Datenschutz im Gesundheitswesen

Dr. Christian Schönfeld, LLM, 9. November 2023

PRAGER DREIFUSS

ATTORNEYS AT LAW

Prager Dreifuss AG
Zürich, Bern, Brüssel
www.prager-dreifuss.com

Mühlebachstrasse 6, CH-8008 Zürich
T +41 44 254 55 55, F +41 44 254 55 99

Schweizerhof-Passage 7, CH-3001 Bern
T +41 31 327 54 54, F +41 31 327 54 99

Avenue Louise 235, B-1050 Bruxelles
T +32 2 537 09 49, F +32 2 537 21 16

Agenda

1. Hintergrund und Ausgangslage
2. Grundlagen / Zulässigkeit von Datenbearbeitungen
3. Betroffenenrechte
4. Flankierende Massnahmen
5. Handlungsbedarf

1. Hintergrund und Ausgangslage

Hintergrund und Ausgangslage

Steigende Bedeutung des Datenschutzes und internationale Bestrebungen

- Insb. DSGVO in der EU

Revision des Schweizer Datenschutzgesetzes (DSG)

- Anpassung an die technologischen Entwicklungen
- Förderung der Wettbewerbsfähigkeit der Schweiz
- Kompatibilität mit Anforderungen der DSGVO
- Inkrafttreten: 1. September 2023
- Strafrechtliche Bussen oder Schadenersatz bei Verletzung des DSG möglich

Wesentlichkeit des Datenschutzes im Gesundheitswesen

- Umfangreiche Bezugspunkte zu Gesundheitsdaten (besonders «heikle» Personendaten)
- Zunehmendes Bewusstsein für Datenschutz bei den betroffenen Personen
- Technische Entwicklungen, z.B. Telemedizin, elektronisches Patientendossier, Forschung, aber auch viele «alltägliche» Datenbearbeitungen, z.B. Website, EDV, Abrechnungen, Personalwesen, Werbung etc.

2. Grundlagen / Zulässigkeit von Datenbearbeitungen

- Wichtigste Begriffe
- Grundregeln für die Bearbeitung von Personendaten
- Grundsätze der Datenbearbeitung
- Datensicherheit
- Datenschutzrechtliche Rollenverteilung und Datenexporte

Wichtigste Begriffe

Personendaten

- Alle Angaben, die sich auf eine bestimmte oder bestimmbare *natürliche* Person beziehen
- Z.B.:
  - Namen
  - Geburtsdatum
  - Adresse
  - AHV-Nummer
  - Versichertennummer
  - Krankengeschichte

Betroffene Person

- Natürliche Person, über die Personendaten bearbeitet werden

Besonders schützenswerte Personendaten

- Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten
- Daten über die **Gesundheit**, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie
- **Genetische Daten**
- **Biometrische Daten**, die eine natürliche Person eindeutig identifizieren
- Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen
- Daten über Massnahmen der sozialen Hilfe

Bearbeiten

- **Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren**, insb. das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten

Bekanntgeben

- Das Übermitteln oder Zugänglichmachen von Personendaten

Grundregeln für die Bearbeitung von Personendaten

Bei **Privaten**
Grundsatz: Bearbeitung zulässig

Unzulässig ist Bearbeitung, wenn sie zu **Persönlichkeitsverletzung** führt, insbesondere

Bearbeitung entgegen den Grundsätzen der Datenbearbeitung (nächste Folie)	Bearbeitung entgegen der ausdrücklichen Willenserklärung der betroffenen Person	*Bekanntgabe von besonders schützenswerten Personendaten an Dritte*

Sofern Persönlichkeitsverletzung: Bearbeitung ist widerrechtlich, falls kein **Rechtfertigungsgrund** vorliegt

Einwilligung (muss ausdrücklich erfolgen bei Bearbeitung besonders schützenswerter Personendaten)	Überwiegende Interessen (d.h. Interessenabwägung im konkreten Einzelfall)	Gesetzliche Bestimmungen

Bei «**Bundesorganen**»

Bearbeitung nur bei Bestehen einer gesetzlichen Grundlage

Grundsatz: Auch in Verordnung möglich	Formelles Gesetz in bestimmten Fällen nötig, insb. bei Bearbeitung von besonders schützenswerten Personendaten

Ausnahmen vom Erfordernis der gesetzlichen Grundlage

Bewilligung des Bundesrates	Einwilligung	Notwendigkeit zum Schutz des Lebens oder der körperlichen Unversehrtheit

Grundsätze der Datenbearbeitung

Grundregeln, welche bei der Bearbeitung eingehalten werden müssen

- **Rechtmässigkeit**
- **Treu und Glauben** und **Verhältnismässigkeit**
- **Zweckbindung**: Bearbeitung nur für diejenigen Zwecke, die bei der Datenbeschaffung erkennbar waren oder mit diesen vereinbar sind
- **Vernichtung** und Grundsatz der **Datenminimierung**, wonach Datenbearbeitungen von Beginn weg so anzusetzen sind, dass möglichst wenig Daten anfallen und bearbeitet werden oder dass Daten zumindest nur kurze Zeit aufbewahrt werden
- **Richtigkeit**: Jede Person, die Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern und angemessene Massnahmen treffen, um im Hinblick auf ihren Zweck unrichtige oder unvollständige Daten zu berichtigten, löschen oder vernichten
- Daneben weitere Grundsätze

Datensicherheit

Prinzip der Datensicherheit

- Gewährleistung einer dem Risiko angemessenen Datensicherheit durch geeignete technische und organisatorische Massnahmen
- Massnahmen zur Vermeidung von Verletzungen der Datensicherheit
- Insb. *Vertraulichkeit*, *Verfügbarkeit* und *Integrität* der bearbeiteten Personendaten
- Beispiele: Zugriffsbeschränkungen, Firewalls, Penetration Tests, Pseudonymisierung einschliesslich Datenverschlüsselung, Backups, Zugangsbeschränkungen, sichere Entsorgungstechniken, Bewachung, Alarmanlagen, Reglemente, Weisungen, Schulungen

Datenschutzrechtliche Rollenverteilung und Bekanntgabe an Dritte

Betroffene Person

- Natürliche Person, über die Daten bearbeitet werden

Verantwortlicher (Controller)

- Private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den *Zweck* und die *Mittel* der Bearbeitung entscheidet

Auftragsbearbeiter (Processor)

- Private Person oder Bundesorgan, die oder das *im Auftrag des Verantwortlichen* Personendaten bearbeitet

Abgrenzung zwischen Controller und Processor oftmals **schwierig**:

- Auftragsverhältnis allein genügt nicht; Schwerpunkt muss in der Bearbeitung von Personendaten liegen
- Mehrere Konstellationen möglich:
  - *Auftragsdatenbearbeitung*: Controller überträgt Datenbearbeitung an Processor
  - *Joint-Controller-Sachverhalt*: Mehrere Controller bestimmen *gemeinsam* über Mittel und Zweck einer Datenbearbeitung
  - Transfers zwischen *unabhängigen Controllern*

→ In all diesen Konstellationen sind vertragliche Regelungen sinnvoll oder sogar zwingend!

Datenexporte (= internationale Datentransfers)

Angemessener Schutz gewährleistet

- Bundesratsbeschluss
- Bekanntgabe zulässig
- Deckt v.a. EWR-Länder ab

Angemessener Schutz durch zusätzliche Massnahmen, z.B.

- Vertragliche Datenschutzklauseln
- Verbindliche unternehmensinterne Datenschutzvorschriften

Ausnahmen, z.B.

- Einwilligung
- Zusammenhang mit Abschluss oder Abwicklung eines Vertrages
- Öffentliches Interesse oder Durchsetzung von Rechtsansprüchen
- Schutz des Lebens oder der körperlichen Unversehrtheit
- Allgemein zugängliche Daten
- Gesetzliches Register

3. Betroffenenrechte

- Informationspflicht
- Auskunftsrecht
- Recht auf Datenherausgabe und -übertragung
- Weitere Rechtsansprüche

Informationspflicht

Informationspflicht bei der Beschaffung von Personendaten

Pflicht des Verantwortlichen

Gilt grundsätzlich für alle Beschaffungen von Personendaten

Diejenigen Informationen, die erforderlich sind, damit die betroffene Person ihre Rechte nach DSG geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist

Beispiel: Datenschutzerklärung auf Website oder Papier

Ausnahmen und Einschränkungen

Informationspflicht entfällt insb.:

- Betroffene Person verfügt bereits über die entsprechenden Informationen
- Bearbeitung ist gesetzlich vorgesehen
- Verantwortlicher ist private Person, die gesetzlich zur Geheimhaltung verpflichtet ist
- Information nicht möglich oder unverhältnismässig aufwendig (nur bei Beschaffung nicht direkt bei der betroffenen Person)

Einschränkung, Aufschub oder Verzicht möglich:

- Überwiegende Interessen Dritter
- Information vereitelt den Zweck der Bearbeitung
- Überwiegende Interessen des Verantwortlichen und keine Bekanntgabe an Dritte

Auskunftsrecht

Anspruch

- Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden
- Insbesondere Informationen zu:
  - Identität und Kontaktdaten des Verantwortlichen
  - Bearbeitete Personendaten als solche
  - Bearbeitungszweck
  - Aufbewahrungsdauer oder Kriterien zu deren Festlegung
  - Verfügbare Angaben über die Herkunft der Personendaten, soweit nicht bei der betroffenen Person beschafft
  - Empfänger oder Kategorien von Empfängern
- Vorgängiger Verzicht unzulässig
- Grundsätzlich kostenlos
- Innert 30 Tagen

Einschränkungen unter Umständen

- Gesetz
- Überwiegende Interessen Dritter
- Gesuch ist offensichtlich unbegründet oder querulatorisch
- Private: Überwiegendes Interesse des Verantwortlichen und keine Bekanntgabe an Dritte
- Bundesorgane: Innere und äussere Sicherheit oder Gefährdung von Verfahren

Recht auf Datenherausgabe und -übertragung

Recht auf **Datenportabilität**

Grundsatz

- Jede Person kann vom Verantwortlichen unter gewissen Voraussetzungen die Herausgabe (oder die Übertragung) ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format verlangen
- Grundsätzlich kostenlos

Einschränkungen

- Grundsätzlich wie beim Auskunftsrecht

Weitere Rechtsansprüche

- Berichtigung
- Verbot der Datenbearbeitung
- Verbot der Bekanntgabe
- Löschung oder Vernichtung von Personendaten
- Bestreitungsvermerk
- Mitteilung an Dritte oder Veröffentlichung der Massnahme

4. Flankierende Massnahmen

- Verzeichnis der Bearbeitungstätigkeiten
- Datenschutz-Folgenabschätzung
- Meldepflicht für Verletzungen der Datensicherheit
- Weitere flankierende Massnahmen

Verzeichnis der Bearbeitungstätigkeiten

Erstellung als Pflicht des Verantwortlichen und des Auftragsbearbeiters

Enthält Angaben zu:

- Identität von Auftragsbearbeiter und/oder Verantwortlichem
- Bearbeitungszweck
- Kategorien betroffener Personen
- Kategorien bearbeiteter Personendaten
- Kategorien von Bearbeitungen
- Kategorien der Empfänger
- Aufbewahrungsdauer
- Massnahmen zur Gewährleistung der Datensicherheit
- Bekanntgabe ins Ausland

Ausnahmen

- Für Private: Unternehmen mit weniger als 250 Mitarbeitern und natürliche Personen müssen kein Verzeichnis der Bearbeitungstätigkeiten führen, ausser:
  - es werden *besonders schützenswerte Personendaten in grossem Umfang* bearbeitet oder
  - es wird ein Profiling mit hohem Risiko durchgeführt

Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzung

- Pflicht des Verantwortlichen, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann
- Hohes Risiko ergibt sich, insb. bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung
- Beschreibung der geplanten Bearbeitung, Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie Massnahmen zum Schutz der Persönlichkeit und der Grundrechte
- Verzicht auf Datenschutz-Folgenabschätzung durch private Verantwortliche möglich bei
  - gesetzlicher Pflicht zur Datenbearbeitung
  - Zertifizierung
  - Verhaltenskodex

Konsultation des EDÖB

- Falls trotz Massnahmen hohes Risiko und kein Datenschutzberater
- EDÖB teilt Einwände und geeignete Massnahme mit

Meldepflicht bei Verletzungen der Datensicherheit

Verantwortlicher meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, ***die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt***

- Vorgängige Festlegung von Prozessen und Aufarbeitung von Standard-Vorlagen empfehlenswert

Meldung beinhaltet insbesondere:

- Art der Verletzung der Datensicherheit
- Deren Folgen
- Ergriffene Massnahmen

EDÖB kann Information der betroffenen Person verlangen

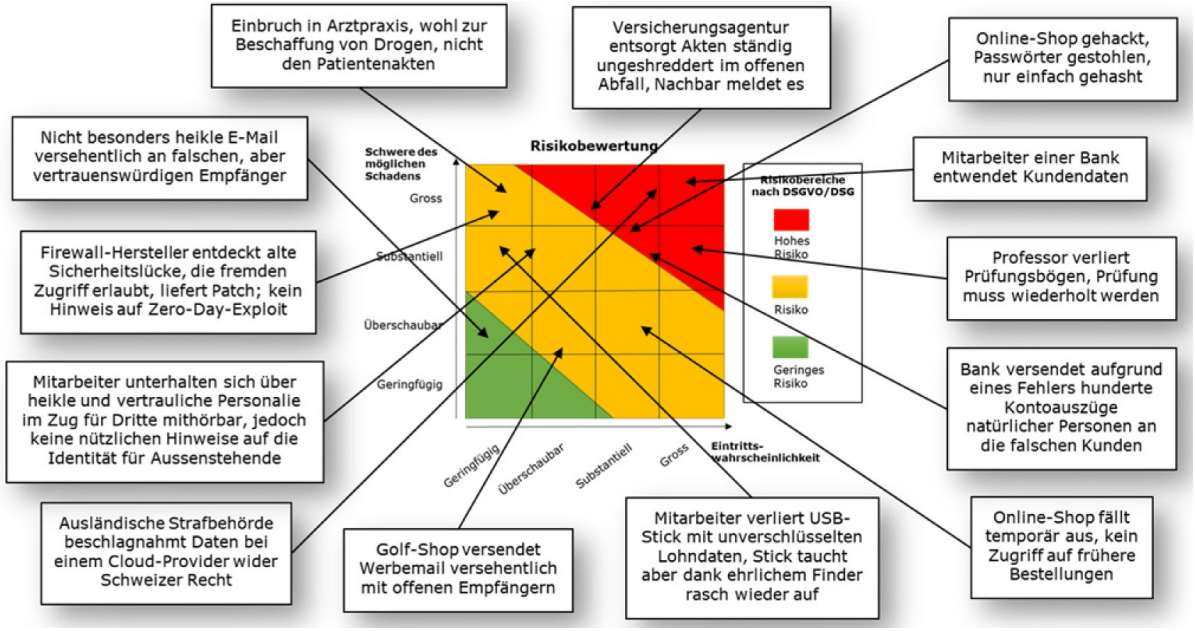
- Aufschub, Einschränkung oder Verzicht unter Umständen möglich

Aber

Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich ***jede*** Verletzung der Datensicherheit

Verletzung der Datensicherheit

Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden



Quelle: Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020, S. 61

Weitere flankierende Massnahmen

Datenschutzberater

- Nicht zwingend für private Verantwortliche
- Anlaufstelle für die betroffenen Personen und für die Behörden, die in der Schweiz für den Datenschutz zuständig sind
- Namentlich folgende Aufgaben
  - Schulung und Beratung des privaten Verantwortlichen in Fragen des Datenschutzes
  - Mitwirkung bei der Anwendung von Datenschutzvorschriften
- Ermöglicht unter gewissen Bedingungen Verzicht auf Konsultation des EDÖB infolge Datenschutz-Folgenabschätzung

Schweizer Vertreter

- Unter Umständen nötig für private Verantwortliche mit ausländischem Sitz oder Wohnsitz, wenn sie Personendaten von Personen in der Schweiz bearbeiten
- Anlaufstelle für betroffene Personen und EDÖB
- Pflichten
  - Führt Verzeichnis der Bearbeitungstätigkeiten
  - Evtl. Weiterleitung von Angaben an EDÖB
  - Auskunft an betroffene Personen

Weitere mögliche Massnahmen

- Verhaltenskodizes von Berufs-, Branchen- und Wirtschaftsverbänden
- Zertifizierungen

- Von untergeordneter Bedeutung

5. Handlungsbedarf

Handlungsbedarf

Feststellung der Ausgangslage

- **Erhebung der verschiedenen aktuellen Prozesse, bei denen Personendaten bearbeitet werden:**

- Betroffene Personen
- Arten von Personendaten
- Zweck der Bearbeitung
- Mögliche Rechtfertigungsgründe
- Externe Dienstleister
- Datenschutzrechtliche Rollen (Verantwortlicher, Auftragsbearbeiter)
- Übermittlungen ins Ausland

Prioritärer Handlungsbedarf

- **Erarbeitung der erforderlichen Datenschutzdokumentation:**

- Datenschutzerklärungen
- AGB
- Verträge
- Verzeichnis der Bearbeitungstätigkeiten
- Vorlagen für Meldungen von Verletzungen der Datensicherheit
- Vorlagen für Beantwortung von Auskunftsbegehren
- Evaluation und Anpassungen bei Transfers in unsichere Drittstaaten

Sekundärer Handlungsbedarf

- **Festlegung der erforderlichen Datenschutzprozesse und -konzepte:**

- Datenschutzverantwortlicher
- Festlegung interner Meldeprozesse bei Verletzung der Datensicherheit
- Festlegung Konzepte zur Aufbewahrung und Vernichtung von Personendaten
- Festlegung von Prozessen zur Nachführung der Datenschutz-Dokumentation
- Festlegung von Prozessen zur Umsetzung der Datenschutz-Folgenabschätzungen
- Festlegung eines Aufbewahrungskonzepts für Einwilligungserklärungen in Datenbearbeitungen
- Festlegung von Prozessen zur Erfüllung des Rechts auf Datenherausgabe und Datenübertragung

Vgl. Bieri/Powell, Die Totalrevision des Bundesgesetzes über den Datenschutz, in: Jusletter, 16. November 2020, S. 17 f.

PRAGER
DREIFUSS

Vielen Dank

Prager Dreifuss AG

Mühlebachstrasse 6, CH-8008 Zürich
T +41 44 254 55 55, F +41 44 254 55 99

www.prager-dreifuss.com