# Die DSGVO und die Revision des DSG

Dr. Jacqueline Sievers, Walder Wyss
Zürich, 21. September 2018

# Einführung

- Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a, DSG, Art. 4 lit. a E-DSG und Art. 4 Ziff. 1 DSGVO)
  - Patienten, Mitarbeiter, Lieferanten
- Anonymisierung und Verschlüsselung
- Besonders schützenswerte Personendaten sind u.a. Daten über
  - genetische, biometrische Informationen zur eindeutigen Identifizierung oder Gesundheitsdaten (Art. 3 lit. c DSG, Art. 4 lit. c E-DSG und Art. 9 Abs. 1 DSGVO)
- Bearbeiten ist jeder Umgang mit Personendaten (Art. 3 lit. e DSG, Art. 4 lit. d E-DSG und Art. 4 Ziff. 2 DSGVO)

# Datenschutzprinzipien


**Rechtmässigkeit:**

Die Bearbeitung darf nicht ohne Rechtfertigung gegen das Gesetz verstossen.

**Transparenz:**

Erkennbarkeit der Bearbeitung, insbesondere der Beschaffung und Zweck.

**Zweckbindung:**

Bearbeitung von Personendaten ist auf den Zweck beschränkt, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

**Verhältnismässigkeit:**

Bearbeitung nur soweit erforderlich.

**Datenrichtigkeit:**

Massnahmen zur Sicherstellung der Richtigkeit und Vollständigkeit.

**Datensicherheit:**

Technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten, insbesondere gegen Verlust, Zerstörung oder unbefugten Zugriff.

# Einbezug Dritter

- Controller (Verantwortlicher)
  - ➢ entscheidet über den Zweck und die Mittel der Datenbearbeitung (Art. 3 lit. i DSG; Art. 4 lit. i E-DSG; Art. 4 Ziff. 7 DSGVO)
- Processor (Auftragsverarbeiter)
  - ➢ bearbeitet im Auftrag und für die Zwecke des Controllers (z.B. Outsourcing-Dienstleister oder Cloud-Anbieter) (Art. Art. 4 lit. j E-DSG; Art. 4 Ziff. 8 DSGVO )
- Vertrag!
- Berufsgeheimnis gemäss Art. 321 StGB!

# Kontrollverlust, Sensibilisierung

Neue Zürcher Zeitung

## Von 800 000 Swisscom-Kunden sind Kontaktdaten entwendet worden

Unbekannte haben sich im Herbst 2017 missbräuchlich die Kontaktangaben von rund 800 000 Swisscom-Kunden verschafft. Sie hatten dafür die Zugriffsrechte eines Vertriebspartners entwendet. Die Swisscom verschärft nun die Sicherheitsmassnahmen.

Neue Zürcher Zeitung

## Wenn der Hacker Spitalpatienten mitbehandelt

Zunehmende Vernetzung, ungeschützte Medizinalgeräte und nicht mehr zeitgemässe IT machen Spitäler anfällig für Cyberattacken: Der Angriff mit «Wanna Cry» war dabei nur der letzte Schrei.

ZEIT ONLINE

## Hacker erbeuten Zehntausende Daten von Inkassofirma

Eine Inkassofirma hat laut einem Zeitungsbericht sensible Schuldnerdaten wie Patientenakten unerlaubt gespeichert. Hacker sollen sich dazu Zugang verschafft haben.

The Guardian International edition

## Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach

Neue Zürcher Zeitung

## Auch Digitec-Galaxus ist von Datenklau betroffen

Neue Zürcher Zeitung

## Uber verschwieg ein Jahr lang den Diebstahl der Daten von 57 Millionen Nutzern

Eine Enthüllung bei Uber offenbart eine schockierende Verantwortungslosigkeit. Uber verschwieg einen Datendiebstahl und zahlte den Hackern 100 000 Dollar. Dieses Vergehen hat weitreichende Konsequenzen.

# Gegenwärtige Rechtslage

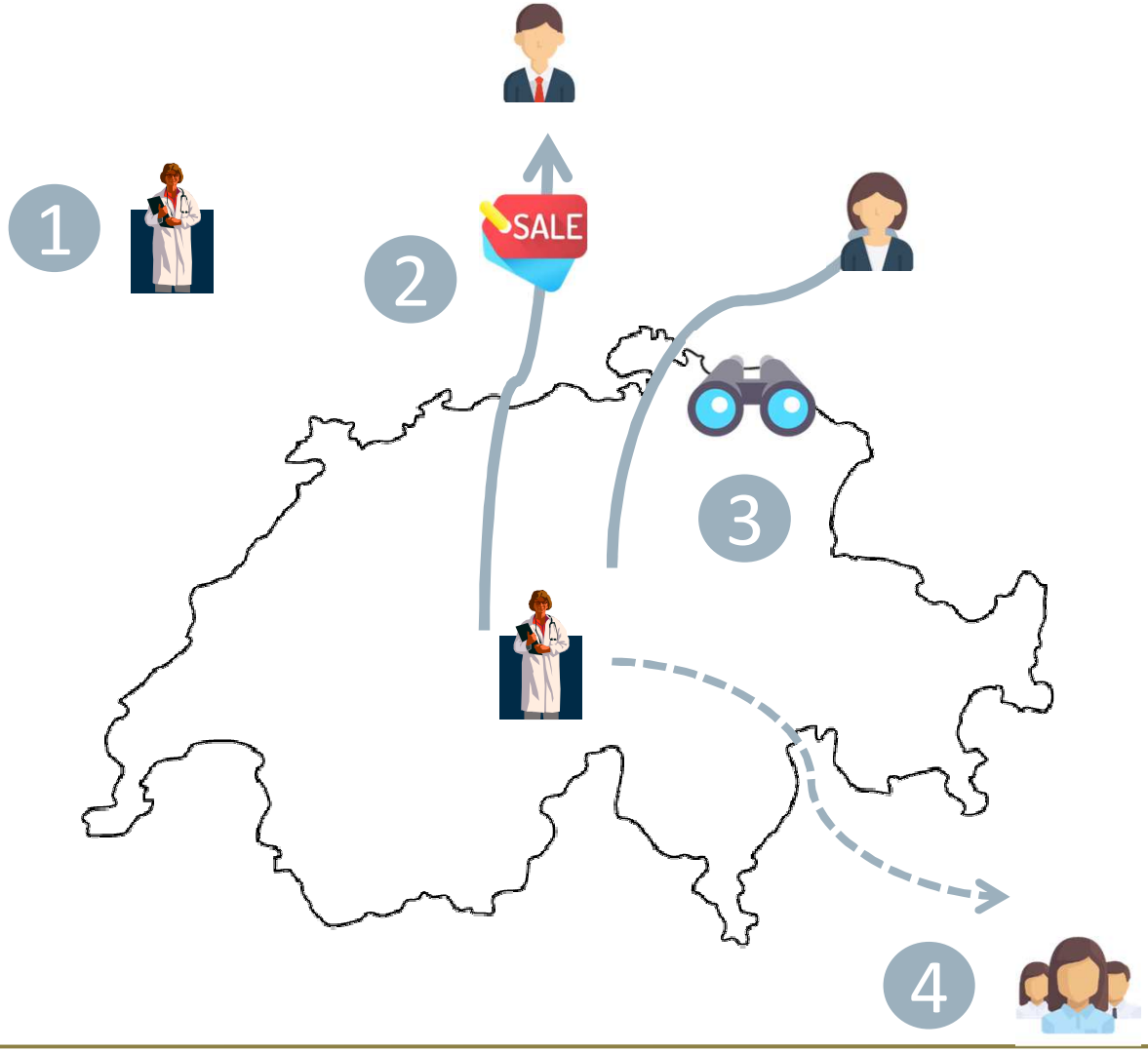
## Europäische Datenschutz-Grundverordnung

- Seit 25. Mai 2018 in Kraft
- Neuordnung und Verschärfung des Datenschutzrechts
- Extraterritoriale Wirkung über das Gebiet der EU hinaus
- Einschneidende Sanktionen

## Revision Schweizer Datenschutzgesetz

- Revision des Datenschutzgesetzes von 1992
- Erhalt eines aus EU-Sicht angemessenen Datenschutzniveaus
- Revision wird sich voraussichtlich an der DSGVO orientieren
- Inkrafttreten frühestens 2019, eher 2020/21

# Anwendbarkeit der DSGVO




Anwendbarkeit der DSGVO:

1. Niederlassung im EWR
2. Marktausrichtung
3. Verhaltensbeobachtung
   - ➢ Benennung eines EU-Vertreters (Art. 27 DSGVO)
4. nur für deliktische Ansprüche: Berufung auf Heimatrecht (Art. 139 IPRG)

# Haftung?

- DSGVO: Unternehmensstrafen - Verwaltungsbussen – Bussen bis EUR 20 Mio. oder 4% des weltweiten Gruppen-Jahresumsatzes (83 DSGVO)
- DSG-Revision: strafrechtliche Bussen bis CHF 250’000 (Art. 54 ff. E-DSG)
  - Heute DSG: Busse bis zu CHF 10’000 (Art. 34 DSG)
  - Subsidiäre Bestrafung von Unternehmen - Busse bis CHF 50’000 möglich (Art. 58 Abs. 2 E-DSG)
- Berufsgeheimnis: Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (Art. 321 StGB)
- Schadenersatz und Schmerzensgeld?

# To-do:
# Aktive Information - Datenschutzerklärung

- Identität und Kontaktdaten des Verantwortlichen (DSGVO: und Vertreter)
- Bearbeitungszwecke
- (Kategorie) der Empfänger im In- und Ausland (E-DSG und DSGVO: Information über unangemessene Datenschutzgesetzgebung und Verweis auf rechtfertigende Garantie)
- Evtl. Interessen auf die sich die Bearbeitung stützt
- Bearbeitete Daten und Kategorien (sofern bei Dritten beschafft)
- Automatische Einzelfallentscheidungen
- Speicherdauer
- Betroffenenrechte (inkl. Beschwerderecht )
- Drittquellen (ausser wenn durch Berufsgeheimnis geschützt)
- Vorhandensein einer vertraglichen oder gesetzlichen Pflicht zur Erhebung der Daten

# To-do:
# Prozesse für Betroffenenrechte

- Recht auf Auskunft (Art. 23 E-DSG; Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 28 E-DSG; Art. 16 DSGVO)
- Recht auf Löschung (Art. 28 E-DSG; Art. 17 DSGVO)
- Nur DSGVO:
  - Höhere Anforderungen an die Wirksamkeit der Einwilligung (Art. 7 DSGVO)
  - Recht auf Datenübertragbarkeit bei auf Einwilligung gestützter Bearbeitung (Art. 20 DSGVO)

# To-do:
# Löschkonzept und Dokumentation

- Heute: In Ausnahmefällen Protokollierung oder Bearbeitungsreglement (Art. 10 f. VDSG)

- DSGVO / Revision: Vollumfängliche Dokumentation der Datenbearbeitungen (Art. 11 Abs. 1 E-DSG; Art. 30 DSGVO)
  - Beispiele
    - (elektronische) Patientenakten;
    - Zahnarztinformationssysteme;
    - elektronische Diktier- und Spracherkennungsprogramme;
    - Buchhaltungssoftware;
    - Abrechnung über die Ärztekassen;
    - Software zur Versendung und Verwaltung von E-Mails;
    - Adressdatenbanken;
    - Software oder Website zur Terminverwaltung;
    - Elektronische Personalakten;
    - Lohnabrechnungen.
  - Ausnahme gemäss DSGVO für kleine Betriebe greift bei Gesundheitsdaten nicht

# To-do:
# Prozesse Meldepflichten

- Datenschutz-Folgenabschätzung bei geplanter Datenbearbeitung mit voraussichtlich hohem Risiko (Art. 20 E-DSG; Art. 35 DSGVO)
  - neue Technologien, Art oder Umfang der Bearbeitung
- Verletzungen des Datenschutzes (Art. 22 E-DSG; Art. 33 DSGVO)
  - Unberechtigter Zugriff, Verlust oder Zerstörung auf/von Personendaten
  - hohes Risiko für betroffene Personen
  - Meldung innert 72 (!) Stunden (E-DSG: «so rasch als möglich»)

# To-do:
# Sicherheit und Verträge

«Technische und organisatorische Massnahmen» (Art. 32 DSGVO)

- Pseudonymisierung und Verschlüsselung
- die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der ToMs

  - ➢ Zugriffs- und Zugangskontrollen
  - ➢ Auftragsdatenverarbeitungsverträge

# To-do:
# Benennung Datenschutzbeauftragten?

- Art. 37 Abs.1 lit. c DSGVO: Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
  - (…)
  - die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 (…) besteht.
- E-DSG: Immer freiwillig (Art. 9 E-DSG)
- Unabhängig – unmittelbare Berichterstattung an Geschäftsleitung

# Bilanz?

- Aufsichtsbehörden wollen lieber beraten als sanktionieren
- Die grosse Abmahnwelle blieb aus
- Reputationsrisiken

| DSGVO und E-DSG | Nur DSGVO |
|---|---|
| – Aktive **Informationspflicht** - ganze Liste von Pflichtinformationen<br>– Jede Datenbearbeitung des Unternehmens muss in ein **Inventar** aufgenommen werden<br>– Pflicht zu **Datenschutz-Folgenabschätzungen** die z.T. der Behörde gemeldet werden müssen<br>– Pflicht zur **Meldung von Sicherheitsverstössen** bei Behörden und betroffenen Personen<br>– Datenschutzfreundlichste Voreinstellung muss Standard sein («**Privacy by Default**»)<br>– Recht auf menschliches Gehör bei rechtlichen/relevanten **automatisierten Einzelentscheiden**<br>– Neue **Sanktionen**, Interventionsmöglichkeiten und -pflichten der Datenschutzbehörden | – **Einwilligungen** müssen jeweils separat ausgewiesen und eingeholt werden und ohne vorangekreuztes Kästchen, aber mit Hinweis auf die jederzeitige Widerrufbarkeit<br>– Service-Nutzer erhalten über sie erhobene Daten zur eigenen Verwendung («**Datenportabilität**»)<br>– Pflicht zur Ernennung eines **betrieblichen Datenschutzbeauftragten** und **Vertreters** in der EU |

# Kontakt

Walder Wyss AG
Dr. iur. Jacqueline Sievers, LL.M., CIPP/E
Seefeldstrasse 123
Postfach 1236
8034 Zürich

Jacqueline.sievers@walderwyss.com
+41 58 658 53 47