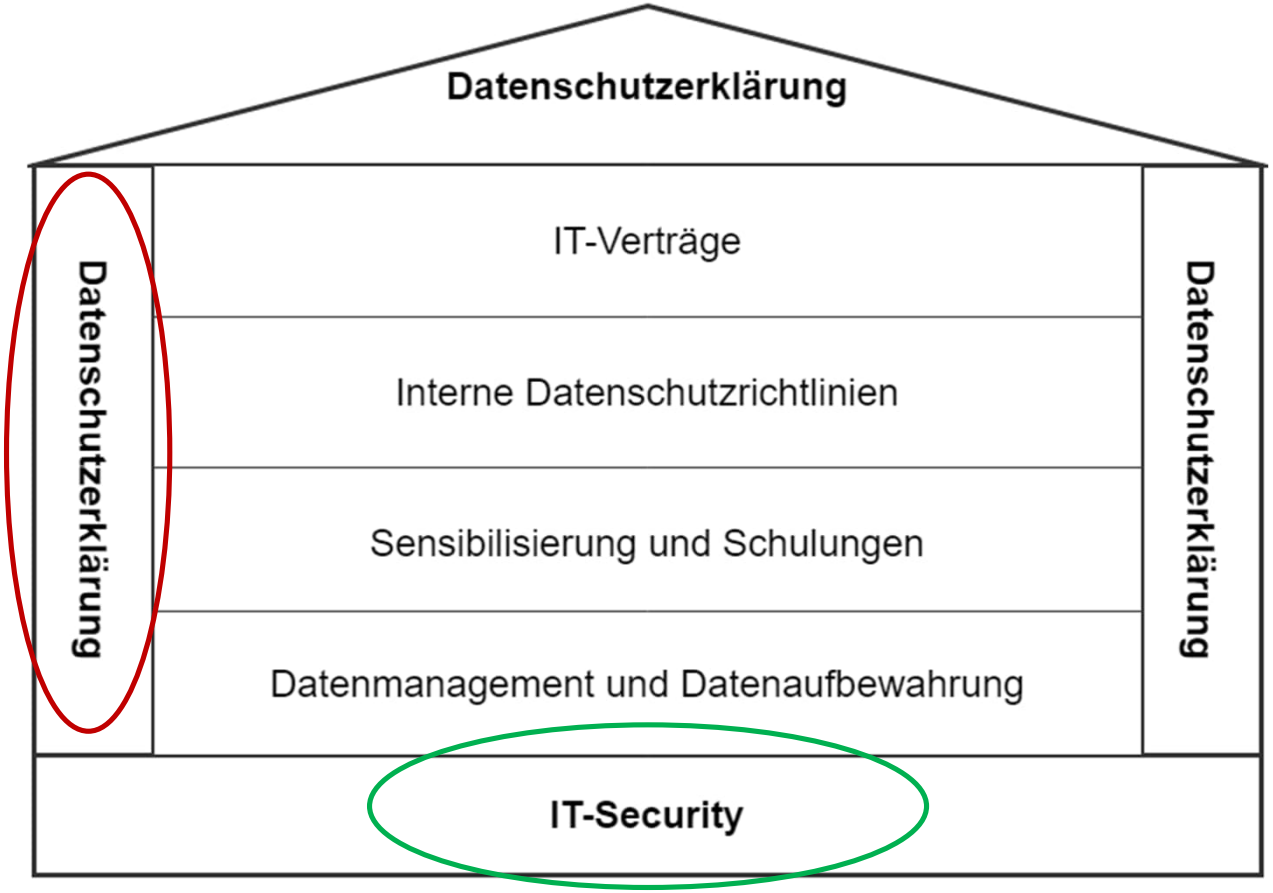
1. **Festlegung des Schutzbedarfs**
2. **Beurteilung des Risikos**
3. **Bestimmung der zu ergreifenden/verbessernden Massnahmen**
4. **Bei Änderungen wieder re-evaluieren**

→ Prozess für Meldung von Datensicherheitsvorfällen (intern und extern) erstellen!

Hilfestellungen

- Beurteilung Schutzbedarf
- Einführung in die Risikoidentifikation und Risikobewertung
- IKT-Minimalstandard (Maturitätsbewertung)
- Vorlage Risikoanalyse des Bundes
- iBarry (Plattform für Internetsicherheit)

Datenschutz Haus



Datenschutzerklärung

- Information über die **Beschaffung** von Personendaten (auch, wenn **Daten bei Dritten** beschafft werden).
- Informationen, die für die Betroffenen notwendig sind, um **Rechte geltend zu machen.**
- **Mindestinhalt**:
  - Identität und Kontaktdaten des **Verantwortlichen**;
  - **Bearbeitungszweck**;
  - Gegebenenfalls die Kategorien von **Empfänger von Personendaten;**
  - **Übermittlungsland** und ggf. die Garantien.
- **Risikobasierter Ansatz**: Je heikler Datenbearbeitung, umso genauer und umfangreicher die Information.
- **Form**: Normalfall Datenschutzerklärung auf Webseite und Link dazu in Vertrag

WERBUNG IN EIGENER SACHE: EINE DATENSCHUTZERKLÄRUNG IN 5 MINUTEN MIT DEM DATENSCHUTZ-GENERATOR VON DOMENIG & PARTNER RECHTSANWÄLTE UND DIGINLAB

Warum PrivacyBee?

- Dank künstlicher Intelligenz liefert PrivacyBee verständliche Erklärungen für jeden eingesetzten Dienst **auf der Webseite**.
- Von Anwälten geprüft – für Kunden gemacht. PrivacyBee erstellt vollautomatisch dank modernster Technologie eine Datenschutzerklärung.
- PrivacyBee erkennt selbständig neue Dienste auf Deiner Internetseite und aktualisiert die Datenschutzerklärung auf den neusten Stand.

How to PrivacyBee

Die Integration von PrivacyBee ist ganz einfach und in 5 Minuten erledigt!

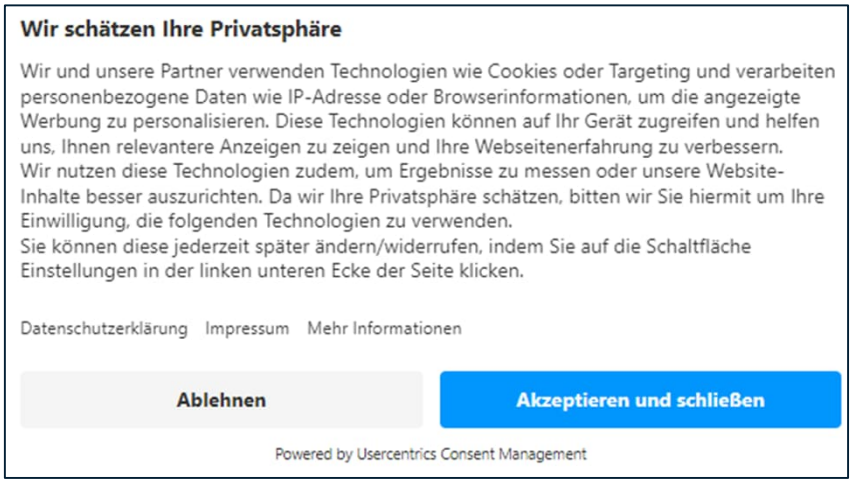
Mit der **kostenlosen 14 Tage Testphase** können Sie PrivacyBee unverbindlich ausprobieren.

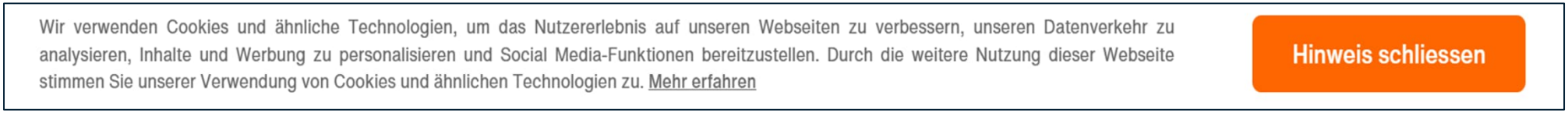
Ihnen wird ein Javascript Snippet zur Verfügung gestellt, welches Sie einfach in Dein CMS einbinden können. Falls das nicht möglich ist, können Sie auf eine Seite verlinken - ganz einfach und unkompliziert.

➢ https://www.privacybee.ch/

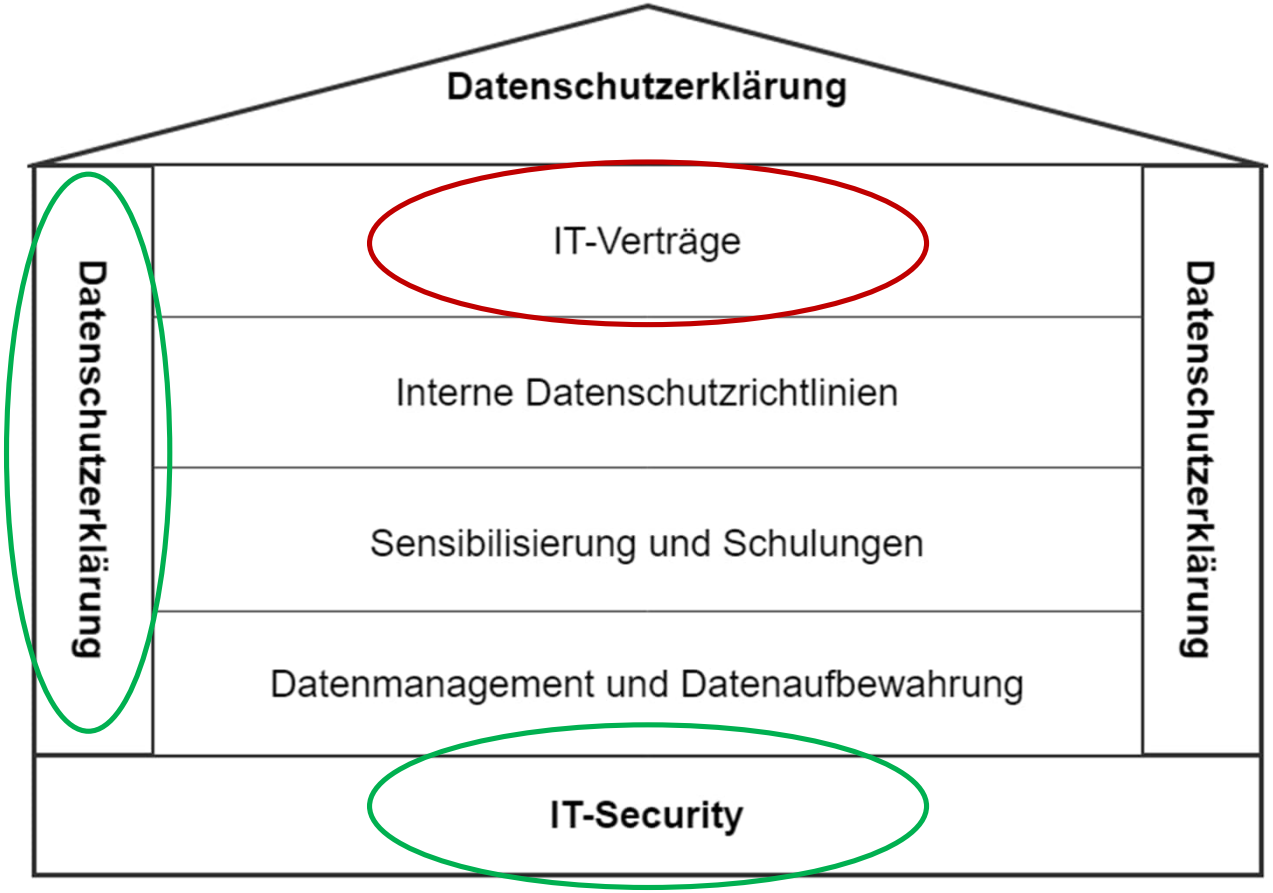
Cookie Banner

- Mit Cookies werden Personendaten bearbeitet (IP-Adresse)
- Unter der DSGVO braucht es einen sog. **Consent-Banner**
- Ein Consent-Banner holt Einwilligungen ein und setzt Cookies erst, wenn der Nutzer zugestimmt hat (vgl. Abb. rechts)
- Es gibt zahlreiche Dienste für Cookie-Banner (bspw. Cookie-Bot)
  - ➢ Für die Schweiz reicht ein **Cookie-Hinweis** in der Datenschutzerklärung aus





Datenschutz Haus



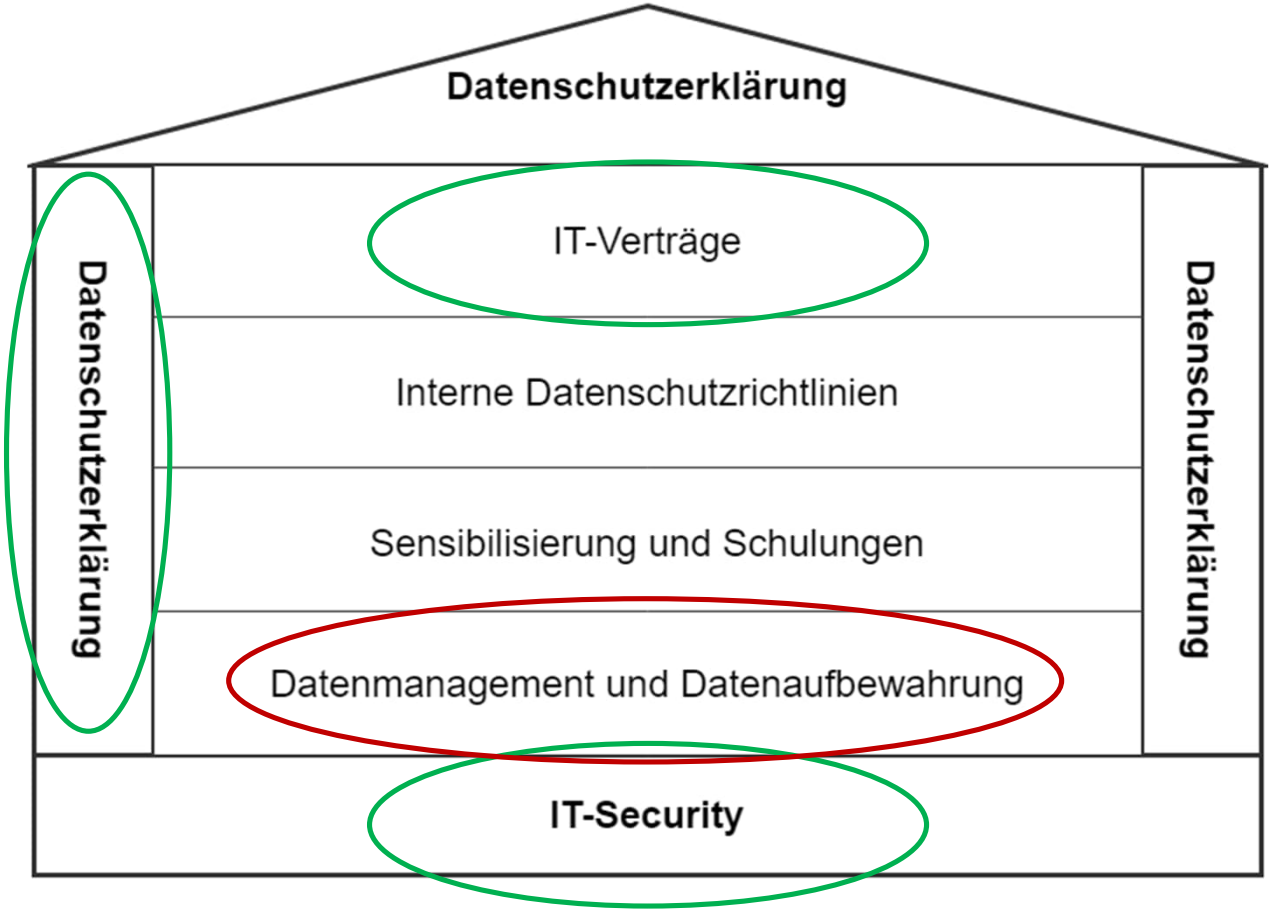
Beispiel: Auftragsdatenbearbeitung

Bei jeder **Auslagerung von Datenbearbeitungen** muss Folgendes beachtet werden:

- Auswahl: **notwendigen Sicherheitsstandards** durch Auftragsbearbeiter erfüllt (z.B. Zertifizierungen wie ISO 27001)?
- Wurde ein **Auftragsdatenbearbeitungsvertrag («ADV»)** abgeschlossen?
- Enthält der ADV einen **Anhang mit technischen und organisatorischen Massnahmen** des Auftragsbearbeiters?
- Kann Auftragsbearbeiter jederzeit **Datenverluste und Beschädigungen** feststellen und Sie umgehend informieren?
- Welche **Subunternehmer** zieht der Auftragsbearbeiter bei?
- Haben Sie die nötigen **Audit- oder Prüfrechte im ADV** vereinbart?

➢ **Machen Sie im Vertrag auf die Hilfspersonenstellung unter dem Berufsgeheimnis aufmerksam!**

Datenschutz Haus



Beispiel: Löschung und Berichtigung

- Personendaten werden **vernichtet oder anonymisiert**, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.
- Wer Personendaten bearbeitet, muss sich **über deren Richtigkeit vergewissern** und die Daten ggf. berichtigen.

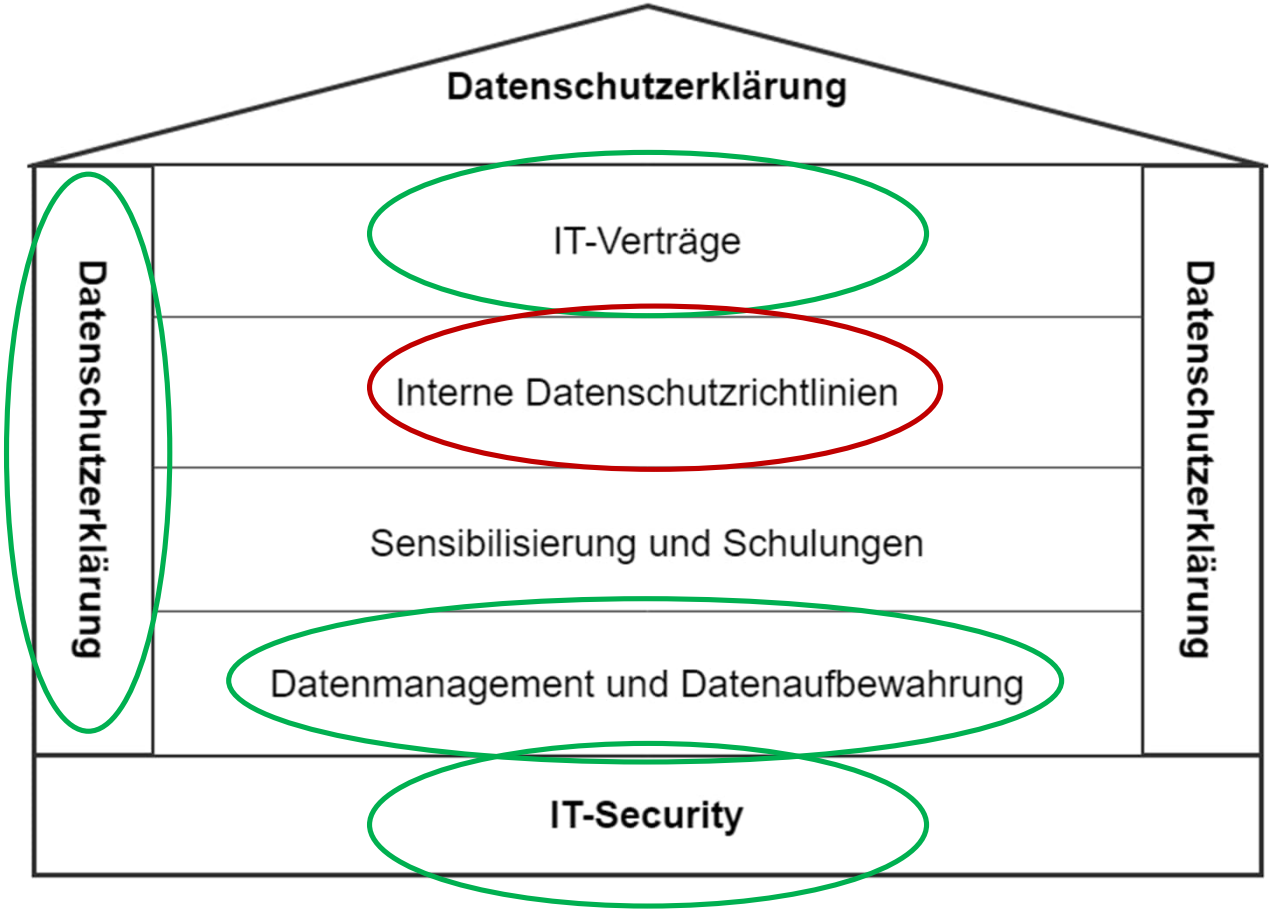
- Markieren Sie **unrichtige Daten** als **falsch** oder **sperren** Sie diese Daten für die weitere Bearbeitung.
- Begründen Sie analog zum Auskunftsrecht die **Verweigerung**, die **Einschränkung** oder den Aufschub der Berichtigungs- und Löschbegehren.
  - ➢ **ACHTUNG:** Ggf. benötigen Sie die «falschen» oder zu vernichtenden Daten zu Beweis-, Buchführungs- oder Rechnungslegungs-zwecken. In diesen Fällen ist die Aufbewahrung zulässig.

Beispiel: Datenschutz-Folgenabschätzung (DSFA)

- Instrument zur **Erkennung von Datenschutzrisiken** bei bestimmten Datenbearbeitungen, zu deren **Bewertung** und **Definition von Massnahmen**.
- Notwendig bei **hohem Risiko** für die Persönlichkeit oder die Grundrechte der betroffenen Personen
- Ein **hohes Risiko** liegt vor:
  - bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;
    - ➢ **Beispiel:** Zahnarztpraxis lagert Personendaten in eine Public Cloud aus
  - wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

➢ Ergibt sich auch aus der DSFA immer noch ein hohes Risiko und wurde kein Datenschutzberater ernannt, muss vor der Aufnahme der geplanten Datenbearbeitung die **Stellungnahme des EDÖB eingeholt** werden.

Datenschutz Haus

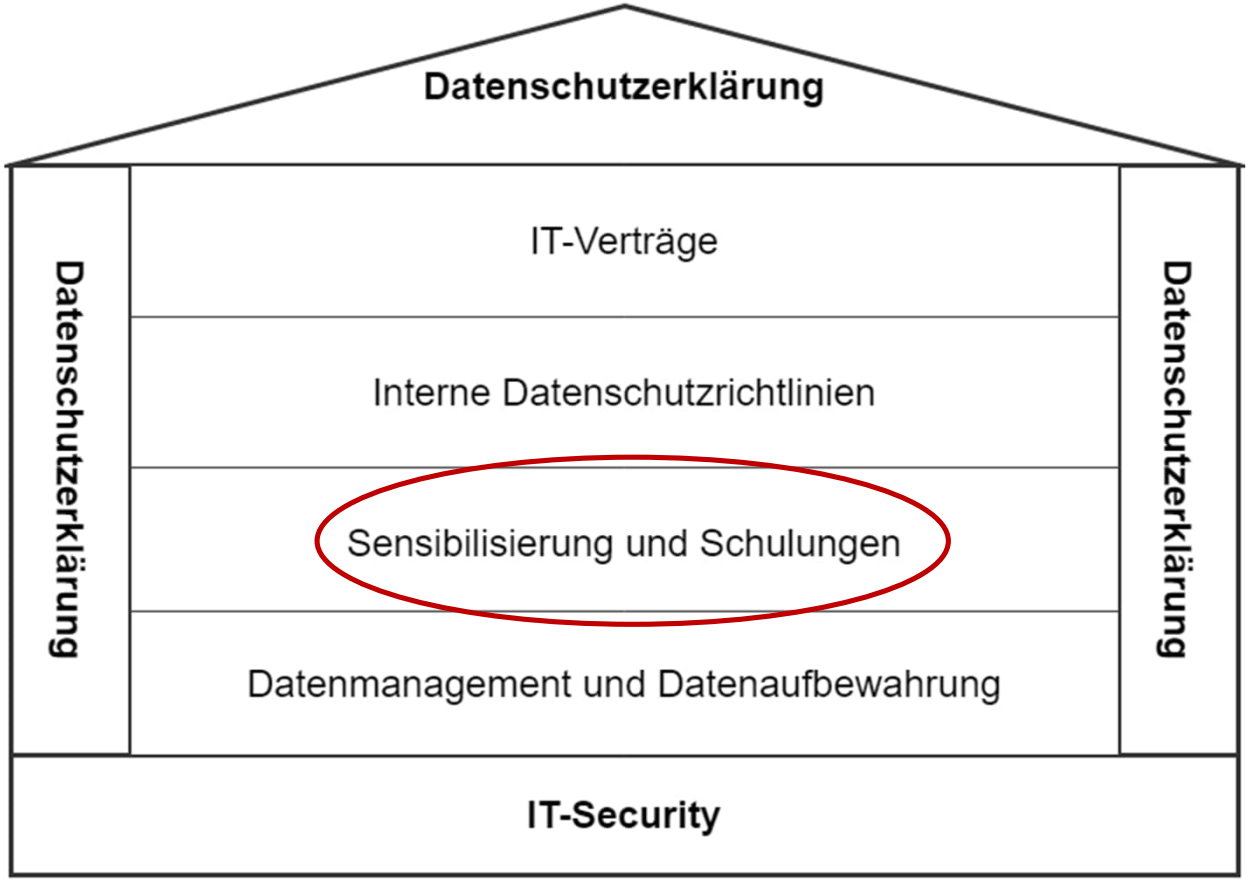


DOMENIG PARTNER
RECHTSANWÄLTE AG

Beispiel: Wie erteile ich Auskunft?

Antrag	Schriftlich, mündlich mit Einverständnis des Verantwortlichen
Zuverlässige Identifikation	heute i.d.R. mit ID-Kopie
Form der Auskunft	Standard: Schriftlich Mündlich oder Einsehen vor Ort nur mit Einverständnis der betroffenen Person
Frist	30 Tage, auch wenn Auskunft eingeschränkt, aufgeschoben oder verweigert wird. Falls nicht möglich, Mitteilung an Betroffene und Frist angeben.
Kosten	Grundsätzlich kostenlos. Bei unverhältnismässigem Aufwand max. CHF 300.00.
Verweigerung, Einschränkung, Aufschiebung	Berufsgeheimnis, überwiegende Interessen Dritter, Gesuch ist offensichtlich querulatorisch, Gesuch verfolgt datenschutzwidrigen Zweck (Prozessvorbereitung). Grund muss angegeben werden.

Datenschutz Haus



Schulungen und Awareness-Trainings

Awareness-Training Angebote finden Sie unter den nachfolgenden Links:

- Cyber security awareness training for your employees (sosafe-awareness.com)
- Phishing Security Test (knowbe4.de)
- Mitarbeiter testen | Lucy Security

Datenschutz-Schulungen werden idealerweise zugeschnitten auf Ihre Praxis durchgeführt.

- Entweder Eigenregie oder Beizug eines Experten/einer Expertin
- Hilfestellung: Das neue Datenschutzgesetz: Was ist zu tun? - YouTube

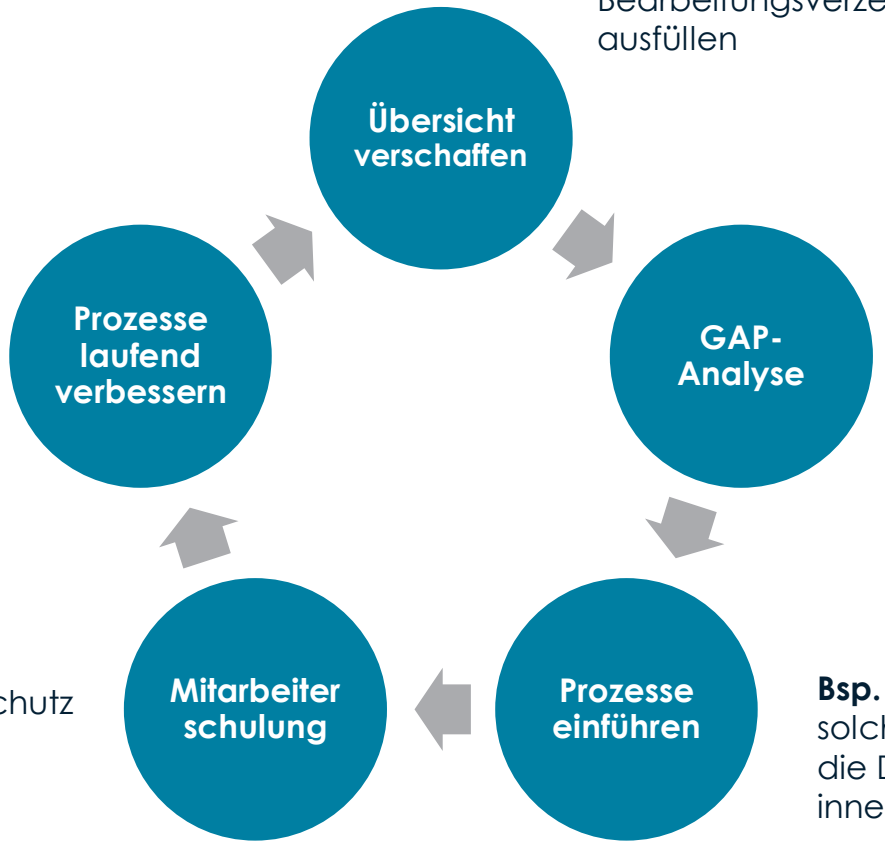
Do's and Dont's im Praxisalltag

DOMENIG PARTNER RECHTSANWÄLTE AG

- **Bei der Bekanntgabe von Patientendaten an Dritte müssen Sie prüfen, ob Sie eine ausdrückliche Einwilligung benötigen.**
- **Geben Sie Ihren Mitarbeitenden klare Anweisungen: wann dürfen welche Patientendaten wie und an welche Empfänger gesendet werden?**
- **Nutzen Sie sichere Kommunikationsmittel. Sofern Patientendaten per Mail versendet werden, sollten Sie die Mails verschlüsseln.**
- **Vermeiden Sie telefonische Auskünfte über Mitarbeitende und Patienten und beantworten Sie Betroffenengesuche stets schriftlich** (und nach Abstimmung mit einer Datenschutzexpertin).
- **Vermeiden Sie IT-Systeme, welche die Daten an unsichere Drittländer auslagern bzw. Wartungs- und Supportzugriffe von dort aus zulassen.**
- **Erstellen Sie bei Cloud- und ähnlich risikoreichen Vorhaben eine Datenschutz-Folgenabschätzung.**
- **Sammeln Sie nur so viele Patientendaten, wie nötig, um Ihren Auftrag zu erbringen.**
- **Überprüfen Sie stichprobenmässig, ob sich das Personal an die Vorgaben hält und führen Sie regelmässig Phishing-Kampagnen durch.**

III. Key Takeaways

Bearbeitungsverzeichnis ausfüllen



- Welche Prozesse bestehen bereits?
- Wo muss ein Prozess eingeführt oder verbessert werden?

Bsp. Betroffenengesuche: Wer ist für solche Gesuche zuständig? Wer sucht wo die Daten zusammen und verschickt sie innert welcher Frist?

Sensibilisierung für Datenschutz wird damit gestärkt

Bsp. aufgrund von neuer Rechtsprechung oder eines Audits muss ein Prozess angepasst werden

Key Takeaways

DOMENIG PARTNER RECHTSANWÄLTE AG

- Berücksichtigen Sie Datenschutz und –Sicherheit bereits bei der Einführung neuer Systeme und Prozesse
- Datenschutz und –Sicherheit müssen regelmässig im Rahmen des Risikomanagements behandelt werden
- Weisen Sie den beiden Themen genügend Ressourcen zu
- Sensibilisieren Sie Ihre Mitarbeitenden
- Nach einem Datenschutzvorfall ist vor dem Vorfall – verbessern Sie Ihre Prozesse laufend

DOMENIG PARTNER
RECHTSANWÄLTE AG

DOMENIG & PARTNER

Kontakt

Domenig & Partner
Rechtsanwälte AG
Laupenstrasse 1
CH-3008 Bern

Tel: +41 31 380 11 00
info@domenig.law