# nDSG: Alles neu oder was?

MediData AG - EDI Podium

Luzern, 30.06.2023

Roman Böhni

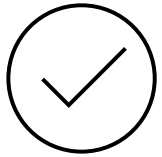
# Inhalt

- «Big Picture»
- Was bleibt bestehen?
- Was ändert sich?

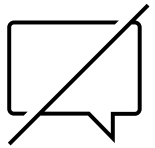
# «Big Picture»

- Totalrevidiertes Datenschutzgesetz tritt am **01.09.2023** in Kraft
  - Neues Datenschutzgesetz (nDSG)
  - Neue Datenschutzverordnung (DSV)
  - Neue Verordnung über die Datenschutzzertifizierung (VDSZ)
- Ziele
  - Erhöhung **Transparenz** bei der Bearbeitung von Personendaten
  - Stärkung **Betroffenenrechte**
  - Stärkung **Datenschutz-Governance**
  - Stärkung **Durchsetzbarkeit**
  - Bewahrung **Angemessenheitsbeschluss** der EU

# Was bleibt bestehen?

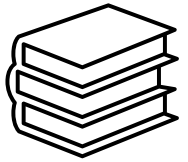


«Erlaubnis mit Verbotsvorbehalt»



Keine grunds. Einwilligungspflicht

Grundsätze der Datenbearbeitung
(nur punktuelle Anpassungen)



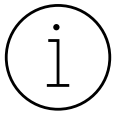
Keine umfassende Rechenschaftspflicht

**Kein Paradigmenwechsel, aber…**

# Was ändert sich? - Übersicht


Geltungsbereich

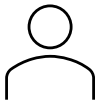

Bearbeitungs-verzeichnis

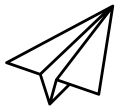

Informations-pflichten


Auftragsbe-arbeitung


Bekanntgabe ins Ausland


Datensicherheit


Betroffenen-rechte


Meldepflichten

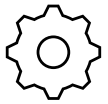

DSFA


Sanktionen


Begriffe

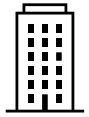

Aut. Einzelentsch. Profiling


«Privacy by design»


«Privacy by default»


Datenschutz-berater:in


«kleines» Berufsgeheimnis


Vertreter in der Schweiz


Kompetenzen EDÖB

**… Handlungsbedarf!**

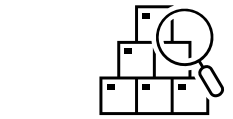
# Was ändert sich? - Geltungsbereich


- Persönlicher und sachlicher Geltungsbereich (Art. 2 nDSG)
  - Bearbeitung von Personendaten **natürlicher Personen** durch:
    - **Private Personen** (natürliche und juristische Personen)
    - **Bundesorgane** (inkl. Personen, die mit öffentlichen Aufgaben des Bundes betraut sind)

    Merke: Kantone, Gemeinden, mit öff. Aufgaben des Kantons betraute Personen etc.
    → kantonale DSG
- Räumlicher Geltungsbereich (Art. 3 nDSG)
  - Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden (**Auswirkungsprinzip**)

**Wichtigster Handlungsbedarf:**
- Klärung der anwendbaren gesetzlichen Bestimmungen (nDSG, kant. DSG, ausl. Recht)

# Was ändert sich? - Bearbeitungsverzeichnis

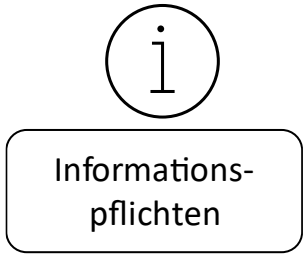


Bearbeitungs-
verzeichnis

- **Dokumentation** der Datenflüsse (mit Personenbezug)
- Für **Unternehmen** nur zwingend, wenn
  - > 250 Mitarbeitende
  - Bearbeitung sensitiver Daten in grossem Umfang
  - Profiling mit hohem Risiko
- **Mindestinhalt** gemäss Art. 12 nDSG
- Keine Vorgaben betr. **Form**
- Bundesorgane müssen ihre Verzeichnisse dem EDÖB melden

**Wichtigster Handlungsbedarf:**
- Klärung Bedarf (Aber: Für sämtliche Unternehmen empfohlen)
- Excel hat sich für KMU bewährt
- Festlegung Aufbewahrungsdauer von (Personen-)Daten

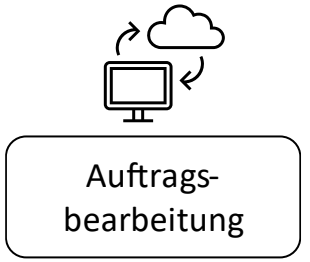
# Was ändert sich? - Informationspflichten




- Informationspflicht bei Beschaffung von Personendaten
- Mindestinhalt gem. Art. 19 nDSG
- Informationspflicht betr. autom. Einzelentscheidungen gem. Art. 21 nDSG
  - sofern Rechtsfolge oder erhebliche Beeinträchtigung für betroffene Person
  - Recht auf Überprüfung durch natürliche Person
  - Bundesorgane müssen autom. Einzelentscheidungen als solche kennzeichnen

**Wichtigster Handlungsbedarf:**
- Erstellung / Aktualisierung von Datenschutzerklärungen (allg. DSE auf Webseite, DSE für Mitarbeiter etc.)

# Was ändert sich? - Auftragsbearbeitung




- Auftragsbearbeiter darf Daten (nur) so bearbeiten wie Verantwortlicher
- Einhaltung Berufs-/Amtsgeheimnis/Vertraulichkeit
- Sorgfältige Auswahl, Instruktion und Kontrolle (**Due Diligence**)
- Abschluss **Auftragsbearbeitungsvertrag**
  - **Weisungsrecht** gegenüber Auftragsbearbeiter
  - Steuerung Beizug von **Subunternehmern** durch Auftragsbearbeiter (vorgängige Genehmigung)
  - Sicherstellung **Datensicherheit** (TOM)

**Wichtigster Handlungsbedarf:**
- Identifikation (beigezogene) Auftragsbearbeiter
- Due Diligence
- Sicherstellung Abschluss Auftragsbearbeitungsvertrag

# Was ändert sich? – Bekanntgabe ins Ausland


- Bekanntgabe ins Ausland zulässig, wenn
  - „sicheres Drittland“: **Angemessenheitsbeschluss** vorhanden (Anhang 1 DSV)
  - „unsicheres Drittland“: kein Angemessenheitsbeschluss vorhanden
    - **Garantien** (z.B. Standardvertragsklauseln, BCR) und **Transfer Impact Assessment** (TIA)
    - **Ausnahmen** (z.B. Einwilligung, Vertragsabwicklung, Rechtsdurchsetzung im Ausland)

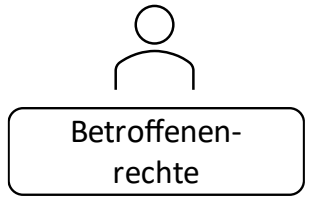
**Wichtigster Handlungsbedarf:**
- Erhebung grenzüberschreitende Bekanntgabe von Personendaten (konzernintern und –extern)
- Prüfung von Alternativen für Bekanntgabe in «unsichere Drittländer»
- Ergreifung zusätzlicher Massnahmen bei Bekanntgabe in «unsichere Drittländer»

# Was ändert sich? - Datensicherheit


- Schutzziele der Informationssicherheit (**Vertraulichkeit**, **Verfügbarkeit**, **Integrität**)
- Implementation und Dokumentation **T**echnische und **O**rganisatorische **M**assnahmen (**TOM**)
- **Risikobasierter** Ansatz (je grösser das Risiko einer Verletzung, desto höher die Anforderungen)
- Prüfung **Protokollierungspflicht** (Art. 4 DSV) und **Bearbeitungsreglement** (Art. 5 resp. 6 DSV)

**Wichtigster Handlungsbedarf:**
- Implementierung und Dokumentation von angemessenen TOM («Stand der Technik»)
- Prüfung Pflicht betr. Protokollierung und Bearbeitungsreglement

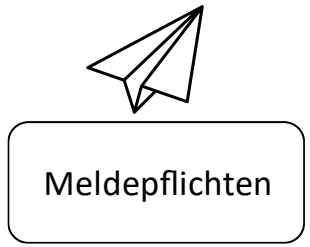
# Was ändert sich? - Betroffenenrechte




- Erweitertes Auskunftsrecht 
- Recht auf Auskunft über automatisierte Einzelentscheide
- Datenportabilität
- Recht auf Löschung und Vernichtung (neu explizit erwähnt)

**Wichtigster Handlungsbedarf:**
- Festlegung Prozess und Zuständigkeiten bei Geltendmachung von Betroffenenrechten
- Schulung Mitarbeitende
- Sicherstellung Funktionalitäten zwecks Datenportabilität («gängiges elektronisches Format»)

# Was ändert sich? - Meldepflichten




- Verletzung der Datensicherheit («Data Breach»)
  - Verletzung von Vertraulichkeit, Integrität und/oder Verfügbarkeit von Personendaten
- Meldung an
  - EDÖB: bei hohem Risiko für die betroffene Person («so rasch als möglich»)
  - betroffene Person: wenn es deren Schutz erfordert oder EDÖB dies verlangt
  - Verantwortliche: durch Auftragsbearbeiterin («so rasch als möglich»)

**Wichtigster Handlungsbedarf:**
- Festlegung Prozess und Zuständigkeiten bei Data Breaches

# Was ändert sich? - DSFA


- strukturierte **Risikoanalyse** bezüglich eines **geplanten** Datenverarbeitungsprozesses mit **hohem Risiko** für Betroffene
- Vorgehen
  - **Schwellenwertanalyse**
  - Beschreibung des Verfahrens
  - Identifikation und Bewertung der **Risiken**
  - Festlegung von **Massnahmen** zur Risikominimierung
  - U.U. **Konsultation** EDÖB oder Datenschutzberater:in
  - Verabschiedung durch **Geschäftsleitung**
  - **Risikoüberwachung** und regelmässige Überprüfung

**Wichtigster Handlungsbedarf:**
- Schwellenwertanalyse der Prozesse im Bearbeitungsverzeichnis
- Bei hohem Risiko: Durchführen DSFA
- Festlegung Zuständigkeiten (DSFA hat vor geplanter Datenbearbeitung zu erfolgen)

# Was ändert sich? - Sanktionen

Sanktionen

- **Höchstbusse**: CHF 250’000.- (evtl. Strafregistereintrag -> nur für Behörden einsehbar)
- **Adressat:** verantwortliche natürliche Person (Ausnahmsweise: fehlbares Unternehmen)
- **Voraussetzung:** Vorsatz / Eventualvorsatz und Strafantrag der betroffenen Person
- **Strafbar:**
  - Vorsätzliche Verletzung von **Informationspflichten**
  - Vorsätzlicher Verstoss gegen **Auskunftsrecht** (falsche/unvollständige Auskunft)
  - Vorsätzliche Nichteinhaltung Mindestvorgaben für angemessene **Datensicherheit**
  - Vorsätzliche Verletzung von Vorgaben bei **Auftragsbearbeitung**
  - Vorsätzliche Verletzung von Vorgaben bei **Datenbekanntgabe ins Ausland**
  - Vorsätzliche Verletzung **berufliche Schweigepflicht**
  - Vorsätzliche Verweigerung **Mitwirkung EDÖB** im Falle einer Untersuchung (inkl. Falschauskünfte)
- **Hinweis:**
  - Busse ist nicht versicherbar (Strafverteidigung und Verfahrenskosten hingegen schon)
  - Busse darf nicht vom Unternehmen übernommen werden (Strafverteidigung und Verfahrenskosten hingegen schon)

**Wichtigster Handlungsbedarf:**
- Einhaltung Datenschutzvorgaben ☺
- Befähigung und Schulung der Mitarbeitenden

# Vielen Dank!

**Roman Böhni**
Rechtsanwalt, MLaw
BSc Wirtschaftsinformatik

Murbacherstrasse 3 , 6003 Luzern
+41 41 227 51 00
www.adlegem.ch