





Schutz von Gästedaten leicht gemacht

Praktische Grundlagen für Tourismusprofis



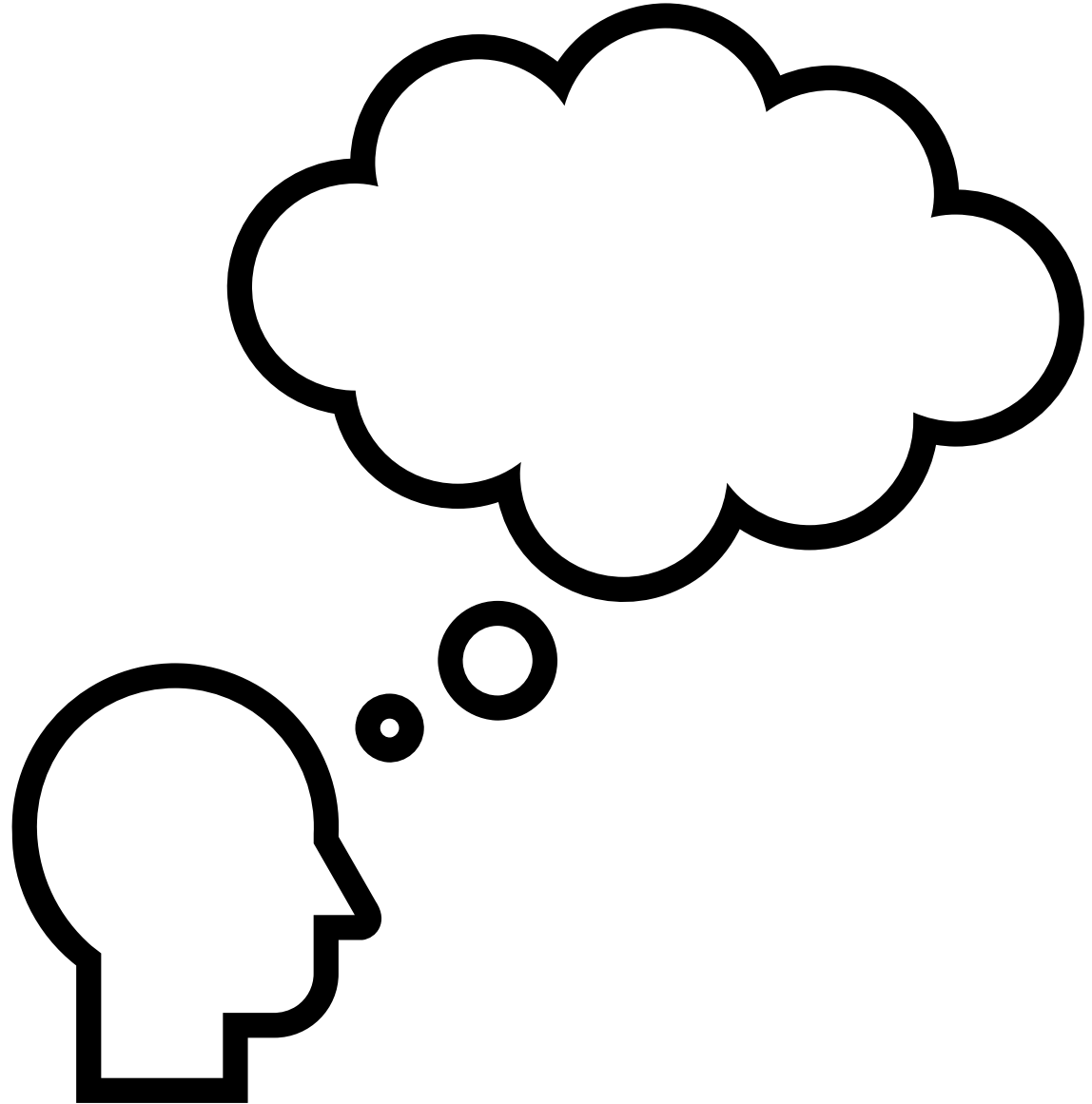
Alexander Stübi
MLaw, CIPP/E



Biel, Schweiz

12.05.2025

**Was
interessiert
euch am
allermeisten?**



Inhaltsverzeichnis

Warum ist Datenschutz wichtig?

Was ist Datenschutz?

Wofür gilt das Datenschutzgesetz?

Was sind Personendaten? Wer ist betroffene Person?

Was bedeutet „bearbeiten“?

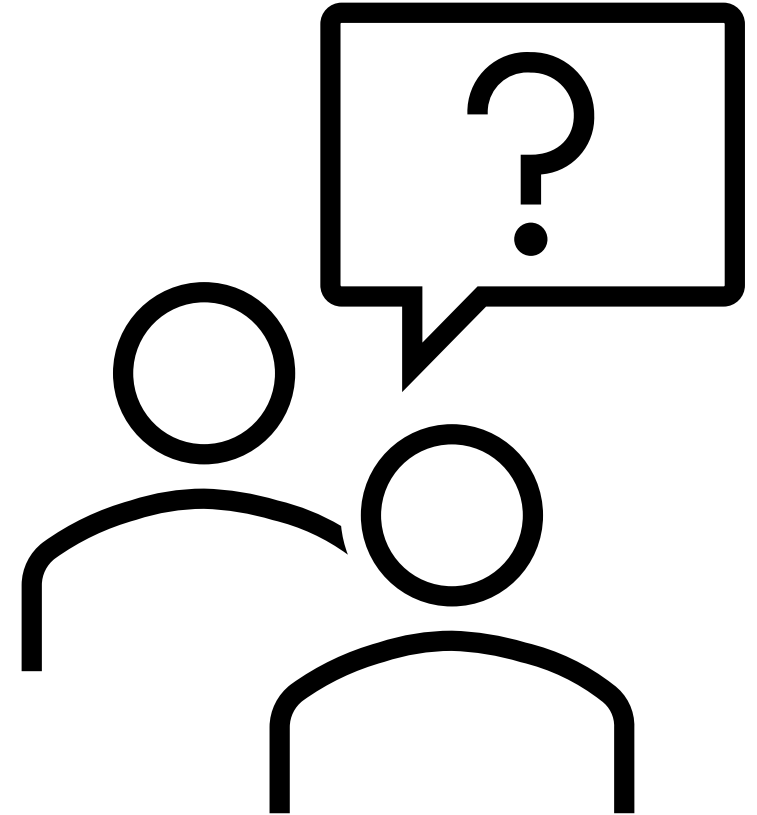
Was gibt es für Rollen?

Ist die Bearbeitung von Personendaten erlaubt?

Fallbeispiele

Warum ist Datenschutz wichtig?

- Reputation
- Betrieb aufrecht erhalten
- Haftungsrisiken minimieren
- Rechtssicherheit



Was ist Datenschutz?

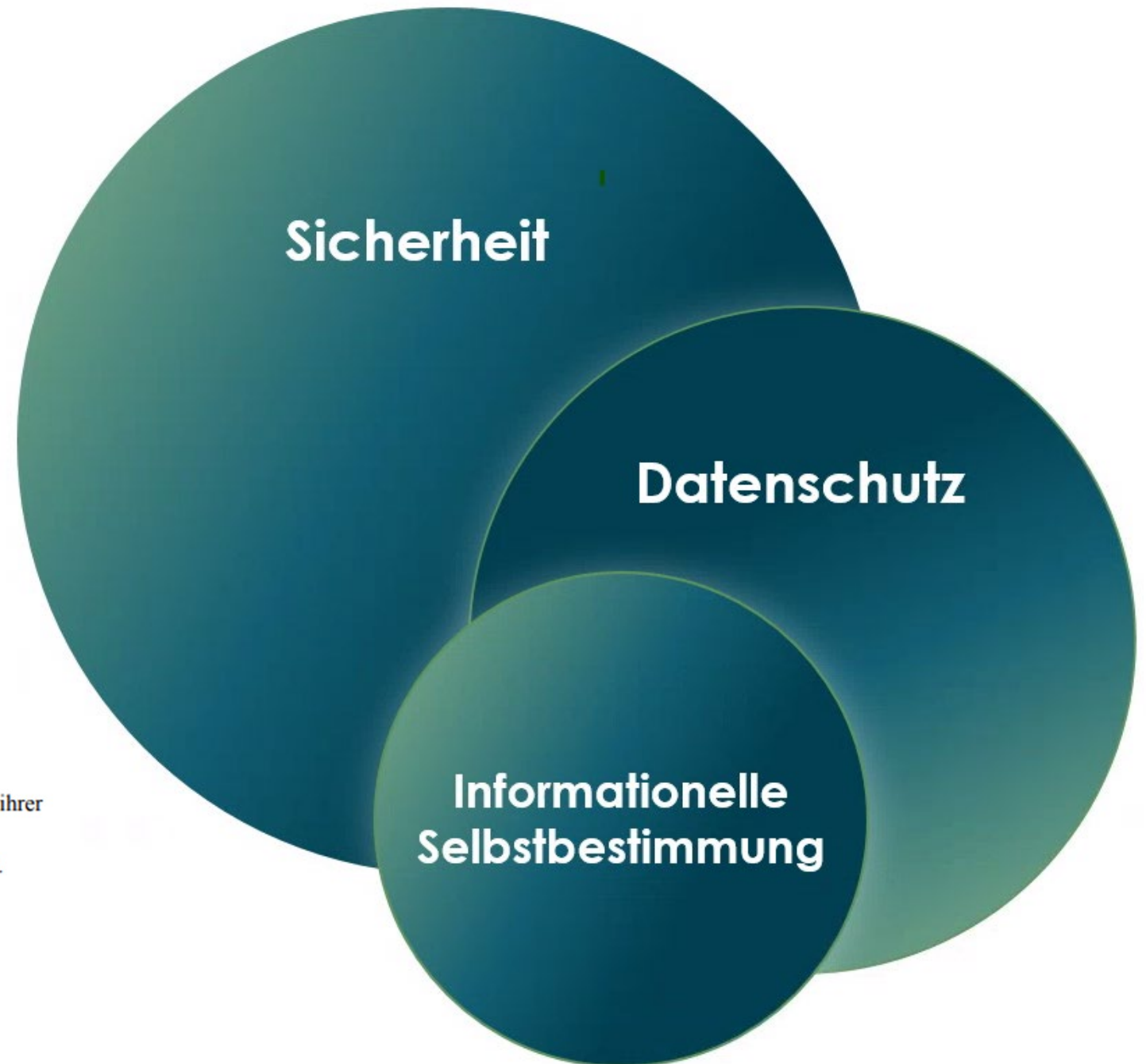
Datenschutz ist die Verwirklichung des Grundrechts auf informationelle Selbstbestimmung.

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.



Wofür gilt das Datenschutzgesetz?

Was ist betroffen?

- Bearbeitung von Personendaten natürlicher Personen (kein Unternehmensschutz mehr)

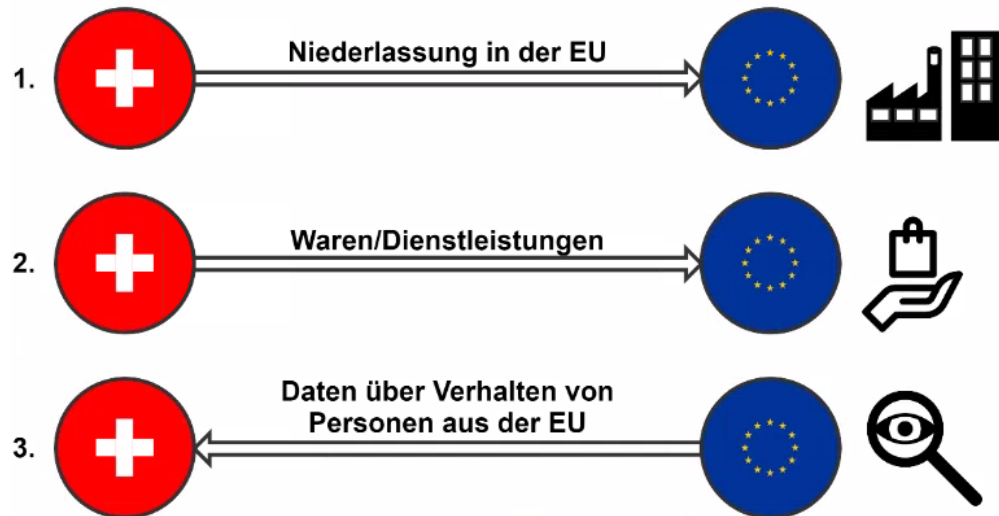
Wer muss sich daran halten?

- Private (natürliche und juristische Personen) und
- Behörden

Anwendbares Recht

Grundsätzlich gilt das DSG in der Schweiz

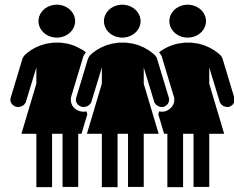
Die DSGVO gilt grundsätzlich nur in der **EU und in EFTA-Staaten** (ausser der Schweiz), kann aber unter Umständen «extraterritoriale Wirkung» entfalten. Dabei sind folgende drei Konstellationen relevant:



Einige Konsequenzen bei DSGVO-Anwendbarkeit

- Einwilligungsmanagement („Cookie-Banner“)
- Rechtsgrundlage
- Datenschutzerklärung
- Betroffenenrechte

Personendaten & betroffene Personen (1/2)



Personendaten:

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

Betroffene Person:

- natürliche Person, über die Personendaten bearbeitet werden

Personendaten & betroffene Personen (2/2)

Personenstammdaten, Kontaktdaten, Finanzdaten

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



Profiling

Auswertungen über persönliche
Interessen, Vorlieben, Leistung



Massnahmen und Sanktionen

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



Aussehen, Identität, Körper und Gesundheit

Ethnie, Gesundheitsdaten,
Intimsphäre, genetische und
biometrische Daten



Weltanschauung

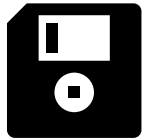
Politische und gewerkschaftliche
Tätigkeit und Überzeugung,
Religion



Bewegungsdaten

Überwachung, Standort,
Tracking (physisch oder online)

Was bedeutet „bearbeiten“?

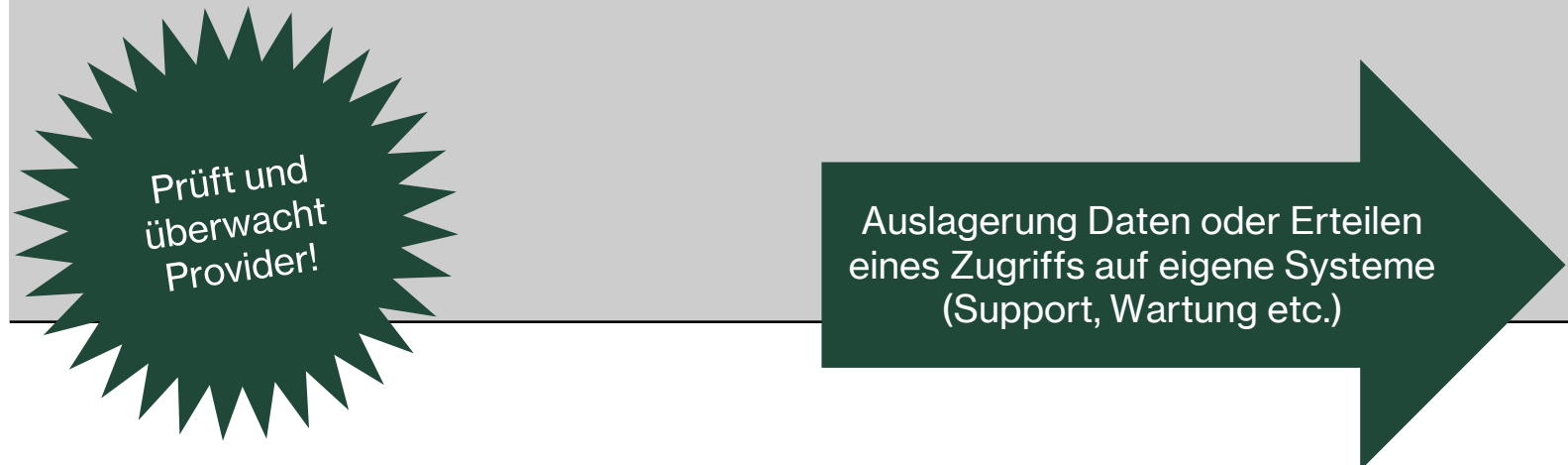


Bearbeiten:

- jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren
- Beispiele: Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten

Was gibt es für Rollen?

Verantwortliche (Sie)	Auftragsdatenbearbeiter (IT-Provider etc.)
<ul style="list-style-type: none">• Entscheidet über die Zwecke und Mittel der Bearbeitung• Tragt Hauptverantwortung und Konsequenzen für Datenbearbeitung	<ul style="list-style-type: none">• Darf keine eigenen Zwecke verfolgen• Hauptpflicht ist die Datensicherheit• Auftragsdatenbearbeitungsvertrag (ADV)



The diagram illustrates the relationship between the responsible party and the service provider. A green starburst on the left contains the text 'Prüft und überwacht Provider!'. A large green arrow points from this starburst to a green box on the right, which contains the text 'Auslagerung Daten oder Erteilen eines Zugriffs auf eigene Systeme (Support, Wartung etc.)'.

Bearbeitung von Personendaten erlaubt? (1/2)

Grundsatz

- Datenbearbeitung ist erlaubt

Aber

- **Bearbeitungsgrundsätze** müssen eingehalten werden
- Wird einer dieser Grundsätze verletzt, liegt eine Persönlichkeitsverletzung vor und es benötigt ein **Rechtfertigungsgrund** für die Datenbearbeitung

Kunden in der EU:

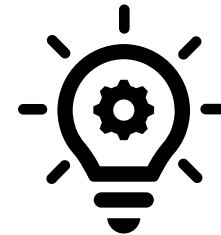
- Datenbearbeitungen ohne Erlaubnistatbestand (entsprechen ungefähr den Rechtfertigungsgründen in der Schweiz) sind grundsätzlich verboten



Verhältnismässigkeit



Zweckbindung



Transparenz

Bearbeitung von Personendaten erlaubt? (2/2)

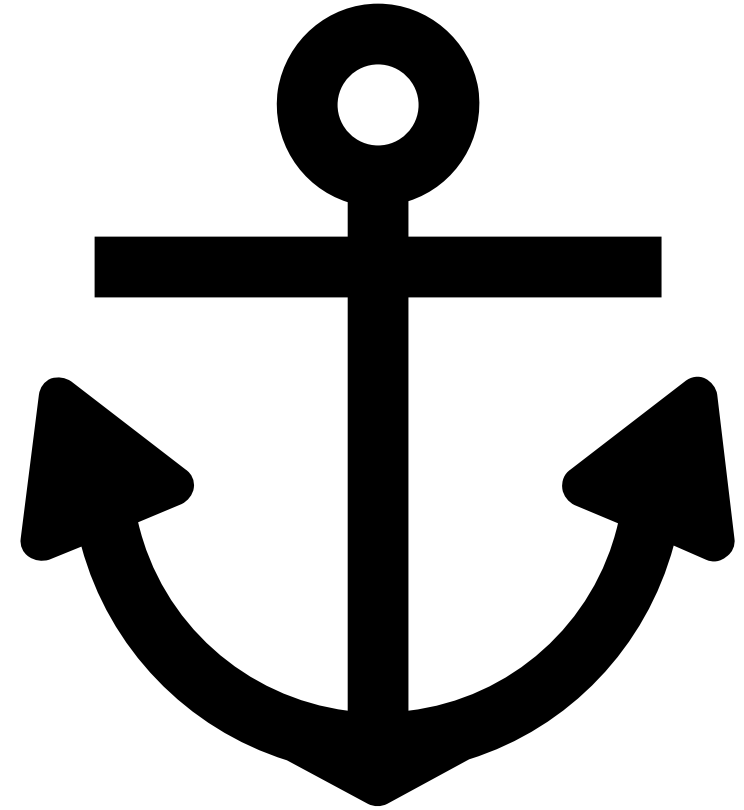
Wird einer der vorhin erwähnten Bearbeitungsgrundsätze verletzt, liegt eine **Persönlichkeitsverletzung** vor, ausser es gibt **Rechtfertigungsgründe!**

Rechtfertigungsgründe:

- Einwilligung
- Überwiegende Interessen
- Gesetzliche Grundlage

Kunden aus EU:

- Liegt kein Erlaubnistatbestand vor, ist die Datenbearbeitung unzulässig.
- Erlaubnistatbestände sind mit Rechtfertigungsgründen ungefähr deckungsgleich



Prozess: Umgang mit Betroffenenrechten (1)

Welche Betroffenenrechte gibt es?

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

Was soll ich dann tun?

1. Prüfung der Gültigkeit und Protokollierung
2. Nachverlangen von Informationen
3. Empfangsbestätigung
4. Evtl. Fristverlängerung und Gebühren
5. Anfrage bearbeiten und Rechte Dritter wahren
6. Kontaktierung der Betroffenen



Prozess: Umgang mit Data Breaches (2)

Was ist ein Data Breach?

Verletzung von:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- (Nachvollziehbarkeit)

Was soll ich dann tun?

1. Sofortmassnahmen ergreifen
2. Fakten zusammentragen
3. Beurteilung, ob und was für ein Data Breach vorliegt
4. Risikoanalyse durchführen
5. Evtl. Meldung an Behörde(-n)
6. Evtl. Meldung an Betroffene
7. Protokollierung



Häufige Beispiele von Data Breaches

- E-Mail an falschen Empfänger senden
- E-Mail mit falschem Anhang versenden
- Diebstahl/Verlust von elektronischen Geräten mit unverschlüsselten Personendaten darauf
- Kein Zugriff auf Datensätze mit Personendaten wegen Server-Ausfall
- Hackerangriff mit Entwendung von Personendaten und/oder Ransomware- Angriff
- Erfolgreiche Phishing-Angriffe / Deep Fakes

Nützliche Tipps für mehr Datensicherheit

- Clean Desk
- Vorsicht bei Remote Work
- MFA
- Passwortmanager
- Bewusstsein für Phishing/Social-Engineering/DeepFakes
- Berechtigungskonzept
- Regelmässige Updates



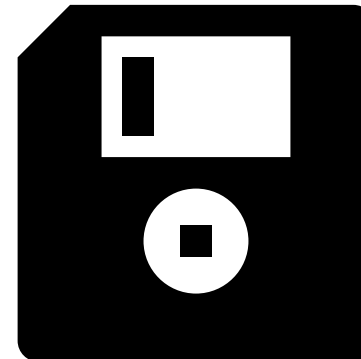
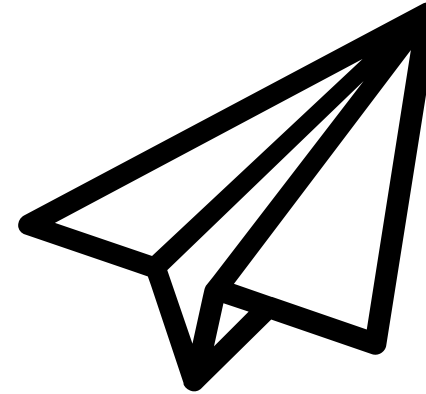
Versand & Speicherung von Daten

Versand:

- «Normale» Personendaten
- Besonders schützenswerte Personendaten verschlüsselt versenden
- Vorsicht bei Auslandübermittlung (Achtung Tools)

Speicherung:

- Datensparsamkeit: So viel wie nötig, so wenig wie möglich
- Faustregel: Anbahnung und Durchführung des Vertrags
- Bewerbungsunterlagen
- Private Speicherung von „geschäftlichen“ Personendaten vermeiden



Umgang mit KI-Tools (z.B. Chat GPT / deepl)

Einhaltung der Rechtsordnung:

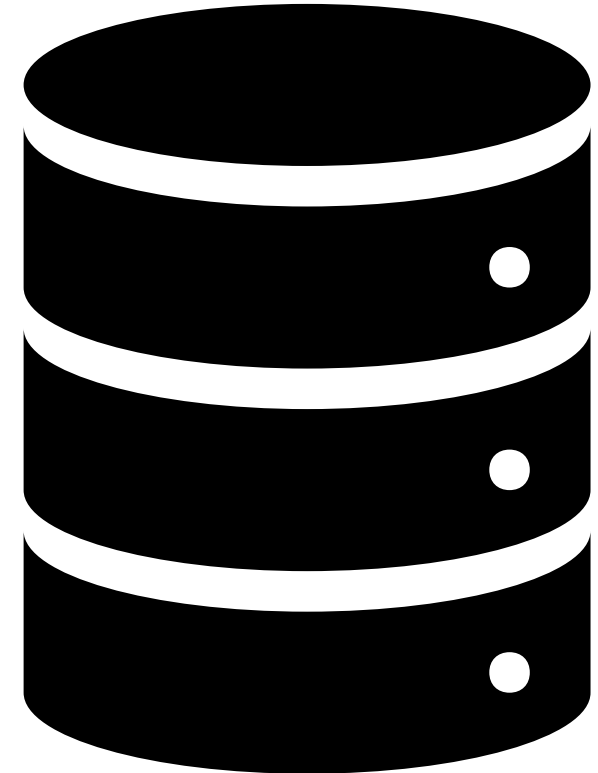
- Verträge mit den Anbietern prüfen auf u.a. Datenschutz, Geheimhaltung, Urheberrecht

Gratisversionen vs. Bezahl-Versionen

- Verträge mit den Anbietern prüfen auf u.a. Datenschutz, Geheimhaltung, Urheberrecht
- **Gratisversionen:** Keine Personendaten, Kundendaten und Geschäftsgeheimnisse eingeben
- **Bezahlversionen:** Verwendung OK, sofern die Anbieterverträge geprüft wurden.

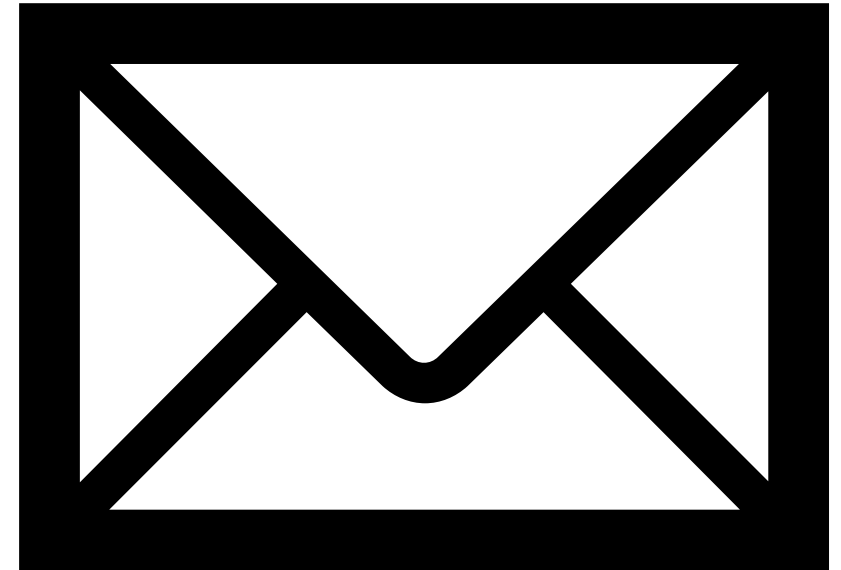
Output stets auf Richtigkeit überprüfen

•



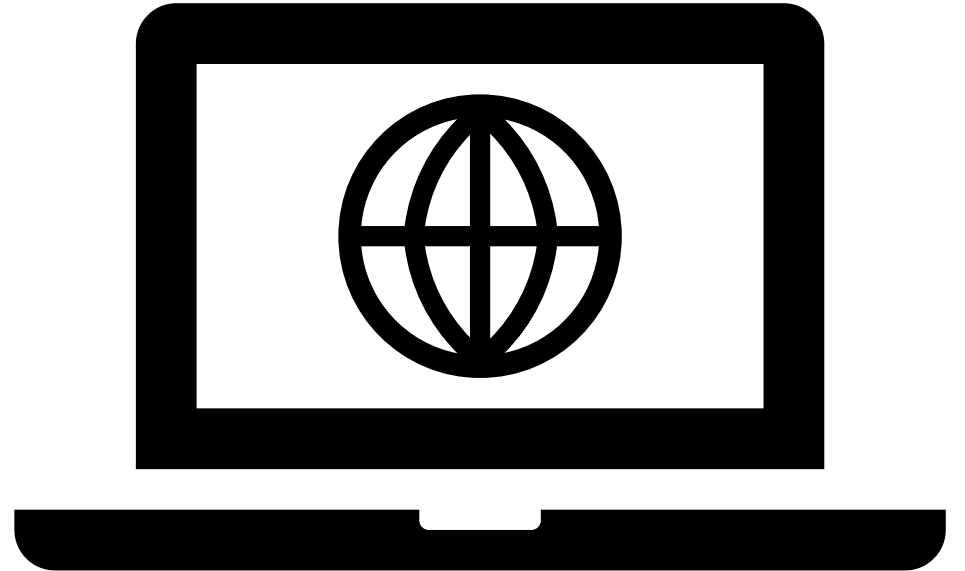
Newsletter

- UWG und DSG
- Einwilligung und Opt-In: Aktive, informierte Zustimmung erforderlich (z.B. Ankreuzen eines Kästchens), AGB genügt nicht.
- Jederzeitige einfache und kostenfreie Abmeldemöglichkeit (Opt-out) inkl. klarer Hinweis in jeder E-Mail
- Ausnahme: Bei bestehenden Geschäftsbeziehungen: Werbung ohne erneute Einwilligung möglich, wenn Bezug auf ähnliche Produkte, aber einfache Abmeldemöglichkeit bleibt Pflicht
- Transparenz und Informationspflichten (DSG)



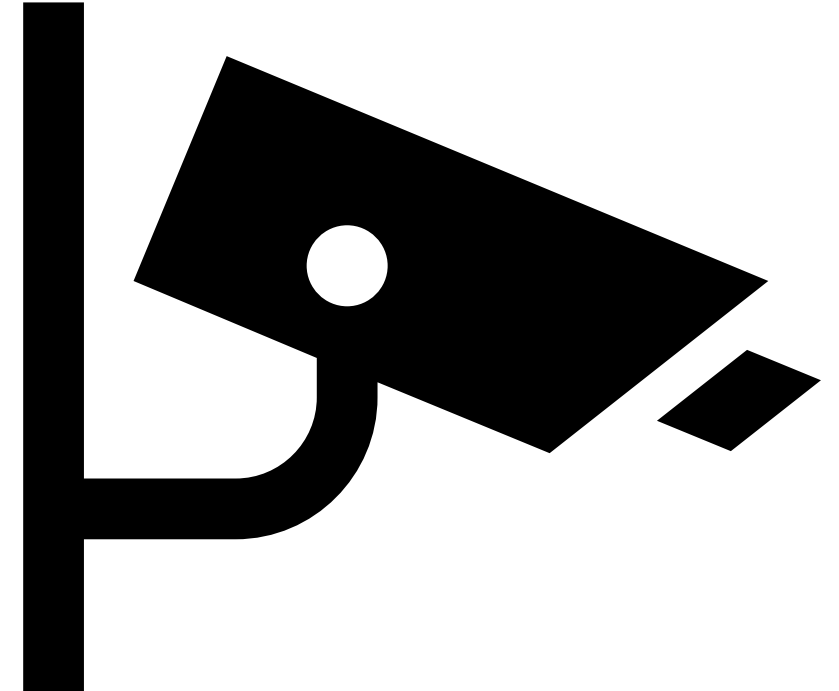
Beispiel: (Rechtstexte auf) Website

- Impressum
- Datenschutzerklärung
- AGB
- Cookies?



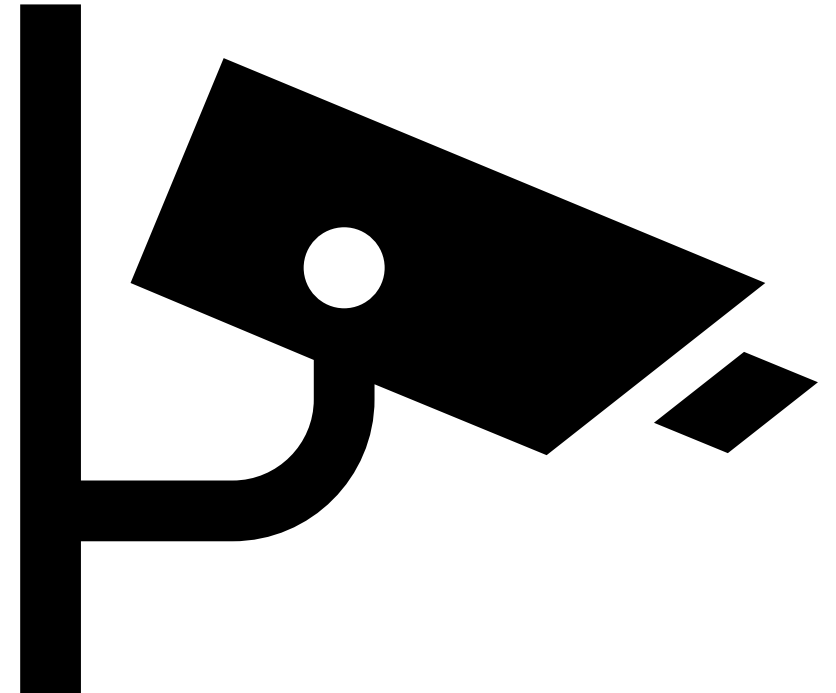
Beispiel: Videoüberwachung generell (1/2)

- Videoaufnahmen, auf denen Personen sind, gelten als Personendaten
- Eingriff in Persönlichkeitsrechte -> Rechtfertigungsgrund nötig
- Informationspflicht -> Piktogramm & QR Code
- Kein öffentlicher Raum



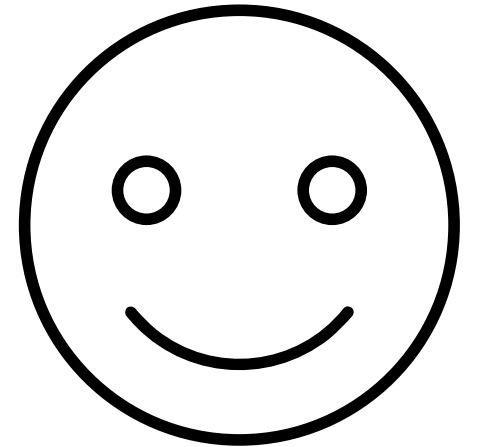
Beispiel: Videoüberwachung am Arbeitsplatz (2/2)

- Fürsorgepflicht des Arbeitgebers
- Keine umfassende Überwachung
- Keine Systeme, die primär der Verhaltenskontrolle dienen
- Informationspflicht



Beispiel: Biometrische Zutrittssysteme

- Besonders schützenswerte Daten (z.B. Gesichtserkennung / Fingerabdrücke)
- Informationspflicht
- Datenschutzfolgeabschätzung (Art. 22 DSGVO)



Beispiel: Buchungen



Anmeldungen an
Events



Buchung von
Zimmern (Hotel /
B&B)



Bestellungen

Beispiel: Gäste-WLAN



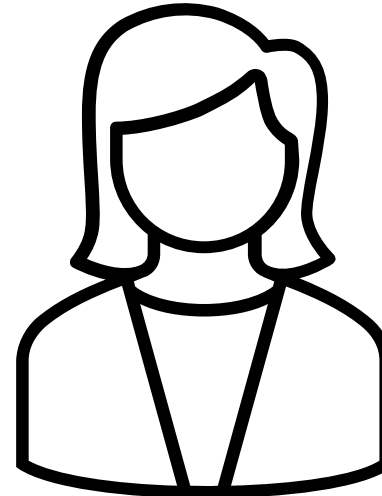
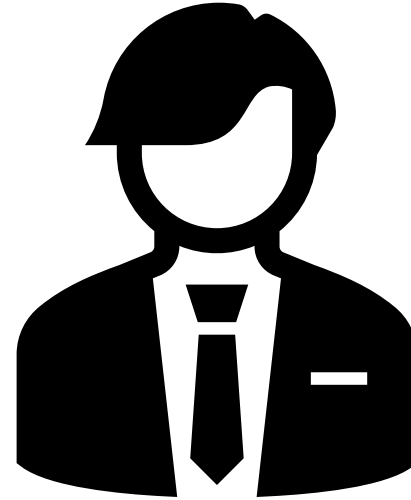
Passwort setzen



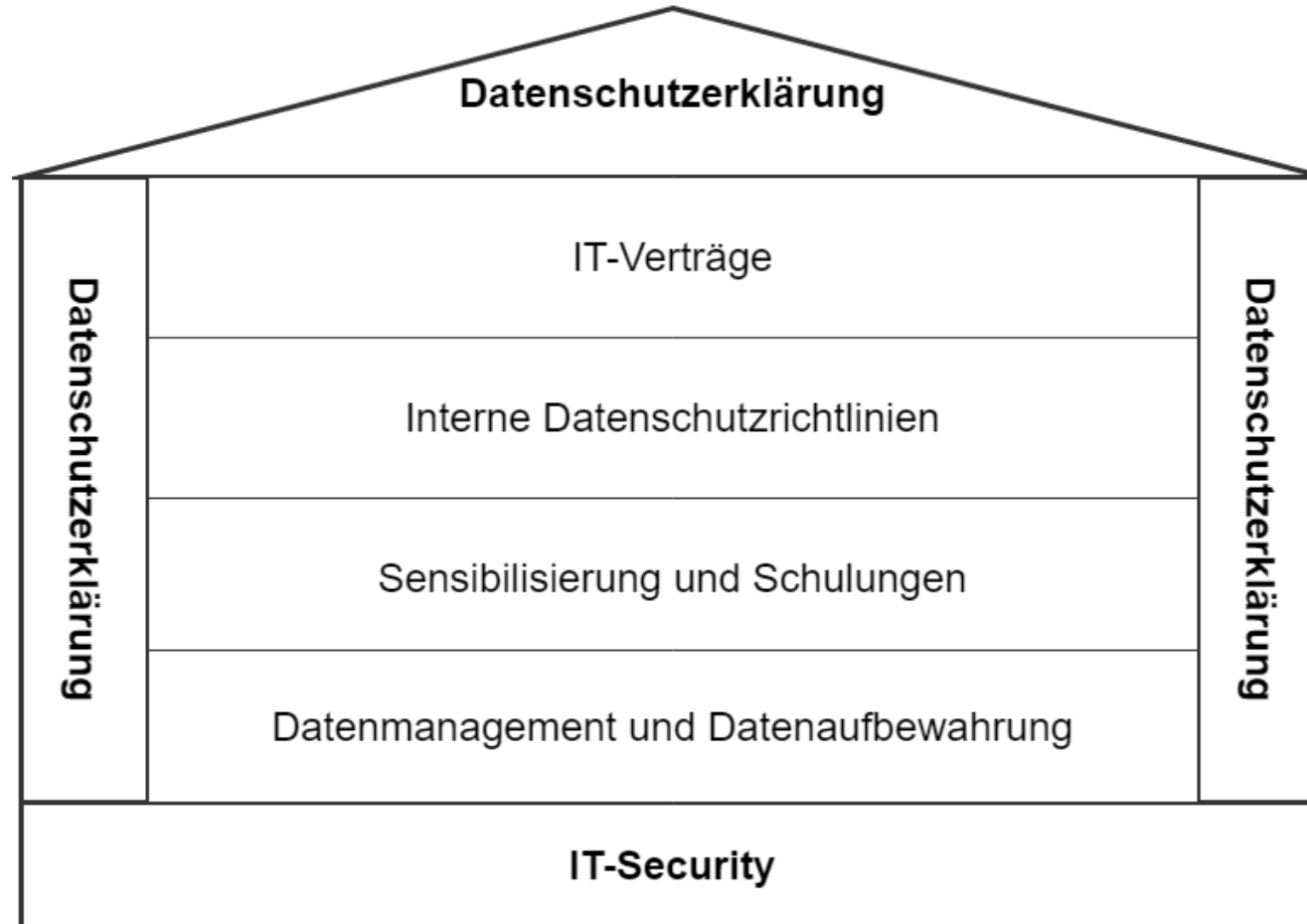
Sicheres Passwort

Beispiel: Mitarbeiterfotos

- Recht am eigenen Bild
- Einwilligung notwendig
- Jederzeitiger Widerruf möglich



Wie anfangen?



DOMENIG & PARTNER

Kontakt

Domenig & Partner
Rechtsanwälte AG
Laupenstrasse 1
CH-3008 Bern

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

