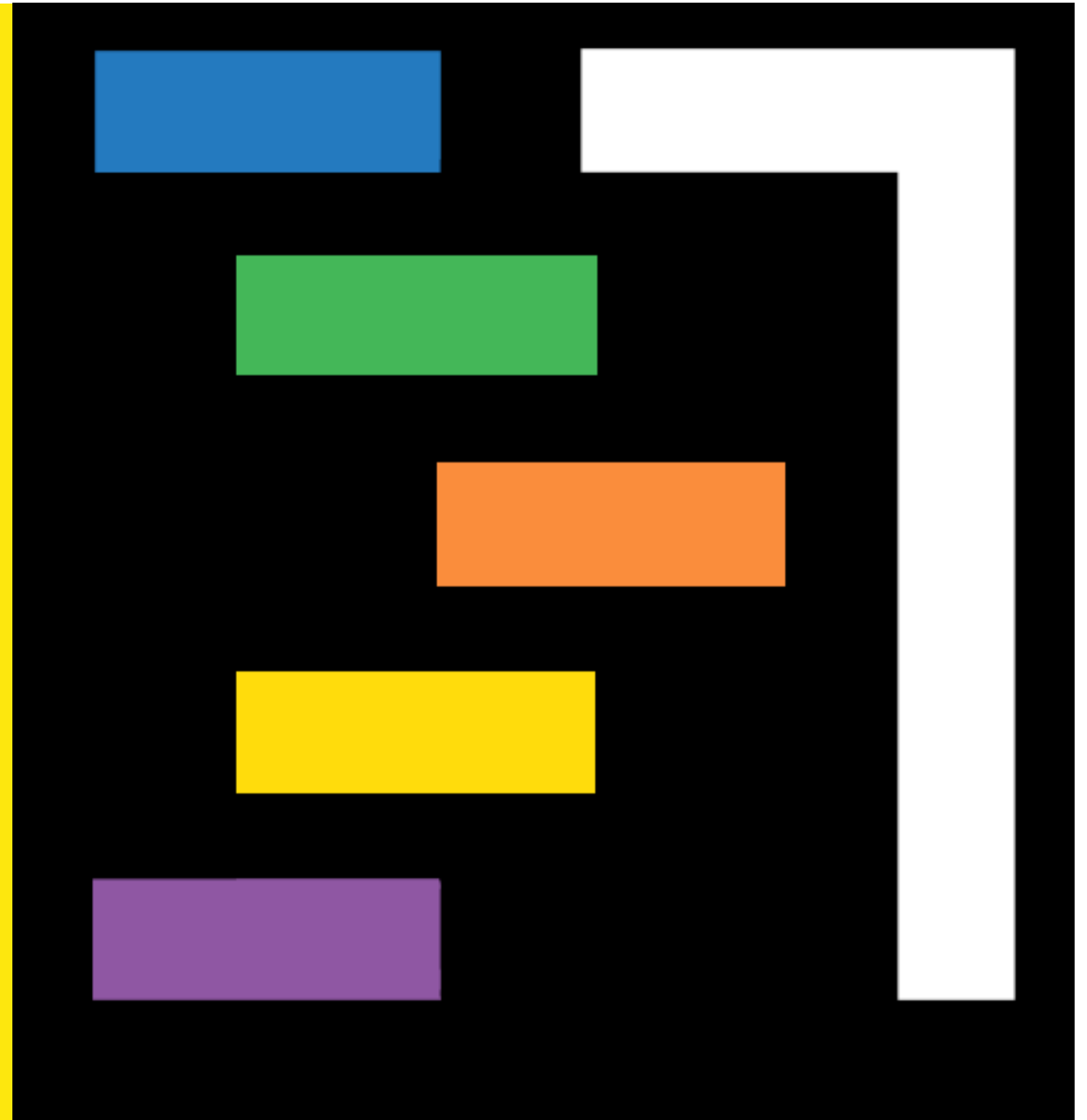


Datenschutz in der Praxis Umsetzung mit Fachwissen und (KI-)Tools

Seminar, 18. Durchführung

Prof. Dr. Bettina Schneider
Programmleiterin
Co-Head Competence Center Digital Trust

03.11.2025



Gliederung

Datenschutz in der Praxis: Umsetzung mit Fachwissen und (KI-)Tools

I. Willkommen

II. Einführung

- Schritt 1 Datenschutz-Policy
- Schritt 2 Bearbeitungsverzeichnis
- Schritt 3 Datenschutz-Folgenabschätzung
- Schritt 4 Technische und organisatorische Massnahmen (TOMs)
- Schritt 5 Datentransfer
- Schritt 6 Web-Präsenz
- Schritt 7 Datenschutzprozesse
- Schritt 8 Audit

III Abschluss

Die Fachhochschule Nordwestschweiz





Studium

Weiterbildung

Forschung und
Dienstleistungen

Die FHNW

DE EN

Standorte und Kontakt

Bibliotheken

Karriere an der FHNW

Media Corner



🏠 ▶ Forschung und Dienstleistungen ▶ Wirtschaft

Studierendenprojekte

Lösungen für Unternehmen und Organisationen

Lassen Sie Studierende mitdenken

Die Hochschule für Wirtschaft FHNW ist eine praxisorientierte Ausbildungsstätte. Eine enge Zusammenarbeit mit Unternehmen und Organisationen ist dabei zentral. Unsere jährlich 350 Studierendenprojekte sind ein wichtiges Instrument, um den Wissenstransfer zwischen Praxis und

<https://www.fhnw.ch/de/forschung-und-dienstleistungen/wirtschaft/studierendenprojekte>

Alles für deine Karriere.

next CAREER SERVICES

Willkommen bei Career Services FHNW. Unser Ziel ist es, den Studierenden in Bewerbungs- und Karrierefragen Unterstützung zu bieten. Career Services FHNW vernetzt unsere Studierenden mit der Unternehmenswelt – und umgekehrt.

Für Studierende

Bei uns ist deine Karriere in guten Händen. Career Services FHNW bietet dir professionelle und praxisorientierte Unterstützung.

Weitere Infos

Für Unternehmen

Bei uns finden Sie die richtigen Mitarbeitenden. Career Services FHNW offeriert Ihnen verschiedene Formen des Kennenlernens.

Weitere Infos

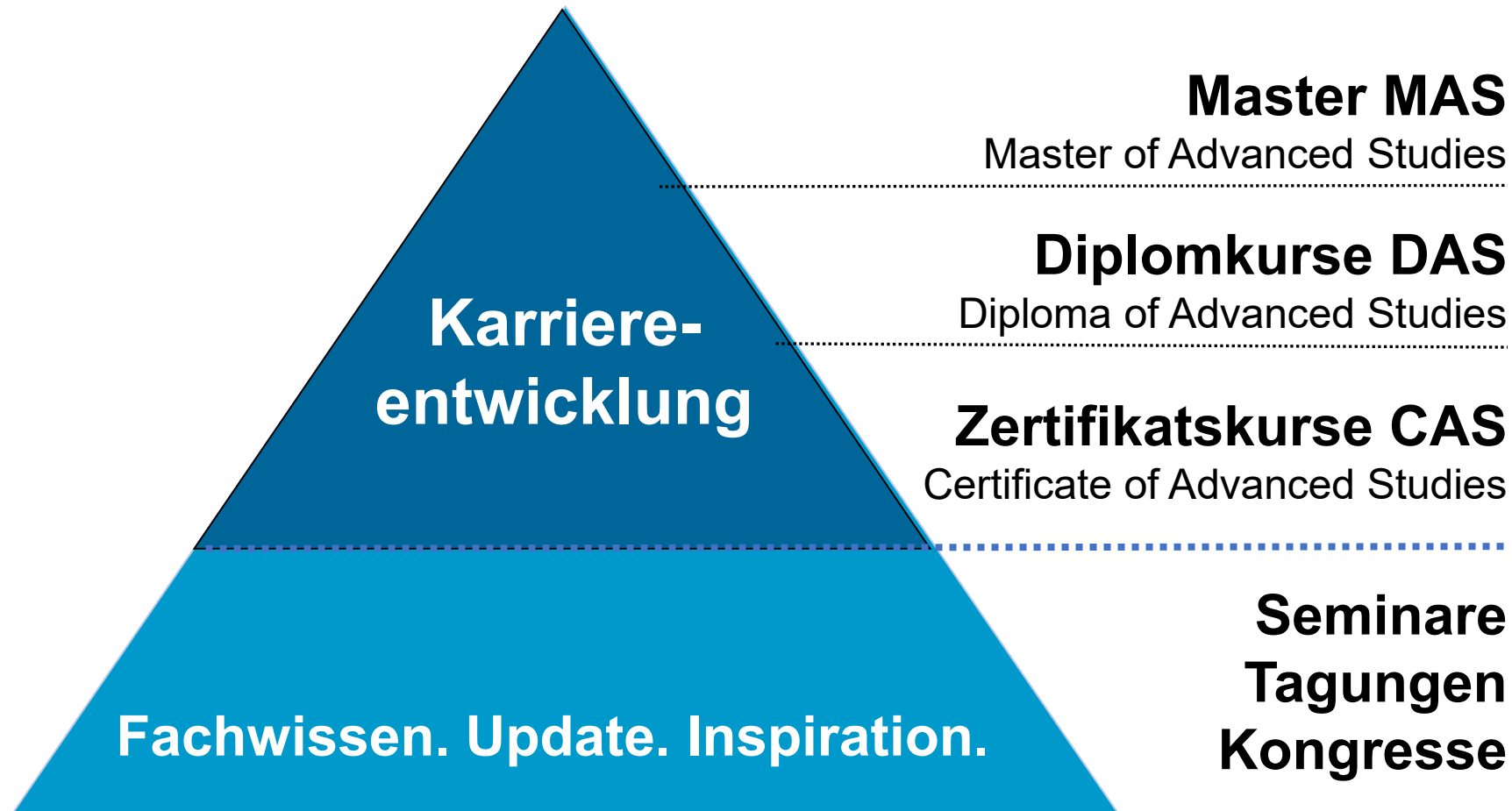
Über uns

Career Services FHNW der «single point of contact» sowohl für unsere Studierenden als auch für Unternehmen.

Weitere Infos

Quelle: <https://next-career.ch/de/>

Weiterbildungspyramide



CAS als Weiterbildung-Meilenstein zum DAS

DAS Digital Leadership in IT (32 ECTS)

CAS Agile Leadership in IT

CAS Cybersecurity & Information Risk Management

Seminar Datenschutz in der Praxis

DAS Cybersecurity, AI & Data Governance (32 ECTS)

CAS AI powered CyberTech

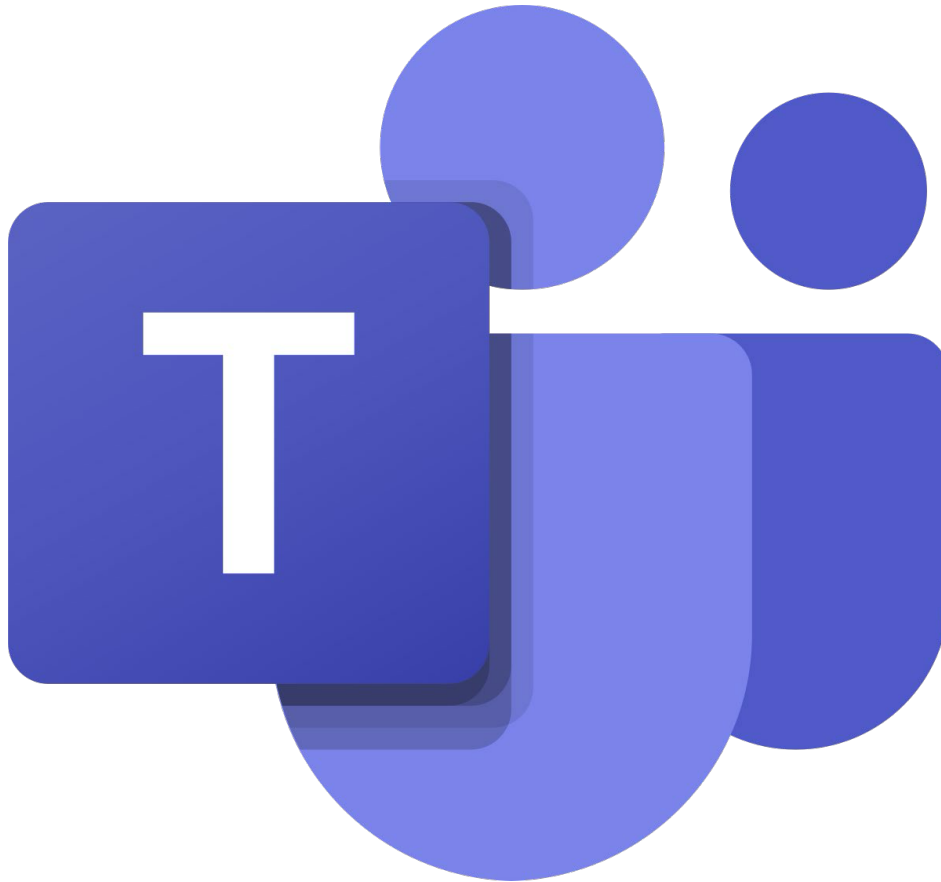
CAS Cybersecurity & Information Risk Management

Seminar Datenschutz in der Praxis

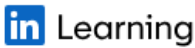
Voraussetzung Seminar-Abschluss

- **80% Anwesenheit**
- **Aktive Mitarbeit**
- **Teamarbeit und -präsentation**
(Ergebnisse auf MS Teams abgelegt)

Lernplattform und Dokumente: MS Teams



E-Learning / Video-Kurse

[Start my free month](#)

Solutions for: [Business](#) [Higher Education](#) [Government](#) | [Buy for my team](#)

Join free for 1 month and learn the most in-demand business, tech, and creative skills. 

English

Type

Time to Complete

Level

All filters

Reset

384 Results for "gdpr" Sort by: Best Match



COURSE

Learning GDPR

 LinkedIn · By: Kalinda Raina · Updated May 2022

 Certificate Eligible · 4.7 ★★★★★ (1,614) · 169,405 learners

 [Save](#)



POPULAR

COURSE

GDPR Compliance: Essential Training

 LinkedIn · By: Mandy Huth · Oct 2021

4.7 ★★★★★ (2,065) · 63,874 learners · Beginner

 [Save](#)

Dozierenden-Team



Esther Zaugg

Applikationsmanagerin
ETH Zürich

Masterarbeit:
Erstellung eines
Datenschutzfolgenabschätzung-Tools für
kleine Unternehmen

esther.zaugg@fhnw.ch

Lukas Fässler

lic. iur. Rechtsanwalt

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b
6340 Baar

Telefon +41 41 727 60 80

Mobile +41 79 209 24 32

faessler@fsdz.ch



Prof. Dr. Bettina Schneider

Head of Competence Center Digital Trust
Institute vor Information Systems

bettina.schneider@fhnw.ch

www.digitaltrust-competence.ch

Teilnehmende dieses Kurses

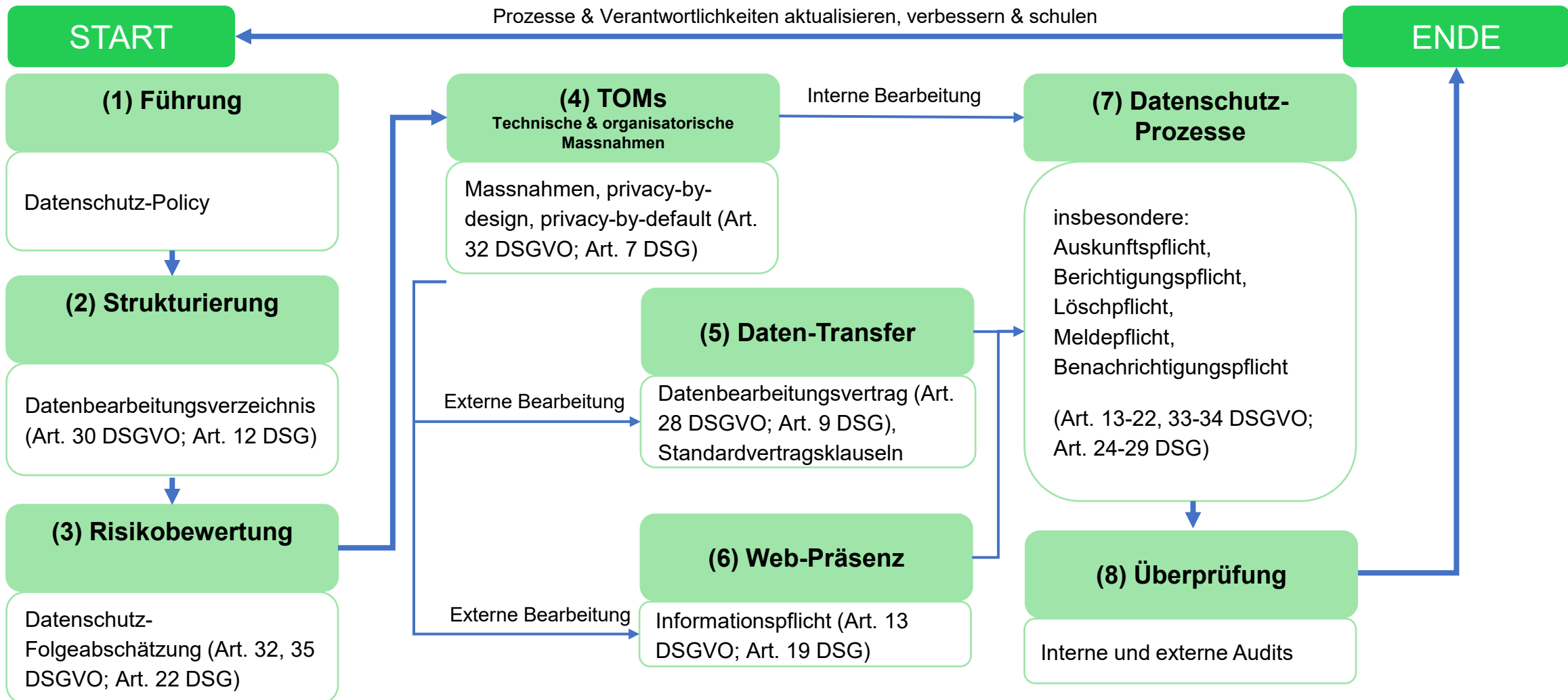
Scannt und antwortet
(wenn ihr möchtet 😊)

<https://forms.office.com/e/SfrSJYUxZJ>

Kennenlernen Praxisseminar Datenschutz



Datenschutz-Compliance – Die Roadmap



1. Seminartag

Begrüssung (Bettina) (20 min)

Intro (Lukas): Verantwortlichkeiten im
Datenschutz; Schritte der **Datenschutz-Roadmap**
im Überblick (30min)

Schritt 1: Erstellung einer Datenschutz-Policy
der obersten Führung (Lukas)

*Input (30 min) – Gruppenarbeit unter Einsatz eines KI-
Tools (60 min) – Präsentation & Diskussion (45 min)*

Tools: Gemini, Mistral, ChatGPT oder anderes

12:15 Mittagspause (60 min)

Schritt 2: Bearbeitungsverzeichnis (Bettina)

*Input (+ Demo, 45 min) - Gruppenarbeit unter Einsatz
von Templates oder Software (60 min) – Diskussion (45
min)*

Tools: Auswahl an Tools (mit oder ohne KI)

Fragen und Abschluss (ca. 15 min)

2. Seminartag

Schritt 3: Datenschutz-Folgenabschätzung (Esther)

*Input (30 min) – Gruppenarbeit unter Einsatz von DSFA-
Tool (45 min) – Präsentation & Diskussion (45 min)*

Tool: Auswahl verschiedener Tools (mit und ohne KI)

Schritt 4: Technische & organisatorische
Massnahmen (TOMs) (Esther)

*Input (+ Bsp., 15 min) – Gruppenarbeit unter
Berücksichtigung des EDÖB-Leitfadens (30 min)*

12:15 Mittagspause (60 min)

– Präsentation & Diskussion (30 min)

Schritt 5: Datentransfer (ADV, SCCs) (Lukas)

*Input (45 min) – Gruppenarbeit unter Einsatz von KI-
Werkzeugen (60 min) – Präsentation & Diskussion (45 min)*

Tool: Gemini, Mistral, ChatGPT oder anderes

Fragen und Abschluss (Abfrage Webscan-Bsp.)

3. Seminartag

Warm-up (Lukas) (ca. 15 min)

Schritt 6: Webauftritt – Cookies-Analyse (Lukas)
*Input (+ Bsp, 60 min) – Gruppenarbeit unter Einsatz eines
Tools (45 min) – Präsentation & Diskussion (45 min)*

Tool: Gemini, Mistral, ChatGPT, oder anderes

12:15 Mittagspause (60 min)

Schritt 7: Datenschutz-Prozesse (Lukas)

*Input (30 min) – Gruppenarbeit unter Einsatz diverser
Werkzeuge (60 min) – Präsentation & Diskussion (45 min)*

Tool: Moderationskoffer oder KI

Schritt 8: Datenschutzaudit (int./ext) (Bettina)

*Input (20 min) – evtl. Gruppenarbeit unter Einsatz eines
Tools (15 min) – evtl. Diskussion & Präsentation (10 min)*

Tool: Auswahl verschiedener Tools (mit und ohne KI)

Zusammenfassung & Feedback (ca. 15 min)

Datenschutz-Compliance – Die Roadmap

Basis für die Seminarstruktur

Am Ende des Seminar haben wir Wissen und praktische Kompetenzen zu

- 1: Datenschutz-Policy
- 2: Bearbeitungsverzeichnis
- 3: Datenschutz-Folgeabschätzung
- 4: abgeleiteten TOMs
- 5: Verträge mit Datenverarbeitern
- 6: Website Datenschutzerklärung
- 7: Prozessabläufe zu Datenschutzpflichten
- 8: Auditfragen

Gliederung

Datenschutz in der Praxis: Umsetzung mit Fachwissen und (KI-)Tools

I. Willkommen

II. Einführung

- | | |
|-----------|---|
| Schritt 1 | Datenschutz-Policy |
| Schritt 2 | Bearbeitungsverzeichnis |
| Schritt 3 | Datenschutz-Folgenabschätzung |
| Schritt 4 | Technische und organisatorische Massnahmen (TOMs) |
| Schritt 5 | Datentransfer |
| Schritt 6 | Web-Präsenz |
| Schritt 7 | Datenschutzprozesse |
| Schritt 8 | Audit |

III Abschluss

Einführung

Personendaten

Bearbeitung

Verhältnismässigkeit
Rechtmässigkeit
Treu und Glauben
Zweckmässigkeit
Privacy by Default
Privacy by Design

Kategorien

- Personendaten (PD)
- Besonders schützenswerte PD
- Profilingdaten
- Profilingdaten mit besonderem Risiko

Rechtfertigungsgründe

- Gesetzliche Grundlage
 - Einwilligung
- Überwiegendes öffentliches Interesse
- Überwiegendes privates Interesse

Verantwortlicher

- Unternehmen
- Organisationen oder
- Privatpersonen, die Personendaten besitzen und bearbeiten

Auftragsdatenverarbeiter

- ADV bei gleichem DS-Niveau
- SCC bei ungleichem DS-Niveau

Sorgfaltspflichten und Verantwortung

- | | | |
|-----------------|-----------------------|------------------|
| • VR | 717 und 754 OR | Beweislastumkehr |
| • GL | 754 OR | Beweislastumkehr |
| • Mitarbeitende | 321a OR | Treuepflicht |

Internes Kontrollsystem IKS

Betroffene

Rechte Betroffener

- Auskunftsrecht
- Berichtigungsrecht
- Löschungsrecht
- Herausgabe
- Rechte bei automatisierter Bearbeitung
- Benachrichtigungsrecht (data breach)

- Bearbeitungsverzeichnis
- Datenschutzfolgeabschätzung
- TOMs
- ADV oder SCC
- DS-Bestimmungen (Online)

Datenschutz-Prozesse

717 OR

VR-Mitglieder ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren müssen.

Das erforderliche Mass an Sorgfalt wird objektiv beurteilt und richtet sich danach, was von einem vernünftigen und gewissenhaften Menschen unter gleichen Umständen erwartet werden kann.

Eine Verletzung dieser Pflicht kann zur persönlichen Haftung des VR-Mitglieds führen, wenn dadurch ein kausaler Schaden entsteht.

754 OR

Art. 754⁶⁴⁵

III. Haftung für
Verwaltung,
Geschäftsfüh-
rung und
Liquidation

¹ Die Mitglieder des Verwaltungsrates und alle mit der Geschäftsführung oder mit der Liquidation befassten Personen sind sowohl der Gesellschaft als den einzelnen Aktionären und Gesellschaftsgläubigern für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.

² Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, **sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.**

Beweislastumkehr zulasten der Führungskräfte

321a OR

Art. 321a

II. Sorgfalts- und Treuepflicht

¹ Der Arbeitnehmer hat die ihm übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen des Arbeitgebers in guten Treuen zu wahren.

Internes Kontrollsystem IKS

Im schweizerischen Obligationenrecht (OR) ist die **Pflicht zur Führung eines internen Kontrollsystems (IKS)** in Artikel 728a OR für Aktiengesellschaften verankert, **die einer ordentlichen Revision unterliegen.** Diese Vorschrift besagt, dass die Revisionsstelle im Rahmen ihrer Prüfung bestätigen muss, dass ein IKS existiert, und dass es den Geschäftsrisiken und der Tätigkeit des Unternehmens angepasst ist. 



Internes Kontrollsystem IKS (2)

Der Kern der gesetzlichen Verpflichtung

- **Artikel 728a OR:** legt fest, dass die Revisionsstelle die Existenz eines internen Kontrollsystems zu prüfen hat. 
- Dies betrifft nur Unternehmen, die zu einer ordentlichen Revision verpflichtet sind. 
- Die Prüfung konzentriert sich auf die Existenz des IKS, also darauf, dass es dokumentiert, den Risiken angepasst und bekannt ist sowie tatsächlich angewendet wird. 

Was das IKS leisten soll

- Das IKS dient dazu, die Zuverlässigkeit der Finanzberichterstattung sicherzustellen und Fehldarstellungen zu vermeiden. 
- Es ist ein wesentlicher Beitrag zum Risikomanagement, da es Schwachstellen aufdeckt und eine wirksame, wiederkehrende Kontrolle ermöglicht. 
- Das IKS soll einen Beitrag zur Sicherheit, Ordnungsmässigkeit und Wirtschaftlichkeit der Unternehmensprozesse leisten. 



https://backend-api.economiesuisse.ch/sites/default/files/nn_migration/swisscode_d_web_1.pdf



Umgang mit Risiken, Compliance und Finanzüberwachung (internes Kontrollsystem)

26

Der Verwaltungsrat sorgt für ein dem Unternehmen angepasstes internes Kontrollsystem, welches Risikomanagement, Compliance und Finanzüberwachung umfasst.

- Das interne Kontrollsystem dient dem Ziel, die Effektivität und die Effizienz der Geschäftstätigkeit (Operations), die Gesetzes- und Normenkonformität (Compliance) sowie die Verlässlichkeit der finanziellen und nichtfinanziellen Berichterstattung (Reporting) sicherzustellen.
- Das operative Management und die es unterstützenden Funktionen sorgen dafür, dass die Kontrollen gemäss den Vorgaben des Verwaltungsrats umgesetzt werden und dass sie wirksam sind.
- Die Ausgestaltung des internen Kontrollsystems hat der Grösse, der Komplexität und dem Risikoprofil des Unternehmens Rechnung zu tragen.

Risikomanagement

27

Das Unternehmen verfügt über ein angemessenes Risikomanagement. Der Verwaltungsrat nimmt eine regelmässige Risikobeurteilung vor.

- Das Risikomanagement umfasst namentlich strategische, operationelle, rechtliche und finanzielle Risiken sowie Marktrisiken bzw. Risiken für die Reputation des Unternehmens.
- Der Verwaltungsrat nimmt mindestens einmal jährlich eine Risikobeurteilung vor und berücksichtigt deren Ergebnis für seine Leitungs- und Aufsichtsaufgaben sowie für die Weiterentwicklung des internen Kontrollsystems.

Compliance und verantwortungsvolles Handeln

28

Der Verwaltungsrat ist dafür besorgt, dass das Unternehmen insgesamt Gesetze und interne Normen einhält (Compliance) und auch darüber hinaus verantwortungsvoll handelt.

- Der Verwaltungsrat ist im Rahmen seiner Oberaufsicht dafür besorgt, dass nicht nur seine Mitglieder, sondern das Unternehmen insgesamt, inklusive Management und Mitarbeitende, die Gesetze und internen Normen einhalten (Compliance) und dass auch darüber hinaus verantwortungsvoll gehandelt wird.
- Der Verwaltungsrat organisiert die Compliance nach den Besonderheiten des Unternehmens und erlässt geeignete Verhaltensrichtlinien. Er orientiert sich dabei an anerkannten Best-Practice-Regeln und beachtet die wichtige Rolle finanzieller wie nichtfinanzieller Anreize für Mitarbeitende und deren Vorgesetzte.³
- Die Geschäftsleitung trifft Massnahmen zur Einhaltung der Gesetze und internen Normen sowie für ein integriertes Geschäftsgebahren im Unternehmensalltag. Sie gewährt hierfür die erforderlichen personellen und finanziellen Ressourcen.



Minimalstandard zur Verbesserung der IKT-Resilienz

https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Gliederung

Datenschutz in der Praxis: Umsetzung mit Fachwissen und (KI-)Tools

- I. Willkommen
- II. Einführung

- | | |
|-----------|---|
| Schritt 1 | Datenschutz-Policy |
| Schritt 2 | Bearbeitungsverzeichnis |
| Schritt 3 | Datenschutz-Folgenabschätzung |
| Schritt 4 | Technische und organisatorische Massnahmen (TOMs) |
| Schritt 5 | Datentransfer |
| Schritt 6 | Web-Präsenz |
| Schritt 7 | Datenschutzprozesse |
| Schritt 8 | Audit |

- III Abschluss

Die Datenschutz-Policy

Erstelle unter Mithilfe eines KI-Werkzeuges (ChatGPT, Mistral, Gemini Google oder andere) in maximal 3 Sätzen eine Data Protection Policy nach ungefähr folgenden Vorgaben:



Schreibe mir eine Data Protection Policy für eine schweizerische Aktiengesellschaft, welche die wesentlichen Grundsätze zur Compliance im Datenschutz und der Datensicherheit der Unternehmung aus Sicht des Verwaltungsrates festhalten. Es dürfen maximal 3 Sätze erstellt werden. Die Sprache ist deutsch und die Inhalte sind in einfacher und verständlicher Form zu schreiben.



Beispiel: Gemini Google, erstellt am 30.9.2025

Gliederung

Datenschutz in der Praxis: Umsetzung mit Fachwissen und (KI-)Tools

- I. Willkommen
- II. Einführung

- | | |
|-----------|---|
| Schritt 1 | Datenschutz-Policy |
| Schritt 2 | Bearbeitungsverzeichnis |
| Schritt 3 | Datenschutz-Folgenabschätzung |
| Schritt 4 | Technische und organisatorische Massnahmen (TOMs) |
| Schritt 5 | Datentransfer |
| Schritt 6 | Web-Präsenz |
| Schritt 7 | Datenschutzprozesse |
| Schritt 8 | Audit |

- III Abschluss

DSGVO:

„Jeder **Verantwortliche** und gegebenenfalls sein **Vertreter** führen ein **Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen.“

nDSG:

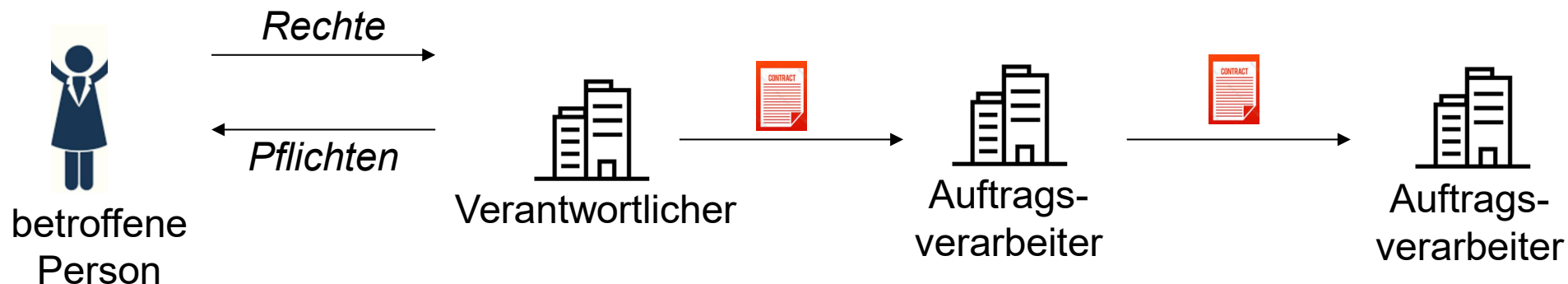
„Die **Verantwortlichen** und **Auftragsbearbeiter** führen je ein **Verzeichnis ihrer Bearbeitungstätigkeiten**.“

Definition Verarbeitung gem. Art. 4 DSGVO:

Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten **Vorgang oder jede solche Vorgangsreihe** im Zusammenhang mit personenbezogenen Daten.

Vorgang z.B. erheben, erfassen ordnen, speichern, auslesen, abgleichen, löschen...

Vorgangsreihe z.B. Lohnabrechnung, Rekrutierung, ...



nDSG Art. 12

«Verzeichnis der Bearbeitungstätigkeiten»

Die **Verantwortlichen** pflegen:

Identität des Verantwortlichen
den Bearbeitungszweck
Beschreibung der <i>Kategorien betroffener Personen</i> und der <i>Kategorien bearbeiteter Personendaten</i>
Kategorien der Empfängerinnen und Empfänger
falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2
Aufbewahrungsdauer oder die Kriterien zur Festlegung dieser Dauer
Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit

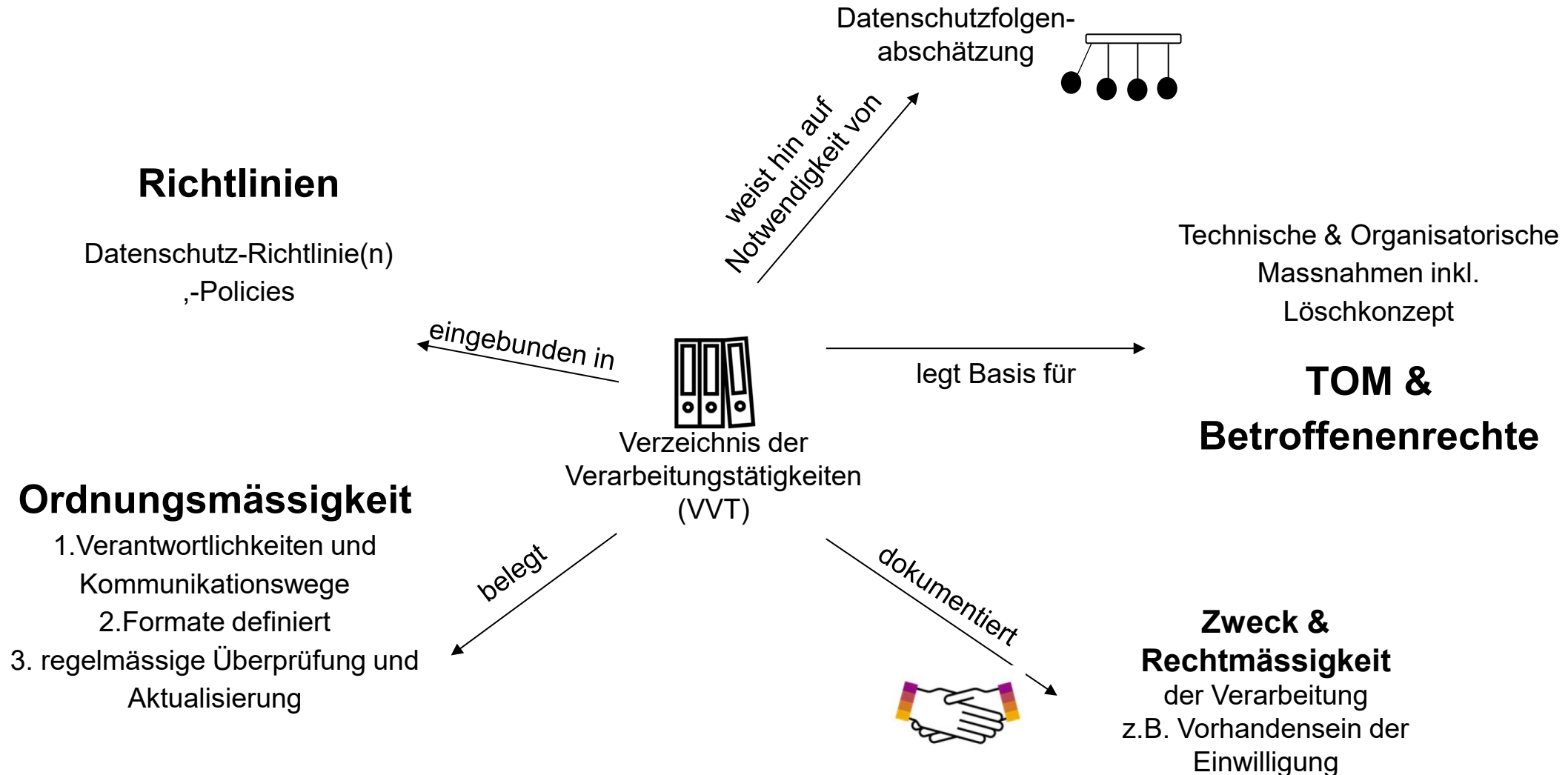
DSGVO Art. 30

«Verzeichnis von Verarbeitungstätigkeiten»

Die **Verantwortlichen** pflegen:

wer*	Namen & Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
wozu	die Zwecke der Verarbeitung
was*	Beschreibung der <i>Kategorien betroffener Personen</i> und der <i>Kategorien personenbezogener Daten</i>
an wen*	Kategorien von Empfängern
an wen*	ggf. Übermittlungen an Drittland oder internationale Organisation, einschl. Angabe des betreffenden Drittlands/ internationalen Organisation, sowie die Dokumentierung geeigneter Garantien
wie lange	vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
wie sicher*	allgemeine Beschreibung der technischen und organisatorischen Massnahmen

Instrument der Rechenschafts- und Dokumentationspflicht



DSGVO

Art. 30 Abs. 5

Verzeichnis beschränkt auf Unternehmen und Einrichtungen > 250 Mitarbeitenden, **es sei denn**

>> Verarbeitung mit einem besonderen Risiko

>> Verarbeitung sensibler Daten

>> es wird nicht nur gelegentlich verarbeitet.

z.B. es werden „regelmäßig“ Mitarbeiterdaten verarbeitet, dann unabhängig von der Mitarbeiterstärke für diese Verarbeitung betroffen.

Fazit: Ausnahmeregelung läuft in der Praxis weitgehend ins Leere.

Verordnung zum nDSG

Art. 24

Unternehmen < 250 Mitarbeitenden sowie natürliche Personen von der Pflicht befreit ausser

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

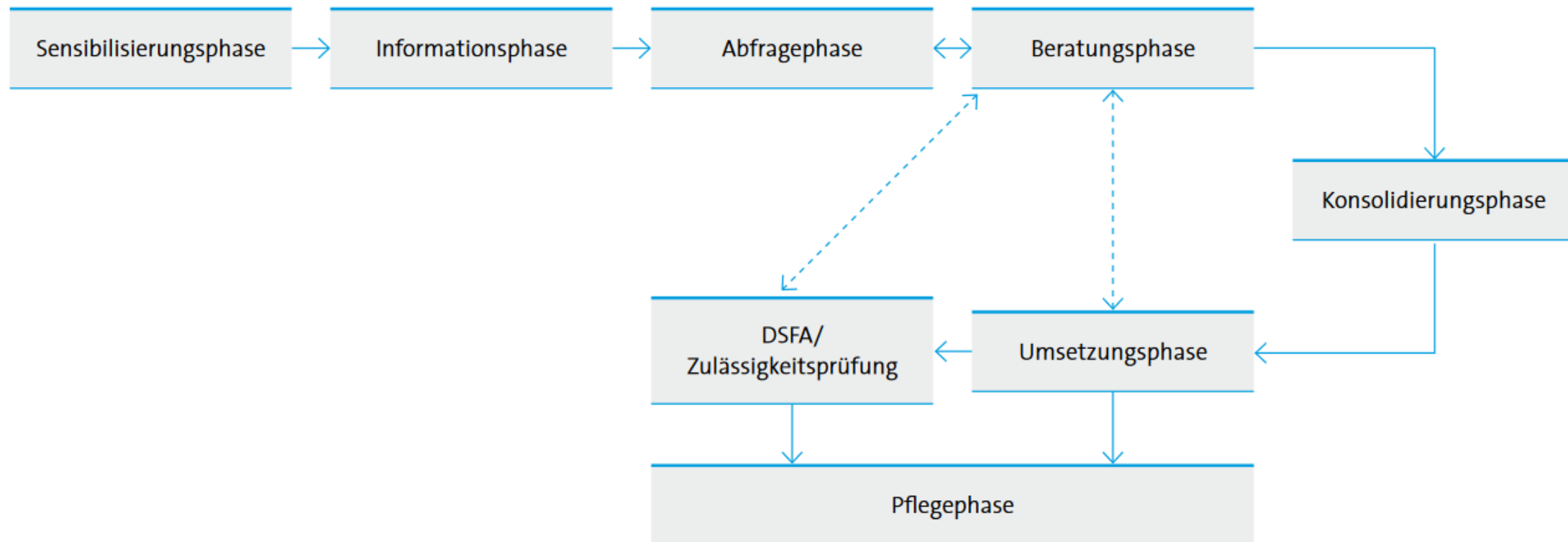
>> Es wird ein Profiling mit hohem Risiko durchgeführt.

Fazit: eine realistische Ausnahmeregelung

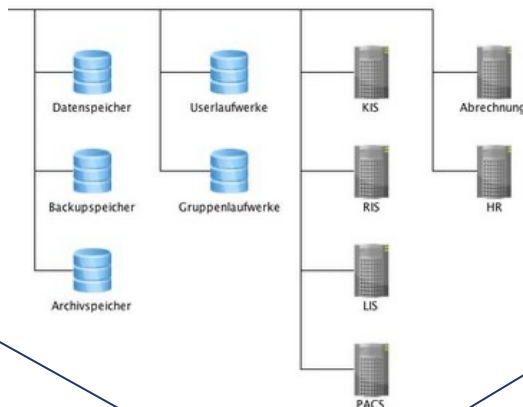
Organisatorische Einbettung

Beispiel der Bitkom

Grafische Darstellung der einzelnen Phasen als Überblick



IT-Systeme

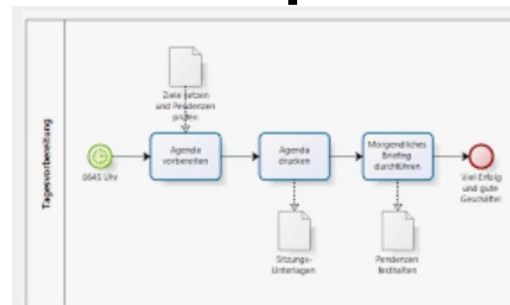


Daten



Abteilungen

Geschäftsprozesse





Sehr einfach gehaltenes Verzeichnis mit
Mustern für Kleinunternehmen
<https://www.lida.bayern.de/de/muster.html>

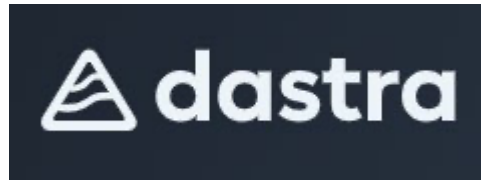


Verzeichnis inkl. Löschkonzept* (teilw. (zu) sehr detailliert)
https://www.baden-wuerttemberg.datenschutz.de/praxishilfen/#verarbeitungsverzeichnis_und_loeschkonzeption



Umfangreiche, englisch-sprachige Templates für
Verantwortliche oder Verarbeiter (runterscrollen!)
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/documentation/>

(Beispiele – keine Kaufempfehlung 😊)



Software mit KI Assistent zur Erstellung eines Registers
(englisch, DSGVO)

<https://www.dastra.eu/de/product-features/data-processing>



KI-Tools für die Prüfung von Datenverarbeitungen und zur
Erstellung eines Verzeichnisses (beta-Version, DSGVO)

<https://www.thomashelbing.com/de/tools>



Klassische Datenschutzmanagement-Software
(deutsch, DSG und DSGVO)

<https://www.siriusag.com/datenschutzmanagement-system.html>

Arbeitsauftrag

Erstellt ein Bearbeitungsverzeichnis

Ziel: Erstellt ein Bearbeitungsverzeichnis für das Unternehmen eurer Gruppe, das die Datenbearbeitungen gemäß den gesetzlichen Vorgaben nachvollziehbar dokumentiert (mind. 8 Zeilen).

Aufgaben:

- Nutzt ein Template oder Tool eurer Wahl, um das Bearbeitungsverzeichnis zu erstellen.
- Begründet, wie ihr das Verzeichnis strukturiert habt und warum diese Struktur für Übersichtlichkeit und gesetzliche Nachvollziehbarkeit geeignet ist.
- Reflektiert, welche Herausforderungen bei der Erstellung aufgetreten sind.

Abgabe / Präsentation:

- Ladet das Bearbeitungsverzeichnis/Screenshot auf MS Teams hoch.
- Stellt das Verzeichnis, die Struktur und die Herausforderungen kurz vor.

Gliederung

Datenschutz in der Praxis: Umsetzung mit Fachwissen und (KI-)Tools

- I. Willkommen
- II. Einführung

- | | |
|-----------|---|
| Schritt 1 | Datenschutz-Policy |
| Schritt 2 | Bearbeitungsverzeichnis |
| Schritt 3 | Datenschutz-Folgenabschätzung |
| Schritt 4 | Technische und organisatorische Massnahmen (TOMs) |
| Schritt 5 | Datentransfer |
| Schritt 6 | Web-Präsenz |
| Schritt 7 | Datenschutzprozesse |
| Schritt 8 | Audit |

- III Abschluss

Was ist die Datenschutzfolgenabschätzung (DSFA)?

Gesetze, Personendaten, Risiko, Massnahmen

Art. 22 DSG / Art. 35 DSGVO

- Compliance- und Arbeitsinstrument
- Selbstevaluation/Risikobewertung von Personendatenbearbeitungen aus datenschutzrechtlicher Sicht
 - Beschreibung der Personendatenbearbeitung
 - Bewertung der Risiken für Persönlichkeit und Grundrechte Betroffener
 - Massnahmen zum Schutz der Persönlichkeit und Grundrechte
- Anwendungsfälle Bearbeitungsvorgänge mit möglichem hohem Risiko für Betroffene:
 - Projekt: geplante Personendatenbearbeitungen
 - Betrieb/Projekt: Weiterentwicklungen und Erweiterungen bestehender Personendatenbearbeitungen
 - Betrieb: Dokumentation bestehender Personendatenbearbeitung

Wann ist eine Datenschutzfolgenabschätzung (DSFA) nötig?

Gesetze, Personendaten, Risiko, Massnahmen

Art. 22 DSG

- Datenbearbeitung könnte in hohem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person resultieren
- Datenbearbeitungen
 - unter Verwendung neuer Technologien,
 - aus der **Art**, dem **Umfang**, den **Umständen** und dem **Zweck** der Bearbeitung
- Zwei Beispiele aus dem Gesetz:
 - eine umfangreiche Bearbeitung besonders schützenswerter Personendaten
 - eine systematische umfangreiche Überwachung öffentlicher Bereiche

Wann ist eine Datenschutzfolgenabschätzung (DSFA) nicht nötig?

Gesetze, Personendaten, Risiko, Massnahmen

Art. 22 DSG

- Private Verantwortliche mit gesetzlicher Verpflichtung zur Bearbeitung der Daten
- Zertifizierung von System, Produkt oder Dienstleistung nach Art. 13
- Abstellen auf Verhaltenskodex nach Art. 11,
 - welcher auf einer DSFA beruht und
 - Massnahmen vorsieht und
 - dem EDÖB vorgelegt wurde

Wie wird hohes Risiko in einer DSFA definiert? – Sicht CH

Gesetze, Risiko

- Begriff weder im Gesetz noch in Verordnung präzisiert → Praxis und Rechtsprechung abwarten
 - Regel: Hohes Risiko ist anzunehmen, je **umfangreicher** die Bearbeitung, je **sensibler** die bearbeiteten Daten, je **umfassender** der Bearbeitungszweck
- Für die Bearbeitung Verantwortlichen müssen
 - die Persönlichkeit und die Grundrechte der betroffenen Personen schützen
 - bestimmen, ab wann das Risiko hoch ist, und in diesem Fall die notwendigen Massnahmen ergreifen.

Vgl. Pflicht zur Durchführung einer DSFA (DSG Art. 22 Abs. 2)

Wie wird hohes Risiko in einer DSFA definiert? – Sicht EU

Personendaten, Risiko

9 Kategorien von Datenverarbeitungen mit hohem Risiko

Sensible oder sehr persönliche Daten

Bearbeitung von Personendaten in grossem Umfang

Einsatz neuer Technologien

Verhindern der Rechteaübung (Vertrag, Service, etc.)

Daten von besonders gefährdeten Personen

Abstützen auf persönliche Aspekte wie bspw. Scoring oder Profiling

Systematische Überwachung

Vergleichen, kombinieren oder abgleichen von Personendaten aus mehreren Quellen

Automatisierte Entscheidungsfindung

Wozu dient die Datenschutzfolgenabschätzung (DSFA)?

Compliance, Risikobewertung und Dokumentation

- **Erfüllung Compliance:** Prüfung, ob Personendatenbearbeitungen die datenschutzrechtlichen Bestimmungen eines Gesetzes erfüllen oder nicht erfüllen.
- **Risikoanalyse:**
 - Bewertung der Risiken aus Sicht der Betroffenen (Mitarbeitende, Kund:innen, Klient:innen, usw.): Stellt Datenverarbeitungsvorgang trotz getroffenen oder geplanten Massnahmen ein hohes Risiko für die betroffenen Individuen dar? (anhand Wahrscheinlichkeit und Schweregrad eines möglichen Schadens)
 - Unterstützt die Risikoerkennung und die Prüfung der Massnahmen zur Reduktion der Risiken
- **Dokumentation Risikobewertung:** Informationen, Bewertungen, Massnahmen unterstützen bei der Bewältigung und Evaluation von Vorfällen (bspw. Verletzung Datensicherheit)

Aufbewahrungsfrist DSFA

Compliance, Risikobewertung und Dokumentation

Art. 14 DSV

Aufbewahrungspflicht einer Datenschutz-Folgenabschätzung durch Verantwortliche nach Beendigung der Datenbearbeitung:

>> mindestens zwei Jahre

(Artikel 14 der Verordnung zum Datenschutzgesetz)

Wie erfolgt die Datenschutzfolgenabschätzung (DSFA)?

Bruttorisiko, Massnahmen, Nettorisiko, Monitoring

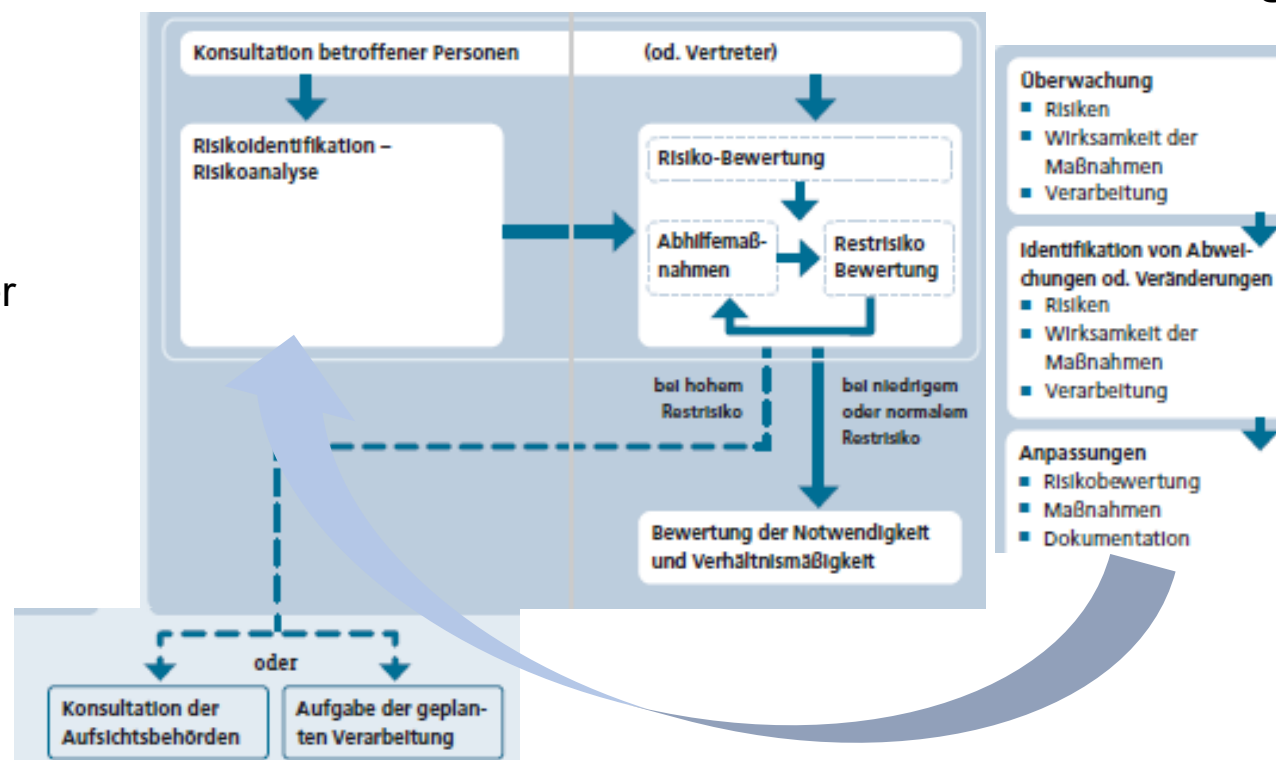
1. Durchführung

- (Konsultation)
- (Risikoidentifikation/-analyse)
- **Bewertung der Risiken (Bruttorisiken)** für die Persönlichkeit oder die Grundrechte der betroffenen Person
- **Beschreibung der Massnahmen** zum Schutz der Persönlichkeit und der Grundrechte
- **Bewertung der Restrisiken** für Betroffene nach Massnahmen (Nettorisiken)
 - Kein hohes Risiko -> (Bewertung der Notwendigkeit & Verhältnismässigkeit)
 - Hohes Risiko -> Konsultation oder Aufgabe

2. Monitoring

- Kontinuierliche Überwachung
- Identifikation von Änderungen
- bei Anpassungen -> allfällige Neubewertung

1. Durchführung DSFA



Arbeitsauftrag

Führt eine Datenschutzfolgenabschätzung durch

Ziel: Durchführung einer Datenschutzfolgenabschätzung (DSFA) anhand bspw. einer Datenverarbeitung aus dem bereits erstellten Bearbeitungsverzeichnis und einer Einschätzung des Risikolevels für Betroffene

Aufgaben:

- Nutzt ein Template oder Tool eurer Wahl, um die Datenschutzfolgenabschätzung durchzuführen.
- Dokumentiert das Ergebnis der Bewertung des Nettorisikos, allenfalls mit Screenshots.
- Reflektiert, ob das Resultat mit eurer Risikoeinschätzung vor der Durchführung zusammenpasst und welche Herausforderungen bei der Durchführung aufgetreten sind.
- Hinweis: Priorisiert bitte die Risikobewertung. Die Massnahmen werden im Detail im nächsten Teil erarbeitet.

Abgabe / Präsentation:

- Ladet das Ergebnis der DSFA allenfalls mit Screenshots auf MS Teams hoch.
- Stellt die gewählte Datenverarbeitung, das Ergebnis und die Herausforderungen kurz vor.

Tools & Checklisten

- Richtlinien und Unterlagen für Bundesorgane:
 - [Risikovorprüfung](#) (Excel)
 - [Leitfaden](#) DSFA (Vorlage im Anhang 2 - PDF)
- [DSFA](#) nach dem DSG (Excel in Deutsch und Englisch)
- [KI-gestützte Vorlage](#) (Excel mit Makros)
- [DSFA Vorlage](#) (Word)
- [DSFA Vorlage](#) KMU Verband (Word - in DE, FR & IT)
- [PIA \(Privacy Impact Assessment\) Software](#)
- [DPIA Tool](#) (Webapplikation FHNW)
- [DPIA – Data Privacy Impact Analyzer](#) (AI Prompts Datenrecht)

Gliederung

Seminar Datenschutz in der Praxis

- I. Willkommen
- II. Einführung

- | | |
|-----------|---|
| Schritt 1 | Datenschutz-Policy |
| Schritt 2 | Bearbeitungsverzeichnis |
| Schritt 3 | Datenschutz-Folgenabschätzung |
| Schritt 4 | Technische und organisatorische Massnahmen (TOMs) |
| Schritt 5 | Datentransfer |
| Schritt 6 | Web-Präsenz |
| Schritt 7 | Datenschutzprozesse |
| Schritt 8 | Audit |

- III Abschluss

Definition technische und organisatorische Massnahmen

Gesetze, Massnahmen

Art. 7 DSG / Art. 32 DSGVO

- Vorkehrungen, Handlungen, Verfahren, Mechanismen, Regeln, Prozess, usw. zum Schutz von Personendaten vor unbefugtem Zugriff, Verlust oder Missbrauch
- Verantwortliche sind gesetzlich verpflichtet den Schutz über Massnahmen sicherzustellen

Technische Massnahmen

Bezug auf technische Aspekte des Informationssystems (Anonymisierung, Verschlüsselung, Authentifizierung usw.)

Organisatorische Massnahmen (umfassender)

Bezug auf Umgebung des Systems, die Nutzenden, und die Art der Nutzung (Berechtigungsregelung, Verzeichnis der Bearbeitungstätigkeiten usw.)

Phase	Beispiele technische Massnahmen	Beispiele organisatorische Massnahmen
Datenerhebung	Datenminimierung, Logging, Protokollierung, usw.	Einwilligung, Transparenz, usw.
Speicherung	Zugriffsschutz, Verschlüsselung, usw.	Zutrittsmanagement Räume, usw.
Verarbeitung	Protokollierung, Anonymisierung, Pseudonymisierung, usw.	Einwilligung, Zweckbindung, Verzeichnis Bearbeitungstätigkeiten, Sensibilisierung Mitarbeitende, usw.
Weitergabe	Zugriffsschutz, Anonymisierung, Protokollierung, usw.	Verträge (ADV), Drittlandtransferprüfung, usw.
Löschung	Löschprozesse, usw.	Transparenz, org. Auskunfts- und Löschprozesse, usw.

Umsetzung technische und organisatorische Massnahmen

Gesetze, Massnahmen, Privacy by design & default, Monitoring

- Umsetzung der Massnahmen -> Zugang zu den Personendaten ist sowohl physisch (bspw. Zugang zu den Servern) als auch im Hinblick auf die Bearbeitung (bspw. Zugang zu den einzelnen Arbeitsplätzen und Anwendungen) sicherer.
- **Beispiel: Datenschutz durch Technik und Design (Privacy by default & design)**

Art. 7 Abs. 1 DSG / Art. 25 Abs. 2 DSGVO

- **Privacy by default:** Datenschutz durch Technik
- **Zuständigkeit:** Verantwortliche
- **Zeitpunkt:** ab der Planung des Systems Grundsätze des Datenschutzes mitberücksichtigen - nicht erst später.
- **Zweck:**
 - Einhaltung Datenschutzbestimmungen sicherstellen
 - Überlegungen zur Rechtfertigung der Datenbeschaffung sowie zur Verwendung, Verwaltung und Organisation der Daten im Voraus

Art. 7 Abs. 3 DSG / Art. 25 Abs. 1 DSGVO

- **Privacy by design:** datenschutzfreundliche Voreinstellungen
- Grundsatz der **Verhältnismässigkeit**
- **Zuständigkeit:** Verantwortliche
- **Zeitpunkt:** ab Datenbeschaffung sowie über gesamten Datenlebenszyklus werden Massnahmen ergriffen
- **Zweck:**
 - im Voraus sichergestellt, dass nur die für den Bearbeitungszweck strikt notwendigen Daten beschafft und bearbeitet werden,
 - namentlich durch Voreinstellungen

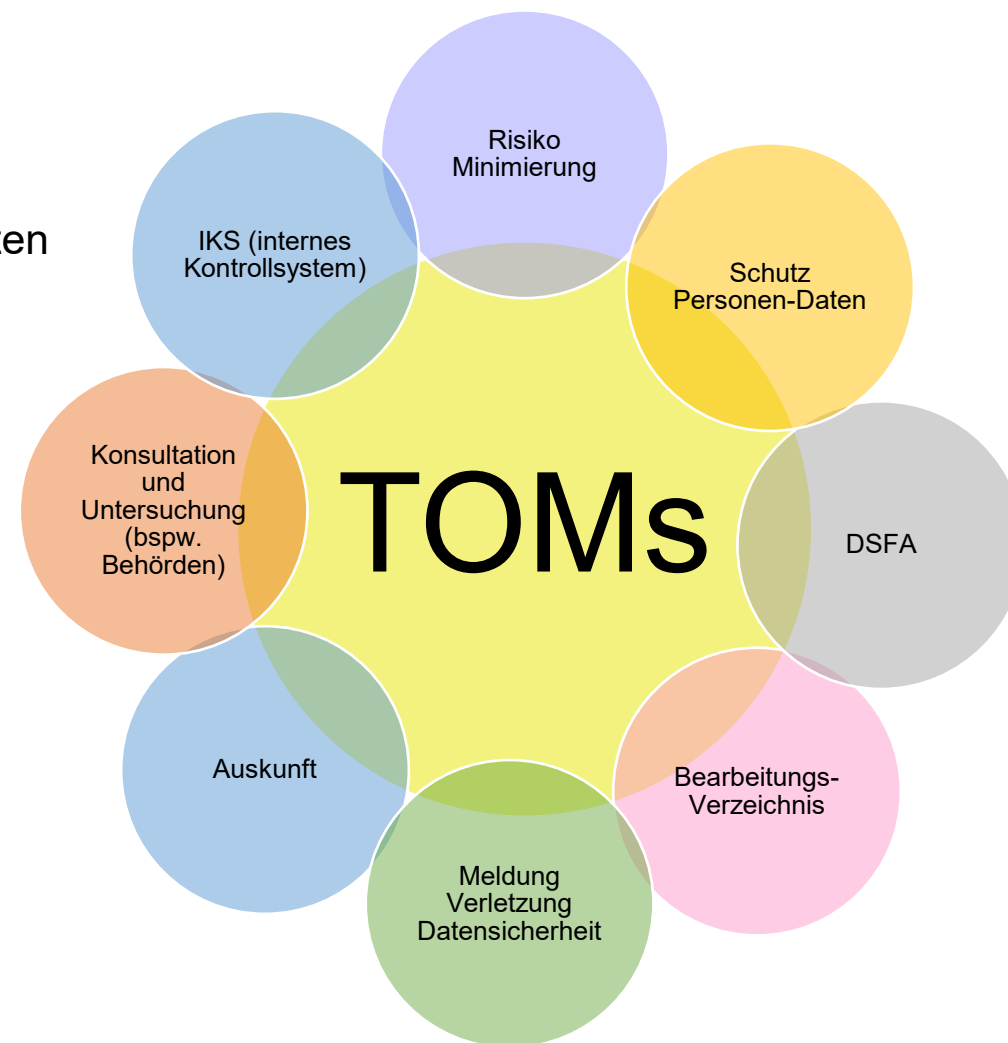
Bezug DSFA: Massnahmen im Regelfall dort beschrieben

Zweck technische und organisatorische Massnahmen

Gesetze, Massnahmen

Art. 7 und 8 DSG, Art. 3 DSV

- **Minimierung der Risiken**, bei der Bearbeitung von Personendaten in (Informations-)Systemen
- **Zusammenspiel beider Arten von Massnahmen** verhindert die Vernichtung oder den Verlust von Daten, aber auch Irrtümer, Fälschungen, unberechtigtem Zugang, usw.
- **Erfüllung der Pflichten im Datenschutz** gemäss DSG, wenn Voraussetzungen erfüllt sind:
 - Datenschutz-Folgenabschätzung
 - Register der Bearbeitungstätigkeiten
- **Weitere Pflichten:**
 - Meldepflichten im Falle einer Verletzung der Datensicherheit
 - Auskunftspflicht gegenüber Betroffenen -> Auskunft über bspw. Aufbewahrungsdauer
 - Konsultation, Untersuchungen, usw. von bspw. Aufsichtsbehörden



Datenschutz & Informationssicherheit bei der Definition von Massnahmen

Daten- schutz Informations- schutz	Nicht perso- nenbez. Daten	«Nicht- sensible» Per- sonendaten	«Sensible» Personenda- ten	«Hochsen- sible» Perso- nendaten
		Risiko: gering/mittel	Risiko: hoch	Risiko: sehr hoch
Nichtklassifizierte Information		Zugang/Zugriff schützen	Schützen + Verschlüsseln + Bearbeitung protokollieren	Schützen Verschlüsseln Protokollieren + Nummerieren*
INTERNE Information	Zugang/Zugriff schützen	Schützen	Schützen Verschlüsseln Protokollieren	Schützen Verschlüsseln Protokollieren Nummerieren
VERTRAULICHE Information	Schützen + Verschlüsseln	Schützen Verschlüsseln	Schützen Verschlüsseln Protokollieren	Schützen Verschlüsseln Protokollieren Nummerieren
GEHEIME Information	Schützen Verschlüsseln + Nummerieren*	Schützen Verschlüsseln Nummerieren	Schützen Verschlüsseln Protokollieren Nummerieren	Schützen Verschlüsseln Protokollieren Nummerieren

* Die Nummerierung der Dokumente ist eine Massnahme zum Schutz der Information.

Geringes Risiko: Personendaten, deren Missbrauch in der Regel für die betroffene Person keine besonderen Folgen hat, beispielsweise Name und Vorname oder öffentliche Informationen.

Mittleres Risiko: Personendaten, deren Missbrauch die wirtschaftliche Situation oder die gesellschaftliche Stellung der betroffenen Person beeinträchtigen kann. Dazu gehören beispielsweise Angaben über eine Mieterin oder einen Mieter oder über die beruflichen Verhältnisse einer Person oder auch ein Profiling.

Hohes Risiko: Personendaten, deren Missbrauch zu einer schweren Beeinträchtigung der wirtschaftlichen Situation oder der gesellschaftlichen Stellung führen kann. Dazu gehören besonders schützenswerte Personendaten und Profiling mit hohem Risiko.

Sehr hohes Risiko: «hochsensible» Personendaten, deren Missbrauch das Leben der betroffenen Person gefährden kann. Dazu gehören Adressen von V-Leuten der Polizei, von Zeuginnen und Zeugen in bestimmten Strafverfahren oder von Personen, die aufgrund ihrer Gesinnung oder ihrer religiösen oder politischen Zugehörigkeit bedroht sind.

Arbeitsauftrag

Erarbeitet die technischen und organisatorischen Massnahmen für den in der DSFA bewerteten Datenverarbeitungsvorgang

Ziel: Erarbeitung der technischen und organisatorischen Massnahmen zum in der DSFA bewerteten Datenverarbeitungsvorgang.

Aufgaben:

- Berücksichtigt den [EDÖB-Leitfaden](#), die Informationen aus der DSFA und nutzt ein Format eurer Wahl (Tool, Template, Word, etc.) um die Massnahmen zu erarbeiten.
- Reflektiert, welche Herausforderungen bei der Erarbeitung aufgetreten sind.

Abgabe / Präsentation:

- Ladet die erarbeiteten Massnahmen auf MS Teams hoch.
- Stellt die erarbeiteten Massnahmen und die Herausforderungen kurz vor.

Templates, Leitfäden & Normen

Technische & organisatorische Massnahmen, Privacy by design & default:

- [Leitfaden EDÖB Deutsch/Englisch](#)
- [KI-gestützte Vorlage](#) (DSFA: Teil Massnahmen)
- [EDÖBot](#) (AI Prompts Datenrecht)
- [ISO/IEC 27701](#) (Norm für Datenschutzmanagementsysteme)
- [ISO/IEC 29100](#) (Rahmen für Informations- und Sicherheitstechnologie und Datenschutz)

Privacy by design & default:

- [ISO Standard 31700](#) (Privacy by Design für Consumer Goods (auch für intangible Güter))
- [Privacy by design guideline](#) des Europäischen Datenschutrates

Gliederung

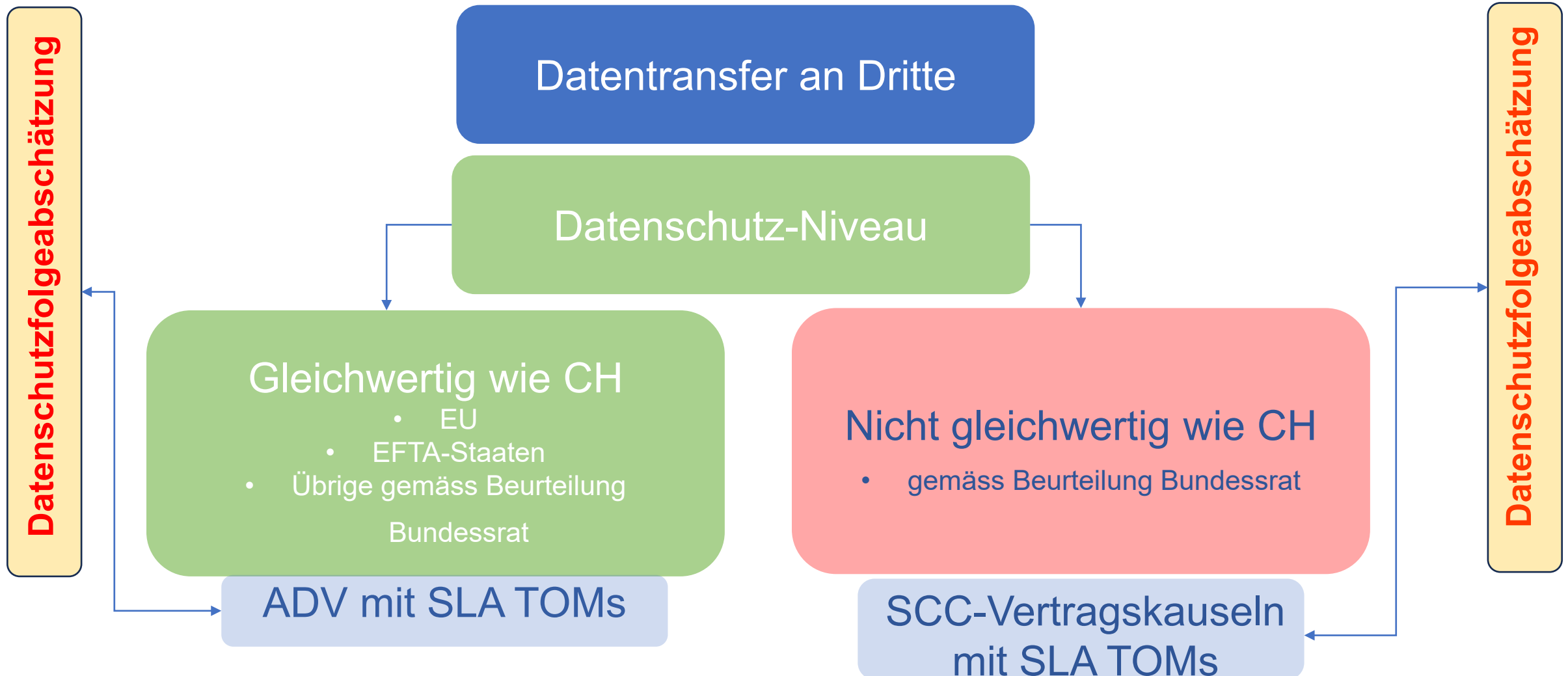
Seminar Datenschutz in der Praxis

- I. Willkommen
- II. Einführung

- | | |
|-----------|---|
| Schritt 1 | Datenschutz-Policy |
| Schritt 2 | Bearbeitungsverzeichnis |
| Schritt 3 | Datenschutz-Folgenabschätzung |
| Schritt 4 | Technische und organisatorische Massnahmen (TOMs) |
| Schritt 5 | Datentransfer |
| Schritt 6 | Web-Präsenz |
| Schritt 7 | Datenschutzprozesse |
| Schritt 8 | Audit |

- III Abschluss

Datentransfer (Datenschutzniveau)



Datentransfer (Auslagerung) an Dritte

Nach dem Schweizer Datenschutzgesetz (revDSG) muss ein Unternehmen einen Auftragsbearbeitungsvertrag (ADV) abschliessen, wenn es personenbezogene Daten von Dritten bearbeiten lässt, z.B. bei Cloud-Diensten oder externer Lohnbuchhaltung.

Dieser Vertrag regelt die datenschutzkonforme Verarbeitung durch den beauftragten Dritten, der als Auftragsbearbeiter fungiert, und muss sicherstellen, dass die Daten nach den Vorgaben des revDSG behandelt werden. Fehlt dieser Vertrag, kann dies nach dem revDSG eine Busse nach sich ziehen. 

Art. 9 nDSG

Art. 9 Bearbeitung durch Auftragsbearbeiter

¹ Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

- a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte;
und
- b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

² Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

³ Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

⁴ Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

Auftragsverarbeiter

Art. 4 § 8 DSGVO / Art. 5 Lit. k und Art. 9 nDSG

- **Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,
- welche die personenbezogenen Daten
- im Auftrag des Verantwortlichen
- verarbeitet.

Es ist der Dritte, der im Auftrag des Verantwortlichen personenbezogene Daten wo auch immer verarbeitet.

Er kommt in eine neue umfassende Mitverantwortung im Rahmen des Datenschutzes

Der **Verantwortliche** muss den **Auftragsverarbeiter** kontrollieren (**Joint Controllingship**)

Der Auftrag und die Auflagen (TOMs) müssen durchgesetzt werden können, auch im Ausland

Art. 28 (1) DSGVO / 9 nDSG

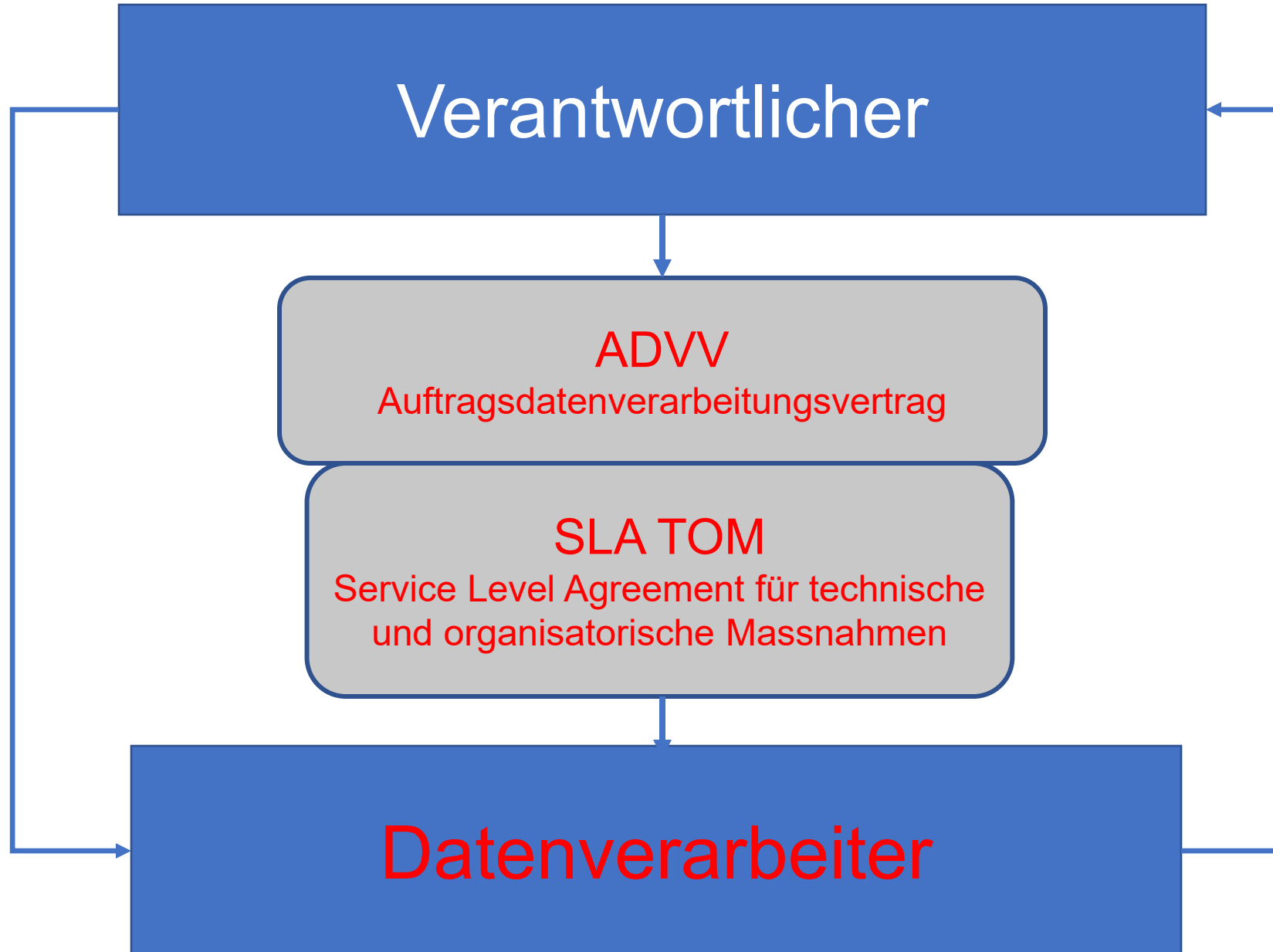
Zusammenarbeit mit Auftragsverarbeiter

Erfolgt eine **Verarbeitung** im Auftrag eines **Verantwortlichen**, so arbeitet dieser **nur mit Auftragsverarbeitern** zusammen,

- die **hinreichende Garantien** dafür bieten,
- dass **geeignete technische und organisatorische Massnahmen** so durchgeführt werden,
- dass die **Verarbeitung im Einklang mit den Bestimmungen der DSGVO** erfolgt und
- der **Schutz der Rechte der Betroffenen** gewährleistet ist.

Alle Verträge mit Auftragsverarbeitern müssen überprüft und allenfalls angepasst werden.

Wer personenbezogene Daten an beigezogene Service-Provider auslagert, **muss einen Auftragsdatenverarbeitungsvertrag (ADV) mit einem Service Level Agreement für TOM's (technische und organisatorische Massnahmen – SLA TOM) abschliessen und vorweisen können.**



Art. 28 (2 und 3a-h) DSGVO / 9 nDSG

Zusammenarbeit mit Auftragsverarbeiter

Verantwortlicher braucht (neue) **Verträge** (ausdrücklich in Art. 28 Abs. 3 DSGVO) mit **Auftragsverarbeiter**, welche

- im Detail die aus der Datenschutz-Folgeabschätzung abgeleiteten organisatorischen oder technischen **Massnahmen vertraglich überbinden**,
- **Selber notwendige und aktuelle Massnahmen sicherstellt**,
- Gegenstand und Dauer der Verarbeitung regelt (3),
- Art und Zweck der Verarbeitung regelt (3),
- Nur auf dokumentierte Weisung verarbeitet (3a),
- Bearbeitende Personen zur Vertraulichkeit verpflichtet werden (3b),
- Art der personenbezogenen Daten festlegt (3),
- Kategorien betroffener Personen festlegt (3),
- die **Rechte und Pflichten des Auftragsverarbeiters** dafür **statuiert**,
- **die Service Levels** für die Massnahmen **definiert**,
- die **Gewährleistung** des Auftragsverarbeiters **festlegt**,
- die **Informationspflichten** bei Verletzungen regelt,
- die **Haftung** des Auftragsverarbeiters **definiert**,
- ein **jederzeitiges Auditrecht** (Kontrollrecht bez. Einhaltung der vertraglichen Auflagen) **sicherstellt**.

Art. 28 (4) DSGVO / **9 nDSG**

Zusammenarbeit mit Auftragsverarbeiter - Drittbeizug

Zieht der Auftragsverarbeiter seinerseits

Dritte für die Verarbeitung

von personenbezogenen Daten bei, muss er diesem

- mittels schriftlichem Vertrag
- dieselben Schutzpflichten auferlegen, die er gemäss Vertrag mit dem Verantwortlichen übernommen hat.

Schriftliche Verträge = kann auch in elektronischem Format (aber rechtsverbindlich) erfolgen

- prüfen ob qualifizierte digitale Signaturen für eigenhändige Unterschriften notwendig sind (Achtung: Behörden- und Unternehmenssiegel sind keine qualifizierten eigenhändigen Unterschriften QES) - Validator des Bundes
- Im Handelsregister eingetragene Personen müssen unterzeichnen (Achtung Kollektivunterschriften beachten)



Dokument validieren

Anleitung zum
Validator

Informationen zur
elektronischen
Signatur

Dokument validieren

Hier können elektronisch signierte Dokumente geprüft werden. Falls der Signatur von berechtigter Stelle eine amtliche Funktion zugeordnet ist, so wird diese angezeigt.

1

Dokument uploaden



Bitte ziehen Sie Ihr Dokument in dieses Fenster oder klicken Sie hier und wählen Sie eine elektronisch signierte Datei aus, die Sie überprüfen möchten.

Erlaubte Dokumente .pdf / .xml

> Datenschutzerklärung, Informationsschutz und Wahrung von Berufs- oder Amtsgeheimnissen
Erklärung zum Datenschutz

2

Einzelheiten zum Prüfer

Hier können Sie optional Ihre Angaben als prüfende Person angeben. Diese erscheinen dann auf dem Prüfbericht.



Die Eingabe dieser Informationen ist nicht Teil des Validierungsprozesses und unterliegt weder einer Überprüfung noch einer Bestätigung.

Name

(Fakultativ)

Organisation

(Fakultativ)

<https://www.validator.admin.ch>

Bekanntgabe Personendaten ins Ausland

3. Abschnitt: Bekanntgabe von Personendaten ins Ausland

Art. 16 Grundsätze

¹ Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.

² Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch:

- a. einen völkerrechtlichen Vertrag;
- b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden;
- c. spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat;
- d. Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat; oder
- e. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden.

³ Der Bundesrat kann andere geeignete Garantien im Sinne von Absatz 2 vorsehen.

Bekanntgabe Personendaten ins Ausland

235.1

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020 (Stand am 7. Juli 2025)

Art. 17 Ausnahmen

¹ Abweichend von Artikel 16 Absätze 1 und 2 dürfen in den folgenden Fällen Personendaten ins Ausland bekanntgegeben werden:

- a. Die betroffene Person hat ausdrücklich in die Bekanntgabe eingewilligt.
- b. Die Bekanntgabe steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags:
 1. zwischen dem Verantwortlichen und der betroffenen Person; oder
 2. zwischen dem Verantwortlichen und seiner Vertragspartnerin oder seinem Vertragspartner im Interesse der betroffenen Person.
- c. Die Bekanntgabe ist notwendig für:
 1. die Wahrung eines überwiegenden öffentlichen Interesses; oder
 2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde.
- d. Die Bekanntgabe ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Eidgenössischer Datenschutz- und
Öffentlichkeitsbeauftragter (EDÖB)**



Aktuell	Datenschutz	Öffentlichkeitsprinzip	Dokumentation	Der EDÖB	
	▼	▼	▼		

[Startseite](#) > [Datenschutz](#) > [Handel und Wirtschaft](#) > Übermittlung ins Ausland

< [Handel und Wirtschaft](#)

Übermittlung ins Ausland

USA - Privacy Shield

Outsourcing

Datenweitergabe an
ausländische Behörden

Übermittlung ins Ausland



- ✓ Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug
- ✓ Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge
- ✓ Standardvertragsklauseln (SCC)
- ✓ Weitere Informationen

Das schweizerische Datenschutzgesetz gewährleistet den Schutz der Privatsphäre für Datenbearbeitungen, die von Personen in der Schweiz vorgenommen werden. Wenn aber Daten ins Ausland

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizraEidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandsbezug (nach Art. 16 Abs. 2 lit. b und d DSG)

(veröffentlicht Juni 2021; angepasst an das revidierte DSG Mai 2023)

1. Zweck der Anleitung

Die vorliegende Anleitung soll Datenbearbeitern die Prüfung der Zulässigkeit von Datenübermittlungen von personenbezogenen Daten ins Ausland erleichtern.

Anhand eines Schemas erläutert diese Anleitung den Anwendungsfall des Datentransfers ins Ausland nach Art. 16 Abs. 2 lit. b DSG, wenn dort eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet, und dieser Mangel durch Datenschutzklauseln in einem Vertrag oder Standarddatenschutzklauseln kompensiert werden muss (vgl. auch Art. 9 Abs. 3 der Verordnung zum Bundesgesetz über den Datenschutz DSV, vom 31. August 2022, SR. 235.11). Auf die Voraussetzungen nach lit. a, c und e und Art. 17 wird in dieser Anleitung nicht eingegangen.

Beilage:

„Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf Standarddatenschutzklauseln nach Art. 16 Abs. 2 lit. d DSG» in den Unterlagen.

Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau
gestützt auf anerkannte Standardvertragsklauseln und Musterverträge

27. August 2021

vom 31. August 2022 (Stand am 1. Januar 2024)

Art. 8 Beurteilung der Angemessenheit des Datenschutzes eines Staates, eines Gebiets, eines spezifischen Sektors in einem Staat oder eines internationalen Organs

¹ Die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz werden **in Anhang 1 aufgeführt.**

Datenschutzverordnung

235.11

Anhang 1
(Art. 8 Abs. 1)

Staaten, Gebiete, spezifische Sektoren in einem Staat und internationale Organe mit einem angemessenen Datenschutz

- 1 Deutschland*
- 2 Andorra***
- 3 Argentinien***
- 4 Österreich*
- 5 Belgien*
- 6 Bulgarien***

- * Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten nach der Richtlinie (EU) 2016/680⁷ mit ein.
- ** Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten gemäss einem Durchführungsbeschluss der Europäischen Kommission, mit welchem die Angemessenheit des Datenschutzes nach der Richtlinie (EU) 2016/680 festgestellt wird, mit ein.
- *** Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten im Rahmen der von der Richtlinie (EU) 2016/680 vorgesehenen Zusammenarbeit nicht mit ein.

- | | | | |
|----|----------------|----|-----------------------------|
| 8 | Zypern*** | 24 | Italien* |
| 9 | Kroatien*** | 25 | Jersey*** |
| 10 | Dänemark* | 26 | Lettland* |
| 11 | Spanien* | 27 | Liechtenstein* |
| 12 | Estland* | 28 | Litauen* |
| 13 | Finnland* | 29 | Luxemburg* |
| 14 | Frankreich* | 30 | Malta* |
| 15 | Gibraltar*** | 31 | Monaco*** |
| 16 | Griechenland* | 32 | Norwegen* |
| 17 | Guernsey*** | 33 | Neuseeland*** |
| 18 | Ungarn* | 34 | Niederlande* |
| 19 | Isle of Man*** | 35 | Polen* |
| 20 | Färöer*** | 36 | Portugal* |
| 21 | Irland*** | 37 | Tschechien* |
| 22 | Island* | 38 | Rumänien*** |
| 23 | Israel*** | 39 | Vereinigtes
Königreich** |

Art. 10 Standarddatenschutzklauseln

¹ Gibt der Verantwortliche oder der Auftragsbearbeiter Personendaten mittels Standarddatenschutzklauseln nach Artikel 16 Absatz 2 Buchstabe d DSG ins Ausland bekannt, so trifft er angemessene Massnahmen, um sicherzustellen, dass die Empfängerin oder der Empfänger diese beachtet.

² Der EDÖB veröffentlicht eine Liste von Standarddatenschutzklauseln, die er genehmigt, ausgestellt oder anerkannt hat. Er teilt das Ergebnis der Prüfung der Standarddatenschutzklauseln, die ihm unterbreitet werden, innerhalb von 90 Tagen mit.

ANHANG I

A. LISTE DER PARTEIEN

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

Datenexporteur(e): [Name und Kontaktdaten des Datenexporteurs/der Datenexporteure und gegebenenfalls seines/ihrer Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union]

1. Name:

Anschrift:

Name, Funktion und Kontaktdaten der Kontaktperson:

Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind:

Unterschrift und Datum:

Rolle (Verantwortlicher/Auftragsverarbeiter):

2.

Datenimporteur(e): [Name und Kontaktdaten des Datenexporteurs/der Datenimporteure, einschließlich jeder für den Datenschutz zuständigen Kontaktperson]

1. Name:

Anschrift:

<https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914>

Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer

Page contents

- Einzelheiten
- Beschreibung
- Dateien

Einzelheiten

Datum der Veröffentlichung 4. Juni 2021

Autor [Generaldirektion Justiz und Verbraucher](#)

Beteiligte dienststelle [Generaldirektion Justiz und Verbraucher](#)

Beschreibung

Haftungsausschluss: Diese Texte sind endgültige Arbeitsdokumente. Der einzige offizielle Text wird in den kommenden Tagen im Amtsblatt veröffentlicht.

[DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung \(EU\) 2016/679](#)

Dateien

Standard Contractual Clauses for controllers and processors in the EU/EEA

25. MAI 2022

Standard contractual clauses for controllers and processors in the EU/EEA (Word)

English
(3.25 MB - ZIP)

[Herunterladen](#)

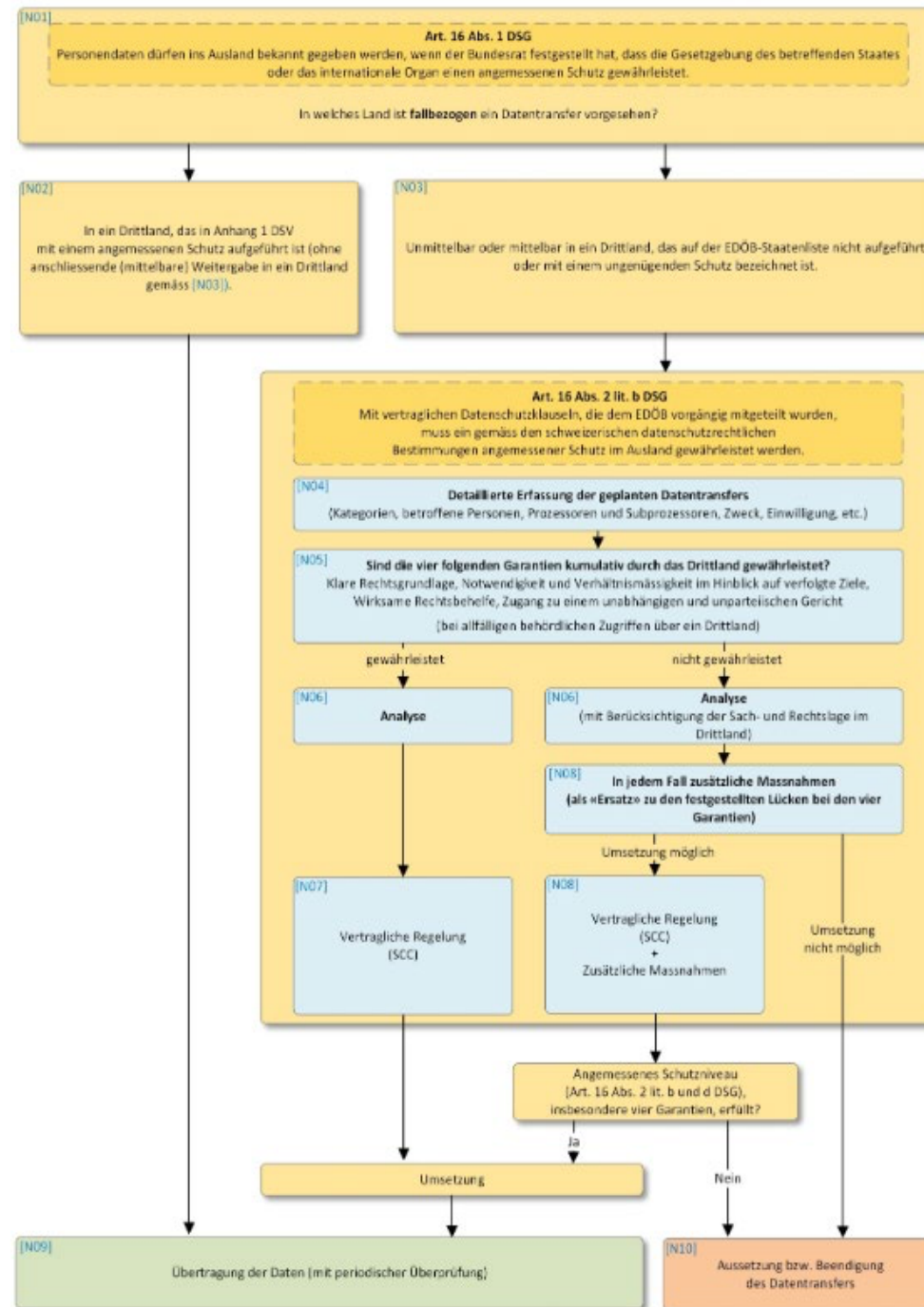
4. JUNI 2021

Commission Implementing Decision on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725

English
(314.16 KB - HTML)

[Herunterladen](#)

https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_de



SEPOS: Standardbestimmungen Informationssicherheit in Beschaffungsverträgen

Die Fachstelle des Bundes für Informationssicherheit im Staatssekretariat für Sicherheitspolitik

SEPOS hat im Auftrag des Bundesrats **Standardbestimmungen für die Informationssicherheit für**

Beschaffungsverträge veröffentlicht, um die Informationssicherheit des Bundes zu erhöhen und Datenabflüsse bei Lieferanten zu verhindern (die **Lehren** aus **Xplain** waren leitend).

Die Standardbestimmungen verstehen sich als **Empfehlung** an die Bedarfs- und Beschaffungsstellen des Bundes und sind per **1. Januar 2026** wirksam.

Zur konkreten Anwendung enthält das Dokument mit **Leitfaden und Kommentare Standardbestimmungen** eine verschachtelte Prüfreihefolge, die eine Kombination aus AGB und Standardbestimmungen empfiehlt, je nach Sensitivität der vom Dienstleister bearbeiteten Informationen, nach Art und Delivery der Dienstleistung und nach dem Personenbezug bearbeiteter Daten.

https://datenrecht.ch/sepos-standardbestimmungen-informationssicherheit-in-beschaffungsvertraegen/?utm_source=datenrecht&utm_campaign=13296bf40b-datenrecht-Mailchimp&utm_medium=email&utm_term=0_15155ce73b-13296bf40b-90792857

Standardbestimmungen Informationssicherheit in Beschaffungsverträgen (2)

Sie **ergänzen die AGB des Bundes** (siehe [hier](#)) und umfassen die folgenden Bestimmungen:

- H1 Standardbestimmung ohne Bezug zu Informatikmitteln des Bundes mit Abgabe von Bundesgeräten
- H2 Standardbestimmung ohne Bezug zu Informatikmitteln des Bundes ohne Abgabe von Bundesgeräten
- I1 Standardbestimmung mit Bezug zu Informatikmitteln des Bundes (Verwaltung, Wartung, Überprüfung) mit Abgabe von Bundesgeräten
- I2 Standardbestimmung mit Bezug zu Informatikmitteln des Bundes (Verwaltung, Wartung, Überprüfung) ohne Abgabe von Bundesgeräten
- J Standardbestimmung mit Bezug zu Informatikmitteln des Bundes (Betrieb)

Aufgabe

A1:

Erstelle mir einen gesetzeskonformen nach schweizerischem Datenschutzgesetz konformen Auftragsdatenverarbeitungsvertrag zwischen Xplain und den Bundesbehörden, welche an diese Unternehmung besonders schützenswerte Personendaten übertragen haben. Dabei ist folgender Sachverhalt in die Formulierung des Vertrages einzubeziehen.

A2: Wie sieht der Auslagerungsvertrag aus, wenn Xplain ihren Sitz in Vietnam hätte?

Schlussbericht und Empfehlungen

vom 25. April 2024

des

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten
(EDÖB)

in Sachen Xplain AG

aufgrund Ransomware-Vorfall

gemäss

Artikel 29 des Bundesgesetzes vom 19. Juni 1992
über den Datenschutz (aDSG) in Verbindung mit Artikel 70 Bundesgesetz vom
25. September 2020 über den Datenschutz (DSG)

Homework 😊

Aufgabe bis zur nächsten Woche

1.Tools-Liste:

Ergänzen Sie unsere gemeinsame Liste mit Tools, die Sie kennen.
Pro Tool nur: **Name – kurze Beschreibung – Link.**

2.Website-Check:

Prüfen Sie Ihren eigenen Webauftritt und notieren Sie mindestens drei mögliche Datenschutz-Herausforderungen.

3.Datenschutz-Audit:

Finden Sie heraus, ob in Ihrer Organisation schon ein Audit durchgeführt wurde. Falls ja: wie?
Falls nein: überlegen Sie, wie eines aussehen könnte.

Gliederung

Seminar Datenschutz in der Praxis

- I. Willkommen
- II. Einführung

- | | |
|-----------|---|
| Schritt 1 | Datenschutz-Policy |
| Schritt 2 | Bearbeitungsverzeichnis |
| Schritt 3 | Datenschutz-Folgenabschätzung |
| Schritt 4 | Technische und organisatorische Massnahmen (TOMs) |
| Schritt 5 | Datentransfer |
| Schritt 6 | Web-Präsenz |
| Schritt 7 | Datenschutzprozesse |
| Schritt 8 | Audit |

- III Abschluss

Informationspflichten – Web – Datenschutzerklärung DSE

3. Kapitel: Pflichten des Verantwortlichen und des Auftragsbearbeiters

Art. 19 Informationspflicht bei der Beschaffung von Personendaten

¹ Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

² Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; er teilt ihr mindestens mit:

- a. die Identität und die Kontaktdaten des Verantwortlichen;
- b. den Bearbeitungszweck;
- c. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

Informationen bei Web-Auftritten

Nach dem Schweizer Datenschutzgesetz (DSG) müssen Unternehmen auf ihrem Webauftritt eine Datenschutzerklärung veröffentlichen, die über die Identität des Verantwortlichen, die bearbeiteten Personendaten, die Bearbeitungszwecke, die Aufbewahrungsdauer und gegebenenfalls den Datenexport ins Ausland informiert. Zusätzlich ist ein Impressum mit vollständigem Namen/Firmennamen, einer ladungsfähigen Adresse und einer E-Mail-Adresse erforderlich, um die Identität des Verantwortlichen für Besucher transparent zu machen. 

Quelle: GOOGLE AI Overview – Abfrage am 30.09.2025

Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien

22. Januar 2025

mit Ergänzung vom 6. Oktober 2025

Version	Datum	Beschreibung
1.0	22.01.2025	Erste finalisierte Version
1.1	06.10.2025	Ergänzung Fussnote 5, Ergänzung eines Satzes im Absatz 3 in Ziff. 3.1.2, Ergänzung im letzten Satz von Ziff. 3.2.2, Präzisierende Ergänzungen und Anpassungen in Ziff. 3.5.2, Präzisierende Ergänzungen in Ziff. 3.6, Ergänzung in Ziffer 3.8.1, Ergänzung eines Verweises im letztem Satz des ersten Absatzes in Ziff. 3.9, Präzisierende Ergänzungen in Ziff. 3.10.1, Ergänzungen und Präzisierung in Ziff. 3.11.1, Präzisierung erster Satz in Ziff. 3.11.3 betr. eingebettete Dritte, Ergänzung eines zweiten Absatzes in Ziff. 3.12.3, Präzisierung in Ziff. 3.12.4. betreffend Gratisdienstleistungen und Cookie Paywalls.

Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien

Insbesondere fand es der EDÖB nützlich zu verdeutlichen, warum der Einsatz von Cookies zum Zwecke der Zustellung von personalisierter Werbung unter Umständen die Einwilligung der betroffenen Personen erfordert. So, wenn der Webseitenbetreiber mittels Einbindung von Third-Party-Cookies oder ähnlicher Technologien Dritten Zugang zu personenbezogenen Informationen der Besuchenden gegen Entgelt verschafft und diese Dritten in mehrere Webseiten eingebettet sind. Da Letztere somit in die Lage versetzt werden, ein Profiling mit hohem Risiko durchzuführen, stellt dies einen besonders intensiven Eingriff in die Persönlichkeit der betroffenen Personen dar.

Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien

Auch brachte der EDÖB **Ergänzungen zum Thema der Erhebung von Standortdaten vor** – einer Datenbearbeitung, die sehr verbreitet ist und besondere Risiken mit sich bringt: Sie begünstigt einerseits die Bestimmbarkeit der realen Identität eines Onlinenutzers (zum Beispiel indem rekonstruiert werden kann, wo sich ein Gerät während der Nacht bzw. Schlafenszeit befindet, oder an welchen Adressen es sich an Werktagen regelmässig befindet). Andererseits eröffnen **Standortdaten die Möglichkeit, Rückschlüsse über wesentliche Aspekte der Persönlichkeit der Nutzer zu ziehen. Ein Profiling, das sich auf Standortdaten stützt, stellt somit oft ein Profiling mit hohem Risiko dar.**

Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien

Weiter thematisiert die aktualisierte Fassung des Leitfadens den Einsatz von sog.

Cookie-Paywalls. Sie legt dar, ob und unter welchen Umständen eine Einwilligung rechtsgültig erteilt werden kann, wenn die betroffene Person vor die Wahl gestellt wird, ihre Einwilligung zu erteilen oder ein bezahltes Abonnement abzuschliessen.

Datenschutzerklärung

Datenschutzerklärung

Eine Datenschutzerklärung ist notwendig, sobald personenbezogene Daten erhoben und verarbeitet werden, beispielsweise über ein Kontaktformular oder Analyse-Tools.

Sie muss folgende Informationen enthalten: ⓘ

- **Identität und Kontaktdaten des Verantwortlichen:** Wer ist für die Datenbearbeitung zuständig? ⓘ
- **Bearbeitungszwecke:** Zu welchen Zwecken werden Personendaten gesammelt und bearbeitet? ⓘ
- **Bearbeitete Personendaten:** Welche Arten von Personendaten werden gesammelt? ⓘ
- **Aufbewahrungsdauer:** Wie lange werden die Daten gespeichert oder welche Kriterien legen die Dauer fest? ⓘ
- **Empfänger der Daten:** Wer erhält die Daten, und an welche Länder werden sie weitergegeben? ⓘ
- **Automatisierte Entscheidungen:** Falls zutreffend, Informationen über automatisierte Entscheidungen und die zugrundeliegende Logik. ⓘ

Quelle: <https://www.edoeb.admin.ch/de/datenschutzerklaerungen-im-internet>

Leitfaden EDÖB

Aufgabe

Erstelle mittels einer frei wählbaren KI-Plattform eine Datenschutzerklärung für den Webshop von www.brack.ch

Binde die Ergebnisse des Web-Scans mit den Feststellungen über die eingesetzten Cookies und Tools sauber und detailliert in die Datenschutzerklärung ein.

Gliederung

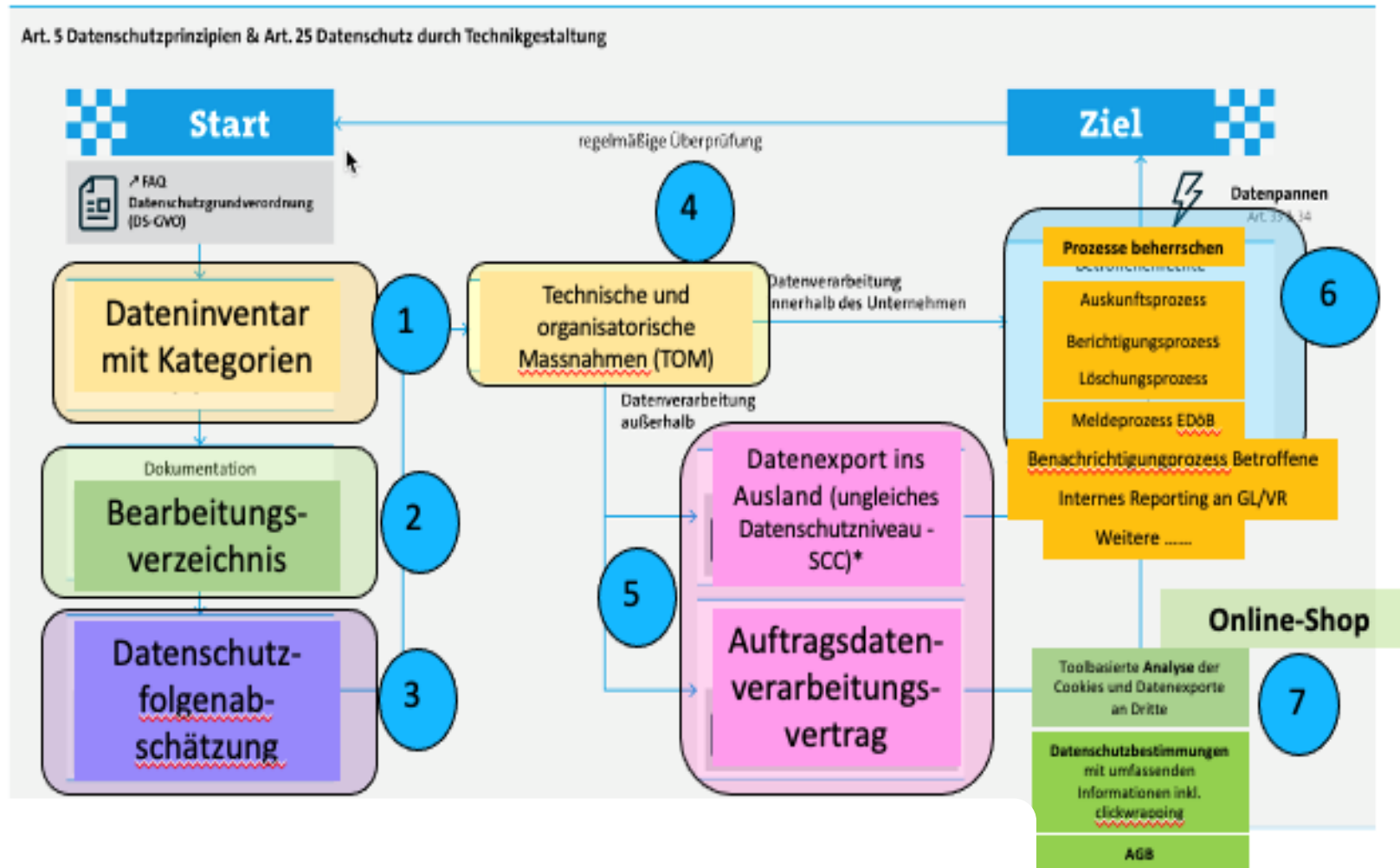
Seminar Datenschutz in der Praxis

- I. Willkommen
- II. Einführung

- | | |
|-----------|---|
| Schritt 1 | Datenschutz-Policy |
| Schritt 2 | Bearbeitungsverzeichnis |
| Schritt 3 | Datenschutz-Folgenabschätzung |
| Schritt 4 | Technische und organisatorische Massnahmen (TOMs) |
| Schritt 5 | Datentransfer |
| Schritt 6 | Web-Präsenz |
| Schritt 7 | Datenschutzprozesse |
| Schritt 8 | Audit |

- III Abschluss

Wesentliche Datenschutzprozesse



Auskunftsbegehren

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

235.1

vom 25. September 2020 (Stand am 7. Juli 2025)

4. Kapitel: Rechte der betroffenen Person

Art. 25 Auskunftsrecht

¹ Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

235.1

vom 25. September 2020 (Stand am 7. Juli 2025)

² Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt:

- a. die Identität und die Kontaktdaten des Verantwortlichen;
- b. die bearbeiteten Personendaten als solche;
- c. der Bearbeitungszweck;
- d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer;
- e. die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden;
- f. gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht;
- g. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden, sowie die Informationen nach Artikel 19 Absatz 4.

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020 (Stand am 7. Juli 2025)

- ³ Personendaten über die Gesundheit können der betroffenen Person mit ihrer Einwilligung durch eine von ihr bezeichnete Gesundheitsfachperson mitgeteilt werden.
- ⁴ Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig.
- ⁵ Niemand kann im Voraus auf das Auskunftsrecht verzichten.
- ⁶ Der Verantwortliche muss kostenlos Auskunft erteilen. Der Bundesrat kann Ausnahmen vorsehen, namentlich wenn der Aufwand unverhältnismässig ist.
- ⁷ Die Auskunft wird in der Regel innerhalb von 30 Tagen erteilt.

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020 (Stand am 7. Juli 2025)

Art. 26 Einschränkungen des Auskunftsrechts

¹ Der Verantwortliche kann die Auskunft verweigern, einschränken oder aufschieben, wenn:

- a. ein Gesetz im formellen Sinn dies vorsieht, namentlich um ein Berufsgeheimnis zu schützen;
- b. dies aufgrund überwiegender Interessen Dritter erforderlich ist; oder
- c. das Auskunftsgesuch offensichtlich unbegründet ist, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist.

**Verordnung
über den Datenschutz
(Datenschutzverordnung, DSV)**

vom 31. August 2022

3. Kapitel: Rechte der betroffenen Person

1. Abschnitt: Auskunftsrecht

Art. 16 Modalitäten

¹ Wer vom Verantwortlichen Auskunft darüber verlangt, ob Personendaten über sie oder ihn bearbeitet werden, muss dies schriftlich tun. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich mitgeteilt werden.

² Die Auskunftserteilung erfolgt schriftlich oder in der Form, in der die Daten vorliegen. Im Einvernehmen mit dem Verantwortlichen kann die betroffene Person ihre Daten an Ort und Stelle einsehen. Die Auskunft kann mündlich erteilt werden, wenn die betroffene Person einverstanden ist.

³ Das Auskunftsbegehren und die Auskunftserteilung können auf elektronischem Weg erfolgen.

⁴ Die Auskunft muss der betroffenen Person in einer verständlichen Form erteilt werden.

⁵ Der Verantwortliche muss angemessene Massnahmen treffen, um die betroffene Person zu identifizieren. Diese ist zur Mitwirkung verpflichtet.

**Verordnung
über den Datenschutz
(Datenschutzverordnung, DSV)**

vom 31. August 2022

Art. 18 Frist

- ¹ Die Auskunft muss innerhalb von 30 Tagen seit dem Eingang des Begehrens erteilt werden.**
- ² Kann die Auskunft nicht innerhalb von 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber informieren und ihr mitteilen, innerhalb welcher Frist die Auskunft erfolgt.**
- ³ Verweigert der Verantwortliche die Auskunft, schränkt er sie ein oder schiebt er sie auf, so muss er dies innerhalb derselben Frist mitteilen.**

**Verordnung
über den Datenschutz
(Datenschutzverordnung, DSV)**

vom 31. August 2022

Art. 19 Ausnahme von der Kostenlosigkeit

- ¹ Ist die Erteilung der Auskunft mit einem unverhältnismässigen Aufwand verbunden, so kann der Verantwortliche von der betroffenen Person verlangen, dass sie sich an den Kosten angemessen beteiligt.
- ² Die Beteiligung beträgt maximal 300 Franken.
- ³ Der Verantwortliche muss der betroffenen Person die Höhe der Beteiligung vor der Auskunftserteilung mitteilen. Bestätigt die betroffene Person das Gesuch nicht innerhalb von zehn Tagen, so gilt es als ohne Kostenfolge zurückgezogen. Die Frist nach Artikel 18 Absatz 1 beginnt nach Ablauf der zehntägigen Bedenkzeit zu laufen.

Aufgabe

- A1 Erstelle mit Hilfe einer KI-Plattform die einzelnen Aktivitäten, welche im Rahmen einer Auskunftserteilung nach schweizerischem Datenschutzgesetz durch den Verantwortlichen zur Erfüllung seiner Auskunftspflichten nach Art. 25 und 26 nDSG zu durchlaufen sind.
- A2 Wenn möglich, erstelle dazu eine Prozessbeschreibung nach einem standardisierten BPM-Modell (zB: Business Process Modell and Notation BPMN mit Verweis auf eCH-Standards 0074, 0158 und 0242; Event driven process chain EPC; Unified Modeling Language UML etc.)

Gliederung

Seminar Datenschutz in der Praxis

- I. Willkommen
- II. Einführung

- | | |
|-----------|---|
| Schritt 1 | Datenschutz-Policy |
| Schritt 2 | Bearbeitungsverzeichnis |
| Schritt 3 | Datenschutz-Folgenabschätzung |
| Schritt 4 | Technische und organisatorische Massnahmen (TOMs) |
| Schritt 5 | Datentransfer |
| Schritt 6 | Web-Präsenz |
| Schritt 7 | Datenschutzprozesse |
| Schritt 8 | Audit |

- III Abschluss

Der Begriff des Audits

Schritt 8 der Datenschutz-Roadmap

lat. „audire“ = „hören“

Ein Audit ist eine systematische und objektive (unabhängige) Überprüfung, mit der festgestellt wird, ob Prozesse, Produkte oder Managementsysteme bestimmte Anforderungen erfüllen.

- Sicherstellung der Einhaltung: Normen, gesetzliche Vorgaben oder interne Richtlinien werden geprüft.
- Transparenz: Prozesse und Abläufe werden nachvollziehbar dargestellt.
- Optimierung: Schwachstellen werden identifiziert, Maßnahmen zur Verbesserung angestoßen.
- Vertrauen: Kunden und Partner erhalten durch Audits Nachweise über Qualität und Verlässlichkeit

<https://www.haufe-akademie.de/blog/glossar/audit/>

Pflicht zu Audit oder Überprüfung (1/2)

Schritt 8 der Datenschutz-Roadmap

Schweiz → Überprüfungspflichten

- **DSG, Art. 5:** Datenschutzgrundsätze – Nachweis, dass diese eingehalten werden.
- **DSG, Art. 8:** Verantwortliche müssen technische und organisatorische Maßnahmen (TOMs) nach dem Stand der Technik umsetzen und deren Wirksamkeit regelmässig überprüfen.
- **OR:** Sorgfaltspflichten und Verantwortung; Führung eines IKS.
→ siehe Folien im Kapitel Einleitung.

Fazit: Schweizer Recht schreibt keine expliziten „Audits“ vor, verlangt aber regelmäßige Überprüfung & Nachweisbarkeit.

Pflicht zu Audit oder Überprüfung (2/2)

Schritt 8 der Datenschutz-Roadmap

EU → Überprüfungs- & Überwachungspflicht (zusätzl. zu Grundsätzen)

- DSGVO, Art. 24: Verantwortliche müssen Nachweis dafür erbringen können, dass die Verarbeitung (von Personendaten) gemäß der DSGVO erfolgt.
- DSGVO, Art. 28: Auftragsverarbeiter müssen Überprüfungen - auch Inspektionen - ermöglichen.
- DSGVO, Art. 32: «Genehmigte Verhaltensregeln oder Zertifizierungsverfahren» können herangezogen werden, um geeignete TOMs nachzuweisen.
- DSGVO, Art. 39: Datenschutzbeauftragter überwacht Einhaltung der DSGVO.

Fazit: Audits nicht explizit als Begriff genannt, aber inhaltlich beschrieben.

Arten von Audits

Schritt 8 der Datenschutz-Roadmap

Intern

- Von der Organisation selbst durchgeführt.
 - Dienen der Selbstkontrolle & kontinuierlichen Verbesserung.
 - Oft Teil von Compliance- oder Qualitätsmanagement.
- Prüfung und Aktualisieren der Schritte unserer Roadmap.
- Datenschutz-Compliance ist eine fortlaufende Aufgabe

Extern

- Durch unabhängige Dritte (z.B. Zertifizierungsstellen, Datenschutz- oder IT-Sicherheitsfirmen).
 - Höhere Glaubwürdigkeit gegenüber Kunden, Partnern, Aufsichtsbehörden.
 - Grundlage für Zertifizierungen.
- Prüfung entlang der Datenkette (Verantwortlicher, Auftragsverarbeiter, deren Auftragsverarbeiter,...)

Auswahl an anerkannten Standards/Frameworks

Schritt 8 der Datenschutz-Roadmap

Name	Beschreibung	Fokus	Link
ISO/IEC 27000-Reihe (insb. ISO 27001)	International anerkannte Normenfamilie für Informationssicherheits-Managementsysteme (ISMS).	Cybersicherheit	ISO 27000 Overview
ISO/IEC 27701	Erweiterung der ISO 27001/27002 für Datenschutz-Managementsysteme (PIMS).	Datenschutz	ISO 27701 Overview
IKT-Minimalstandard (Schweiz)	Vorgaben des Bundes für Mindestmaßnahmen zur Cybersicherheit in Verwaltungen und Unternehmen.	Cybersicherheit	IKT-Minimalstandard Bund
Good Practice Guides (z. B. EDÖB, economiesuisse)	Praxisleitfäden mit konkreten Empfehlungen zur Umsetzung von Datenschutzmaßnahmen.	Datenschutz	EDÖB DSFA-Leitfaden, economiesuisse Datenschutz-Leitfaden

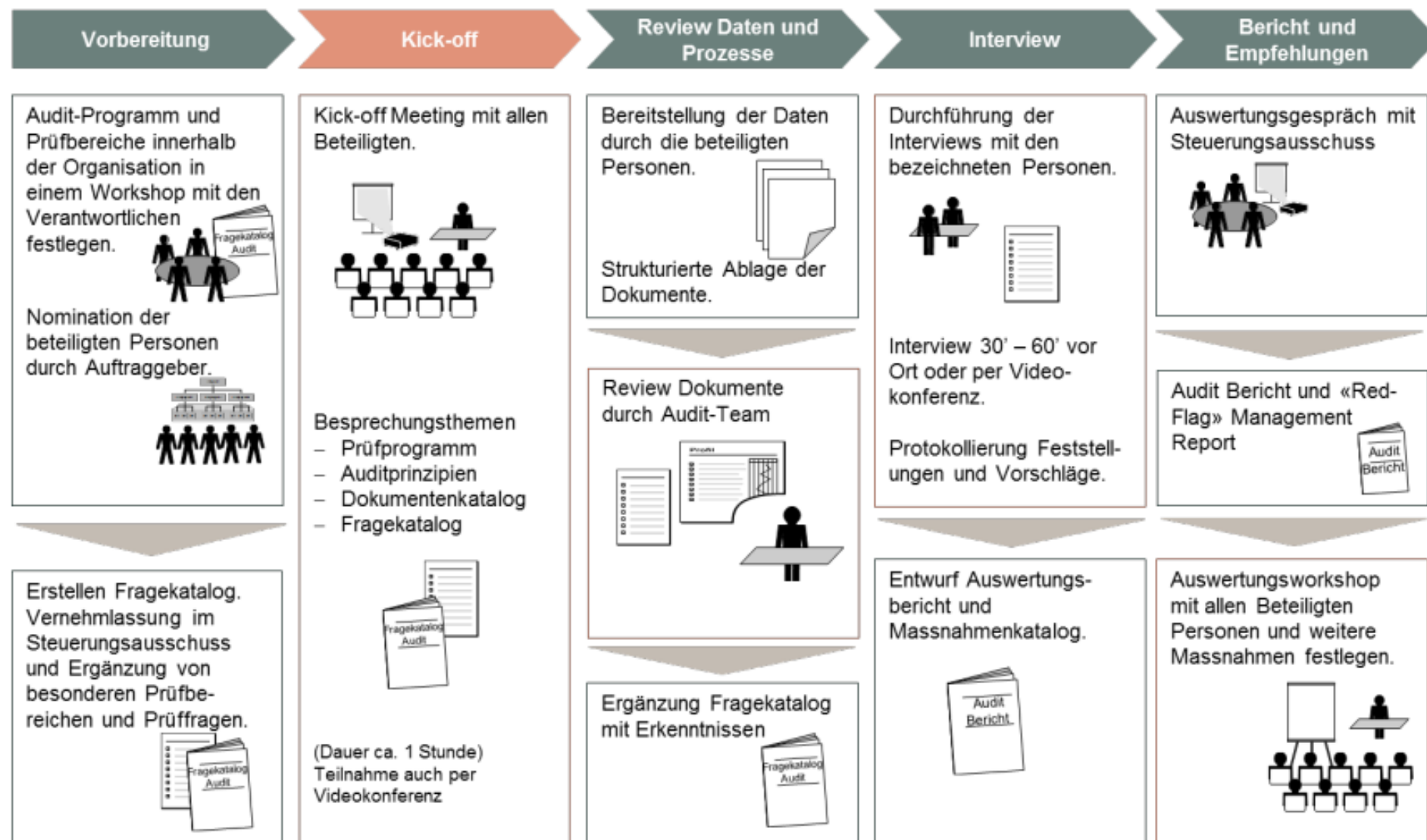
Auswahl an Audit-Institutionen/Anbietern in der Schweiz

Schritt 8 der Datenschutz-Roadmap

Name	Beschreibung	Link
SQS (Swiss Association for Quality and Management Systems)	Bietet die Zertifizierung GoodPriv@cy® an, die Unternehmen für vorbildliche Datenschutzpraktiken und hohe Informationssicherheitsstandards auszeichnet.	SQS GoodPriv@cy®
Private IT-Beratungsunternehmen	Verschiedene private Anbieter mit Fokus auf Cybersecurity, die auch Datenschutzberatung leisten und Audits durchführen; unterstützen Unternehmen bei DSG/DSGVO-Compliance und IT-Sicherheitsmaßnahmen.	Firmenseiten (z.B. GoSecurity, infoSec, InfoGuard, RedGuard usw.)
Datenrecht.ch – AI Prompt Library	Bietet KI-gestützte Tools zur Überprüfung von Datenschutzdokumenten: analysiert Verträge, prüft Datenschutzerklärungen, unterstützt Compliance und Audits nach DSG/DSGVO.	Datenrecht AI Prompts
Swiss Digital Initiative – Digital Trust Label	Stiftung, die Unternehmen mit dem Digital Trust Label auszeichnet; Fokus auf vertrauenswürdige digitale Services, Transparenz, Datenschutz, Sicherheit und ethische Standards.	Swiss Digital Initiative

Audit- Vorgehen in 5 Phasen

https://www.bratschi.ch/assets/content/files/publikationen/Jaehrlicher_Datenschutzaudit_im_Unternehmen_-_Wunsch_oder_Pflicht_-_Markus_Naef_und_Julian_Powell.pdf



Arbeitsauftrag

Erstellt Fragekatalog

Ziel: Erstellt einen Fragekatalog für das Unternehmen eurer Gruppe.

Aufgaben:

- Nutzt ein KI-Tool eurer Wahl (ChatGPT, Gemini,...) um
 - a) die Prüfbereiche festzulegen (welche Bereiche/Themen/Kategorien sollen geprüft werden)
 - b) die Fragen pro Prüfbereich festzulegen (was soll pro Themenbereich gefragt werden).
- Erklärt wie ihr beim Prompting vorgegangen seid, um das Ergebnis zu erzielen.
- Reflektiert, welche Herausforderungen bei der Erstellung aufgetreten sind.

Abgabe / Präsentation:

- Ladet den Fragekatalog auf MS Teams hoch.
- Stellt den Fragekatalog, das Prompting und die Herausforderungen kurz vor.

ggf. Abkürzung: Nehmt direkt die Prüfbereiche von Markus Näf als Input.

https://www.bratschi.ch/assets/content/files/publikationen/Jaehrlicher_Datenschutzaudit_im_Unternehmen_-_Wunsch_oder_Pflicht_-_Markus_Naef_und_Julian_Powel.pdf

Gliederung

Seminar Datenschutz in der Praxis

- I. Willkommen
- II. Einführung

- Schritt 1 Datenschutz-Policy
- Schritt 2 Bearbeitungsverzeichnis
- Schritt 3 Datenschutz-Folgenabschätzung
- Schritt 4 Technische und organisatorische Massnahmen (TOMs)
- Schritt 5 Datentransfer
- Schritt 6 Web-Präsenz
- Schritt 7 Datenschutzprozesse
- Schritt 8 Audit

III Abschluss

Abschluss

Offene Fragerunde

Q&A

Abschluss

Feedback



Danke!

03.11.2025

