Webinar
Datenschutz aus KMU-Sicht

20. September 2023, 10.30-12:00

factum advocatur

lic.iur.HSG Urs Freytag
Teufenerstrasse 3, 9000 St. Gallen
Telefon: 071 421 41 41
Mail: freytag@factum.pro

SWISS MEDTECH

Inhalt des Webinars

1. Theoretischer Teil

1. Definition Datenschutz
2. Rechtsgrundlagen
3. Verhältnis DSG / DSGVO
4. Grundsätze des Datenschutzes
5. Rechtfertigungsgründe
6. Rechte der Privatpersonen / Pflichten der Datenbearbeiter
7. Profiling
8. Sanktionen
9. Neuerungen im DSG

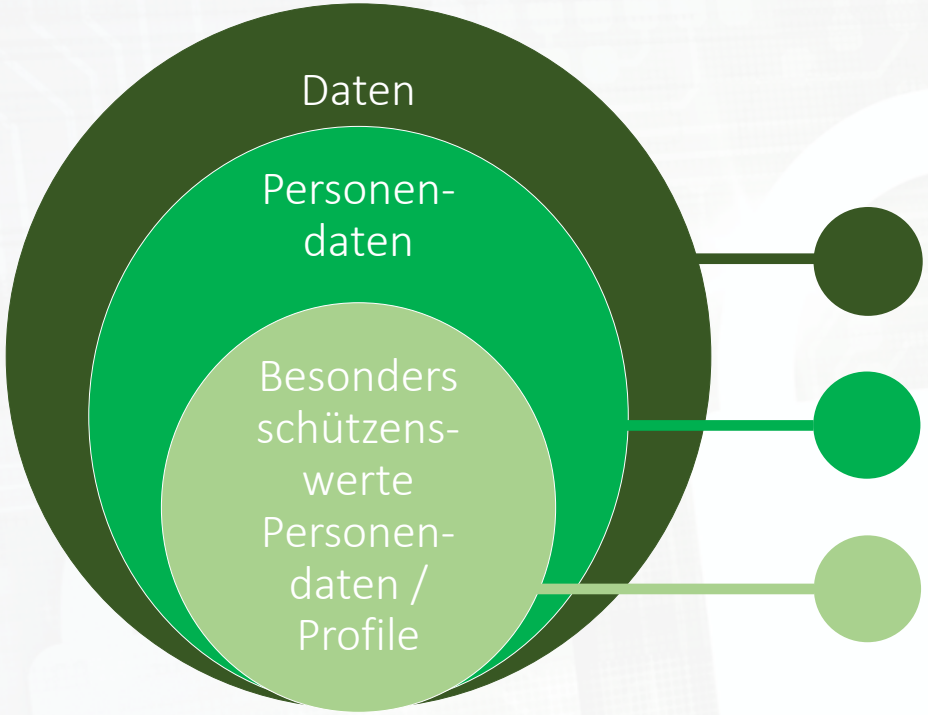
2. Praktische Umsetzung

10. Datenschutzerklärung
11. Verzeichnis der Bearbeitungstätigkeiten
12. Auftragsverarbeiter
13. Datenschutzberater / -beauftragter
14. Datenschutz im Arbeitsrecht
15. Praktische Umsetzung Website

3. Fragen und Antworten

Fragen bitte richten an: **freytag@factum.pro**

1. Definition Datenschutz - Sphären



Alle Daten, auch nicht personenbezogene (z.B. Wetterdaten, Börsenkurse, etc.)

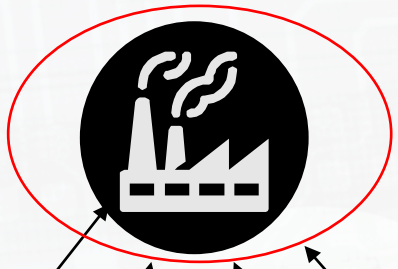
Daten, die sich auf einen **bestimmte** oder **bestimmbare** Person beziehen (z.B. Name, Adresse, Zivilstand, Telefonnummer, Geschlecht, IP-Nummer, etc.)

Daten über Gesundheit, Religion, Intimsphäre, politische Anschauungen, biometrische Daten

Ziel das Datenschutzes: Schutz der *Privatshpäre* natürlicher Personen gegen Persönlichkeits-verletzungen (und nicht etwa der “Schutz der Daten”)

1. Definition Datenschutz - Rollenverteilung

Verantwortlicher Datenbearbeiter
Organisation/Staat; entscheidet über Zweck und Mittel

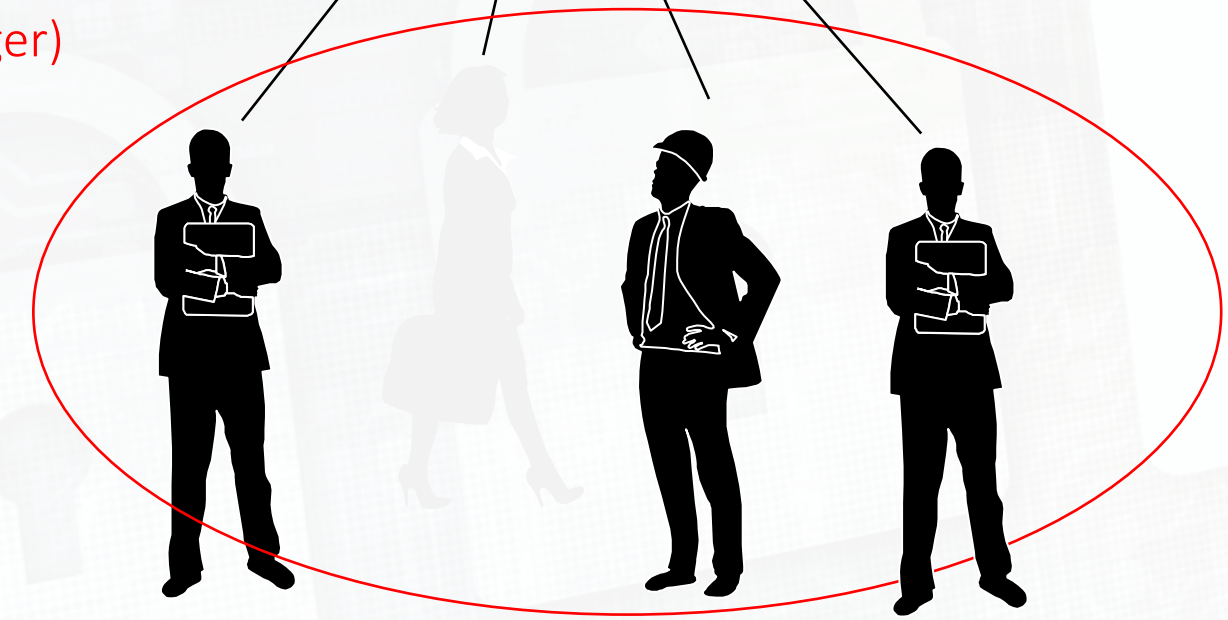


speichert Daten

Auftragsbearbeiter (z.B. IT-Firma, Cloud-Anbieter, Treuhänder, Marketing-Unternehmen, Hersteller von Medtech-Geräten)

Auftragsdatenbearbeiter-vertrag notwendig

Datensubjekte („Personen“, z.B. Kunden, Arbeitnehmer, Bürger)



Microsoft

z.B. Microsoft 365

2. Rechtsgrundlagen im Datenschutz

Schweiz:

- Datenschutzgesetz bzw. –verordnung (DSG / VDSG)
- Kantonale Datenschutzgesetze

  Datenbearbeitung von Personendaten durch Kantone und Gemeinden

- Datenschutzbestimmungen in anderen Gesetzen (z.B. Art. 328b OR – Arbeitsvertrag)

EU:

- Datenschutzgrundverordnung (DSGVO), in Kraft seit 25.5.2018
- Nationale Datenschutzgesetze

Rest der Welt:

- Nationale Datenschutzgesetze

3. Verhältnis DSG / DSGVO

Wann ist DSGVO in der Schweiz anwendbar?

Kriterien
- Niederlassungsprinzip
- Marktortprinzip

(Art. 3 DSGVO)

Aber: CH-DSG ist gleichermassen auch im EU-Raum anwendbar, wenn sich Datenbearbeitungen aus der EU in der Schweiz auswirken.

Schweizer Unternehmen:	Anwendbares Recht	
	CH DSG	EU DS-GVO
Hat Niederlassung in der EU	●	●
Bietet nur Leistungen in der Schweiz an	●	
Bietet Leistungen im EU-Raum an	●	●
Bearbeiten von Schweizer Personendaten	●	
Bearbeiten von Personen-daten von Betroffenen, die sich in der EU befinden	●	●

3. Verhältnis DSG / DSGVO

DSG (Schweiz)

«Erlaubnis mit Verbotsvorbehalt»

Datenbearbeitungen sind erlaubt, wenn datenschutzrechtliche Grundsätze (Folie 8) eingehalten sind und das Gesetz eine Datenbearbeitung nicht verbietet

DSGVO (EU)

«Verbot mit Erlaubnisvorbehalt»

Datenbearbeitungen sind verboten, wenn sie das Gesetz nicht erlaubt, d.h. es muss einer von sechs Rechtfertigungsgründen vorliegen (Folie 10)

Beweislastumkehr:

- Schweiz (DSG): Wer Datenschutzverletzung geltend macht, muss diese nachweisen
- DSGVO: Verantwortliche muss Rechtmässigkeit der Datenbearbeitung nachweisen

4. Grundsätze des Datenschutzes (Art. 6 – 8 DSG)

1. **Rechtmässigkeit** (Art. 6 Ziff. 1)
2. **Verhältnismässigkeit / Treu und Glauben** und (Art. 6 Ziff. 2)
3. **Zweckgebundenheit** (Art. 6 Ziff. 3)
4. **Datensparsamkeit** (Vernichtung oder Anonymisierung, wenn für Zweck nicht mehr erforderlich) Art. 6 Ziff. 4
5. **Richtigkeit** der Daten sicherstellen (Art. 6 Ziff. 5)
6. Falls **Einwilligung** erforderlich, muss diese nach angemessener Information **freiwillig** erfolgen Art. 6 Ziff. 6
7. **Ausdrückliche** Einwilligung bei besonders schützenswerten Personendaten bzw. Profiling mit hohem Risiko (Art. 6 Ziff. 3)
8. **Datenschutz durch Technik** („*privacy by design*“) (Art. 7)
9. **Datenschutz durch datenschutzfreundliche Voreinstellungen** („*privacy by default*“) (Art. 7)
10. **Datensicherheit** (Art. 8)

! Grundsätze sind einzuhalten. Missachtung kann Persönlichkeitsverletzung darstellen (Art. 30 Abs. 2 DSG)

5. Rechtfertigung der Datenbearbeitung (Rechtmässigkeit)

5. Kapitel:
Besondere Bestimmungen zur Datenbearbeitung durch private Personen

Art. 30 Persönlichkeitsverletzungen

[1] Wer Personendaten bearbeitet, darf die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen.

[2] Eine Persönlichkeitsverletzung liegt insbesondere vor, wenn:

a. Personendaten entgegen den Grundsätzen nach den Artikeln 6 und 8 bearbeitet werden;

b. Personendaten entgegen der ausdrücklichen Willenserklärung der betroffenen Person bearbeitet werden;

c. Dritten besonders schützenswerte Personendaten bekanntgegeben werden.

[3] In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Personendaten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

5. Rechtfertigung der Datenbearbeitung (Rechtmässigkeit)

Art. 31 DSG / Art. 6 DSGVO

Rechtfertigungsgründe	Beispiel
1. **Einwilligung** der betroffenen Person	E-Mail-Newsletter
2. **Überwiegendes privates Interesse**	Direktmarketing, Kreditwürdigkeitsprüfung, sowie andere, nicht personenbezogene Zwecke (wie z.B. Forschung)
3. **Überwiegendes öffentliches Interesse**	v.a. staatliche Aufgaben (z.B. Einwohnerverzeichnis/Steuerdaten)
4. **Gesetzliche** Verpflichtung	Aufbewahrungspflicht von Akten (10 Jahre)
5. **Vertragserfüllung** (nur DSGVO)	Offertstellung/ Lieferung / Service
6. **Lebenswichtige Interessen** (nur DSGVO)	Notfallmässige medizinische Behandlung

5. Rechtfertigung der Datenbearbeitung (Rechtmässigkeit)

Sind Marketingaktivitäten überhaupt noch zulässig ohne Einwilligung?

SCHWEIZ: Art. 6 Abs. 7 bzw. Art. 30 DSG:

Datenbearbeitungen im Rahmen von Marketingaktivitäten sind erlaubt, sofern die Grundsätze des Datenschutzes (Folie 8) eingehalten werden.

Dabei darf die Persönlichkeit der betroffenen Person aber nicht verletzt werden (Art. 30 DSG).

EU (DSGVO Art. 6 f):

Datenbearbeitung ist zulässig, wenn die Verarbeitung zur Wahrung der **berechtigten Interessen des Verantwortlichen** erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, **überwiegen** (…).

DSGVO Erwägungsgrund Nr. **Nr. 47** (bezüglich Art. 6 f): «Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.»

6. Rechte der Privatpersonen / Pflichten der Datenbearbeiter

1. Recht auf **Transparenz** durch Datenschutzerklärung, Art. 6 Abs. 3 DSG (erkennbarer Zweck)
2. Recht auf **Information** bei Datenerhebung, Art. 19 DSG
3. Recht auf **Auskunft**, ob und welche Daten zu welchem Zweck bearbeitet werden, Art. 25 DSG
4. Recht auf **Datenherausgabe** und **Datenübertragung**, Art. 28 DSG
5. Recht auf **Berichtigung** (bei falschen Daten), Art. 6 Abs. 5 / Art. 32 DSG
6. Recht auf **Löschung** („Recht auf Vergessen“), Art. 6 Abs. 5 DSG
7. Recht auf **Überprüfung** automatisierter Einzelfallentscheidungen, Art. 21 Abs. 2 DSG
8. Recht auf **Widerspruch**

6. Rechte der Privatpersonen / Pflichten der Datenbearbeiter

NEU: Datenschutzfolgeabschätzung erstellen (Art. 22 DSG)

- vorgängige Risikoanalyse bei mutmasslich hohen Risiken für betroffene Person
- Beschreibung der geplanten Bearbeitung mit Bewertung der Risiken für die betroffenen Personen und den zu treffenden Massnahmen zum Persönlichkeitsschutz
- Bsp: Umfangreiche Bearbeitung besonders schützenswerter Personendaten
- Pflicht zur Meldung an EDÖB, wenn trotz Massnahmen hohes Risiko besteht (Art. 23 DSG)
    - Pflicht fällt weg, wenn Datenschutzberater/-in gemäss Art. 10 DSG eingesetzt wurde

NEU: Meldepflicht bei Verletzungen der Datensicherheit (Art. 24 DSG)

- z.B. nach Hackerangriff, sofern Verletzung voraussichtlich zu einem **hohen Risiko** für die Persönlichkeit oder die Grundrechte der betroffenen Person führt

7. Profiling (Art. 5 lit. f/g DSG)

Art. 5 lit. f DSG: Profiling bedeutet jede Art der automatisierten Bearbeitung von Personendaten, um bestimmte **persönliche Aspekte**, z.B. bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel zu bewerten, zu analysieren oder vorherzusagen.

Art. 5 lit. g DSG: *Profiling mit **hohem Risiko**: Verknüpfung von Daten führt, die eine **Beurteilung wesentlicher Aspekte der Persönlichkeit** einer natürlichen Person erlaubt.*

Wann besteht ein **hohes** Risiko? Faustregel: Wenn Aussagen über finanzielle Verhältnisse, Familienverhältnisse, Bildungsstand, politische Ansichten, Freizeitaktivitäten etc. ein Werturteil über eine Person zulässt

Profiling mit hohem Risiko ist nur mit ausdrücklicher Einwilligung zulässig (Art. 6 Abs. 7 DSG)

8. Sanktionen

Schweiz (DSG / DSG)

- Geldbussen bis zu CHF 250‘000.-
- Strafsubjekt sind verantwortliche Mitarbeiter (!), also Privatpersonen, nicht die Firma wird bestraft

EU (DSGVO)

- Geldbussen bis 20 Millionen Euro
- oder 4% des Jahresumsatzes
- Strafsubjekt ist das Unternehmen

9. Neuerungen im revidierten DSG

- Inkrafttreten **01.09.2023**
- Grundprinzipien zum Datenschutz bleiben gleich (Rechtmässigkeit / Zweckgebundenheit / Verhältnismässigkeit etc.)
- Erweiterte Dokumentationspflichten (Verzeichnis der Bearbeitungstätigkeiten; Ausnahmen für KMU)
- Ausgebaute Informationsrechte der betroffenen Personen
- Einwilligung für Datenbearbeitung weiterhin kaum erforderlich (im Gegensatz zur DSGVO)
- Profiling kaum eingeschränkt, aber Einführung von Profiling mit hohem Risiko
- Datentransfer ins Ausland vereinfacht
- Neu: Funktion des Datenschutzberaters (freiwillig)
- Neu: Strafbestimmungen: Bussen bis CHF 250‘000 / Strafsubjekt: natürlichen Personen (!)
- Mehr Kompetenzen für eidgenössischen Datenschutzbeauftragten („EDÖB“)

Teil 2: Praktische Umsetzung

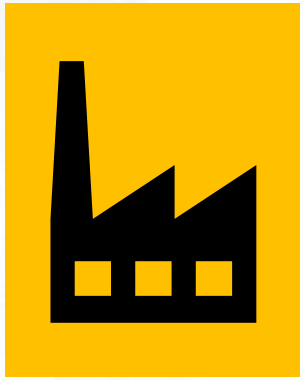
Bestehende Kunden /
Lieferanten /
Mitarbeiter (im CRM)

Vertragsbeziehung!

Überwiegendes privates Interesse für Marketing?

Namentlich bekannte Personen (nicht im CRM)

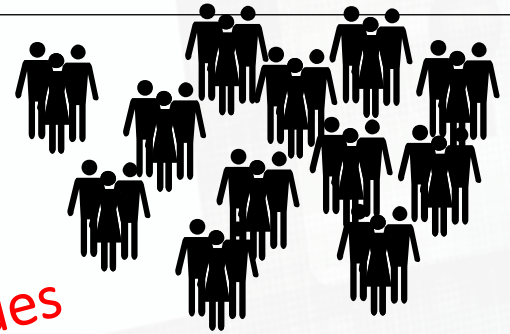
Firma XY
(Datenbearbeiter)



CRM-System

Einwilligung!

Bestehende Kontakte ohne Vertragsbeziehung, z.B. Newsletter-Abonnent (im CRM)



Überwiegendes privates Interesse für Marketing?

Potenzielle Kunden (nicht im CRM)

Erster Schritt zum Erfolg: IST-Analyse erstellen

1. Welche Datensammlungen haben wir?
2. Welche Datensammlungen enthalten personenbezogene Daten?
3. Wo, von wem, zu welchem Zweck und wie lange speichern wir diese personenbezogenen Daten?
4. Wem übermitteln wir personenbezogene Daten?
5. Wie steht es um die Datensicherheit?

10. Datenschutzerklärung

Informationspflicht: Art. 19 DSG: Ausfluss des Transparenzgebots

- *Angemessene* Information ist eine gesetzliche Pflicht (Art. 19 DSG)
- **Worüber** ist zu informieren? Alle Informationen, die erforderlich sind, damit die betroffene Person ihre Rechte geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist
- **Wann** ist zu informieren? Im Zeitpunkt der Beschaffung der Personendaten
- **Wie** ist zu informieren? Gesetz enthält keine Hinweise, üblicherweise mittels Publikation einer **Datenschutzerklärung** (DSE)
- DSE ist eine einseitige Erklärung und kein Vertrag
- Muss auf einfache, leicht zugängliche Weise zur Kenntnis genommen werden können
- WICHTIG: Ein Verstoss gegen Informationspflicht ist strafbewehrt (vgl. Art. 60 Abs. 1 DSG)

10. Datenschutzerklärung

Was ist der Mindestinhalt einer DSE?

- Identität und Kontaktdaten des Verantwortlichen
- Zweck und Umfang der Datenbearbeitung (z.B. Vertragserfüllung)
- Empfänger oder Kategorien von Empfängern, denen Personendaten bekannt gegeben werden
- Verweis auf eingebettete Dienste Dritter wie Facebook, LinkedIn, Google-Dienste etc.
- Hinweise auf die Verwendung von sog. Cookies

10. Datenschutzerklärung

Wie erstellt man eine DSE?

- Klärung der Vorfrage, ob DSGVO anwendbar ist
- Vorlage downloaden und auf individuelle Bedürfnisse anpassen, z.B. bei

  http://www.dsat.ch/download

  http://www.weka.ch

  http://www.sgv-usam.ch/schwerpunkte/wirtschaftspolitik/unterseiten/neues-datenschutzrecht)
- Generator nutzen für individuelle DSE (z.B. https://brainbox.swiss/datenschutz-generator-schweiz/ [gratis])
- Beratung durch Anwaltskanzlei oder spezialisierte Unternehmen
- Vollautomatisierte Lösung mit externem Anbieter
- Aufschalten auf Website (auf oberster Ebene anklickbar)

11. Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG/Art. 30 DSGVO)

Dokumentationspflicht für **alle** Verantwortlichen sowie Auftragsbearbeiter (Art. 12 DSG / Art. 30 DSGVO)

Wie erstellt man ein Verzeichnis der Verarbeitungstätigkeiten?

- Gesetz und Verordnung enthalten keine Vorgaben
- Vorlage downloaden und auf individuelle Bedürfnisse anpassen
- Beratung durch Anwaltskanzlei oder spezialisiertes Unternehmen
- Es genügt ein Verzeichnis für DSG und DSGVO

11. Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG/Art. 30 DSGVO)

Art. 12 Verzeichnis der Bearbeitungstätigkeiten

[1] Die Verantwortlichen und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten.

[2] Das Verzeichnis des Verantwortlichen enthält mindestens:

a. die Identität des Verantwortlichen;

b. den Bearbeitungszweck;

c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;

d. die Kategorien der Empfängerinnen und Empfänger;

e. wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;

f. wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8;

g. falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2.

[3] Das Verzeichnis des Auftragsbearbeiters enthält Angaben zur Identität des Auftragsbearbeiters und des Verantwortlichen, zu den Kategorien von Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden, sowie die Angaben nach Absatz 2 Buchstaben f und g.

[4] Die Bundesorgane melden ihre Verzeichnisse dem EDÖB.

[5] 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.

11. Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG/Art. 30 DSGVO)

Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
ABC Installation GmbH
Steinbauerstr. 45a
9999 Steinhausen

Tel. +41 999 99 99
E-Mail: team@abcinstallation.ch
Web: www.abcinstallation.ch

Verarbeitungs-tätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personen-bezogenen Daten	Kategorie von Emp-fängern	Drittlands-transfer	Aufbewahrungsdauer / Löschfristen	Technische/or-ganisatorische Massnahmen
Lohnabrech-nung	Hans Bauer 099 999 99 99 hans@abcinstallation.ch	02.03.2018	• Auszahlung der Löhne / Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name, Geburtsdatum • Adresse • Bankverbindungsdaten • Lohn-/Entgeltdaten • ggf. Religionszugehörigkeit • Sozialversicherungsdaten	Steuer-berater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept
Personal-verwaltung	Hans Bauer 099 999 99 99 hans@abcinstallation.ch	02.03.2018	• Personaladministration • Personalführung • Arbeitszeitverwaltung • Personalbeschaffung (betrifft Bewerber)	• Beschäftigte • Auszubil-dende • Bewerber	• Name, Adressen • Zeitwirtschaftsdaten • Daten zur Arbeitsleistung • Leistungsbeurteilung • Lebenslauf und Bewer-bungsunterlagen (betr. Bewerber)	Keine	Keine	• Beschäftigte: in der Regel ca. 3 Jahre nach Aus-scheiden • abgelehnte Bewerber: 6 Monate nach Abschluss des Bewer-bungsverfah-rens	Siehe IT-Sicherheits-konzept
Betrieb der Firmenwebseite (über Hosting-Dienstleister)	Max Meier 099 999 99 98 max@abcinstallation.ch	28.02.2018	Aussendarstellung	• Webseiten-besucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheits-konzept + HTTPS-Verschlüsse-lung
Kunden-verwaltung	Jutta Klein 099 999 99 97 jutta@abcinstallation.ch	02.03.2018	• Bearbeitung von Aufträgen inkl. Rechnungstellung • postalische Werbung	• Kunden	• Name, Adresse • Angaben zum Auftrag • ggf. Bankverbindungsdaten	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheits-konzept

11. Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG/Art. 30 DSGVO)

Erleichterungen für KMU in Art. 24 Verordnung zum DSG

Art. 24 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten

Unternehmen und andere privatrechtliche Organisationen, die am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:

a. Es werden besonders schützenswerte Personendaten in grossem Umfang bearbeitet.

b. Es wird ein Profiling mit hohem Risiko durchgeführt.

12. Auftragsbearbeiter / Cloud

- Datenweitergabe an Dritte zwecks Auslagerung von Datenbearbeitungen (Art. 9 DSG).
- Betroffene Personen müssen nicht informiert werden
- Beispiele: Cloud-Lösungen (z.B. OneDrive), Treuhänder, Mail-Chimp, etc.
- Voraussetzungen:
  - Vertragliche Vereinbarung mit Auftragsbearbeiter formfrei, somit auch mündlich)
  - Einhaltung der Datenschutzgrundsätze durch Auftragsbearbeiter
  - Keine vertragliche oder gesetzliche Geheimhaltungspflicht
- Auftragsbearbeiter darf Daten nur so bearbeiten, wie es der Verantwortliche tun dürfte
- WICHTIG: Der Auftraggeber (Verantwortlicher) bleibt in jedem Fall für die Einhaltung der Datenschutzbestimmungen verantwortlich
- Handlungsbedarf: Prüfen, wo ADVs fehlen und mit Auftragsbearbeiter
- Bei Grossfirmen: Datenschutzbestimmungen sind in sog. Standardvertragsklauseln oder AGB bereits enthalten.

13. Datenschutzberater / -beauftragter

Braucht ein Unternehmen einen Datenschutzbeauftragten (DSGVO) / Datenschutzberater (DSG)?

- **DSG**: **Datenschutzberater** -> Ist freiwillig (Art. 10 DSG)
  - Aufgaben: Anlaufstelle für betroffene Privatpersonen und Behörden / Interne Beratung / Schulung / Überwachung der Datenschutz-Compliance
  - Unabhängig und weisungsungebunden
  - Vorteile für Ug: Keine Konsultationspflicht des EDÖB bei Datenschutz-Folgeabschätzung

- **DSGVO**: **Datenschutzbeauftragter ->** Nein (Ausnahme: Wenn Kerntätigkeit in der Verarbeitung personenbezogener Daten besteht und systematische Überwachung beinhaltet)

Empfehlung:

Die Einsetzung eines Datenschutzberaters ist grundsätzlich sinnvoll. Bei kleinen Unternehmen rechtfertigt sich der Aufwand jedoch kaum. Alternativ kann ein „betrieblicher Datenschutzbeauftragter“ eingesetzt werden.

14. Datenschutz im Arbeitsrecht

Grundsatz: Personendaten müssen **Eignung** des AN betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sein!

Rechtsgrundlagen:

- Art. 28 ZGB (Schutz der Persönlichkeit)
- Art. 328 OR (Fürsorgepflicht / Schutz der Persönlichkeit des Arbeitnehmers)
- Art. 328b OR (mit Verweis auf Datenschutzgesetz) – analog anzuwenden bei **Bewerbungen**
- Art. 26 ArGV 3 (Verbot von Überwachungs- und Kontrollsystemen zur Verhaltensüberwachung)
- Einsichtsrecht: Art. 23 DSG / Art. 15 DSGVO
- Eigene Datenschutzerklärung für Personal empfehlenswert
- Technische Überwachung am Arbeitsplatz (Internet / E-Mail / Video / Zugangskontrolle, etc.)

  https://www.seco.admin.ch/seco/de/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Arbeit/Arbeitsbedingungen/Broschuren/technische-ueberwachung-am-arbeitsplatz.html

15. Praktische Umsetzung: Vorkehrungen Website

- Datenschutzerklärung aufschalten auf oberster Ebene
- Checkbox (unchecked!) für Datenschutzerklärung in online-Shops (Link auf Dokument)
- Checkboxen für Einverständniserklärung bei Anmeldungen („Opt-In“)
- E-Mail mit Bestätigung der Anmeldung (“Double-Opt-In”)
- Abmeldemöglichkeit („Opt-Out“)
- Cookies:
  - Schweiz: Informations-Banner (zum Wegklicken; kein Einverständnis nötig)
  - EU: Consentbanner mit Einwilligungserklärung zwingend (gemäss E-Privacy-Verordnung)
- Aufzeichnung der An- bzw. Abmeldungen zu Dokumentationszwecken

15. Praktische Umsetzung: Zusammenfassung (ToDo's)

1. **Verantwortlichkeit** im Unternehmen festlegen! Wer ist für das Thema Datenschutz zuständig?
2. **Anwendbarkeit DSGVO** prüfen
3. **Identifikation** der Datensammlungen
4. **Rechtfertigungsgründe** für Datenbearbeitungen prüfen
5. **Dokumentation:** Verzeichnis der Datenbearbeitungen erstellen
6. **Datenschutzerklärungen** überprüfen auf die neuen Vorgaben im DSG (bzw. DSGVO)
7. **Auftragsbearbeitungen** identifizieren und vertragliche Grundlagen schaffen wo nötig
8. **Datentransfer ins Ausland** identifizieren und auf Rechtmässigkeit prüfen
9. **Interne Prozesse** festlegen für Informationsrechte der betroffenen Personen (Auskunftsbegehren, Meldung von Datenschutzverstössen, Datenschutz-Folgenabschätzung)
10. **Technische und organisatorische Massnahmen („TOMS")** vornehmen (Website, Social Media, Marketing)
11. **Datensicherheit** sicherstellen durch geeignete TOMs

15. Praktische Umsetzung

«Recht auf Vergessen»

Quelle: https://khalawgroup.com/the-right-to-be-forgotten-gdpr/gdpr-right-to-be-forgotten-cartoon/

Durch Datenschutz-Compliance Vertrauen schaffen beim Kunden und der Öffentlichkeit

Quelle: https://khalawgroup.com/the-right-to-be-forgotten-gdpr/gdpr-right-to-be-forgotten-cartoon/

Weiterführende Links

- Eidgenössischer Datenschutzbeauftragter: https://www.edoeb.admin.ch/edoeb/de/home.html
- Aktuell gültiges Datenschutzgesetz: https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de
- Revidiertes Datenschutzgesetz: https://www.fedlex.admin.ch/eli/cc/2022/491/de
- Revidierte Datenschutzverordnung: https://www.fedlex.admin.ch/eli/cc/2022/568/de
- EU-DSGVO: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=de
- Aktuelle Informationen zum Datenschutzrecht: https://datenrecht.ch/

Teil 3: Fragen und Antworten

Q&A

Fragen und Antworten

Arbeitsrecht:
Datenschutz «im Kopf»: Dürfen ehemalige Kandidaten (Dossiers bereits gelöscht), aus der baren Erinnerung heraus, für die gleiche Vakanz zu späterem Zeitpunkt kontaktiert werden?

Grundsätzlich gilt Datenschutz für jede «Speicherungsart» von Daten. Das Bundesgericht musste im Urteil 4A_125/2020 entscheiden, ob bei einem Auskunftsersuchen die «**verfügbaren Angaben über die Herkunft der Daten**» nach Art. 8 Abs. 2 lit. a [altes]DSG auch **das im Gedächtnis abgespeicherte Wissen** von umfassen kann. Dies hat das Bundesgericht verneint, was für eine Zulässigkeit der Kontaktaufnahme «aus dem Kopf» spricht.

Arbeitsrecht:
Dürfen Gesundheitsthemen von Mitarbeitenden im Kreise der Geschäftsleitung thematisiert werden?

Grundsätzlich nein. Es darf lediglich die **Tatsache**, dass jemand krank ist, thematisiert werden, hingegen keine Details über die Krankheit diskutiert werden, solange MA dafür nicht sein Einverständnis gibt. Welche Krankheit jemand hat usw. geht auch die Geschäftsleitung nichts an.

Fragen und Antworten

Gibt es Unterscheidungsmerkmale rund um die Pflichten bei der Bearbeitung von Personendaten, welche nicht direkt den Personen gehören, resp. der Beschäftigung bei einem Unternehmen entspringen, gegenüber Daten des privaten Lebens? Z.B. private vs. geschäftliche Mailadresse oder private Tel-Nr. vs. Direktwahl im Geschäft?

Nein, jedes personenbezogene Datum fällt gleichermassen unter den Datenschutz.
Grundsatz: Es dürfen nur jene Daten bearbeitet werden, welche für den Zweck der Bearbeitung benötigt werden (Grundsatz der Datensparsamkeit bzw. Privacy by default).

Datenaustausch mit Bundesorganen
Was gilt bezüglich Austausch von Personendaten (wie KK, IV-Nummern usw.) mit SUVA, IV, SAHB und Institutionen (Alters-/Pflegeheime)?

Da der Datenaustausch gesetzlich vorgesehen ist, dürfen (bzw. müssen) Personendaten an diese Bundesorgane weitergegeben werden (Rechtfertigungsgrund «Gesetz»).
Das DSG ist normal anwendbar. Für Bundesorgane gelten jedoch besondere Bestimmungen im 6. Kapitel des DSG (Art. 33ff).

Fragen und Antworten

Recht auf Löschung
Was ist mit personenbezogenen Daten, die in einem Backup enthalten sind? Diese können nicht einzeln geändert oder gelöscht werden, ohne das gesamte Backup zu löschen.

Grundsätzlich gilt Löschpflicht auch für Backups, unter Beachtung gesetzlicher Aufbewahrungsfristen.
Problem: Bei Datenwiederherstellung aus Backup würden die eigentlich im Produktivsystem gelöschten Daten wieder produktiv und müssten erneut gelöscht werden.
Sofern Löschung unzumutbar ist, bzw. einen unverhältnismässigen Aufwand verursacht, kann die Löschung m.E. nicht verlangt werden (Privilegierung für «echte» Backups).
Grundsatz: **Privacy by Design** (Löschprozesse in IT-Architektur berücksichtigen), d.h. so vorgehen, dass Löschung möglich ist.

Arbeitsrecht
- Auskunftsrecht des Arbeitnehmers?
- Datenschutzerklärung für Mitarbeitende?

- Auskunftsrecht:
Arbeitnehmer hat Auskunftsrecht ins Personaldossier (Art. 25 DSG).

- Datenschutzerklärung für MA: Es empfiehlt sich, eine separate DSE für MA zu erstellen und im Intranet zu publizieren bzw. als Beilage zum Arbeitsvertrag abzugeben.

Fragen und Antworten

Auftragsbearbeitung
Muss im B2B-Bereich (Herstellung und Vertrieb von individuellen Contactlinsen) eine zusätzliche "Auftragsdatenbearbeitungsvereinbarung" unterzeichnet werden?

Ja, aber nur wenn personenbezogene Daten des Endkunden, welcher die individuell hergestellten Contactlinsen verwenden wird, übermittelt werden. Da die personenbezogenen Daten für die Herstellung der Linsen nicht nötig sind, sollte auf den Datenaustausch personenbezogener Daten verzichtet werden.

Pseudonymisierung / Auftragsbearbeitung / DSGVO
Was müssen Schweizer Unternehmen beachten, wenn sie Gerätedaten, oder **pseudonymisierte** medizinische Daten von an die Cloud angebundenen Geräten für automatisierte aktive «Predictive Maintenance» bzw. Produktweiterentwicklung nutzen wollen, die in der EU eingesetzt werden?

Was müssen deutsche Unternehmen beachten, wenn Sie Daten ihrer in der Schweiz genutzten Geräte nutzen wollen?

Zunächst: Reine Gerätedaten und **anonymisierte Daten** sind datenschutzrechtlich unbedenklich. Bei **pseudonymisierten** Daten ist Rechtslage unklar, ob DSGVO/DSG anwendbar sind.
Der Verantwortliche (in EU) sollte mit CH-Firma einen **Auftragsverarbeitervertrag** nach Art. 28 DSGVO schliessen. Im umgekehrten Fall gleiche Ausgangslage, Auftragsbearbeitervertrag nach Art. 9 DSG.

Fragen und Antworten

Marketing (Rechtfertigungsgründe)
Wie wird uns das DSG im Alltag in Bezug auf Direkt Marketing Aktivitäten beeinflussen?

Direktmarketing ist in der Schweiz erlaubt, solange Grundsätze des Datenschutzes (s. Folie 8) eingehalten werden, insbesondere die Bearbeitung verhältnismässig ist, d.h. die Schwelle zur **Persönlichkeitsverletzung** darf nicht überschritten werden. Wo diese legt, hängt vom Einzelfall und von zukünftiger Gerichtspraxis ab.
DSGVO: Der Rechtfertigungsgrund des «überwiegenden privaten Interesses» muss erfüllt sein (s. Folie 9)

Auftragsverarbeitung
Wir haben mit unserem Software-Partner XY einen Vertrag über die Auftragsverarbeitung personenbezogener Daten abgeschlossen. Müssen wir als Händler von Reha-Hilfsmitteln weitere Vorkehrungen treffen? Gegenüber unseren direkten Kunden? E-Mail-technisch (wir arbeiten im Moment mit Outlook)?

Nein, Auftragsverarbeitervertrag genügt. Der Einsatz von Software bzw. eines Auftragsdatenverarbeiters ist zulässig, Kunden müssen darüber nicht informiert werden.

Die Nutzung von Outlook ändert an der datenschutzrechtlichen Ausgangslage nichts.

Fragen und Antworten

Besonders schützenswerte Daten

a) Was müssen wir als Importeur und Distributor berücksichtigen?

b) Was machen wir mit Patientendaten, welche uns unverlangt, z.B. auf Rezepten oder von einer Klinik, geschickt werden? Reicht es aus, das E-Mail zu löschen?

a) Allgemeine Datenschutzgrundsätze berücksichtigen (Folie 8).

b) Unverlangte Patientendaten: Löschen und Absender darauf hinweisen, Übermittlung zu unterlassen. Wenn die Übermittlung zulässigerweise erfolgt, müsste eigentlich ein Auftragsverarbeitervertrag geschlossen werden (Pflicht aus Sicht Absender).

Datenschutzbeauftragter /Datenschutzberater

Müssen wir als kleine KMU einen Datenschutzbeauftragten bestimmen oder haben?

Nein, ist gesetzlich nicht vorgesehen. Dennoch muss DSG / DSGVO eingehalten werden, d.h. jede Organisation sollte die Verantwortung klären und einen **betrieblichen** Datenschutzbeauftragten ernennen, welcher sich um das Thema kümmert (s. Folie 28). Prüfen, ob allenfalls die (gesetzlich vorgesehene) Funktion des Datenschutzberaters auf freiwilliger Basis Sinn ergibt.

Fragen und Antworten

Arbeitsrecht
Benötige Vorlage für ein Mitarbeiterschreiben, das die Mitarbeiter unterschreiben können bzw. müssen (worauf muss geachtet werden, was ist strafbar etc.)

→ Das Verhalten in Bezug auf Datenschutz sollte in einem internen Reglement (z.B. Weisung IT-Nutzung) thematisiert werden. Weisungen sind einseitige Anordnungen des Arbeitgebers. Eine Vorlage muss individuell erarbeitet werden.

Verzeichnis der Bearbeitungstätigkeiten
Welche Verzeichnisse müssen geführt werden (Speicherorte, Mitarbeiterdaten etc.)?

→ Siehe Folie 24/25

Fragen und Antworten

Recht auf Löschung vs. Aufbewahrungspflicht
Löschung von Kundendaten ist nicht einfach im ERP, da Rechnungen in der Buchhaltung ja noch vorhanden sein müssen.

Die Aufbewahrungspflicht beträgt 10 Jahre (vgl. Art. 958 lit. f OR). Dieser gesetzliche Rechtfertigungsgrund geht einem Löschungsantrag vor.

Teil 3: Fragen und Antworten

Q&A

Vielen Dank für Ihre Aufmerksamkeit

Kontaktangaben:

factum advocatur

lic. iur. HSG Urs Freytag

Teufenerstrasse 3, 9000 St. Gallen

Telefon: 071 421 41 41

Mail: freytag@factum.pro