10. Management Symposium für Führungspersonen im Gesundheitswesen

26. Oktober 2023

Datenschutz
– Was muss die Praxis tun?

Michael Hochstrasser

Prof. Dr. iur., Rechtsanwalt

Einleitung

(Neue Zürcher Zeitung, 24. Oktober 2023)

Abo-Modell für Facebook und Instagram

Meta-Chef Mark Zuckerberg will Geld oder Daten von den Nutzern

cah. · In Zukunft sollen die Konsumenten wählen können: Entweder entscheiden sie sich für eine werbefreie Version von Facebook und Instagram, dann haben sie eine Abonnementsgebühr zu entrichten; oder sie stellen dem Meta-Konzern ihre Daten zur Verfügung und erhalten dann personalisierte Werbung. Die EU will die Nutzung personalisierter Daten eigentlich verbieten. Mit der Möglichkeit des Abonnements lässt Zuckerberg den Nutzern nun die Wahl. Die EU prüft gegenwärtig die Vorschläge. Ein Facebook-Abonnement soll 13 Euro pro Monat kosten, Instagram dazu soll noch 6 Euro zusätzlich kosten.

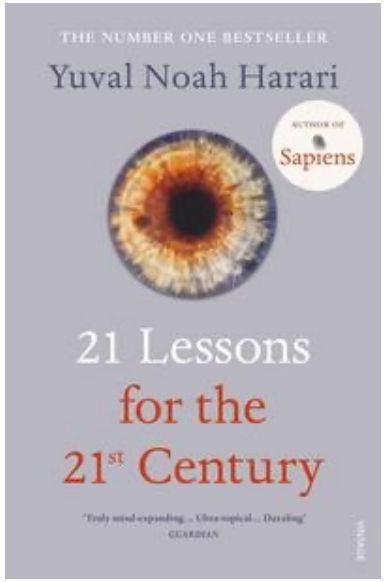
Von Interesse wäre die Abo-Version auch für die Ökonomen. Sie könnten berechnen, wie hoch der volkswirtschaftliche Wert der Online-Dienste ist. Durch die Gratisversionen mit der Werbung werden diese Zahlen verschleiert. Gleichzeitig würde sich auch zeigen, wie wichtig den Nutzern der Datenschutz ist.

Wirtschaft, Seite 20

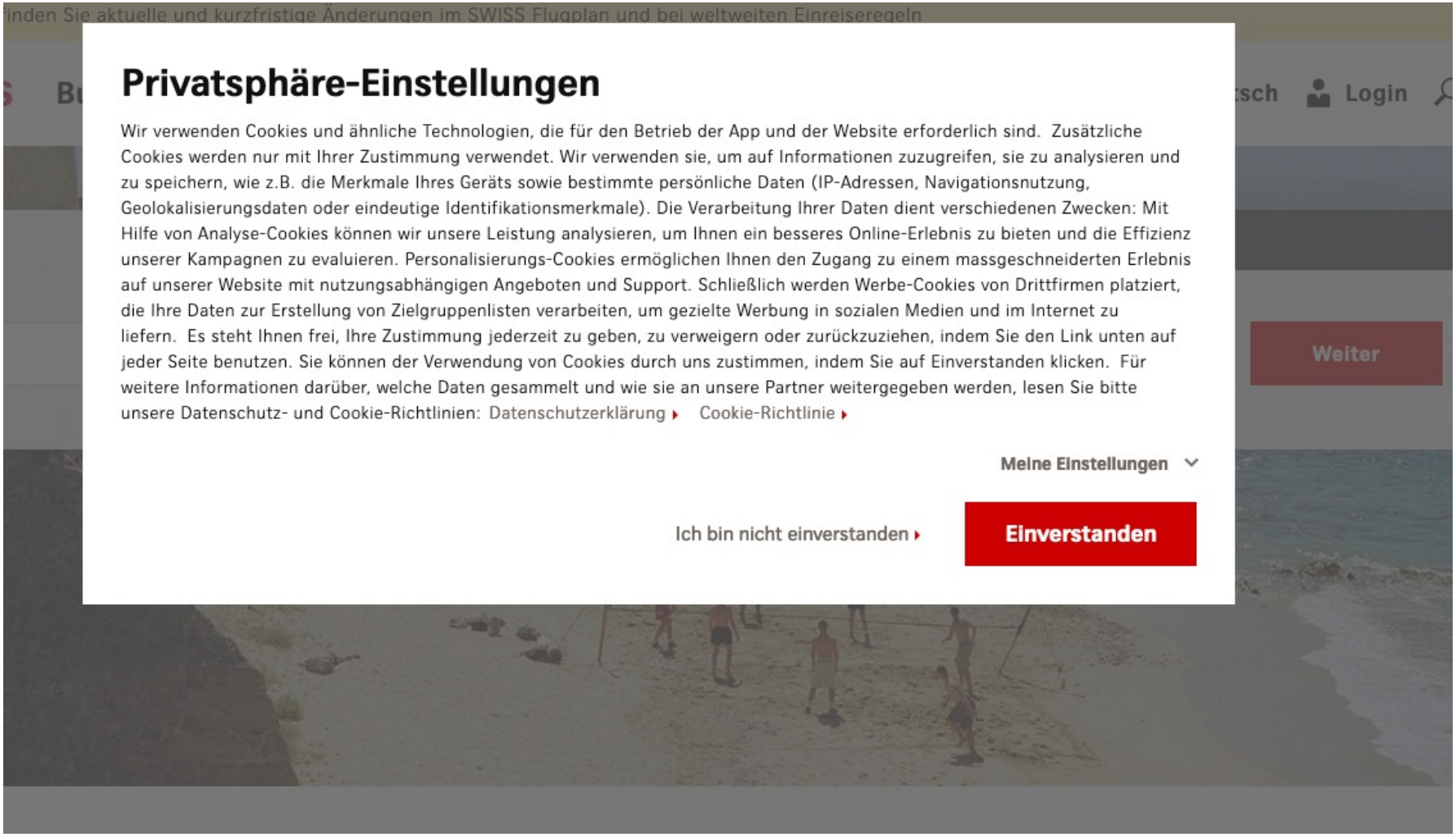
Einleitung

"People are happy to give away their most valuable asset – their personal data – in exchange for free email services and funny cat videos. It is a bit like African and Native America tribes who unwittingly sold entire countries to European imperialists in exchange for colourful beads and cheap trinkets."

(Yuval Noah Harari, 21 Lessons for the 21st Century)



Einleitung


inden Sie aktuelle und kurzfristige Änderungen im SWISS Flugplan und bei weltweiten Einreiseregeln
Login
Weiter
Privatsphäre-Einstellungen
Wir verwenden Cookies und ähnliche Technologien, die für den Betrieb der App und der Website erforderlich sind. Zusätzliche Cookies werden nur mit Ihrer Zustimmung verwendet. Wir verwenden sie, um auf Informationen zuzugreifen, sie zu analysieren und zu speichern, wie z.B. die Merkmale Ihres Geräts sowie bestimmte persönliche Daten (IP-Adressen, Navigationsnutzung, Geolokalisierungsdaten oder eindeutige Identifikationsmerkmale). Die Verarbeitung Ihrer Daten dient verschiedenen Zwecken: Mit Hilfe von Analyse-Cookies können wir unsere Leistung analysieren, um Ihnen ein besseres Online-Erlebnis zu bieten und die Effizienz unserer Kampagnen zu evaluieren. Personalisierungs-Cookies ermöglichen Ihnen den Zugang zu einem massgeschneiderten Erlebnis auf unserer Website mit nutzungsabhängigen Angeboten und Support. Schließlich werden Werbe-Cookies von Drittfirmen platziert, die Ihre Daten zur Erstellung von Zielgruppenlisten verarbeiten, um gezielte Werbung in sozialen Medien und im Internet zu liefern. Es steht Ihnen frei, Ihre Zustimmung jederzeit zu geben, zu verweigern oder zurückzuziehen, indem Sie den Link unten auf jeder Seite benutzen. Sie können der Verwendung von Cookies durch uns zustimmen, indem Sie auf Einverstanden klicken. Für weitere Informationen darüber, welche Daten gesammelt und wie sie an unsere Partner weitergegeben werden, lesen Sie bitte unsere Datenschutz- und Cookie-Richtlinien: Datenschutzerklärung Cookie-Richtlinie
Meine Einstellungen
Ich bin nicht einverstanden
Einverstanden

Einleitung

Art. 321 StGB (Verletzung des Berufsgeheimnisses)

"Geistliche, Rechtsanwälte, […], Ärzte, Zahnärzte, Chiropraktoren, Apotheker, Hebammen, Psychologen, Pflegefachpersonen, Physiotherapeuten, Ergotherapeuten, Ernährungsberater, Optometristen, Osteopathen sowie ihre Hilfspersonen, die ein Geheimnis offenbaren, das ihnen infolge ihres Berufes anvertraut worden ist oder das sie in dessen Ausübung wahrgenommen haben, werden, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft."

- über Beendigung der Berufsausübung hinaus
- keine Strafbarkeit bei Einwilligung und Entbindung
- Vorbehalt Meldepflichten, Zeugnispflicht etc.

Einleitung

Übersicht

1. Ziele und Grundsätze des Datenschutzes
2. das revidierte DSG: neue Pflichten
3. Datenschutz im Alltag einer Arztpraxis
4. Fragen

1.

Ziele und Grundsätze des Datenschutzes

Der Begriff der "Personendaten"

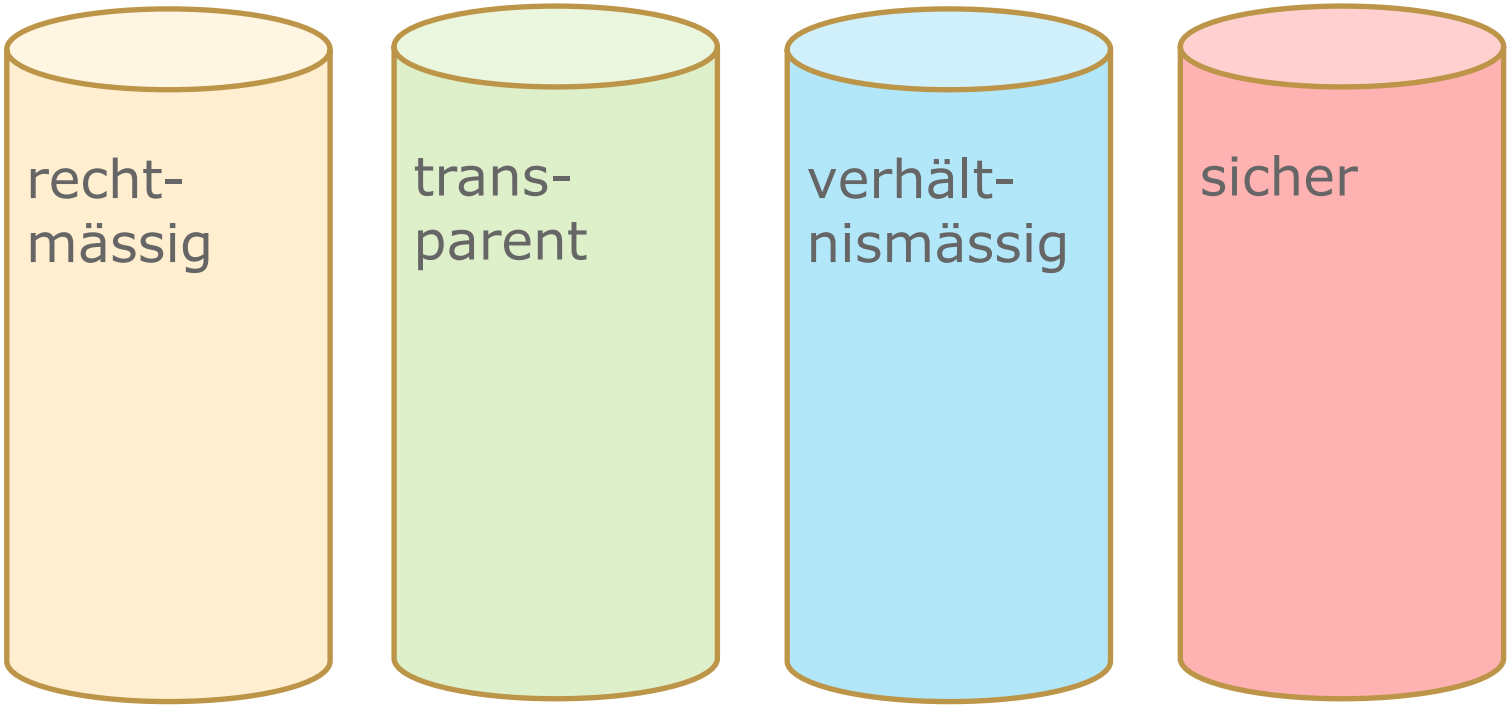
- **Personendaten** = alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 5 lit. a nDSG)

  Beispiele:
  - Name, Adresse
  - Geburtsdatum, Geschlecht
  - E-Mail-Adresse
  - Log-in Daten
  - Bilder (einer identifizierbaren Person)
  - Diagnose
  - AHV-Nummer
  - Kontonummer

- **besonders schützenswerte Personendaten** = (u.a.) Daten über Gesundheit oder Intimsphäre; religiöse, weltanschauliche oder politische Ansichten oder Tätigkeiten; genetische Daten

Grundsätze des Datenschutzes

Eine Datenbearbeitung muss Folgendes sein:



Rechtmässigkeit

- Personendaten dürfen nur rechtmässig bearbeitet werden (Art. 6 Abs. 1 DSG)
- die Datenbearbeitung ist unzulässig, wenn sie gegen gesetzliche Bestimmungen verstösst

  Beispiel: Öffnen eines Briefes/einer E-Mail durch einen Nichtberechtigten

Bearbeitung nach Treu+Glauben / Transparenz

- die Bearbeitung von Personendaten hat nach Treu und Glauben zu erfolgen (Art. 6 Abs. 2 DSG)
- Zweckbindung: Daten dürfen nur zu einem bestimmten Zweck beschafft werden (Art. 6 Abs. 3 DSG)
- die Beschaffung der Personendaten und deren Bearbeitungszweck müssen für die betroffene Person **erkennbar** sein (Art. 6 Abs. 3 DSG)

  Beispiel: Das Einholen von Auskünften bei Dritten (Referenzen) ohne das potentielle Wissen der Bewerber widerspricht dem Grundsatz von Treu und Glauben

Verhältnismässigkeit

- die Datenbearbeitung muss verhältnismässig sein (Art. 6 Abs. 2 DSG)

  dazu gehört unter anderem:

- nur jene Daten erheben, die erforderlich sind
- die Daten vernichten oder anonymisieren, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 6 Abs. 4 DSG)
  - Anonymisierung: Zuordnung der Daten zu einer bestimmten Person wird verhindert oder ist nur noch mit grossem Aufwand möglich
  - Pseudonymisierung: Ersetzung der intendifizierbaren Daten durch eine neutralen Datensatz (Pseudonym); mit dem Schlüssel lässt sich die Pseudonymisierung rückgängig machen
- Datenschutz durch Technikgestaltung (Privacy by Design)
- Datenschutzfreundliche Voreinstellungen (Privacy by Default)

Datensicherheit

- Personendaten müssen durch angemessene technische oder organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 8 DSG)

  dazu gehört unter anderem:

  - kein Zugang für unbefugte Dritte (Zugangskontrolle)
  - nur Zugriff auf Daten, die zur Aufgabenerfüllung nötig sind; keine Dokumente herumliegen lassen; Passwortschutz; Bildschirmsperre etc. (Zugriffskontrolle)
  - der Verantwortliche muss gewährleisten, dass Gesundheitsdaten ausschliesslich an den berechtigten Empfänger gelangen (Bekanntgabekontrolle)
  - Verhindern von unbefugtem Verändern der Daten; regelmässige Sicherungskopien (Speicherkontrolle)
  - Virenschutz (Firewall, Verschlüsselung etc.)
  - Schulung von Mitarbeitern, Erlass von Weisungen etc.

Ausserdem: Richtigkeit

- der Datenbearbeiter hat sich zu vergewissern, dass die bearbeiteten Personendaten richtig sind
- er hat angemessene Massnahmen zu treffen, um unrichtige oder unvollständige Daten zu berichtigen oder zu löschen (Art. 6 Abs. 5 DSG)

  Beispiel: Sicherstellung, ob Daten richtig in EDV-Systeme eingegeben wurden oder keine Verwechslungen vorliegen

Ausserdem: Betroffenenrechte

- Auskunftsrecht (Art. 25 DSG)
  - Jede betroffene Person kann verlangen, dass der Verantwortliche bekannt gibt, ob er Personendaten von ihr bearbeitet und wenn ja, welche
  - Auskunftserteilung grundsätzlich innert 30 Tagen
  - grundsätzlich kostenlos; Ausnahme: wenn die Beantwortung des Auskunftsgesuchs besonders aufwendig ist, kann eine Kostenbeteiligung von max. CHF 300.-- verlangt werden; die anfallenden Kosten sind vorgängig mitzuteilen
- Berichtigungsrecht (Art. 32 Abs. 1 DSG)
- Anbringung eines Bestreitungsvermerks (Art. 32 Abs. 3 DSG)
- Recht auf Datenherausgabe und -übertragung (Datenportabilität; Art. 28 DSG): Herausgabe in einem gängigen elektronischen Format

2.

das revidierte DSG: neue Pflichten

Das revidierte Datenschutzgesetz

- Das schweizerische Datenschutzgesetz (DSG) ist revidiert worden:
  - am **1. September 2023** in Kraft getreten
  - sofort anwendbar (keine Übergangsfrist)
- Das neue Recht bringt neue Pflichten – auch für Arztpraxen, insbesondere:
  - Datenschutzerklärung
  - Verzeichnis der Bearbeitungstätigkeiten
  - Verträge mit Auftragsdatenbearbeitern
  - Datenschutz-Folgenabschätzung

Informationspflicht

- Grundsatz: Wer Personendaten beschafft, muss die betroffene Person darüber informieren (Art. 19 DSG)
- Inhalt der Information: Identität und Kontaktdaten des Verantwortlichen, Bearbeitungszweck, ggf. Empfänger
- keine Formvorschrift;
  häufig mittels **Datenschutzerklärung** auf Webseite;
  auch möglich: in der Praxis auflegen, auf Patientenformular etc.
- Ausnahmen (Art. 20 DSG):
  keine Information ist (u.a.) nötig, wenn
  - die betroffene Person bereits über entsprechende Informationen verfügt
  - die Bearbeitung gesetzlich vorgesehen ist (z.B. Dokumentation Krankengeschichte; Führen Personaldossier)
  - überwiegende private oder öffentliche Interessen dies erfordern.

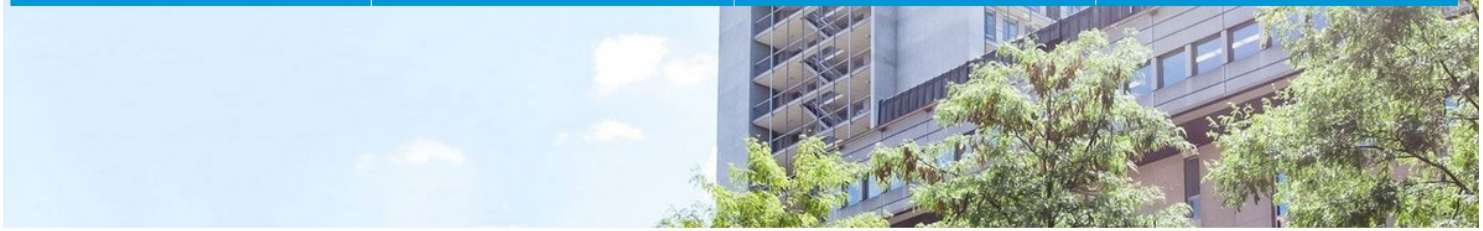
Beispiel: Datenschutzerklärung

+NOTFALL VERANSTALTUNGEN BAUINFO KONTAKT Suchbegriff

KSW
KANTONSSPITAL WINTERTHUR

PATIENTEN & BESUCHER ZUWEISENDE KARRIERE & BERUFE ÜBER DAS KSW

GESUNDHEITSTHEMEN FACHGEBIETE KLINIKEN ÄRZTE



Datenschutzerklärung des KSW

Gültigkeit: September 2019

In dieser Datenschutzerklärung informieren wir Sie darüber, wie wir als Kantonsspital Winterthur (KSW) Ihre Personendaten erheben und verarbeiten, wenn Sie mit uns über einen Web-Dienst in Kontakt treten.

Die Bearbeitung von Daten, welche nicht über unsere Web-Dienste erhoben werden, ist in entsprechenden Dokumenten geregelt. Sofern zudem auf

Verzeichnis der Bearbeitungstätigkeiten

- (Fast) jeder Verantwortliche muss ein **Verzeichnis der Bearbeitungstätigkeiten** führen (Art. 12 DSG)
- Im Verzeichnis wird beschrieben, welche Daten bearbeitet werden, wer Zugriff auf die Daten hat, wie sie gesichert sind etc. Das Verzeichnis gibt einen Überblick über die datenschutzrelevanten Aktivitäten in einem Betrieb.
- Das Gesetz schreibt folgenden Mindestinhalt vor:
  - Identität des Verantwortlichen
  - Bearbeitungszweck
  - Kategorien der betroffenen Personen, der bearbeiteten Personendaten und der Empfänger
  - Aufbewahrungsdauer
  - wenn möglich: ergriffene Massnahmen zur Datensicherheit
  - falls Daten ins Ausland: Empfängerstaat
- keine Vorgabe wie das Verzeichnis zu gliedern ist etc.

Beispiel: Verzeichnis Bearbeitungstätigkeiten

Verzeichnis der Bearbeitungstätigkeiten — **Muster / mediX**

Personal	**Bewerbungsmanagement**	**Personalwesen**	**Arbeitszeiterfassung**
Verantwortlicher	- Name	- Name	- angestellte Ärzte und MPA (Erfassung) - Vorgesetzter (Kontrolle)
Bearbeitungszweck	- Rekrutierung neue Mitarbeiter - Vorstellungsgespräch	- Personaladministration - Einsatz- und Ferienplanung - Personalführung, Erstellen Zeugnisse - Auszahlung der Löhne	- Kontrolle Einhaltung Arbeitsvertrag und -gesetz - Gesundheit der Arbeitnehmer - Messung der Arbeitsleistung - Berechnung der Löhne
Betroffene Personen (Kategorie)	- Bewerber, künftige Mitarbeiter	- Mitarbeiter	- Mitarbeiter
Bearbeitete Daten (Kategorie)	- Kontaktdaten (einschl. Telefon und E-Mail) - Lebenslauf - Zeugnisse - Referenzen	- Kontaktdaten (einschl. Telefon und E-Mail) - Sozialversicherungsdaten (AHV-Nr. etc.) - Lohndaten, Kontoverbindungen - Arbeitsunfähigkeit (Unfall, Krankheit etc.) - Mitarbeiterbeurteilungen, Zeugnisse etc. - Login-Daten	- Arbeitszeit, Ferien, Absenzen - Daten zur Arbeitsleistung
Empfänger (Kategorie)	- Personalverantwortliche (- u.U. Referenzgeber)	- Personalverantwortliche, Buchhaltung, IT - Sozialversicherungen (AHV, BVG etc.) - Bank	- Personalverantwortliche - Buchhaltung (- u.U. Vollzugs- und Aufsichtsorgane)
Aufbewahrungsdauer oder Kriterien zur Festlegung der Dauer	- abgewiesene Bewerber: bis Ende des Bewerbungsprozesses - künftige Mitarbeiter: vgl. Personalwesen	10 Jahre nach Austritt	5 Jahre nach Erfassung
Massnahmen zur Gewährleistung der Datensicherheit	- E-Mail aus Praxis via HIN - Postversand zur Unterschrift - Rücksendung/Vernichtung der Unterlagen bei Absage; aktive Zustimmung der Bewerber bei Einbehalt für künftige offene Stellen - aktive Zustimmung vor Einholung von Referenzauskünften	- Zugriff eingeschränkt: auf Dossier nur Name / nur mit Schlüssel auf Laufwerk X nur Name / nur mit Passwort - Papieraktenvernichtung mit Shredder	- Zugriff eingeschränkt: auf Ordner nur Name / nur mit Schlüssel auf Laufwerk X nur Name / nur mit Passwort
Übermittlung an Drittstaaten	nein	nein	nein
Zugriff / Speicherung	- Bewerbungsdossier (physisch) - Laufwerk X	- Personaldossier (physisch) - Laufwerk X - Buchhaltungssoftware	- Arbeitserfassungssystem - Personaldossier (physisch)
Rechtsgrundlage für die Bearbeitung	Bewerbung (Einwilligung)	Arbeitsvertrag (Einwilligung) Art. 328b OR	Art. 46 ArG; Art. 73 Abs. 1 lit. c ARGV1
Weitere Informationen			

Auftragsbearbeitung

- **Auftragsbearbeiter** = Person, die im Auftrag des Verantwortlichen Personendaten bearbeitet (Art. 5 lit. k DSG)
- Beispiel: externe Lohnbuchhaltung
- Die Weitergabe von Daten zur Bearbeitung an einen Dritten ist grundsätzlich zulässig, auch ohne Einwilligung der betroffenen Person. Voraussetzung aber ist (vgl. Art. 9 DSG):
  - der Auftragsbearbeiter bearbeitet die Daten so, wie der Verantwortliche es selber tun dürfte
  - die Übertragung ist nicht durch eine gesetzliche oder vertragliche Geheimhaltungspflicht verboten
- Der Verantwortliche muss sich vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.
- Die Rechte und Pflichten werden meist geregelt in einer sog. **Auftragsdatenbearbeitungsvereinbarung** (kurz: ADV)

Beispiel: ADV

Auftragsdatenbearbeitungsvereinbarung

Diese Auftragsdatenbearbeitungsvereinbarung (im Folgenden die **ADV**) wird zwischen BlueCare AG, Pflanzschulstrasse 3, 8400 Winterthur (im Folgenden der **Auftragsbearbeiter**) und dem unterzeichnenden Ärztenetzwerk (dem **Verantwortlichen**) geschlossen.

Sie betrifft die Bearbeitung von Personendaten (im Folgenden die **Auftragsdaten**) im Zusammenhang mit einer separaten Vereinbarung zwischen dem Auftragsbearbeiter und der Managed-Care-Organisation des Verantwortlichen (im Folgenden die **MCO**) oder direkt mit dem Verantwortlichen zur Nutzung von «BlueEvidence» (im Folgenden die **BlueEvidence-Vereinbarung**).

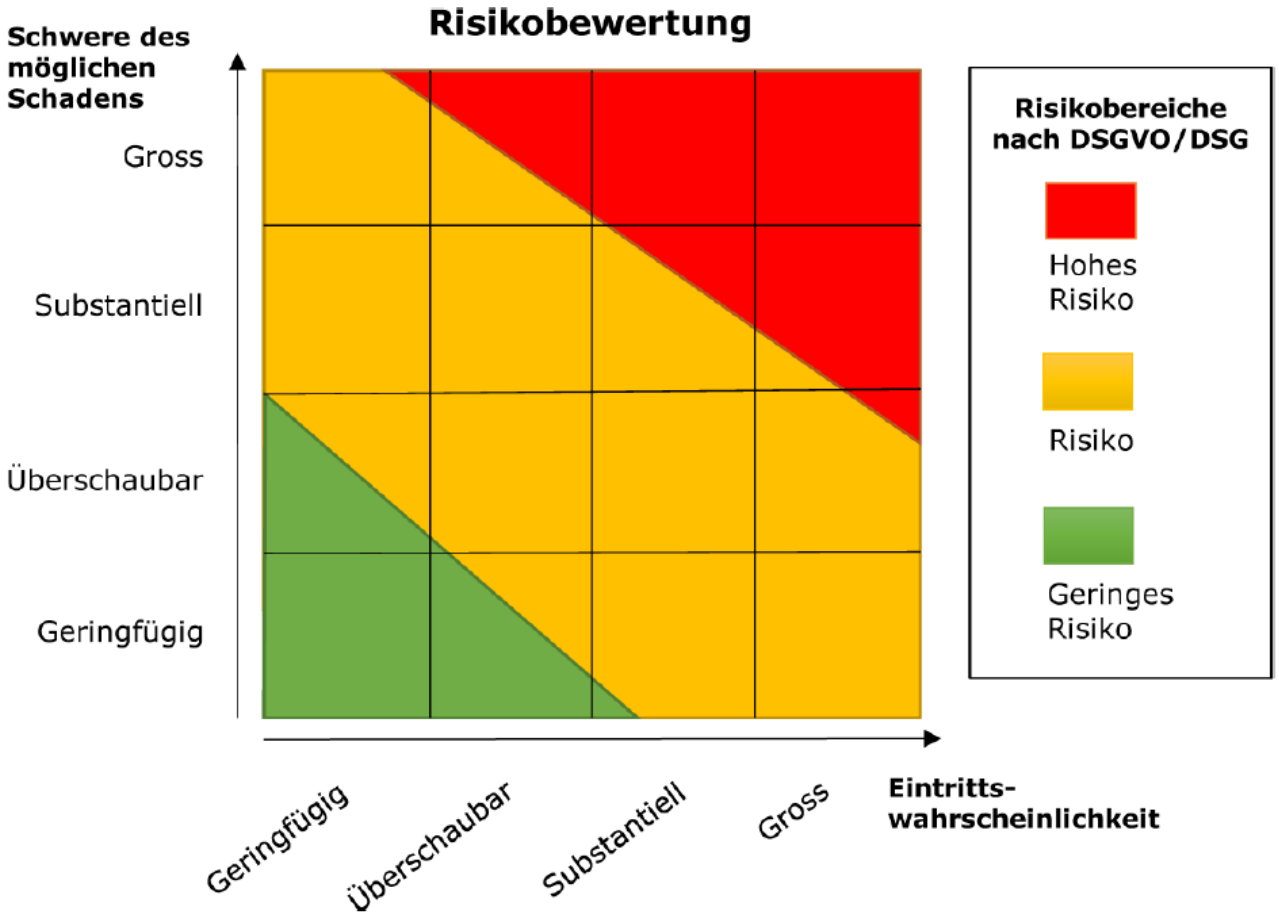
1. Angaben zur Auftragsbearbeitung

Gegenstand, Art und Zweck:	— Die Bearbeitung von Personendaten durch den Auftragsbearbeiter zur Erbringung von IT-Dienstleistungen im Zusammenhang mit BlueEvidence, gemäss der BlueEvidence-Vereinbarung
Dauer der Bearbeitung:	— unbefristet, bis zur Löschung der Auftragsdaten
Kategorien betroffener Personen:	— Versicherte, die in einem Hausarztversicherungsmodell eines Krankenversicherer versichert sind, der mit der MCO einen entsprechenden Vertrag hat — beim Netzwerk angeschlossene Ärzte
Kategorien von Personendaten:	— Bestandsdaten (inkl. Zuordnung zu Hausarzt)

Datenschutz-Folgenabschätzung

- Bringt eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich, ist eine **Datenschutz-Folgenabschätzung** (DSFA) zu erstellen (Art. 22 DSG).
- In der DSFA sind die Risiken der Bearbeitung und die getroffenen Massnahmen zu beschreiben und zu bewerten (Selbst-Evaluation).
- Ergibt sich aus der DSFA, dass die geplante Bearbeitung trotz der vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat, ist die Stellungnahme des EDÖB einzuholen.

Beispiel: Datenschutz-Folgenabschätzung



(David Rosenthal, Das neue Datenschutzgesetz, in: Jusletter 16.11.2020, Rz. 153)

Sanktionen

- Strafbestimmungen: Busse bis CHF 250'000
  - insbesondere bei vorsätzlicher Verletzung der Informationspflicht oder der Pflichten bei einer Auftragsdatenbearbeitung

- grundsätzlich gegen die verantwortliche natürliche Person

3.

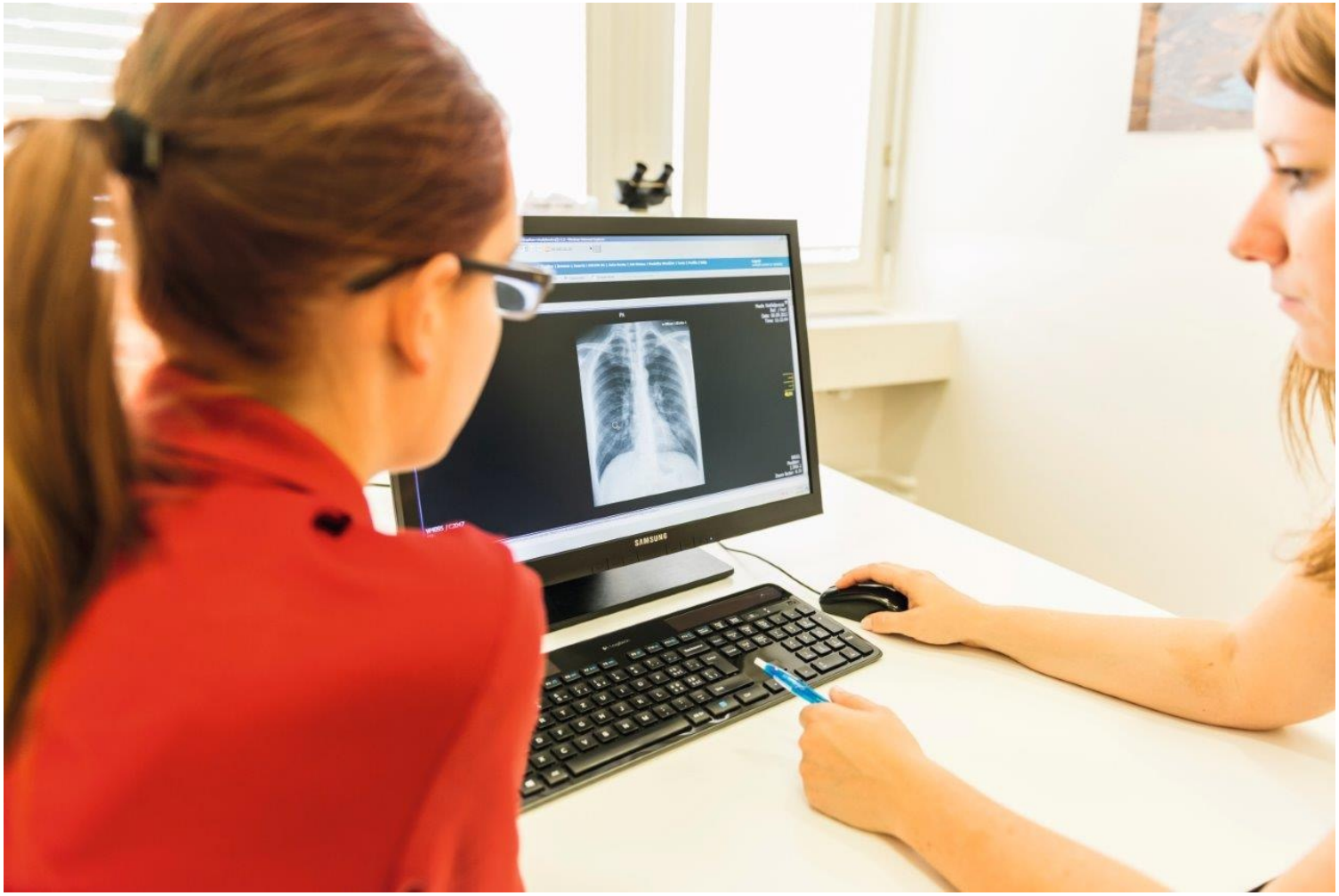
Datenschutz
im Alltag einer Arztpraxis

Datenschutz in der Arztpraxis

- Nicht alles im revidierten DSG ist neu. Wer Personendaten bearbeitete, musste auch schon vor dem 1. September 2023 die Grundsätze des Datenschutzes einhalten.
- Datenschutz ist wichtig. Gerade in einer Arztpraxis, wo viele viele besonders schützenswerte Daten bearbeitet werden.
- Die gute Nachricht: Sie alle betreiben in der Praxis jeden Tag (bewusst oder unbewusst) Datenschutz.
- Einige der neuen Pflichten sind lästig und verursachen Aufwand. Aber versuchen Sie, es auch als Chance zu sehen, eine Standortbestimmung vorzunehmen und zu überlegen, wo beim Datenschutz noch Verbesserungspotential besteht.
- Betrachten Sie den Datenschutz nicht isoliert. Daneben gibt es das Arztgeheimnis und Vorschriften im Gesundheitsrecht (z.B. zur Patientendokumentation)

Datenschutz in der Arztpraxis

Datenschutz in der Arztpraxis



Datenschutz in der Arztpraxis

- Machen Sie einen Rundgang durch Ihre Praxis: Wo werden Daten bearbeitet? Sind Ihre MPA in Bezug auf Datenschutz sensibilisiert? Welche Bereiche sind "kritisch"?
- Sind die Grundsätze des Datenschutzes eingehalten:
  - Ist die Bearbeitung rechtmässig?
  - Ist für die Patientin erkennbar, dass und zu welchem Zweck Daten erhoben werden?
  - Werden alle Daten, die erhoben werden, auch wirklich gebraucht? Werden sie nach Gebrauch gelöscht?
  - Sind die Daten sicher? Hat kein Unberechtigter Zugriff darauf?
- Oft ist es gar nicht so einfach: z.B. am Empfang, wenn das Telefon läutet und der nächste Patient wartet
- Deshalb: Es braucht ein Konzept (Datenschutzkonzept), das Ziele, Massnahmen und Verantwortlichkeiten definiert.

Beispiel 1: Am Empfang

- Wo werden am Empfang Daten bearbeitet? Sind die Vorschriften des Datenschutzes eingehalten?

Mögliche Risiken	Mögliche Lösungen

Beispiel 1: Am Empfang

- Wo werden am Empfang Daten bearbeitet? Sind die Vorschriften des Datenschutzes eingehalten?

Mögliche Risiken	**Mögliche Lösungen**
Patienten am Empfang (oder im Wartezimmer) könnten etwas hören, das sie nichts angeht (z.B. Telefongespräch)	
Patienten oder Dritte könnten etwas sehen, das sie nichts angeht	
Das Reinigungsinstitut könnte einen Bericht sehen oder mitgehen lassen	

Beispiel 1: Am Empfang

- Wo werden am Empfang Daten bearbeitet? Sind die Vorschriften des Datenschutzes eingehalten?

Mögliche Risiken	**Mögliche Lösungen**
Patienten am Empfang (oder im Wartezimmer) könnten etwas hören, das sie nichts angeht (z.B. Telefongespräch)	- Abstand einhalten - achten auf Lautstärke und Gesprächsinhalt (keine Namen mit Diagnose) - schalldämpfende Türe, Hintergrundmusik etc.
Patienten oder Dritte könnten etwas sehen, das sie nichts angeht	- PC so stellen, dass Bildschirm nicht einsehbar ist - keine personenbezogenen Dokumente herumliegen lassen (clean desk) - Sichtschutz, Vorhang
Das Reinigungsinstitut könnte einen Bericht sehen oder mitgehen lassen	- Unterlagen abends einschliessen (clean desk) - Verschwiegenheitserklärung

Beispiel 2: IT

- Ist die Datensicherheit gewährleistet? Besteht ein Konzept mit dem IT-Dienstleister? Sind die Mitarbeitenden geschult?

Mögliche Risiken	Mögliche Lösungen

Beispiel 2: IT

- Ist die Datensicherheit gewährleistet? Besteht ein Konzept mit dem IT-Dienstleister? Sind die Mitarbeitenden geschult?

Mögliche Risiken	**Mögliche Lösungen**
Versand E-Mail an falschen Empfänger	
Passwort wird geknackt	
Viren, Trojaner etc.	

Beispiel 2: IT

- Ist die Datensicherheit gewährleistet? Besteht ein Konzept mit dem IT-Dienstleister? Sind die Mitarbeitenden geschult?

Mögliche Risiken	**Mögliche Lösungen**
Versand E-Mail an falschen Empfänger	- Kontrolle vor Versand - ev. 4-Augen-Prinzip
Passwort wird geknackt	- sichere Passwörter - regelmässiges Wechseln der Passwörter - Passwort nicht auf post-it am PC; Passwort-Liste in Safe
Viren, Trojaner etc.	- aktueller Virenschutz und Firewall (regelmässige Updates) - regelmässige Datensicherung - Schulung der Mitarbeitenden und Erteilen von Weisungen (z.B. Öffnen von Anhängen, Links, Dateiendownload, privates Surfen)

Beispiel 3: Krankengeschichte

- Ist sichergestellt, dass die Einträge richtig sind? Werden die Daten korrekt und sicher aufbewahrt? Umgang mit Auskunftsbegehren?

Mögliche Risiken	Mögliche Lösungen

Beispiel 3: Krankengeschichte

- Ist sichergestellt, dass die Einträge richtig sind? Werden die Daten korrekt und sicher aufbewahrt? Umgang mit Auskunftsbegehren?

Mögliche Risiken	**Mögliche Lösungen**
Einträge: könnten falsch oder unvollständig sein	
Aufbewahrung: Daten könnten zu früh gelöscht werden oder verloren gehen, sodass die Aufbewahrungs-pflicht verletzt ist	
Auskunftsrecht der Patienten: es ist nicht klar, wie damit umzugehen ist	

Beispiel 3: Krankengeschichte

- Ist sichergestellt, dass die Einträge richtig sind? Werden die Daten korrekt und sicher aufbewahrt? Umgang mit Auskunftsbegehren?

Mögliche Risiken	**Mögliche Lösungen**
Einträge: könnten falsch oder unvollständig sein	- jeder Benutzer macht Einträge mit seinem Kürzel - Zugriffe werden protokolliert - keine nachträgliche Veränderung
Aufbewahrung: Daten könnten zu früh gelöscht werden oder verloren gehen, sodass die Aufbewahrungs-pflicht verletzt ist	- physische und elektronische Ablage - regelmässige Datensicherung - Aufbewahrung für 20 Jahre (mind. 10 Jahre) - Regelung bei Praxisnachfolge
Auskunftsrecht der Patienten: es ist nicht klar, wie damit umzugehen ist	- Regelung der Abläufe - Schulung Mitarbeitende - Auskunft an Dritte grundsätzlich nur mit Einwilligung der Patientin

Schlussfolgerung

- Ausgangspunkt: Verzeichnis der Bearbeitungstätigkeiten
- Befolgen Sie nicht einfach Vorschriften. Betreiben Sie "vernünftigen" Datenschutz
  (Negativbeispiel: Hinweis auf Cookies)
- Machen Sie die Augen auf; hören Sie auf Ihr Bauchgefühl
- Schulen Sie die Mitarbeitenden (und bilden Sie sich weiter); Wiederholen Sie die Schulung

4.

Fragen?

Schluss

Vielen Dank für Ihre Aufmerksamkeit!

Michael Hochstrasser
Prof. Dr. iur., Rechtsanwalt
Schiller Rechtsanwälte AG
Kasinostrasse 2 / Postfach
8401 Winterthur

Tel. 052 269 16 16

hochstrasser@schillerlegal.ch
http://www.schillerlegal.ch