5. MPA - Symposium

25. September 2021

Datenschutz – Was muss die Praxis tun?

Michael Hochstrasser

PD Dr. iur. Rechtsanwalt

1. Teil:

Einführung und Übersicht

Weshalb Datenschutz?

Was ist bei der Bearbeitung von Daten zu beachten?

Das revidierte Datenschutzgesetz

- Das schweizerische Datenschutzgesetz (DSG) wird revidiert:
  - am 25.9.2020 verabschiedet im Parlament
  - Inkrafttreten frühestens Anfang 2023
  - keine Übergangsfrist (!)
- Das neue Recht bringt neue Pflichten – auch für die Arztpraxis
- Aber: nicht alles ist neu. Datenschutz gilt schon heute. Und Datenschutz ist wichtig – auch und gerade in der Arztpraxis

Datenschutz: Beispiele

- Clean Desk
- Autovervollständigung der E-Mail-Adresse
- Telefonieren in der Öffentlichkeit
- Patientendaten im Altpapier
- Social Media
- …

Der Begriff der "Personendaten"

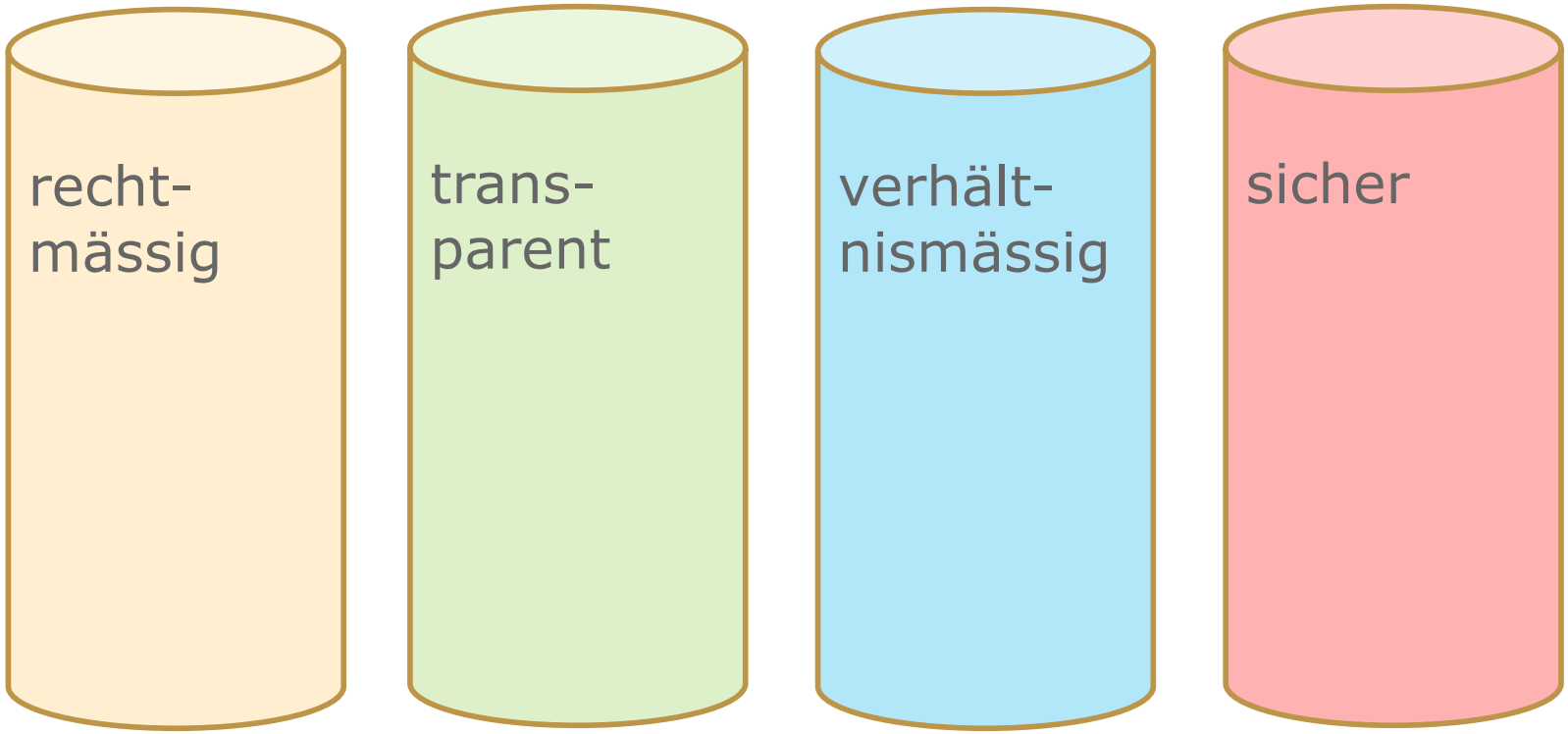
- **Personendaten** = alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 5 lit. a nDSG)

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

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

Wichtigste Grundsätze

Eine Datenbearbeitung muss Folgendes sein:



Frage 1:
Ist es in Ihrer Praxis schon einmal zu einer Verletzung der Datensicherheit gekommen?

2. Teil:

Datenschutz in der Arztpraxis: Datenschutzkonzept

Datenschutz in der Arztpraxis

- Viele Daten, viele besonders schützenswerte Daten
- Augen auf: Wo hat es Daten? Wie werden Daten bearbeitet? Machen Sie einen Rundgang durch die Praxis!
- 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

- Ein Datenschutzkonzept dokumentiert die Massnahmen zum Datenschutz in der Praxis. Es beinhaltet Ziele, Massnahmen sowie Verantwortlichkeiten.

  Zum Beispiel:

- Am Empfang:
  - gebührender Abstand
  - achten auf Lautstärke, diskreten Inhalt
  - keine Einsicht in den Computer

- Im Behandlungszimmer:
  - es liegen keine schriftlichen Befunde oder Berichte herum
  - Untersuchung und Gespräch hinter geschlossenen Türen
  - Verlässt die Ärztin oder die MPA den Raum, wird der Computer gesperrt

Datenschutzkonzept

- IT:
  - Verwendung von sicheren Passwörtern
  - regelmässiges Wechseln der Passwörter
  - aktueller Virenschutz und Firewall
  - tägliche Datensicherung
- Datenübermittlung:
  - mit der Post oder bei Verwendung von E-Mails nur über HIN-Mail
  - Verwendung von sicheren Systemen (z.B. BlueConnect)
  - 4-Augen-Prinzip
- Ausserdem:
  - alles Papier mit Patientendaten wird geschreddert
  - das Pult ist aufgeräumt (clean desk)
  - regelmässiges Löschen/Vernichten nicht mehr benötigter Daten
  - und, und, und …

3. Teil:

Neuerungen mit dem revidierten Datenschutzgesetz (DSG):

(neue) Pflichten für die Praxis

(Neue) Pflichten für die Arztpraxis

Das revidierte Datenschutzgesetz bringt zum Teil neue Pflichten für die Praxen, insbesondere:

- Datenschutzerklärung
- Verzeichnis der Bearbeitungstätigkeiten
- Verträge mit Auftragsdatenbearbeitern
- Datenschutz-Folgenabschätzung

(zum Teil gibt es Ausnahmen von diesen Pflichten)

Informationspflicht

- Grundsatz: Wer Personendaten beschafft, muss die betroffene Person darüber informieren (Art. 19 nDSG)
- 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 nDSG):
  Keine Information ist nötig, wenn (u.a.)
  - die betroffene Person bereits über entsprechende Informationen verfügt
  - die Bearbeitung gesetzlich vorgesehen ist (z.B. Führen Personaldossier; Geldwäschereibekämpfung) oder
  - 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

- Jeder Verantwortliche muss ein **Verzeichnis der Bearbeitungstätigkeiten** führen (Art. 12 nDSG)
- 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 betroffener 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 nDSG)
- 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 nDSG):
  - 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

Nachtrag zum Datenschutz – Vertrag zur Auftragsverarbeitung

zwischen

Unternehmen X

als Verantwortlicher (nachfolgend Auftraggeber)

und

Unternehmen Y

als Auftragsverarbeiter (nachfolgend Auftragnehmer)

Präambel

a) Der Auftraggeber und der Auftragnehmer haben am [Datum] eine Vereinbarung [Beschreibung mit Leistungsgegenstand] abgeschlossen (nachfolgend **Hauptvertrag)**, in dessen Rahmen der Auftragnehmer für den Auftraggeber Arbeiten oder Dienstleistungen oder gegebenenfalls sonstige Leistungen, wie im Hauptvertrag festgelegt, erbringt.

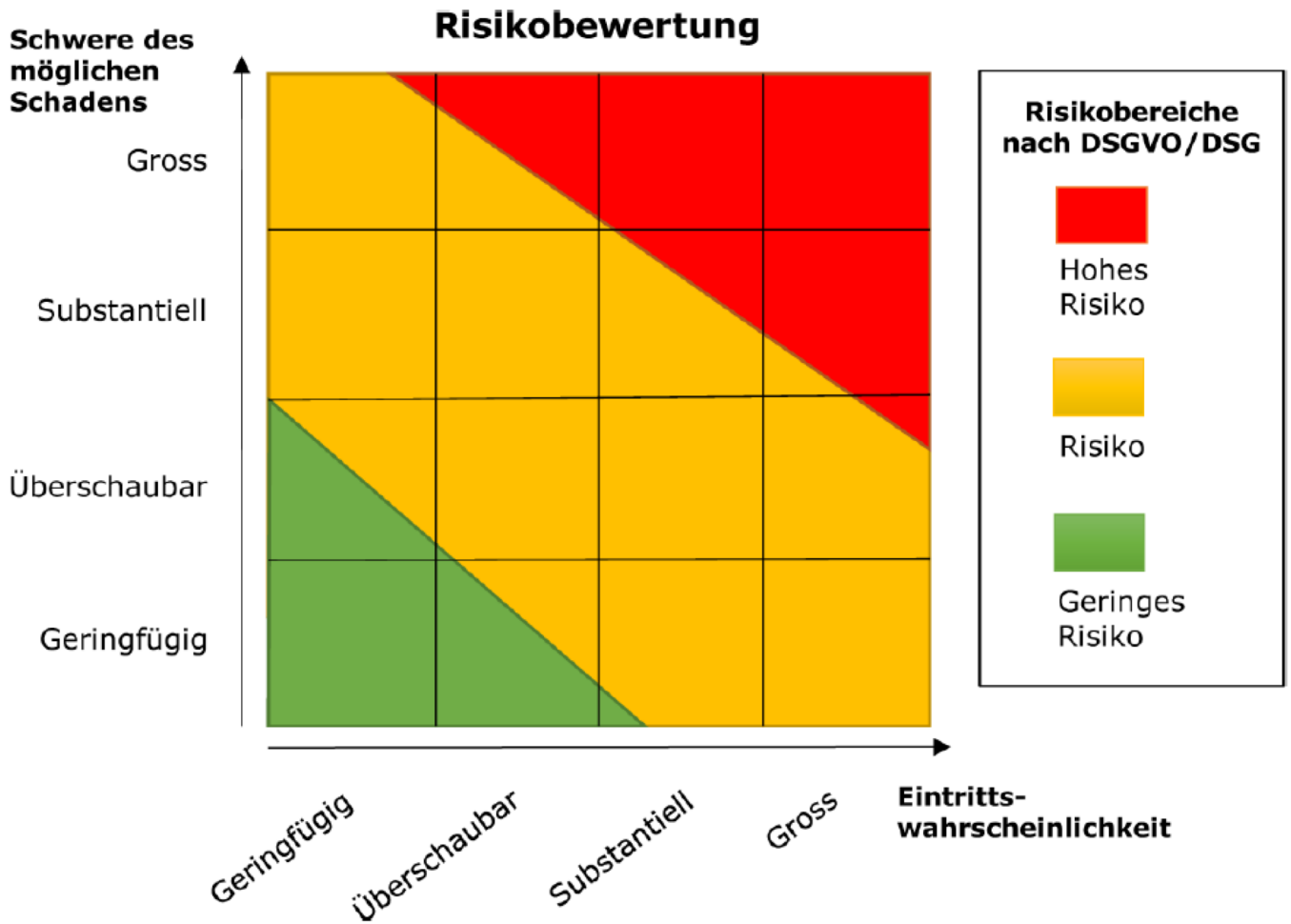
b) Zum Zwecke der Erfüllung des Hauptvertrags erhält der Auftragnehmer unter Umständen Zugang zu personenbezogenen Daten, die dem Auftragnehmer durch den Auftraggeber direkt oder in dessen Auftrag durch Dritte offengelegt oder auf andere Weise zur Verfügung gestellt werden (nachfolgend **personenbezogene Daten**).

c) Die Parteien möchten sicherstellen, dass die durch den Auftragnehmer im Auftrag des Auftraggebers direkt oder durch Dritte durchgeführte Verarbeitung personenbezogener Daten im Rahmen des Hauptvertrags den geltenden Datenschutzgesetzen entspricht, und sich dabei auf

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 nDSG).
- 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 nicht bei Verletzung von Pflichten im Zusammenhang mit dem Verzeichnis der Bearbeitungstätigkeiten oder der Datenschutz-Folgenabschätzung

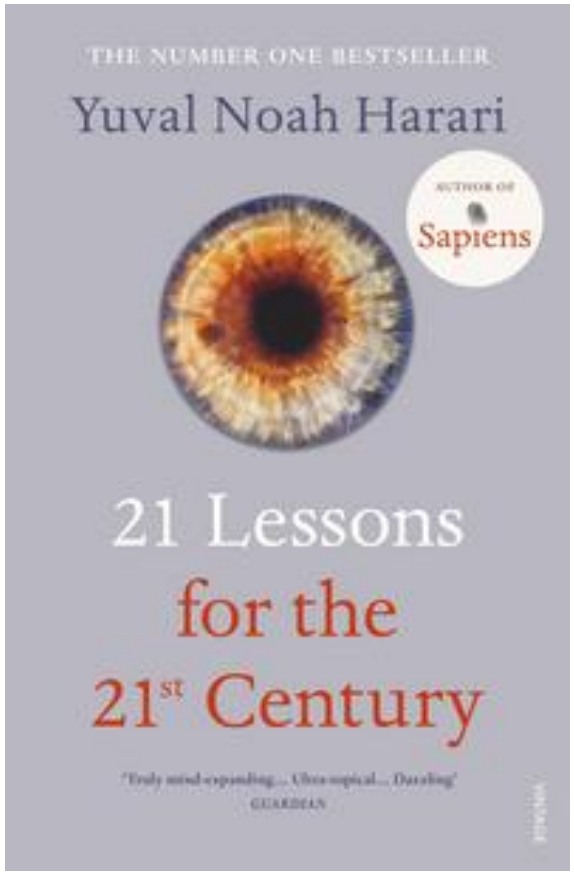
Zusammenfassung

- Mit dem revidierten Datenschutzgesetz (DSG) kommen einige neue Pflichten auf die Arztpraxis zu
- Datenschutz war in der Arztpraxis aber schon bisher wichtig und wird es weiterhin sein (unabhängig vom revidierten DSG)
- Für die Verzeichnisse und Formulare wird es Muster geben
- Lassen Sie sich keine Angst machen – aber nehmen Sie das Thema ernst und gehen Sie mit offenen Augen durch den Praxisalltag!

Zum Schluss

"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)



4. Teil:

Fragen

Schluss

Vielen Dank für Ihre Aufmerksamkeit!

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

Tel. 052 269 16 16
e-mail
hochstrasser@schillerlegal.ch
http://www.schillerlegal.ch

Anne Sybil Götschi
Dr. med.
MedSolution AG
Sumatrastrasse 10
8006 Zürich

Tel. 044 366 53 70
e-mail
annesybil.goetschi@medsolution.ch
https://www.medsolution.ch