Zürcher Hochschule
für Angewandte Wissenschaften

zh
aw

INFORMATIKRECHT

HS 2021

DATENSCHUTZ

Zürcher Hochschule
für Angewandte Wissenschaften

FAHRPLAN

- Weshalb Privacy & Datenschutz?
- Rechtsgrundlagen
- Datenschutz-Prinzipien
- Anwendungsbereiche
- Rechte und Pflichten
- DSGVO
- My TakeAway

Zürcher Hochschule
für Angewandte Wissenschaften

LERNZIELE

- Sphärentheorie verstehen
- 3 Datenschutzprinzipien kennen
- Vorgehen Auskunftsrecht kennen
- Vorgehen bei DSGVO kennen

Zürcher Hochschule
für Angewandte Wissenschaften

WESHALB PRIVACY & DATENSCHUTZ?

- Menschen sind **soziale Wesen** - aber auch **Individualisten**! Ständiger Konflikt zwischen diesen beiden Naturen.
- Wenn sie der liberalen Idee folgen, dass Menschen unabhängig sind - **wer** entscheidet, **welche** Informationen über eine Person **wie** benutzt werden dürfen?
- Menschliches Lernen beinhaltet Fehler zu machen. Was passiert, wenn „die Gesellschaft“ sie ihr ganzes Leben immer wieder an lang zurückliegendes Fehlverhalten erinnert?
- Privatsphäre ist ein Menschenrecht. Alle modernen Demokratien schützen diese.
- „Datenschutz“ bedeutet nicht Schutz von Daten!
- Für die meisten Unternehmen gilt: **grosse Reputationsrisiken**, wenn Personendaten missbraucht werden! **Vertrauensverlust!**

Zürcher Hochschule
für Angewandte Wissenschaften

WIE KÖNNTE DIE ZUKUNFT DES DATENSCHUTZES AUSSEHEN?

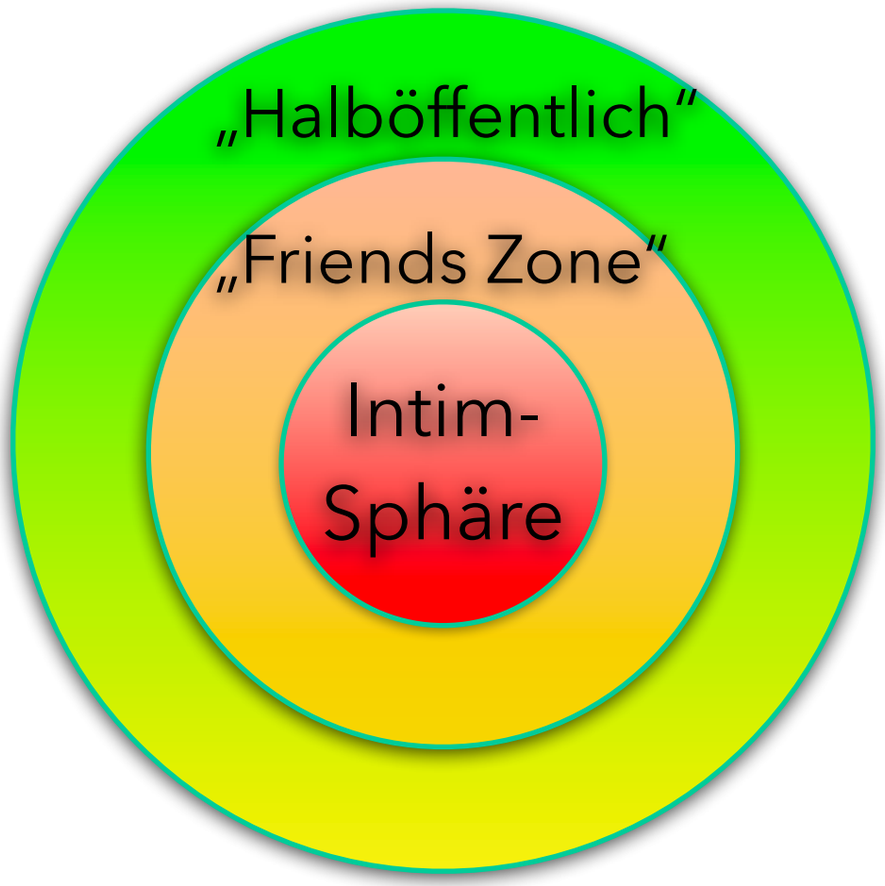
- Zukunft: Totaler Kontrollverlust (Modell „China“ oder Google, Palpitier & Co.) oder immer restriktiver (Modell „DSGVO“)?
- Auf dem Papier haben die Menschen viele Rechte, aber auch in der Praxis?
- Daten sind (rechtlich) kein Eigentum - sie erzeugen nur einen Mehrwert, wenn sie genutzt werden!
- Schutz würde auch bieten, wenn die Datensammler gesetzlich verpflichtet würden, andern (anonymisierte) Personendaten nutzen zu lassen. Analoges Beispiel: Open Banking Standard über definierte API’s. Wettbewerbsvorteil durch (begrenzte) Offenheit & Vernetzung.
- EU-Projekt „GAIA-X“ mit dem Ziel, eine sichere, vertrauenswürdige Dateninfrastruktur aufzubauen. Sinnvoll? AWS ist in den Cloud-Diensten immer noch grösser als MS, Google & FB…
- **Schwingt das Pendel zurück?**

Zürcher Hochschule
für Angewandte Wissenschaften

PRIVACY – SPHÄRENTHEORIE

ÖFFENTLICHKEIT

ÖFFENTLICHKEIT



ÖFFENTLICHKEIT

ÖFFENTLICHKEIT

Zürcher Hochschule
für Angewandte Wissenschaften

INTEGRITÄTSSCHUTZ – SCHUTZ DER PERSÖNLICHKEIT (ART. 28 ZGB / 30 revDSG)

„Wer in seiner Persönlichkeit **widerrechtlich** verletzt wird, kann zu seinem Schutz gegen jeden, der in der Verletzung mitwirkt, das **Gericht** anrufen.

Eine Verletzung ist **widerrechtlich**, wenn sie nicht durch **Einwilligung des Verletzten**, durch ein **überwiegend privates oder öffentliches Interessen** oder durch **Gesetz** gerechtfertigt ist.“

Zürcher Hochschule
für Angewandte Wissenschaften

GESETZLICHE GRUNDLAGEN

- Schweizerische Bundesverfassung (Art. 13 BV)
- (revidiertes) Bundesgesetz über den Datenschutz (DSG) (sollte Anfangs 2022 in Kraft treten, vermutlich aber verschoben bis Anfangs 2023) und Verordnung dazu (Vernehmlassung zur VDSG ergab viele negative Rückmeldungen!)
- Zahlreiche datenschutzrechtliche Bestimmungen in anderen Gesetzen (z.B. OR)
- Kantonales und Gemeinderecht: zahlreiche Gesetze und Verordnungen
- International: **EU-DSGVO** (Europäische DatenSchutzGrundeVerOrdnung)

Zürcher Hochschule
für Angewandte Wissenschaften

ARBEITSVERHÄLTNIS & DATENSCHUTZ – ART. 328B OR

*„Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen **Eignung** für das Arbeitsverhältnis betreffen oder zur **Durchführung des Arbeitsvertrages erforderlich** sind. Im Übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz.“*

Zürcher Hochschule
für Angewandte Wissenschaften

Revision CH-Datenschutzgesetz (revDSG)

- Am 25. September 2020 hat das Parlament nach Bereinigungen das revidierte DSG angenommen. Das neue DSG tritt wohl erst 2023 in Kraft
- Die Grundprinzipien des Datenschutzes ändern sich nicht; Einwilligungen für das Bearbeiten von Personendaten sind nach wie vor meist keine erforderlich (anders als unter der DSGVO)
- Governance-Pflichten, wie das Führen von Datenbearbeitungs-Inventaren, eine Meldepflicht von Datenverlusten und anderen Sicherheitsverstössen und die Pflicht zur Vornahme von Datenschutz-Folgenabschätzungen
- Neu ist vorgesehen, dass Unternehmen Datenschutzberater ernennen können und ausländische Unternehmen mit wesentlichen Aktivitäten in der Schweiz eine Schweizer Vertretung bestimmen müssen
- Die Rechte der betroffenen Personen werden etwas ausgebaut; es wird einfacher, die eigenen Daten von einem Unternehmen heraus zu verlangen
- Verträge müssen auf DSG-Konformität überprüft werden; namentlich bei sog. Auftragsbearbeitern wird der Beizug von Subakkordanten strenger geregelt (analog DSGVO)
- Informationspflicht bei Datenbeschaffungen wird inhaltlich (d.h. worüber informiert werden muss ausgeweitet; Unternehmen müssen daher ihre Datenschutzerklärungen überprüfen)
- Der Auslandstransfer von Daten wird zwar liberalisiert, aber Verstösse sind neu strafbewehrt
- Bearbeitung von Daten zur Prüfung der Kreditwürdigkeit wird insb. zeitlich eingeschränkt
- Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte kann neu Bearbeitungsverbote und Verfügungen erlassen und nicht mehr nur «Empfehlungen»
- Die Strafbestimmungen (CHF 250'000) zielen auf verantwortliche Mitarbeiter, nicht Firmen betreffen aber nur wenige Fälle (Information, Auskunft, Exporte, Sicherheit, Outsourcing)

Zürcher Hochschule
für Angewandte Wissenschaften

GELTUNGSBEREICH – ART. 2 revDSG

1 Dieses Gesetz gilt für die Bearbeitung von Personendaten **natürlicher Personen** durch:

a. **private Personen**;

b. **Bundesorgane**.

2 Es ist **nicht** anwendbar auf:

a. Personendaten, die von einer natürlichen Person **ausschliesslich zum persönlichen Gebrauch** bearbeitet werden;

b. Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

c. Personendaten, die bearbeitet werden durch institutionelle Begünstigte nach Artikel 2 Absatz 1 des Gaststaatgesetzes vom 22. Juni 2007, die in der Schweiz Immunität von der Gerichtsbarkeit geniessen.

3 Das anwendbare Verfahrensrecht regelt die Bearbeitung von Personendaten und die Rechte der betroffenen Personen in Gerichtsverfahren und in Verfahren nach bundesrechtlichen Verfahrensordnungen. Auf erstinstanzliche Verwaltungsverfahren sind die Bestimmungen dieses Gesetzes anwendbar.

4 Die öffentlichen Register des Privatrechtsverkehrs, insbesondere der Zugang zu diesen Registern und die Rechte der betroffenen Personen, werden durch die Spezialbestimmungen des anwendbaren Bundesrechts geregelt. Enthalten die Spezialbestimmungen keine Regelung, so ist dieses Gesetz anwendbar.

Zürcher Hochschule
für Angewandte Wissenschaften

RÄUMLICHER GELTUNGSBEREICH – ART. 3 revDSG

Auch das Schweizer Datenschutzrecht untersteht neu dem „Marktortsprinzip“!

1 Dieses Gesetz gilt für Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.

2 Für privatrechtliche Ansprüche gilt das Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht.
Vorbehalten bleiben zudem die Bestimmungen zum räumlichen Geltungsbereich des Strafgesetzbuchs.

Zürcher Hochschule
für Angewandte Wissenschaften

BEGRIFFE & DEFINITIONEN – ART. 5 revDSG (1)

a. **Personendaten: alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen**;

b. betroffene Person: natürliche Person, über die Personendaten bearbeitet werden;

c. besonders schützenswerte Personendaten:

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
3. genetische Daten,
4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,
5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
6. Daten über Massnahmen der sozialen Hilfe;

d. **Bearbeiten: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten**;

Zürcher Hochschule
für Angewandte Wissenschaften

BEGRIFFE & DEFINITIONEN – ART. 5 revDSG (2)

e. Bekanntgeben: das Übermitteln oder Zugänglichmachen von Personendaten;

f. Profiling: jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

g. Profiling mit hohem Risiko: Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;

h. Verletzung der Datensicherheit: eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden;

i. Bundesorgan: Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist;

j. **Verantwortlicher: private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet;**

k. **Auftragsbearbeiter: private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.**

Zürcher Hochschule
für Angewandte Wissenschaften

DATENSCHUTZGRUNDSÄTZE – ART. 6 revDSG

1 **Personendaten müssen rechtmässig bearbeitet werden.**

2 **Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein.**

3 **Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden**; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.

4 **Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind**.

5 **Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern**. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich ab von der Art und dem Umfang der Bearbeitung sowie vom Risiko, das die Bearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringt.

6 Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.

7 **Die Einwilligung muss ausdrücklich** erfolgen für:

a. **die Bearbeitung von besonders schützenswerten Personendaten**;

b. **ein Profiling mit hohem Risiko durch eine private Person**; oder

c. **ein Profiling durch ein Bundesorgan**.

Zürcher Hochschule
für Angewandte Wissenschaften

DATA PROTECTION BY DESIGN AND BY DEFAULT – ART. 7 revDSG

Art. 7 - Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

1 Der Verantwortliche ist verpflichtet, die Datenbearbeitung **technisch und organisatorisch** so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung.

2 Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, **angemessen** sein.

3 Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

Zürcher Hochschule
für Angewandte Wissenschaften

DATENSICHERHEIT – ART. 8 revDSG

1 Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

2 Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

3 Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Zürcher Hochschule
für Angewandte Wissenschaften

BEARBEITUNG DURCH AUFTRAGSBEARBEITER (CLOUD-COMPUTING) – ART. 9 revDSG

1 Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

2 **Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten**.

3 Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

4 Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

Zürcher Hochschule
für Angewandte Wissenschaften

VERZEICHNIS DER BEARBEITUNGSTÄTIGKEITEN – ART. 12 revDSG

1 **Die Verantwortlichen und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten**.

2 Das Verzeichnis des Verantwortlichen enthält mindestens:

a. die Identität des Verantwortlichen;

b. den **Bearbeitungszweck**;

c. eine Beschreibung der **Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten**;

d. die **Kategorien der Empfängerinnen und Empfänger**;

e. wenn möglich die **Aufbewahrungsdauer der Personendaten** oder die Kriterien zur Festlegung dieser Dauer;

f. wenn möglich eine allgemeine **Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit** nach Artikel 8;

g. falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2.

3 Das Verzeichnis des Auftragsbearbeiters enthält Angaben zur Identität des Auftragsbearbeiters und des Verantwortlichen, zu den Kategorien von Bearbeitungen, die im Auftrag des Verantwortlichen durchgeführt werden, sowie die Angaben nach Absatz 2 Buchstaben f und g.

4 Die Bundesorgane melden ihre Verzeichnisse dem EDÖB. **Der Bundesrat sieht Ausnahmen für Unternehmen vor, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.**

Zürcher Hochschule
für Angewandte Wissenschaften

DATENSCHUTZ-FOLGENABSCHÄTZUNG – ART. 22 revDSG

1 **Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.**

2 Das hohe Risiko ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:

a. bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;

b. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

3 Die **Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte**.

4 Von der Erstellung einer Datenschutz-Folgenabschätzung ausgenommen sind private Verantwortliche, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind.

5 Der private Verantwortliche kann von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn er ein System, **ein Produkt oder eine Dienstleistung einsetzt, das oder die für die vorgesehene Verwendung nach Artikel 13 zertifiziert ist**, oder wenn er einen **Verhaltenskodex** nach Artikel 11 einhält, der die folgenden Voraussetzungen erfüllt:

a. Der Verhaltenskodex beruht auf einer Datenschutz-Folgenabschätzung.

b. Er sieht Massnahmen zum Schutz der Persönlichkeit und der Grundrechte der betroffenen Person vor.

c. **Er wurde dem EDÖB vorgelegt**.

Zürcher Hochschule
für Angewandte Wissenschaften

MELDUNGEN VON VERLETZUNGEN DER DATENSICHERHEIT – ART. 24 revDSG

1 **Der Verantwortliche 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.**

2 In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.

3 Der Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich eine Verletzung der Datensicherheit.

4 **Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt**.

5 Er kann die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten, wenn:

a. ein Grund nach Artikel 26 Absatz 1 Buchstabe b oder Absatz 2 Buchstabe b vorliegt oder eine gesetzliche Geheimhaltungspflicht dies verbietet;

b. die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert; oder

c. **die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist.**

6 Eine Meldung, die aufgrund dieses Artikels erfolgt, darf in einem Strafverfahren gegen die meldepflichtige Person nur mit deren Einverständnis verwendet werden.

Zürcher Hochschule
für Angewandte Wissenschaften

AUSKUNFTSRECHT – ART. 25 revDSG

1 **Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.**

2 Die betroffene Person erhält diejenigen Informationen, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist. In jedem Fall werden ihr folgende Informationen mitgeteilt:

a. die Identität und die Kontaktdaten des Verantwortlichen;

b. die bearbeiteten Personendaten als solche;

c. der Bearbeitungszweck;

d. die Aufbewahrungsdauer der Personendaten oder, falls dies nicht möglich ist, die Kriterien zur Festlegung dieser Dauer;

e. die verfügbaren Angaben über die Herkunft der Personendaten, soweit sie nicht bei der betroffenen Person beschafft wurden;

f. gegebenenfalls das Vorliegen einer automatisierten Einzelentscheidung sowie die Logik, auf der die Entscheidung beruht;

g. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden, sowie die Informationen nach Absatz 4.

3 Personendaten über die Gesundheit können der betroffenen Person mit ihrer Einwilligung durch eine von ihr bezeichnete Gesundheitsfachperson mitgeteilt werden.

4 Lässt der Verantwortliche Personendaten von einem Auftragsbearbeiter bearbeiten, so bleibt er auskunftspflichtig.

5 **Niemand kann im Voraus auf das Auskunftsrecht verzichten.**

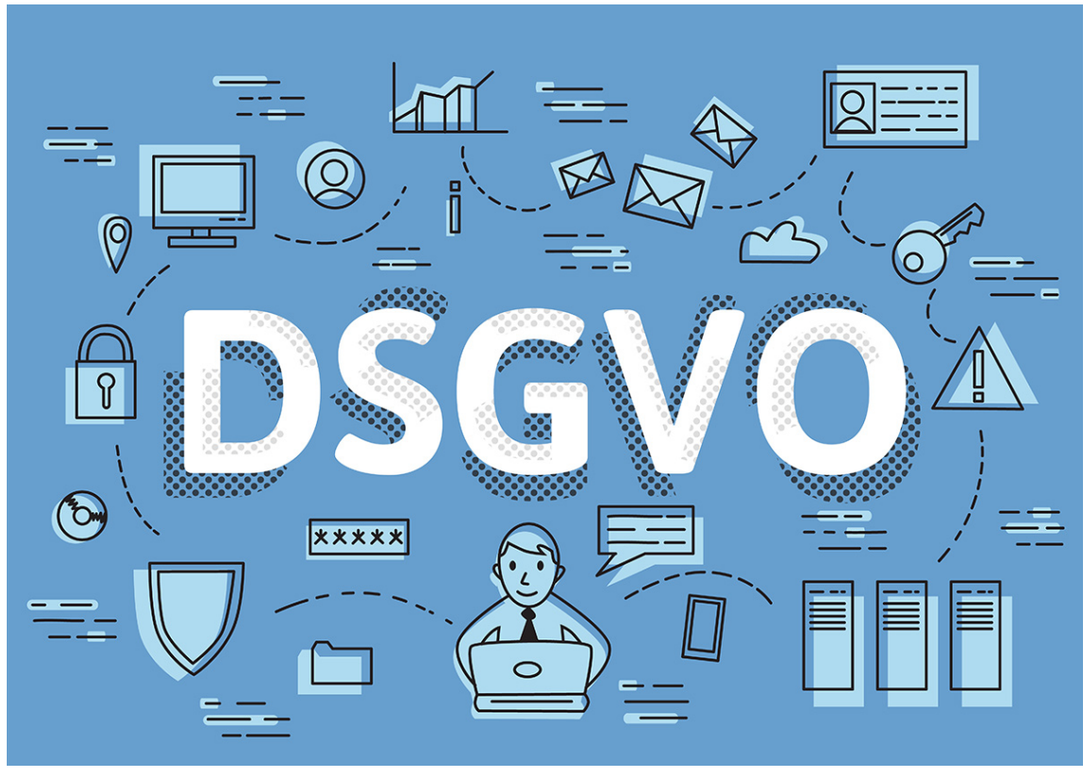
6 **Der Verantwortliche muss kostenlos Auskunft erteilen. Der Bundesrat kann Ausnahmen vorsehen, namentlich wenn der Aufwand unverhältnismässig ist.**

7 **Die Auskunft wird in der Regel innerhalb von 30 Tagen erteilt.**

Zürcher Hochschule
für Angewandte Wissenschaften

HEIDILAND, DATENSCHUTZ & DSGVO

&



Zürcher Hochschule
für Angewandte Wissenschaften

DSGVO AUS SCHWEIZER SICHT 1

Die DSGVO ist seit Ende Mai 2018 auch für Schweizer Unternehmen **direkt** anwendbar, wenn:

- **diese Waren oder Dienstleistungen in der EU/EWR anbieten (die Angabe des Preises in Euro genügt) und dazu personenbezogene Daten (z.B. Adressdaten, Kundenprofil) bearbeiten (Marktortprinzip: Art. 3 Abs. 2 DSGVO), oder**
- **diese das Verhalten von Website-Besuchern aus der EU sammeln und auswerten (Tracking durch Cookies, Profiling mit Tools wie Google Analytics, Facebook Pixel etc.), oder**
- **diese regelmässig Newsletter an Empfänger in der EU versendet, oder**
- **diese im Auftrag oder als Konzernzentrale resp. -Mitglied eines in der EU domizilierten Unternehmens personenbezogene Daten bearbeiten.**

Wenn einer dieser Fälle auf ein Unternehmen zutrifft, besteht unmittelbar Handlungsbedarf!

Zürcher Hochschule
für Angewandte Wissenschaften

DSGVO AUS SCHWEIZER SICHT 2

- Grundsätzlich handelt es sich bei der DSGVO „nur“ um ein europäisch vereinheitlichtes Datenschutzrecht zur Durchsetzung von mehrheitlich (auch bei uns!) bereits bestehenden Grundsätzen!
- Zur Durchsetzung können die EU-Aufsichtsbehörden nun aber Auskünfte und Überprüfungen veranlassen, Anweisungen erteilen sowie - bei wiederholter schwerer Missachtung - Geldbussen bis zu € 10 resp. 20 Mio. oder bis zu 2% resp. 4% des weltweit erzielten Jahresumsatzes verfügen. Die Massnahmen müssen jeweils aber verhältnismässig und wirksam sein. „Bestrafung“ von Unternehmen in der Schweiz noch unklar.
- DSGVO ist nur „Mindeststandard“! EU-Länder können weitergehende Regelungen erlassen (z.B. § 26 deutsches BDSG-neu)

Zürcher Hochschule
für Angewandte Wissenschaften

DSGVO AUS SCHWEIZER SICHT 3

Vereinfacht geht es um die Durchsetzung der (selbstverständlichen!) Rechte der Bürger bezüglich:

- **Auskunftsrecht** und **Recht auf Datenübertragbarkeit**
- **Erweiterte Informationspflichten** gegenüber der betroffenen Person
- **Widerspruchsrecht**
- **Recht auf Löschung** (Recht auf Vergessen)
- Möglichkeit für **Abmahnungen** und Klagen von **Genugtuung** und **Schadenersatz** für die betroffene Person
- **Privacy by design** und **privacy by default** (!)
- Erweiterte **Dokumentationspflichten** (TOM's, Verarbeitungsverzeichnisse, Beweislastumkehr)

Zürcher Hochschule
für Angewandte Wissenschaften

DSGVO – IM DETAIL!

- **Ausbau der Rechte der betroffenen Personen** (Aufklärungspflichten, Transparenz, Zweckbindung, ausdrückliche Einwilligung oder Bezug auf Rechtfertigungsgrund, Art. 5/6 DSGVO).
- **Datenhaltung nur solange es der Zweck erfordert** (Speicherbegrenzung, Art. 5 DSGVO).
- **Datenschutz durch Technikgestaltung** (Privacy by Design; Art. 25 Abs. 1 DSGVO) und datenschutzfreundliche Voreinstellungen (Privacy by Default; Art. 25 Abs. 2 DSGVO).
- **Big Data**: Pflicht zur vorgängigen Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO).
- **Meldepflichten bei Datenschutzverletzungen** an die zuständige Aufsichtsbehörde (Art. 33 DSGVO) sowie direkte Benachrichtigung der betroffenen Personen bei hohem Risiko von Persönlichkeitsverletzungen.
- **Benennung eines Datenschutzbeauftragten** (Art. 37 DSGVO). Gegebenenfalls muss ein Vertreter des Unternehmens in der EU bestimmt werden (Art. 27 Abs. 1 DSGVO).
- **Auslagerung der Datenverarbeitung** (Auftragsverarbeitung) nur auf der Grundlage eines Vertrages mit **Standardvertragsklausel** bei hinreichenden Garantien („Datenschutzsiegel“) des Auftragsdatenverarbeiters (Art. 28 Abs. 1 DSGVO).
- **Recht der betroffenen Person auf Datenübertragbarkeit** in strukturierter, maschinenlesbarer Form (Art. 20 DSGVO).
- Weitgehende **Rechenschaftspflichten** über die Verarbeitungsprozesse.
- **Keine Unter-Auftragsverarbeitung** (Sub-Sub-Akkordanten) ohne schriftliche Genehmigung des Verantwortlichen (Art. 28 Abs. 2 DSGVO).

Zürcher Hochschule
für Angewandte Wissenschaften

NOTWENDIGE SCHRITTE – STEP BY STEP

Zürcher Hochschule
für Angewandte Wissenschaften

WAS NEHME ICH VON HEUTE MIT?

- ...
- ...
- ...
- ...
- ...