



# Revidiertes Datenschutzgesetz

Gesetzliche Anforderungen /  
Umsetzungsmassnahmen

Stefan Kunz und Fabiola Weilenmann

Schwarzenburg, 6. Februar 2024

# Inhalt der Präsentation



- Grundlagen
- Handlungsbedarf Implementierung revDSG
  - Sieben grundlegende Umsetzungsmassnahmen als Handlungsempfehlung
- Sanktionen bei Verstössen
- Datenschutz und KI
- Fragen

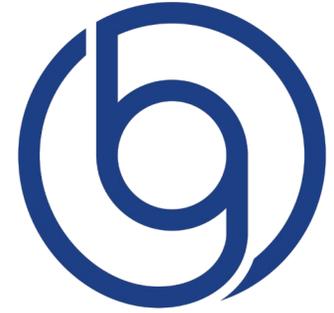


# Inkrafttreten revDSG und revDSV

- Per 1. September 2023, keine Übergangsfrist
- Reaktion auf europäische Datenschutzgrundverordnung “DSGVO“ (Angleichung an Schutzniveau EU)
- 15. Januar 2024: Angemessenheitsbeschluss EU
- Div. Handlungsbedarf für Unternehmen: Ausgebaut werden insb. die Governance und die Betroffenenrechte.
- Verschärfte Strafbestimmungen



# Gesetzeszweck



- Art. 1 DSGVO: Zweck

## **Art. 1**            **Zweck**

Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden.

- Nur noch natürliche Personen geschützt.
- Persönlichkeitsschutz: privatrechtlicher Aspekt
- Grundrechtsschutz: öffentlich-rechtlicher Aspekt



# Persönlicher und sachlicher Anwendungsbereich revDSG

## **Art. 2** Persönlicher und sachlicher Geltungsbereich

<sup>1</sup> Dieses Gesetz gilt für die Bearbeitung von Personendaten natürlicher Personen durch:

- a. private Personen;
- b. Bundesorgane.

<sup>2</sup> Es ist nicht anwendbar auf:

- a. Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden;
- b. Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

# Räumlicher Anwendungsbereich revDSG



## Art. 3 Räumlicher Geltungsbereich

<sup>1</sup> Dieses Gesetz gilt für Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.

<sup>2</sup> Für privatrechtliche Ansprüche gilt das Bundesgesetz vom 18. Dezember 1987<sup>4</sup> über das Internationale Privatrecht. Vorbehalten bleiben zudem die Bestimmungen zum räumlichen Geltungsbereich des Strafgesetzbuchs<sup>5</sup>.



# Räumlicher Anwendungsbereich

## Art. 3 DSGVO

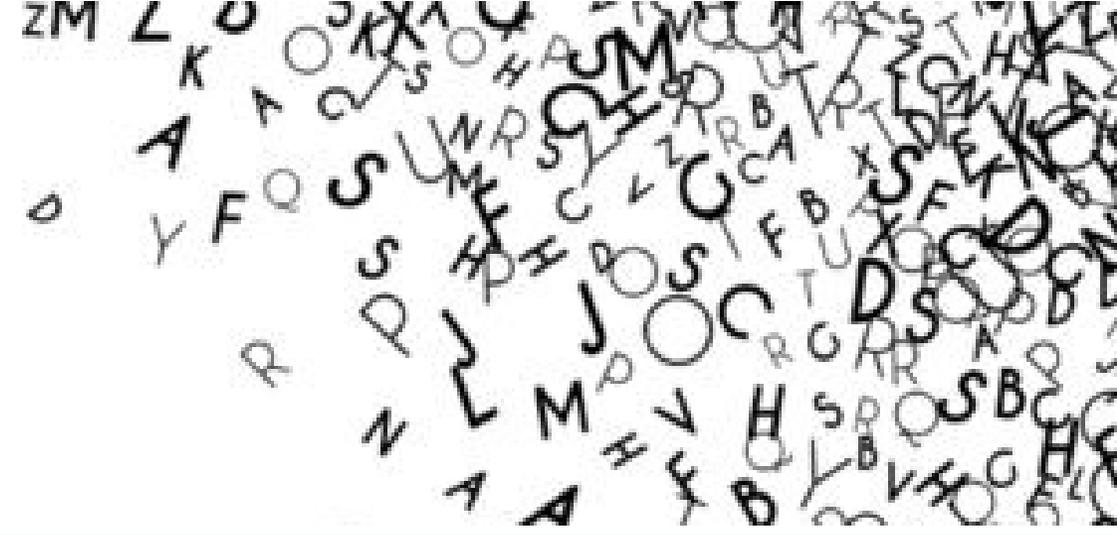


- (2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht
- a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
  - b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.





**BGP Partner**  
Rechtsanwalte  
Bern – Zurich



# Was sind Personendaten?



# Definition Personendaten



## Art. 5 Begriffe

In diesem Gesetz bedeuten:

- a. *Personendaten*: alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;



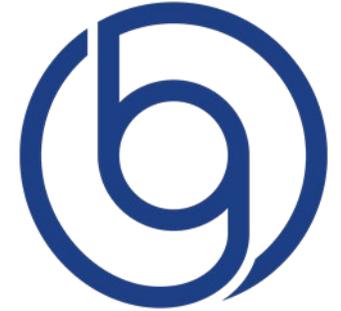
# Begriff: Bearbeiten



- Bearbeiten:
  - *„Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insb. Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten“ (Art. 5 lit. d DSGVO).*



# Rolle Verantwortlicher / Auftragsdatenbearbeiter

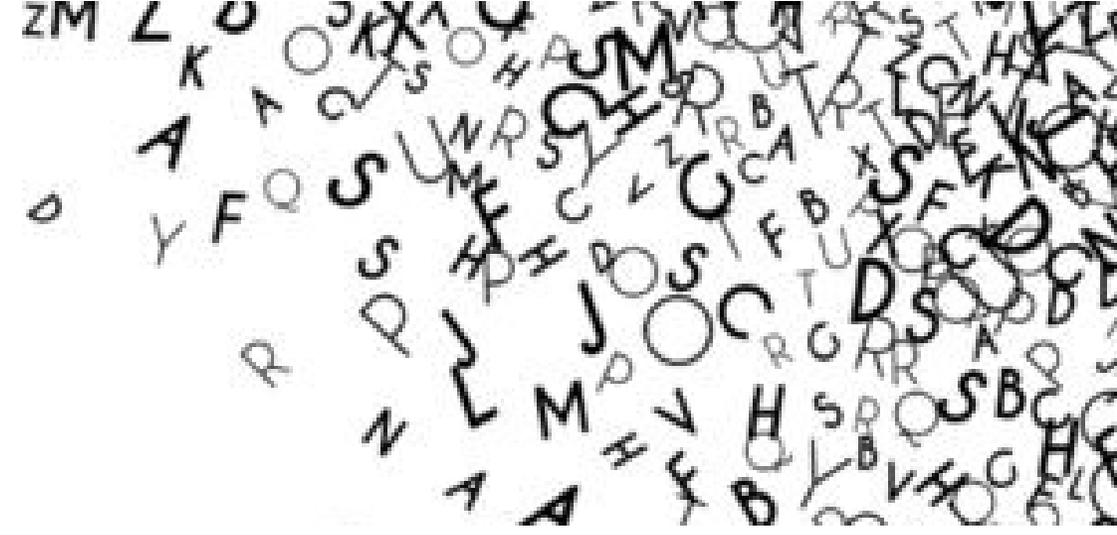


- **Verantwortlicher:** Private Person, die über den Zweck und die Mittel der Bearbeitung entscheidet (Art. 5 lit. j DSGVO).
- **Auftragsbearbeiter:** Private Person, die im Auftrag des Verantwortlichen Personendaten bearbeitet (Art. 5 lit. k DSGVO).





**BGP Partner**  
Rechtsanwalte  
Bern – Zurich



# Sieben empfohlene Umsetzungsmassnahmen



# Wesentliche neue Anforderungen / Umsetzung revDSG



- **Erstellung Bearbeitungsverzeichnis (Art. 12 DSGVO) -> Innenperspektive**
  - u.U. gesetzlich nicht zwingend\*, aber letztlich erforderlich für Umsetzung des Datenschutzes -> Überblick verschaffen
  - Mindestinhalt: Art. 12 Abs. 2 DSGVO
  - Verpflichtende Personen: Verantwortlicher und Auftragsbearbeiter
  - **Massnahme 1**: Darstellung der allerwichtigsten Geschäftstätigkeiten in einem Excel-Sheet (A4-Seite) -> Template

\*(< 250 Mitarbeitende, keine Bearbeitung von besonders schützenswerten Personendaten in grossem Umfang, Profiling mit hohem Risiko)



Nr.	Bearbeitungstätigkeit / Geschäftsprozess (Kurzbeschreibung der Tätigkeit)	Zwecke der Bearbeitung (z.B. - Leistungserbringung - Beschaffung - Kommunikation - Buchhaltung etc.)	Kategorien betroffener Personen (z.B. - Kunden - Lieferanten - Kooperationspartner - Mitarbeiter - Bewerber etc.)	Kategorien bearbeiteter Personendaten (z.B. -Kontaktdaten - Bankdaten - Vertragsdaten - Transaktionsdaten - Korrespondenz / E-Mails etc.	Besondere Datenkategorien gem. Art. 5 it. c revDSG (bspw. - Gesundheitsdaten, - religiöse, politische oder gewerkschaftliche Ansichten - Massnahmen der sozialen Hilfe etc.)	Kategorien der Daten-Empfänger (z.B. -Auftragsverarbeiter [externe Dienstleister wie IT-Support, Hosting- und Cloud-Anbieter etc.]
-----	--	--	--	---	---	--

### HAUPTTÄTIGKEIT

Beispiel 1	Erbringung von Rechtsdienstleistungen (inkl. Klient-Anwaltskorrespondenz)	Dokumentation der Leistungen, Kommunikation mit Klienten, Gegenparteien, Behörden, Gerichten und weiteren Kontakten	Klienten, Gegenparteien, Behörden	Kontaktdaten, Bankdaten, Vertragsdaten, Korrespondenz / E-Mails	ja / nein	
Beispiel 2	Lieferantenverwaltung	Beschaffung, Administration, Buchhaltung	Lieferanten	Kontaktdaten etc.	ja / nein	

### PERSONAL

Beispiel 3	Bewerbungsprozess (Analyse und Auswertung der Bewerbungsunterlagen; Interviews etc.)	Analyse und Beurteilung der Bewerbungsunterlagen, allenfalls Begründung eines Beschäftigungsverhältnisses, Kommunikation	BewerberInnen	Adressdaten, Lebenslauf, Qualifikationen, Familienstand, Berufsangaben	ja / nein	
Beispiel 4	Personalwesen / Führen von Personalakten	Personaladministration, Onboarding, Leistungsbeurteilung etc.	Mitarbeitende	Adressdaten, Lebenslauf, Qualifikationen, Familienstand, Berufsangaben, Arbeitszeiten, Bankdaten, Sozialversicherungsdaten Bestandes- und Vertragsdaten, Leistungsbewertungen, Gesundheitsdaten, Arbeitszeugnisse	ja / nein	



# Wesentliche neue Anforderungen / Umsetzung revDSG



- **Informationspflicht** (Art. 19 DSGVO)
  - Neu bei jeder Datenbeschaffung
  - Sinn und Zweck: Transparenz betr. Datenbearbeitungen
  - Mindestinhalt: Art. 19 Abs. 2 DSGVO
  - **Massnahme 2**: Datenschutzerklärung (für Website + Geschäftstätigkeit sowie für Mitarbeitende) -> *Aussendarstellung*

# Wesentliche neue Anforderungen / Umsetzung revDSG



- **Informationspflicht** (Art. 19 DSGVO / Art. 45c lit. b FMG)
  - Informationspflicht betr. Einsatz von Cookies und deren Zwecke in Datenschutzerklärung
  - Hinweis auf Ablehnungsmöglichkeit (sog. Opt-out-Prinzip)
  - **In CH: Kein Cookie-Banner auf Website erforderlich**

# Wesentliche neue Anforderungen / Umsetzung revDSG



- **Stärkung der Betroffenenrechte: wie insb. Auskunftsrecht (Art. 25 f. DSGVO / Art. 16 ff. DSV)**
  - Mindestinhalt der Auskunft (Art. 25 Abs. 2 lit. a – g DSGVO)
  - Allfällige Auskunftsbegehren ernst nehmen und standardisieren (Bestätigung, Identität überprüfen, Zuständigkeiten festlegen etc.)
  - Grds. Kostenlose Auskunftserteilung innert 30 Tagen
  - Einschränkungen des Auskunftsrecht (Verweigern, einschränken, aufschieben)
  - **Massnahme 3**: Betriebsintern Zuständigkeiten und Prozesse festlegen



# Wesentliche neue Anforderungen / Umsetzung revDSG



## • Outsourcing (Auftragsdatenbearbeitung), Art. 9 DSGVO

- Begriff: Auftragsdatenbearbeiter
- Auslagerung ist zulässig, wenn:
  - Übertragung durch Vertrag oder Gesetz erfolgt
  - Auftragsbearbeiter Personendaten bearbeitet wie Verantwortlicher
  - Keine Geheimhaltungspflicht entgegensteht und Datensicherheit gewährleistet ist
- Beizug Sub-Auftragsbearbeiter -> vorgängige Genehmigung des Verantwortlichen erforderlich
- **Massnahme 4**: Auftragsbearbeitungsvertrag schliessen (mit IT-Anbietern etc.).

# Wesentliche neue Anforderungen / Umsetzung revDSG

- **Datentransfer ins Ausland (Art. 16 DSGVO)**

- Angemessenheitsentscheid (Bundesrat) -> vgl. Liste mit Länder mit angemessenen Datenschutz in Anhang 1 der DSV
- Land mit angemessenem Schutzniveau -> unproblematisch
- Land ohne hinreichenden Schutz (wie z.B. USA) -> geeignete Garantien treffen (bspw. EU-Standarddatenschutzklauseln (SCC) inkl. Data Transfer Impact Assessment etc.) oder Einwilligung für konkreten Einzelfall einholen.
- **Massnahme 5**: SCC abschliessen mitsamt Data Transfer Impact Assessment (bei unsicheren Drittstaaten)



# Wesentliche neue Anforderungen / Umsetzung revDSG



- **Gewährung Datensicherheit** (Art. 8 DSGVO, Art. 1 ff. DSV)
  - Angemessene technische und organisatorische Massnahmen (TOM) treffen
  - Mindestanforderungen hängen von den jeweiligen Umständen und den daraus resultierenden Risiken ab\*, vgl. Art. 1 f. DSV):
  - **Massnahme 6**: Ergriffene TOM stichwortartig schriftlich festhalten.

\*Art der bearbeiteten Daten; Zweck, Art, Umfang der Bearbeitung; Ursachen des Risikos / hauptsächliche Gefahren; Stand der Technik und Implementierungskosten



# Technische und organisatorische Massnahmen: Bsp. Zugriffskontrolle

## 1. → Zugriffskontrolle¶

Massnahmen, damit berechnigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen.¶

¶

Getroffene Massnahmen:¶

- Login mit Benutzername und Passwort¶
- Anti-Virus-Software¶
- Firewall¶
- Schutz vor Schadsoftware / Einsatz Spamfilter¶
- Verwalten von Benutzerberechtigungen¶
- Bildschirmsperre¶
- IT-Reglement / Passwort-Policy¶
- Clean-Desk-Policy¶
- Aktenschredder / Datereg-Container¶
- Minimale Anzahl an Administratoren¶
- Sensibilisierung Mitarbeitende¶
- NDA mit Mitarbeitenden¶

# Wesentliche neue Anforderungen / Umsetzung revDSG



- **Meldepflicht von Verletzungen der Datensicherheit** (Art. 24 Abs. 1 DSG)
  - Meldung an Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (“EDÖB“)
  - Bei Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt (**Risikoabschätzung**)
  - So rasch als möglich (keine explizite Frist; EU: innert 72 h (Vergleichswert))
  - zusätzliche Meldung an betroffene Person, wenn zu ihrem Schutz erforderlich oder es der EDÖB verlangt
  - Mindestinhalt der Meldung: Art. 24 Abs. 2 DSG
  - **Massnahme 7**: Betriebsintern Zuständigkeiten und Prozesse festlegen
- **Nicht abschliessend: Ggf. weiterer Handlungsbedarf: DSFA, IT-Policy etc.**



# Zivil- und strafrechtliche Sanktionen bei Verstößen



- Klagen zum Schutz der Persönlichkeit nach Art. 28 ff. ZGB
- Bei Verletzung von Informations- und Auskunftspflichten sowie bei Verletzung von Sorgfaltspflichten\*:
  - Busse bis zu CHF 250'000 (Art. 60 DSG); Antragsdelikt
  - Busse richtet sich gegen die verantwortliche natürliche Person (i.d.R. Leitungsperson)
  - Imageschaden im Allgemeinen

\* insb. widerrechtliche Datenübermittlung ins Ausland, gesetzwidriger Beizug von Dritten sowie Nichteinhalten von Datensicherheitsstandards



# Datenschutz und Künstliche Intelligenz (KI)



- Das Datenschutzgesetz findet auch auf KI Anwendung.
- Beim Einsatz von KI-Tools -> immer Risikobeurteilung empfohlen
- Insb. kostenlos nutzbare Tools (wie ChatGPT Free, Microsoft Copilot etc.) sind aufgrund ihrer Ausgestaltung (Nutzung der Daten fürs Training etc.) für die Verwendung in KMU grundsätzlich nicht geeignet.
- **Empfehlung bei geschäftlicher Nutzung von KI:**
  - Kommerzielle, kostenpflichtige Tools verwenden.
  - Kurze Weisung zuhanden der Mitarbeitenden verfassen.



# Fragen



# Kontakt



BGPartner AG

Fabiola Weilenmann, Rechtsanwältin

Länggassstrasse 10, 3012 Bern

Tel: +41 (0)31 329 55 55

E-Mail: [weilenmann@bgpartner.ch](mailto:weilenmann@bgpartner.ch)





**Vielen Dank für Ihre  
geschätzte  
Aufmerksamkeit!**