ZV-Tagung 2025
Brunnen, 6. November 2025

Öffentliches Personal Schweiz
Impiegati del settore pubblico Svizzera
Employés du secteur public Suisse

KI und Datenschutz – Herausforderungen für die öffentliche Verwaltung

Beat Rudin
ehem. Datenschutzbeauftragter des Kantons Basel-Stadt

KI statt n

ChatGPT 27.10.2025 18:04

Was sage ich Personalverantwortlichen zu den Datenschutzrisiken von KI?

Das ist ein spannendes, aber auch komplexes Thema. Wenn du mit Personalverantwortlichen über die Datenschutz-Herausforderungen von KI sprichst, ist es wichtig, die verschiedenen Aspekte zu berücksichtigen, wie etwa den Umgang mit sensiblen personenbezogenen Daten, Transparenz und rechtliche Anforderungen. Hier sind einige Schlüsselpunkte, die du ansprechen könntest:

1. Sensibilisierung für Datenschutzrisiken

KI-Systeme benötigen oft große Mengen an Daten, um effektiv zu funktionieren. Dies kann die Verarbeitung von personenbezogenen Daten umfassen. Daher müssen Personalverantwortliche sich der Risiken bewusst sein, die mit der Sammlung und Nutzung solcher Daten verbunden sind, wie etwa:

- Datenmissbrauch: KI-Systeme könnten versehentlich oder absichtlich falsche Entscheidungen treffen, die auf unsachgemäß verwendeten oder ungenauen Daten basieren.
- Fehlende Transparenz: KI-Modelle, insbesondere sogenannte "Black Boxes", sind oft schwer zu durchdringen. Dies erschwert die Nachvollziehbarkeit von Entscheidungen, was insbesondere im Hinblick auf den Datenschutz problematisch sein kann.
- Diskriminierung: KI-Algorithmen könnten unbewusst Vorurteile verstärken und bestimmte Personengruppen benachteiligen. Dies ist nicht nur ein ethisches Problem, sondern auch ein datenschutzrechtliches.

Einhalten der Datenschutz-Grundverordnung (DSGVO)

DSGVO legt strenge Anforderungen an die Verarbeitung personenbezogener
Personalverantwortliche sollten darauf achten, dass KI-gestützte Systeme
entsprechen:
und Fairness: Die Datennutzung muss klar und
digen Daten dürfen erfasst und
das Recht, zu

4. Verantwortlichkeit und Aufsicht

Es sollte klar geregelt sein, wer die Verantwortung für den Eins
trägt. Dies bedeutet, dass Personalverantwortliche für die Kontro
über den Einsatz von KI im Unternehmen zuständig sind und sich
dass alle Datenschutzvorgaben eingehalten werden.

Training und Awareness

weiteres wichtiges Thema ist die Schulung der Mitarbeiter im U
n damit verbundenen Datenschutzfragen. Personalverantwortl
llen, dass alle Beteiligten die rechtlichen, ethischen und
tzrechtlichen Implikationen des KI-Einsatzes verstehen.

Was Sie erwartet



«Künstliche Intelligenz»
- Begriff(e)
- Phasen

Datenschutz
- Anwendbares Datenschutzrecht
- Datenschutz-Grundsätze, Pflichten und Rechte
- «allgemeines» und «besonderes (bereichsspezifisches) Datenschutzrecht»

Datenschutzrechtliche Herausforderungen (bei gKI)
- Datenschutz-Grundsätze
- i.d.R. keine Personendaten: Anonymisierung, Pseudonymisierung

Massnahmen,
- für eine (auch datenschutzkonforme) Nutzung der KI

«Künstliche Intelligenz»?



Black Box?

Wikipedia: **«Künstliche Intelligenz»**

> Künstliche Intelligenz (KI) (…) bezeichnet im weitesten Sinne computerbasierte Systeme, die ihre (virtuelle oder reale) Umgebung analysieren können, um daraus relevante Informationen zu abstrahieren, welche sie nutzen, um Entscheidungen zu treffen, die ihre Chance erhöhen, definierte Ziele zu erreichen.
>
> Damit unterscheiden sich KI-gestützte Systeme von regelbasierten Systemen ohne Fähigkeit zur eigenständigen Anpassung ihres Verhaltens, die ausschließlich fest vorgegebene Anweisungen ausführen.

Machine learning. Black Box.

«Generative KI»



Wikipedia: **«Generatives KI-Modell»**

> Der Begriff *generativ* bedeutet bei künstlicher Intelligenz (KI), dass KI-Systeme aus Eingaben mittels generativer Modelle und gespeicherter Lerndaten neue Ergebnisse/Ausgaben wie Texte, Sprachaussagen, Vertonungen, Bilder oder Videos erzeugen. Generative KI-Modelle erlernen Muster und Strukturen vorgängig eingegebener Trainingsdaten und generieren daraus neue Daten mit ähnlichen Eigenschaften. (…)
>
> Ein *generatives Modell* ist ein statistisches Modell der gemeinsamen Wahrscheinlichkeitsverteilung (…)

ZHAW

> Generative KI ist eine Art von künstlicher Intelligenz, die in der Lage ist, neue Daten zu erstellen, die teilweise schwer von menschlichen Inhalten zu unterscheiden sind. Zu den generierten Inhalten zählen zum Beispiel Text, Ton und Bild.

z.B. ChatGPT, Microsoft Copilot, Google Bard, DeepL, Leonardo AI, DALL·E 2, Midjourney …

Phasen der generativen KI (gKI)

Beschaffen von Inhalt für das Training des Modells	**Trainieren** bzw. Aufbau des Modells	**Besitz & Betrieb** des Modells	**Verwenden** des Modells zum Generieren von Output
i.d.R. Anbieter:in evtl. das öffentliche Organ, wenn es selber ein Modell aufbauen will	i.d.R. Anbieter:in evtl. das öffentliche Organ, wenn es selber ein Modell aufbauen will	i.d.R. Anbieter:in evtl. das öffentliche Organ, wenn es selber ein Modell betreibt	**Mitarbeiter:innen des öffentlichen Organs**

Rollenverteilung: Wer hat in welcher Phase welche **Verantwortung**?
Verantwortliche:r: entscheidet über Mittel und Zweck («*controller*»)
Auftragsdatenbearbeiter:in: bearbeitet Daten i.A. der Verantwortlichen («*processor*»)

© 2025 Beat Rudin

Datenschutz?

Datenschutz
ist …



Schutz der Grundrechte der Menschen,
über die wir Daten bearbeiten

Datenschutzrecht?



Datenschutzrecht kommt zum Zug, wenn

jemand	eine Privatperson, ein Bundesorgan, ein kantonales oder kommunales öffentliches Organ
Personendaten	Angaben, die sich auf eine natürliche Person beziehen oder beziehen lassen, wobei diese Person bestimmt oder mindestens bestimmbar sein muss
bearbeitet	jeder Umgang mit solchen Informationen, vom Beschaffen über das Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren bis zum Vernichten

Aber: Welches Datenschutzrecht?

Rechtsgrundlagen Datenschutz (Schweiz)

Europarat: Europarats-Konvention 108+ (1981/2018)

Europäische Union: DSGVO 2016/679 /
Richtlinie 2016/680 für justizielle und polizeiliche Zusammenarbeit

Bund 	**Kantone** 
Bundesverfassung	+ z.T. Kantonsverfassungen
DSG/Bund (2020)	kantonales DSG/IDG/IDAG usw.
Datenbearbeiten durch Bundesorgane	Datenbearbeiten durch kantonale und kommunale Organe
Datenbearbeiten durch Private	

Anwendbares (Informations- und) Datenschutzgesetz: Wer ist Datenbearbeiter:in?



Private:

→ DSG/Bund (insb. Art. 5–32)

Bundesorgane:

→ DSG/Bund (insb. Art. 5–29, 33–42)

«Private Bundesorgane»: Personen, die mit einer öffentlichen Aufgabe des Bundes betraut sind (Art. 5 lit. i DSG) (z.B. Krankenkassen OKP, Branchenausgleichskasse)

→ DSG/Bund (insb. Art. 5–29, 33–42)

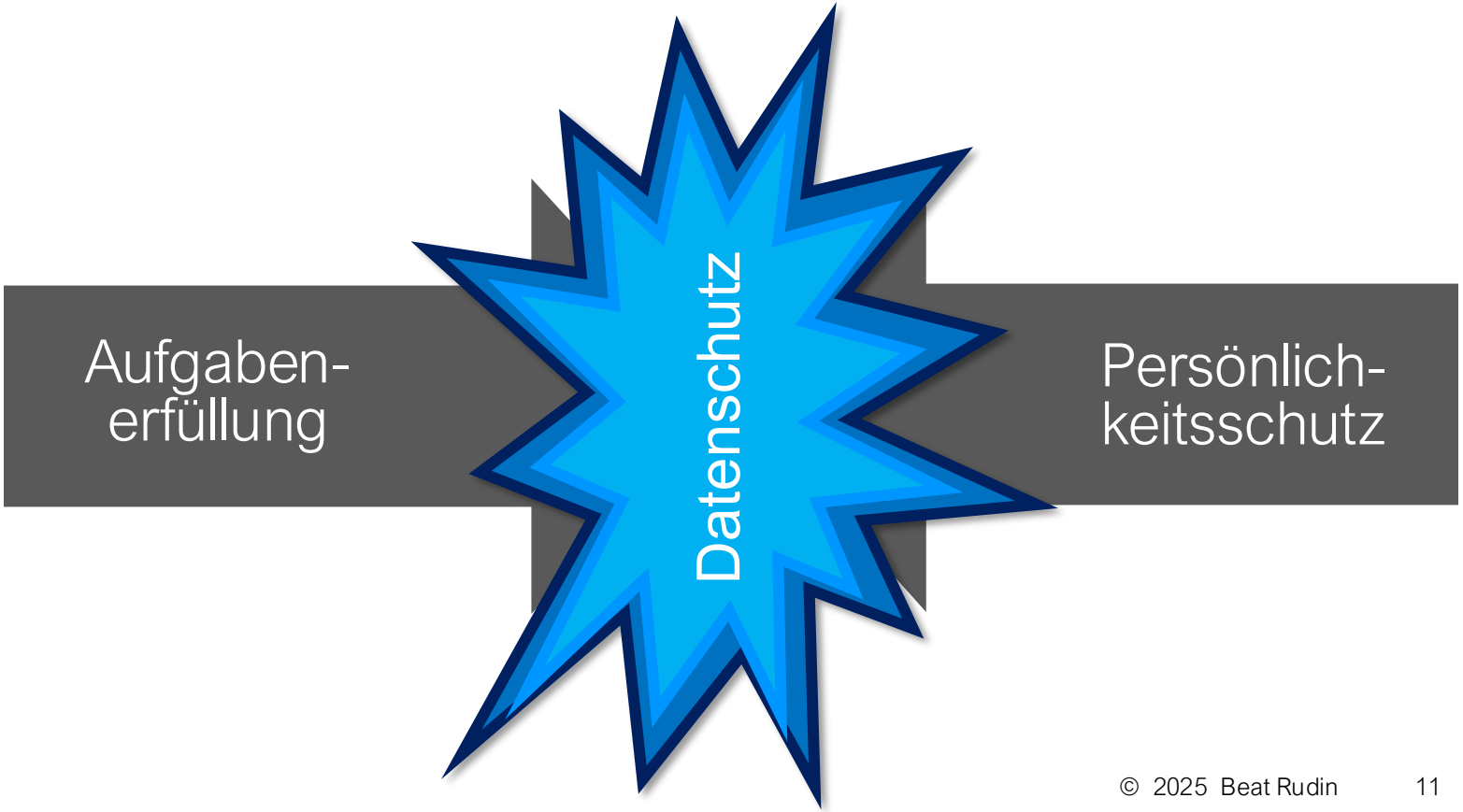
Kantonale (oder kommunale) öffentliche Organe:

→ Kantonales DSG (z.B. IDG/BS, KDSG/BE, IDAG/AG, InfoDG/SO, IDG/ZH, …)

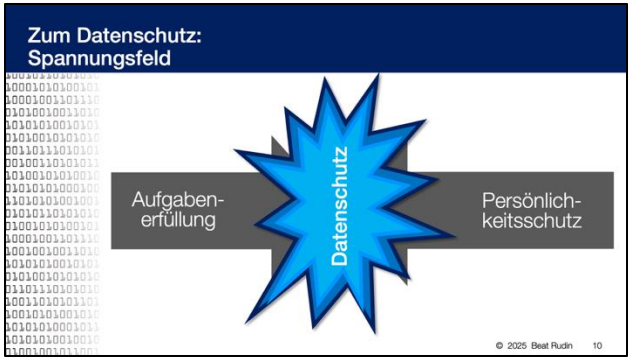
«Private kantonale (oder kommunale) öffentliche Organe»: Private, denen von Kanton (oder einer Gemeinde) die Erfüllung einer öffentlichen Aufgabe übertragen ist (z.B. § 3 Abs. 1 lit. c IDG/BS) (z.B. Listenspitäler usw.)

→ Kantonales DSG (z.B. IDG/BS, KDSG/BE, IDAG/AG, InfoDG/SO, IDG/ZH, …)

Zum Datenschutz: Spannungsfeld



Ausgleich im Spannungsfeld: Datenschutz-Grundsätze



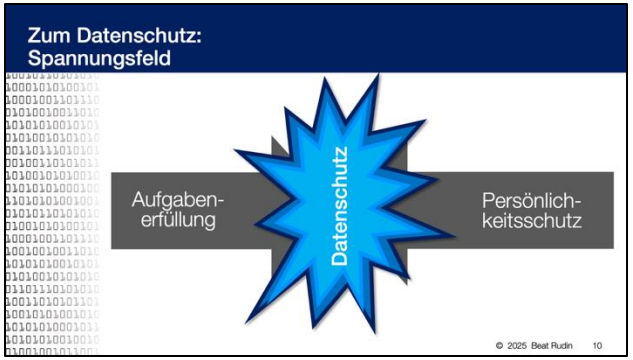
Prinzipien des Datenschutzrechts – von der Europarats-Konvention bis zu den kantonalen (Informations- und) Datenschutzgesetzen

- **Treu und Glauben**
- **Rechtmässigkeit** der Datenbearbeitung
- **Verhältnismässigkeit** der Datenbearbeitung
- **Zweckbindung** der Daten
- **Integrität** (Richtigkeit)
- **Transparenz** (Auskunftsrecht, Informationspflicht)
- **Datensicherheit**
- \+ Unabhängige Aufsicht

Gestaltungsprinzipien

- **Privacy by design** (Datenschutz durch Technikgestaltung)
- **Privacy by default** (datenschutzfreundliche Voreinstellungen)

Ausgleich im Spannungsfeld: Pflichten der Datenbearbeiter:innen und Betroffenenrechte



Pflichten der Verantwortlichen:

- Informationspflicht
  - insb. bei automatisierten Einzelentscheidung
- Meldepflicht bei Datenschutz-/Datensicherheitsverletzungen
- Transparenz und rechtliches (menschliches) Gehör bei automatisierten Einzelentscheidungen
- Datenschutz-Folgenabschätzung bei Vorhaben mit hohem Risiko
- Vorabkonsultation der Datenschutzaufsichtsbehörde

Rechte/Ansprüche der Betroffenen:

- Recht auf Auskunft
- Anspruch auf Berichtigung unrichtiger Personendaten, auf Unterlassung widerrechtlicher Datenbearbeitungen, auf Beseitigung der Folgen widerrechtlicher Datenbearbeitungen und Feststellung der Widerrechtlichkeit einer Datenbearbeitung
- Widerspruchsrecht

Unterscheidung sog. «allgemeines» / sog. «besonderes Datenschutzrecht»

	Bund	Kantone
	Sog. «allgemeines Datenschutzrecht» (Grundsätze des Datenschutzes)	
gestützt auf	Organisationsautonomie, Art. 122 BV, B-Monopole	Organisationsautonomie
gilt für	Bundesorgane, Private	kantonale/kommunale öffentliche Organe
Form	DSG/Bund	Kantonales DSG/IDG/IDAG …

Und:
Finden wir jetzt in den Datenschutzgesetzen die Antworten?



Ein Beispiel:

Eine **Ärztin** (mit einer eigenen Praxis/im Universitätsspital Basel) diagnostiziert bei einem Patienten **Masern**.

Darf/muss sie diese Beobachtung jemandem **melden**?

Darf/muss sie dies **namentlich** tun (also Personendaten melden)?

Findet sie die Antworten im DSG, IDG, IDAG usw.?

«Antworten» in den (Informations- und) Datenschutzgesetzen

Privatärztin → DSG/Bund	Ärztin z.B. im Universitätsspital → IDG/BS, IDG/ZH usw.
Das Bearbeiten von Personendaten kann eine **Persönlichkeitsverletzung** sein. Eine Persönlichkeitsverletzung ist **widerrechtlich**. Diese Widerrechtlichkeit kann beseitigt werden durch **Einwilligung** der betroffenen Person oder durch ein **überwiegendes öffentliches oder privates Interesse** oder durch **Gesetz**.	Das Bearbeiten von Personendaten ist ein **Grundrechtseingriff** Grundrechtseinschränkungen sind nur zulässig, wenn sie auf einer **gesetzlichen Grundlage** beruhen, im öffentlichen Interesse liegen (oder zum Schutz Grundrechte anderer erforderlich sind), **verhältnismässig** sind und den Kerngehalt des Grundrechts respektieren.

Antworten im «Sachrecht»



Die Ärztin findet die Antwort nicht im (Informations- und) Datenschutzgesetz, sondern:

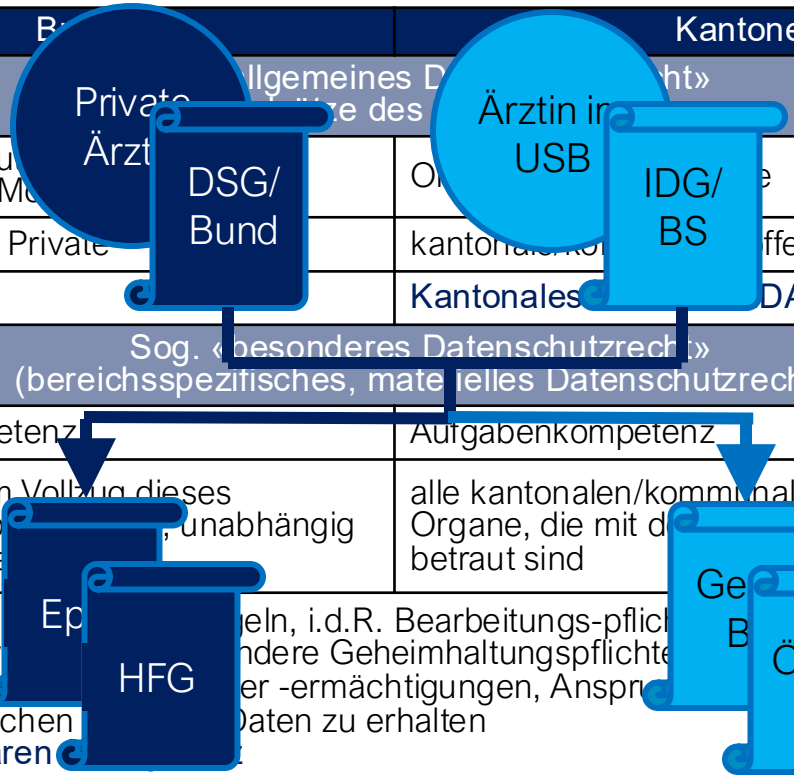
- Das **Epidemiengesetz** (EpG) auferlegt den Ärzt:innen bei übertragbaren Krankheiten eine Meldepflicht; der Bundesrat soll die Details regeln.
- Der Bundesrat überträgt den Regelungsauftrag in seiner **Epidemienverordnung** (EpV) weiter an das Eidgenössische Departement des Innern (EDI).
- Im Anhang der **EDI-Verordnung über die Meldung von Beobachtungen übertragbarer Krankheiten** wird festgelegt, was die Ärzt:innen den zuständigen Kantonsärzt:innen melden müssen – bei Masern auch identifizierende Angaben zu den Patient:innen.

Unterscheidung sog. «allgemeines» / sog. «besonderes Datenschutzrecht»

	Bund	Kantone
	Sog. «allgemeines Datenschutzrecht» (Grundsätze des Datenschutzes)	
gestützt auf	Organisationsautonomie, Art. 122 BV, B-Monopole	Organisationsautonomie
gilt für	Bundesorgane, Private	kantonale/kommunale öffentliche Organe
Form	DSG/Bund	Kantonales DSG/IDG/IDAG …
	Sog. «besonderes Datenschutzrecht» (bereichsspezifisches, materielles Datenschutzrecht)	
gestützt auf	Aufgabenkompetenz	Aufgabenkompetenz
gilt für	alle, die mit dem Vollzug dieses Bundesrechts betraut sind, unabhängig von der föderalen Stufe	alle kantonalen/kommunalen öffentlichen Organe, die mit dem Vollzug dieses Rechts betraut sind
Form	Konkrete Datenbearbeitungsregeln, i.d.R. Bearbeitungs-pflichten oder –ermächtigungen, Schweige- oder besondere Geheimhaltungspflichten, Bekanntgabepflichten (Anzeige- oder Meldepflicht) oder -ermächtigungen, Anspruch, von Privaten oder anderen öffentlichen Organen Daten zu erhalten – im anwendbaren Sachgesetz	

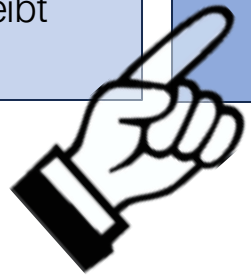
Unterscheidung sog. «allgemeines» / sog. «besonderes Datenschutzrecht»

	B	Kantone
	Allgemeines D… «…ht»	
gestützt auf	Organisationsau… Art. 122 BV, B-M…	O…
gilt für	Bundesorgane, Private	kantonale/ko… öffentliche Organe
Form	DSG/Bund	Kantonales … DAG …
	Sog. «besonderes Datenschutzrecht» (bereichsspezifisches, materielles Datenschutzrecht)	
gestützt auf	Aufgabenkompetenz…	Aufgabenkompetenz…
gilt für	alle, die mit dem Vollzug dieses Bundesrechts b… unabhängig von der föderale…	alle kantonalen/kommunalen öffentlichen Organe, die mit d… dieses Rechts betraut sind
Form	Konkrete Daten… geln, i.d.R. Bearbeitungs-pflich… ch-tigungen, Schw… ndere Geheimhaltungspflichte… pflichten (Anzeige- ode… er -ermächtigungen, Anspru… oder anderen öffentlichen … Daten zu erhalten – im anwendbaren …	



Phasen der generativen KI (gKI)

Beschaffen von Inhalt für das Training des Modells *	**Trainieren** bzw. Aufbau des Modells *	**Besitz & Betrieb** des Modells *	**Verwenden** des Modells zum Generieren von Output *
i.d.R. Anbieter:in evtl. das öffentliche Organ, wenn es selber ein Modell aufbauen will	i.d.R. Anbieter:in evtl. das öffentliche Organ, wenn es selber ein Modell aufbauen will	i.d.R. Anbieter:in evtl. das öffentliche Organ, wenn es selber ein Modell betreibt	**Mitarbeiter:innen des öffentlichen Organs**



* Personendaten?

Zurück zur KI: Welche datenschutzrechtlichen Herausforderungen stellen sich in den verschiedenen Phasen der gKI?

Beschaffen von Inhalt für das Training des Modells	Trainieren bzw. Aufbau des Modells	Besitz & Betrieb des Modells	Verwenden des Modells zum Generieren von Output
Treu und Glauben	Richtigkeit	Automatisierte Einzelentscheidung	Rechtmässigkeit
Transparenz	Verhältnismässigk.	Durchsetzung von Betroffenenrechten	Verhältnismässigk.
Zweckbindung	Schutz vor Re-Identifikation	KI-Modelle als Personendaten	Richtigkeit
Verhältnismässigk.	Datensicherheit	Datensicherheit	Datensicherheit
Rechtmässigkeit	Widerspruchsrecht		Zweckbindung
			Transparenz

(nach David Rosenthal)

© 2025 Beat Rudin

Verantwortung

Als Beispiel: **IDG/BS** (SG 153.260)

§ 6 *Verantwortung*

[1] Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet.

[2] Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortung und legen fest, welches öffentliche Organ die Gesamtver-antwortung trägt.

[3] Das öffentliche Organ muss nachweisen können, dass es die Datenschutzbestimmun-gen einhält. (…)

Verantwortung

für die Einhaltung der Gesetze (inkl. Datenschutzvorschriften)
auch bei der Nutzung von KI (mit Personendaten)

Gesamtverantwortung bei mehreren Bearbeiter:innen

nicht für alle Details, aber dafür, dass alle Verantwortlichkeiten zugewiesen sind

© 2025 Beat Rudin

Verantwortung 2

§ 7 *Bearbeiten im Auftrag*

[1] Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, wenn:
a) keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht und
b) sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte.

[2] Es bleibt für den Umgang mit Informationen nach diesem Gesetz verantwortlich. (…)

Auftragsdatenbearbeitung

grundsätzlich erlaubt ohne entgegenstehende rechtliche Bestimmung (z.B. Amts-, Berufsgeheimnis)

Auflage: sicherstellen, dass Auftragsdatenbearbeiter:innen Informationen nur so bearbeiten, wie das auftraggebende öffentliche Organ das auch tun dürfte

Verantwortung bleibt beim auftraggebenden öffentlichen Organ

Drei Sorgfaltspflichten:

Auswahl (*cura in eligendo*), Instruktion (*cura in instruendo*), Überwachung (*cura in custodiendo*)

Rechtmässigkeit (Gesetzmässigkeit): Bearbeiten

§ 9 *Voraussetzungen für das Bearbeiten von Personendaten*

[1] Ein öffentliches Organ darf Personendaten bearbeiten, wenn

a) dafür eine gesetzliche Grundlage besteht oder

b) dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist.

[2] Besondere Personendaten dürfen bearbeitet und ein Profiling darf vorgenommen werden, wenn:

a) ein Gesetz dazu ausdrücklich ermächtigt oder verpflichtet oder

b) es für eine in einem Gesetz klar umschriebene Aufgabe zwingend notwendig ist.

Unmittelbare (lit. a) oder mittelbare (lit. b) gesetzliche Grundlage

- unmittelbar: Datenbearbeiten geregelt
- mittelbar: Aufgabe, die nur erfüllt werden kann, wenn Personendaten bearbeitet werden

Qualifizierte gesetzliche Grundlage (Abs. 2)

- besondere Personendaten, Profiling

Rechtmässigkeit (Gesetzmässigkeit): Bekanntgeben 1

§ 21 *Bekanntgabe von Personendaten*

[1] Das öffentliche Organ gibt Personendaten bekannt, wenn

a) eine gesetzliche Bestimmung dazu verpflichtet oder ermächtigt, oder

b) dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder

c) im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf.

[2] Besondere Personendaten oder Resultate eines Profilings gibt das öffentliche Organ bekannt, wenn:

a) ein Gesetz dazu ausdrücklich verpflichtet oder ermächtigt oder

b) dies zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe zwingend notwendig ist oder

c) im Einzelfall die betroffene Person ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf.

Dito sowie ausdrückliche oder mutmassliche Zustimmung im Einzelfall (Abs. 3)

© 2025 Beat Rudin

Rechtmässigkeit (Gesetzmässigkeit): Bekanntgeben 2



Personendaten als Input?

Gesetzliche Grundlage für das Bekanntgeben von (besonderen) Personendaten an die Anbieterin von KI?

- Soweit ersichtlich nicht (ausser es wären Daten, die jeder Person voraussetzungslos bekannt gegeben werden dürften)

Ausdrückliche oder mutmassliche Einwilligung der Betroffenen im Einzelfall?

- Ausdrücklich im Einzelfall – kaum
- Mutmasslich: falls nicht in der Lage, ausdrücklich zuzustimmen, und die Bekanntgabe in ihrem Interesse liegt und ihre Zustimmung in guten Treuen vorausgesetzt werden darf - kaum

Verhältnismässigkeit

§ 9 *Voraussetzungen für das Bearbeiten von Personendaten*

[3] Das Bearbeiten von Personendaten hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.

[4] Personendaten dürfen nur so lange bearbeitet werden, als es zur Erfüllung der gesetzlichen Aufgabe erforderlich ist.

Verhältnismässig?

- *geeignet* zur Zweckerreichung (= zur Erfüllung der gesetzlichen Aufgabe)
- *erforderlich* zur Zweckerreichung (= zur Erfüllung der gesetzlichen Aufgabe), bei besonderen Personendaten: *zwingend notwendig*
- *zumutbar*: vertretbares Verhältnis zwischen Eingriffswirkung und Eingriffszweck

persönlich, sachlich und zeitlich

Personendaten als Input?

- Ist das Bekanntgeben von (besonderen) Personendaten an die Anbieterin erforderlich (oder gar zwingend notwendig) zur Erfüllung der gesetzlichen Aufgabe? – kaum

Richtigkeit

§ 11 *Richtigkeit*

[1] Personendaten müssen richtig und, soweit es der Verwendungszweck erfordert, vollständig sein.

[2] Das öffentliche Organ, das Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.

[3] Es sind alle angemessenen Massnahmen zu treffen, damit Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.

Richtigkeit?

Eines der Hauptprobleme der generativen KI: Wahrscheinlichkeit, nicht Wahrheit

Auch wenn der Output der KI nicht Personendaten enthält: Die *Verwendung des Outputs* in Bezug auf Personen unterliegt dem Gebot der Richtigkeit.

Vergewisserungspflicht des öffentlichen Organs

Falls unrichtig → Berichtigungsanspruch (gegenüber dem öffentlichen Organ / gegenüber der KI?

Datensicherheit

§ 8 *Informationssicherheit*

[1] Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.

[2] Die Massnahmen richten sich nach den folgenden Schutzzielen:

a) Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen (Vertraulichkeit);
b) Informationen müssen richtig und vollständig sein (Integrität);
c) Informationen müssen bei Bedarf vorhanden sein (Verfügbarkeit);
d) Informationsbearbeitungen müssen einer Person zugerechnet werden können (Zurechenbarkeit);
e) Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein (Nachvollziehbarkeit).

[3] Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik. (…)

Datensicherheit

ganz generell, sobald (Personen-)Daten bearbeitet werden.

© 2025 Beat Rudin

Zweckbindung

§ 12 *Zweckbindung*

[1] Personendaten dürfen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben worden sind, soweit nicht eine gesetzliche Grundlage ausdrücklich eine weitere Verwendung vorsieht oder die betroffene Person im Einzelfall einwilligt.

Zweckbindung

hängt eng mit der gesetzlichen Grundlage zusammen: → begrenzt die Reichweite der Rechtfertigung

Personendaten als Input?

Rechtfertigung für das Bearbeiten zur Aufgabenerfüllung; Zweckänderung gerechtfertigt? – kaum

Verwendung der Personendaten zum Training der KI: Rechtfertigung durch gesetzliche Grundlage oder Einwilligung der betroffenen Person? – kaum

Personendaten als Output?

weniger problematisch (für das öffentliche Organ)

Transparenz

§ 15 *Informationspflicht bei der Beschaffung*

[1] Das verantwortliche öffentliche Organ informiert die betroffene Person über jede Beschaffung von Personendaten. Diese Informationspflicht gilt auch, wenn die Daten bei Dritten beschafft werden. (…)

§ 26 *Zugang zu den eigenen Personendaten*

[1] Jede Person hat Anspruch darauf zu wissen, ob bei einem öffentlichen Organ Personendaten über sie vorhanden sind, und gegebenenfalls auf Zugang zu diesen eigenen Personendaten. (…)

Erkennbarkeit

hat früher gereicht (Aspekt von Treu und Glauben)

Informationspflicht

bei der Beschaffung von (auch «gewöhnlichen») Personendaten (mit Ausnahmen)

Recht auf Auskunft (Zugang zu den eigenen Daten)

Gegenüber dem öffentlichen Organ / gegenüber der KI-Anbieterin?

«Black Box» KI: Nachvollziehbarkeit?

Automatische Einzelents… 1

Als Beispiel: **DSG/Bund** (SR 235.1)

Art. 21 DSG *Informationspflicht bei einer automatisierten Einzelentscheidung*

[1] Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (automatisierte Einzelentscheidung).

[2] Er gibt der betroffenen Person auf Antrag die Möglichkeit, ihren Standpunkt darzulegen. Die betroffene Person kann verlangen, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird.

[3] Die Absätze 1 und 2 gelten nicht, wenn:

a. die automatisierte Einzelentscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird; oder
b. die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.

[4] Ergeht die automatisierte Einzelentscheidung durch ein Bundesorgan, so muss es die Entscheidung entsprechend kennzeichnen. Absatz 2 ist nicht anwendbar, wenn die betroffene Person nach [Art. 30 Abs. 2 VwVG] oder nach einem anderen Bundesgesetz vor dem Entscheid nicht angehört werden muss.

Automatische Einzelentscheidung 2



Automatisierte Einzelentscheidung

Die Maschine *entscheidet*, nicht ein Mensch (nicht bloss einen Vorschlag machen)

Rechtsfolge oder erhebliche Beeinträchtigung (im Privatrecht z.B. Entscheid über Kreditgewährung)

Im öffentlichen Recht: Vorauswahl bei Bewerbungen? Entscheid über Steuereinsprachen?

Informationspflicht

über die Tatsache der automatisierten Einzelentscheidung (Bundesorgane: Kennzeichnung)

Recht auf (menschliches) rechtliches Gehör

Standpunkt einbringen, Überprüfung der Entscheidung durch einen Menschen (Bundesorgane: ausser gesetzlich vorgesehen: keine Anhörung vor dem Entscheid)

Gestaltungsgrundsätze: Privacy by design, Privacy by default

§ 14 *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*

[1] Das öffentliche Organ trifft bei Datenbearbeitungen von Anfang an Massnahmen, die das Risiko von Verletzungen der Grundrechte verringern und solchen Verletzungen vorbeugen.

[2] Es stellt mittels geeigneter Voreinstellungen sicher, dass standardmässig nur diejenigen Personendaten bearbeitet werden, die für den jeweiligen Verwendungszweck erforderlich sind.

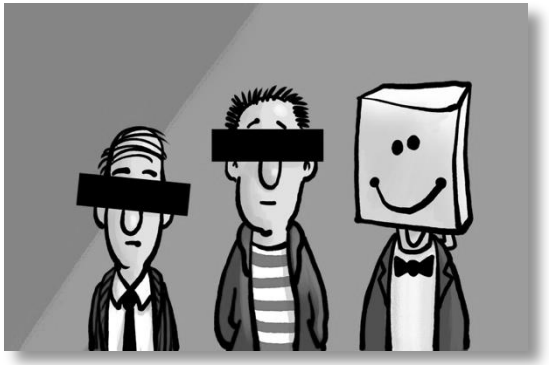
Datenminimierung

Anonymisierung, Pseudonymisierung

sobald nicht mehr identifizierende Daten zur Aufgabenerfüllung erforderlich sind

Opt in, nicht opt out

Anonymisierung, Pseudonymisierung



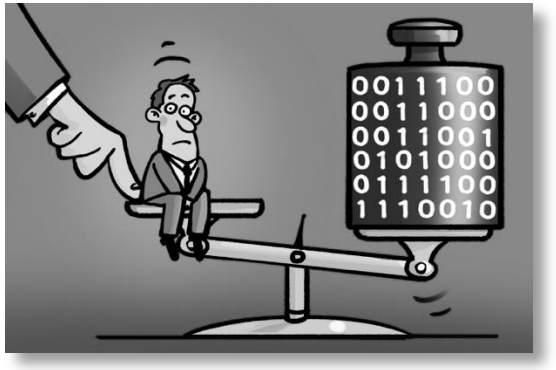
Anonymisierung = (irreversible) Entfernung des Personenbezuges

- nicht bloss Vorname Name, auch Geburtsdatum, Adresse und alle anderen identifizierenden Merkmale
- anonymisierte Personendaten: keine Personendaten mehr
- Big Data, KI: Gefahr der Re-Identifizierbarkeit

Pseudonymisierung = (reversible) Entfernung des Personenbezuges

- gleiche Vorkehrungen, aber es bleibt ein Schlüssel, mit dem der Personenbezug wieder hergestellt werden kann
- pseudonymisierte Personendaten: keine Personendaten mehr für Personen/Stellen, die keine Möglichkeit des Zugangs zum Schlüssel haben / für Personen/Stellen mit Zugangmöglichkeit zum Schlüssel bleiben es Personendaten

Massnahmen



Schulen, Sensibilisieren

- Chancen (Nutzungsmöglichkeiten) und
- Risiken (Fehlerhaftigkeit, fehlende Transparenz, Diskriminierung usw.)

Regeln

- Wer darf welche KI nutzen?
- Datenschutz: keine Personendaten
- KI-Ethik?

Entwicklungen aufmerksam verfolgen

- rasch reagieren, wenn Probleme erkannt werden

KI-Hype: Erwartungen und Enttäuschungen

KI kann **wertvolle Unterstützung** leisten.

Aber:

- KI ist nicht klug, sondern naiv.
- Die KI beherrscht die Sprache zwar perfekt, hat aber keine Ahnung, was die generierten Sätze, Bilder usw. bedeuten.
- KI ist nicht objektiv (Bias aufgrund der Trainingsdaten).
- KI-Resultate sind nicht replizierbar.
- KI ist nicht nachvollziehbar (kann halluzinieren).
- KI kann handeln, aber keine Verantwortung übernehmen.

KI kann wertvolle Unterstützung leisten – aber der Mensch/die Organisation muss entscheiden, wie die Unterstützung verwendet wird.

Die **Verantwortung bleibt beim Menschen**.

Ihre Fragen? Ihre Meinung?



Besten Dank
für Ihr Interesse und

viel Erfolg
beim (auch datenschutzkonformen) Verwenden von KI!

Beat Rudin
Prof. (em.) Dr. iur., Advokat
beat.rudin@unibas.ch

Cartoons: Reto Fontana