VISCHER

Das neue Datenschutzgesetz.
Übersicht und Abstecher zur KI

Lucian Hunger, Rechtsanwalt, VISCHER AG
29. August 2023

Worum geht es?

- Ab 1. September 2023 ein neues **Datenschutzgesetz**
- Ähnlich wie die **EU DSGVO**, aber (zum Glück) **keine Kopie**
  - Pragmatischer und weniger formalistisch als das EU-Recht
  - Nur in wenigen Bereichen strenger als DSGVO
- Was bisher erlaubt war, **bleibt** meistens **weiterhin erlaubt**

Die Grundsätze verändern sich nicht!

Was muss bei Personendaten beachtet werden?

- Einhaltung der "**Bearbeitungsgrundsätze**" (Art. 6 revDSG)
  - Rechtmässigkeit, inklusive Transparenz
  - Zweckbindung (was kommuniziert wurde)
  - Verhältnismässigkeit (im Hinblick auf den Zweck)
    inklusive Datensparsamkeit und Pflicht zur Löschung
  - Richtigkeit (in Bezug auf den Zweck)
  - Datensicherheit (Vertraulichkeit, Integrität, Verfügbarkeit)
- Es ist grundsätzlich **kein Rechtsgrund** nötig (≠ DSGVO)
  - Aber eine **Rechtfertigung** bei:
    (i) Verstoss gegen Bearbeitungsgrundsätze, (ii) Widerspruch der betroffenen Person, (iii) Bekanntgabe besonders schützenswerter Personendaten
  - Rechtfertigungsgründe: z.B. Einwilligung, überwiegendes Interesse, Gesetz

Was ändert sich? Was ist neu?

1. Ausgebaute Pflicht zur **Datenschutzerklärung***
2. Pflicht für ein **Verzeichnis der Datenbearbeitungen** (mit Ausnahmen)
3. Leicht strengere Vorgaben für **Auftragsbearbeitungen***
4. Pflicht zur **Datenschutz-Folgenabschätzung** in heiklen Fällen
5. Pflicht zur **Meldung von Sicherheitsverstössen** an EDÖB
6. Anpassung des **Auskunfts-* und Korrekturrechts**
7. Neues Recht auf **Datenportabilität** für Kunden
8. Regelung zu **automatisierten Einzelentscheiden***
9. Anpassung diverser **Begrifflichkeiten**
10. Aufsichtsinstrumente und **Strafbarkeit ausgebaut**

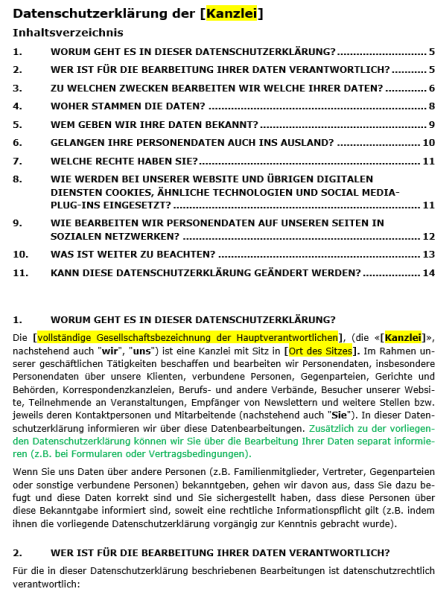
* Strafbarkeit möglich

Wer ist verantwortlich?

- **Controller / Verantwortlicher** – derjenige, der die Ausgestaltung einer Datenbearbeitung definiert
  - z.B. Auftraggeber, Anwaltsbüro, PR-Agentur, Eventveranstalter
- **Gemeinsame Controller = «Joint Controller»**
  - z.B. Immobilieneigentümer und Bewirtschafter
- **Processor / Auftragsbearbeiter** – wer Personendaten für einen Verantwortlichen bearbeitet
  - z.B. SaaS-Anbieter, Webhoster
- **Darum ist das wichtig**
  - Viele der DSG-Pflichten knüpfen daran an (z.B. Pflicht zur Datenschutzerklärung)

Die Datenschutzerklärung

- **Informationspflicht des Verantwortlichen**
  - Pflichtinhalt nach Art. 19 ff. revDSG
    - Identität und Kontaktdaten des Verantwortlichen
    - Bearbeitungszweck
    - Kategorien von Empfängern, Angaben zur Bekanntgabe ins Ausland […]
    - Kategorien der Personendaten, die nicht bei der betroffenen Person erhoben werden
  - Allgemeine Datenschutzerklärung, nicht nur für die Website
  - Separate DSE für die Mitarbeitenden
- **Darum ist das wichtig**
  - Fehlende / unvollständige DSE kann strafbar sein



Datenschutzerklärung der [Kanzlei]

Inhaltsverzeichnis

1. WORUM GEHT ES IN DIESER DATENSCHUTZERKLÄRUNG?

Die [vollständige Gesellschaftsbezeichnung der Hauptverantwortlichen], (die «[Kanzlei]», nachstehend auch "**wir**", "**uns**") ist eine Kanzlei mit Sitz in [Ort des Sitzes]. Im Rahmen unserer geschäftlichen Tätigkeiten beschaffen und bearbeiten wir Personendaten, insbesondere Personendaten über unsere Klienten, verbundene Personen, Gegenparteien, Gerichte und Behörden, Korrespondenzkanzleien, Berufs- und andere Verbände, Besucher unserer Website, Teilnehmende an Veranstaltungen, Empfänger von Newslettern und weitere Stellen bzw. Jeweils deren Kontaktpersonen und Mitarbeitende (nachstehend auch "**Sie**"). In dieser Datenschutzerklärung informieren wir über diese Datenbearbeitungen. Zusätzlich zu der vorliegenden Datenschutzerklärung können wir Sie über die Bearbeitung Ihrer Daten separat informieren (z.B. bei Formularen oder Vertragsbedingungen).

Wenn Sie uns Daten über andere Personen (z.B. Familienmitglieder, Vertreter, Gegenparteien oder sonstige verbundene Personen) bekanntgeben, gehen wir davon aus, dass Sie dazu befugt und diese Daten korrekt sind und Sie sichergestellt haben, dass diese Personen über diese Bekanntgabe informiert sind, soweit eine rechtliche Informationspflicht gilt (z.B. indem ihnen die vorliegende Datenschutzerklärung vorgängig zur Kenntnis gebracht wurde).

2. WER IST FÜR DIE BEARBEITUNG IHRER DATEN VERANTWORTLICH?

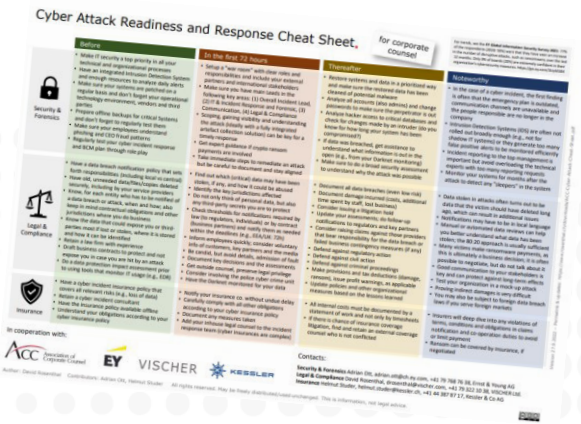
Für die in dieser Datenschutzerklärung beschriebenen Bearbeitungen ist datenschutzrechtlich verantwortlich:

Auftragsbearbeiter

- **Auftragsbearbeitungsverträge** (AVV)
  - Überall dort, wo jemand als Auftragsbearbeiter tätig ist (Art. 9)
  - DSGVO-Verträge können nicht einfach übernommen werden
- **Darum ist das wichtig**
  - Auftragsbearbeitungen kommen häufig vor, aber ebenso oft fehlen korrekte AVVs in der Schweiz noch
  - Fehlender / unvollständiger AVV kann strafbar sein (für den Verantwortlichen)
- **Verträge zwischen Verantwortlichen**
  - Sind in der Schweiz nicht zwingend, aber zu empfehlen

Informationssicherheit

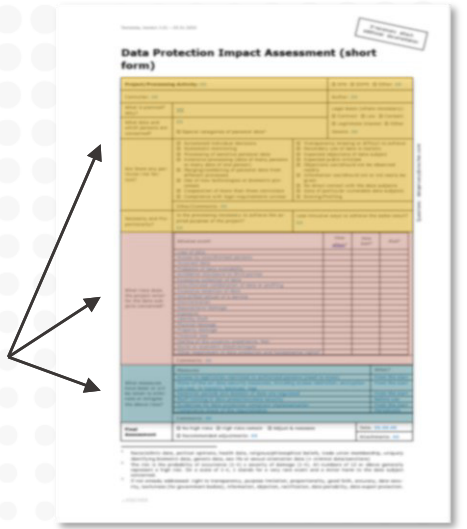
- **Informationssicherheit!** (Art. 8 + DSV)
  - Schutz vor Angreifern durch geeignete technische und organisatorische Massnahmen
  - Plan für die Reaktion im Notfall (inkl. Kontakte)
  - Plan für die Geschäftsfortführung im Notfall
- **Neu:** Meldepflicht für Data Breaches mit hohem Risiko (Art. 24)
  - Meldung an den EDÖB
  - ggf. auch Meldung an betroffene Personen



https://www.rosenthal.ch/downloads/ACC-Cyber-Attack-Cheat-Sheet.pdf

Datenschutz-Folgenabschätzung (DSFA)

- Strukturierte Prüfung der **Risiken einer Bearbeitungstätigkeit** für die betroffene Person
- Pflicht, wenn Bearbeitung **ein hohes Risiko für die betroffene Person** mit sich bringt (Art. 22 revDSG)
  - z.B. bei Installation einer Sicherheitskamera
- Verwendung einer Vorlage sinnvoll, typischer Aufbau:
  - Beschreibung des Vorhabens; Bewertung der Risiken für die betroffene Person; Massnahmen zur Eindämmung der Risiken
- Pflicht für **Verantwortlichen** (i.d.R. unterstützt durch Provider)



Anweisung und Schulung der Mitarbeitenden

- **Weisung, Schulung und Kontrolle**
  - Weisung mit den Grundregeln des Datenschutzes, den Prozessen und den Verantwortlichkeiten
  - Schulung
  - Kontrollen
- **Darum ist das wichtig**
  - Internes Signal
  - Fehler vermeiden
  - Damit sich jemand für den Datenschutz verantwortlich fühlt
  - Schutz vor Strafbarkeit

Strafbarkeit

"Mit Busse bis zu 250'000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich …"

Strafrechtliche Verantwortlichkeit

- Auskunftsrecht
- Informationspflicht
- Pflicht zum AVV
- Bekanntgabe ins Ausland
- Datensicherheit
- Weisungen des EDÖB
- Berufsgeheimnis (tw.)

Durch Handeln

Jeder, der handelt

Beispiele:

- Wer in Kauf nimmt, eine falsche Auskunft an einen Betroffenen zu erteilen
- Wer entscheidet, die Datenschutz-Erklärung nicht wie erforderlich nachzuführen

Durch Unterlassen

Wer eine Garantenstellung hat

- Wer als GL-Mitglied nicht dafür sorgt, dass Auskunftsersuchen richtig behandelt werden
- Wer als leitender Inhaber einer Bearbeitung keine korrekte DSE in Auftrag gibt
- Der untätige VR, weil er keinen Bericht will

1. Person muss Pflicht haben, Rechtsverletzungen zu verhindern und die dafür nötigen Befugnisse
2. Sie kommt ihrer Pflicht zur sorgfältigen Auswahl, Instruktion und Überwachung nicht nach

Einige häufige Irrtümer

- Nein, das revidierte Datenschutzgesetz schreibt weiterhin **keine Einwilligung** vor – auch nicht für Profiling und Cookies
- Nein, **Cloud-Lösungen** sind trotz US-Bezug weiterhin erlaubt
- Nein, es muss nicht jede **Verletzung des Datenschutzes** nach Bern gemeldet werden, sondern nur Verletzungen der Datensicherheit und nur falls das Risiko für Betroffene hoch ist
- Nein, das **Recht auf Vergessen** ist weder neu noch absolut
- Nein, nicht alles, was **DSGVO-"konform"** ist genügt für das neue DSG (z.B. Datenschutzerklärung, Providerverträge nicht)
- Nein, ein **Datenschutzbeauftragter** ist i.d.R. keine Pflicht

Anders ist es unter der DSGVO und im EU-Cookie-Recht: In der EU braucht es für Datenbearbeitungen einen Rechtsgrund, und Marketing- und Tracking-Cookies und ähnliche Verfahren oft eine Einwilligung.

Es galt und gilt: Personendaten müssen gelöscht oder anonymisiert werden, sobald sie ihren erlaubten Zweck erfüllt haben

Was sagt ChatGPT zum DSG und KI?

Neues Schweizer Datenschutzgesetz (DSG) - Wesentliche Änderungen

1. **Stärkerer Schutz von Persönlichkeitsrechten**: Erhöhter Schutz personenbezogener Daten und Erweiterung der Rechte der betroffenen Personen.
2. **Transparenzprinzip**: Unternehmen müssen klar und umfassend über die Verarbeitung personenbezogener Daten informieren.
3. **Datenschutz-Folgenabschätzung (DSFA)**: Bei hohem Risiko für Persönlichkeitsrechte muss vor der Datenverarbeitung eine Abschätzung durchgeführt werden.
4. **Meldepflicht bei Datenpannen**: Bei Verletzungen des Schutzes personenbezogener Daten müssen diese dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden.
5. **Vertreter in der Schweiz**: Ausländische Unternehmen, die in der Schweiz Daten verarbeiten, müssen einen Vertreter in der Schweiz benennen.
6. **Erhöhte Sanktionen**: Bei Verstößen gegen das DSG können nun höhere Bussen verhängt werden.
7. **Datenübertragung ins Ausland**: Stärkere Regelungen zum Schutz von Daten, die ins Ausland übermittelt werden.
8. **Erweiterung der Betroffenenrechte**: Betroffene haben erweiterte Rechte, z. B. das Recht auf Datenportabilität.

Es ist wichtig zu beachten, dass dies eine vereinfachte Übersicht der wichtigsten Änderungen des neuen DSG ist. Für eine detaillierte Beratung und vollständige Information sollten Sie einen Fachexperten oder Anwalt für Datenschutzrecht konsultieren.

Datenschutzrechtliche Herausforderungen bei KI-Einsatz in Unternehmen (Schweizer DSG)

1. **Datenerhebung**: Verarbeitung nur bei Einwilligung oder gesetzlicher Grundlage.
2. **Automatisierte Einzelentscheidungen**: Betroffene können Entscheidungen, die auf einer automatisierten Datenbearbeitung beruhen, anfechten.
3. **Transparenz**: Recht der Betroffenen, den Zweck einer Datenbearbeitung zu kennen.
4. **Datenspeicherung**: Sicherstellung, dass keine Daten unzulässigerweise offenbart werden.
5. **Bias**: Risiko ungenauer oder diskriminierender Entscheidungen.
6. **Datenübertragung ins Ausland**: Daten dürfen nur bei ausreichendem Datenschutzniveau übermittelt werden.
7. **Sicherheit**: Schutz der Daten vor unbefugtem Zugriff.
8. **Grundsatz der Verhältnismäßigkeit**: Datenbearbeitung muss zum Zweck geeignet und nicht übertrieben sein.
9. **Datenqualität**: Gewährleistung der Richtigkeit der Daten.

Unternehmen in der Schweiz sollten rechtliche Beratung in Anspruch nehmen, um sicherzustellen, dass sie den Bestimmungen des DSG entsprechen.

Bitte beachten Sie, dass diese Zusammenfassung allgemein gehalten ist und das DSG weitere spezifische Anforderungen und Bestimmungen enthält, die je nach spezifischem Einsatz von KI relevant sein könnten.

Generative KI-Systeme und Datenschutz

Transparenz	Richtigkeit	Automatisierte Einzelentscheide	Transparenz
Zweckbindung	Verhältnismässigkeit	Durchsetzung von Betroffenenrechten	Verhältnismässigkeit
Verhältnismässigkeit	Schutz vor Re-Identifikation	KI-Modelle als Personendaten	Richtigkeit
(Rechtsgrundlage)	Datensicherheit	Datensicherheit	Datensicherheit
	Widerspruchsrecht		Zweckbindung
			(Rechtsgrundlage)

Datenschutzrechtliche Rollenverteilung

Wer ist der Verantwortliche?

- **Hersteller / Betreiber** des Modells
  - Bei Angeboten an Private in der Regel Verantwortlicher
  - Gegenüber Unternehmen in der Regel Auftragsbearbeiter (ausser bei Nutzung der Daten für eigene Zwecke)
- **Verwender der KI**
  - KI ist ein Werkzeug, das er einsetzt
  - Verantwortlich dafür, dass die Nutzung (der erzeugte Output) den datenschutzrechtlichen Grundsätzen entspricht
    - ist das *Ergebnis* richtig und die *Nutzung* vertretbar?
  - Nicht verantwortlich für allenfalls unrechtmässige Herstellung des Modells
  - Personendaten als Input: gleiche Voraussetzungen wie bei anderen Datenbearbeitungen (z.B. AVV)

Einige Praxisempfehlungen

- Datenschutzrechtliche Rollen vorab klären; AVV abschliessen
- Verträge mit Providern auf KI-Nutzung prüfen und sorgfältig abwägen, ob eigene Daten dafür benutzt werden sollen/dürfen
- Falls eine KI trainiert werden soll: Der Qualitätssicherung und Anonymisierung besonderes Augenmerk schenken
- Betroffene Personen auf solche geplanten Zwecke hinweisen und Einhaltung von Betroffenenrechten vorgängig abklären
- Mitarbeiter darauf hinweisen, dass an eine KI übermittelte Daten möglicherweise nicht vertraulich bleiben
- Sich der Funktionsweise und Grenzen von KI bewusst sein

VISCHER

Vielen Dank für Ihre Aufmerksamkeit!

lhunger@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com