Universität Basel

Fact Sheet Datenschutz – wichtigste Definitionen & Beispiele

Bitte beachten Sie, dass wir in diesem Fact Sheet verzichtet haben auf die jeweiligen Gesetzesartikel zu verweisen, die Ziffern in diesem Dokument korrespondieren aber mit den Ziffern des Fact Sheet – Auszug wichtiger gesetzlicher Grundlagen vom 28. Juni 2019, wo sie die Gesetzesartikel finden. Die aktuellste Version der jeweiligen Gesetzestexte finden sie unter folgenden Links:

Europäische Datenschutz-Grundverordnung

Bundesgesetz über den Datenschutz Schweiz

Datenschutzgesetz Kanton Basel-Stadt

Datenschutzgesetz Kanton Bern

Im Weiteren bitten wir zu beachten, dass die Angaben im Text rechtlich nicht verbindlich sind, sie sollen Ihnen als Hilfestellung dienen.

30. August 2019/ lic. iur. Danielle Kaufmann

1. Was sind (Personen-)Daten?

- Angaben, Informationen, Aussagen, die sich auf eine bestimmte oder mittels der Informationen bestimmbare Person beziehen

Beispiele für Personendaten:

- *Name, Geburtsdatum, (Mail-)Adresse, Telefon/Mobile, AHV-Nr., MatrikelNr., Bankdaten, IP-Adresse (mit Ausnahmen), Geschlecht, Fotografie, eine Person besonders charakterisierende Merkmale (zB einzige Frau im Team), genetische Daten, Autokennzeichen, etc.*

1.1. **keine** Personendaten: **Sachdaten**

- Sachdaten sind Angaben, die sich — auch im Zusammenhang mit weiteren Angaben — nicht auf eine (bestimmte oder bestimmbare) Person beziehen. Auf ihre Bearbeitung ist das Datenschutzrecht nicht anwendbar.

Beispiele für Sachdaten

- *Reine Sachdaten wie zB Geldbeträge pro Haushaltsbereich, Daten über Flugbewegungen, Wassertemperaturen, Klimadaten*

1.2. **keine** Personendaten **mehr**: **Daten mit aufgehobenem Personenbezug**

- Personendaten, die anonymisiert (vgl. Ziff. 9) wurden. **Nach** der Anonymisierung unterstehen diese Daten nicht mehr dem Datenschutzrecht.

➢ **Achtung: die Abgrenzung Personendaten – Sachdaten/anonymisierte Daten ist fliessend und durch zusätzliche Informationen oder technische Bearbeitung können Sachdaten bzw. anonymisierte Daten (wieder) zu Personendaten werden.**

2. Was sind besondere/ besonders schützenswerte/ sensible Personendaten/ besondere Kategorien von Personendaten?
   - Personendaten, bei denen aufgrund ihrer Aussagekraft, der Art ihrer Bearbeitung oder auch weil sie geeignet sind ein Profil der betroffenen Person zu erstellen, eine besondere Gefahr einer Persönlichkeitsverletzung besteht.
   - Hier ist auch an Daten zu denken von Kindern, urteilsunfähigen Personen, und anderen besonders verletzlichen Personen wie z.B. Flüchtlinge, Angehörige einer ethnischen Minderheit, etc.

   Beispiele für besonders schützenswerte Personendaten
   - religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten über Gesundheit, Intimsphäre oder die Rassenzugehörigkeit, genetische und biometrische Daten, Angaben zu Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen;

3. Was ist das sog. **Forschungsprivileg**? Was das Bearbeiten von Personendaten zu einem **nicht personenbezogenen Zweck**?
   - Vereinfacht gesagt geht es darum, dass einmal erhobene Daten, sei es durch ein öffentliches Organ oder durch den/die ForscherIn selber, für eine Datenbearbeitung mit Personenbezug (z.B. Erhebung von Steuerdaten durch den Kanton zum Zweck der Steuererhebung), durch Anonymisierung oder Pseudonymisierung für eine **Datenbearbeitung ohne Personenbezug** (z.B. Nutzung der erhobenen Steuerdaten in anonymisierter/pseudonymisierter Form für ein statistisches Forschungsprojekt) genutzt werden dürfen. Für die Datenbearbeitung ohne Personenbezug ist dann keine weitere Rechtfertigung wie eine Einwilligung mehr notwendig.
   - Datenschutzrechtlich liegt eine sog. **Zweckänderung** vor
   - Voraussetzungen: personenbezogene Daten sind, sobald es der Bearbeitungszweck erlaubt, zu anonymisieren bzw. pseudonymisieren
   - Die Forschungsergebnisse sind immer in anonymisierter Art und Weise zu publizieren
   - Das Datenschutzrecht privilegiert die nicht personenbezogene Bearbeitung von Personendaten aufgrund des **öffentlichen Interesses an der Forschung** und der Annahme, dass dadurch die Gefahr einer Persönlichkeitsverletzung gering ist.

➢ **Achtung: für die vorgängige Datenerhebung/ -bearbeitung (jene mit Personenbezug) sind aber in jedem Fall die allgemeinen Prinzipien des Datenschutzes zu beachten!**

4. Was ist eine Datenbearbeitung/ Datenverarbeitung?
   - **Alles was man mit Personendaten machen kann**, unabhängig von der Technik, unabhängig vom Medium (Papier, digital, …), unabhängig von der Dauer (flüchtig, für immer, etc.)

   Beispiele für Datenbearbeitung
   - Beschaffen, Speichern, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben (Einsichtgewähren, Weitergeben oder Veröffentlichen), Archivieren oder Vernichten von Daten, ...

5. Unter welchen grundsätzlichen Voraussetzungen dürfen Daten bearbeitet werden? (wichtigste Prinzipien des Datenschutzrechts)

5.1. Rechtmässigkeit:
   - Datenbearbeitung stellt eine Persönlichkeitsverletzung dar und muss daher immer gerechtfertigt sein, d.h. sie muss immer **rechtmässig** erfolgen:
     - entweder aufgrund einer **gesetzlichen Bestimmung**
     - und/oder aufgrund einer **Einwilligung der betroffenen Person**
     - oder aufgrund eines überwiegenden Interesses der bearbeitenden Person*

Beispiele für gesetzliche Bestimmungen bei Forschungsprojekten

- Oftmals kann als gesetzliche Grundlage für die Datenbearbeitung bei Forschungsprojekten nur auf den «**allgemeinen Forschungsauftrag der Universitäten»** abgestützt werden (z.B. Universitätsgesetz Bern Art. 2 Abs. 2 «*Sie fördert durch Forschung die wissenschaftliche Erkenntnis.* »; Statut der Universität Basel §1 Abs. 1 «*Die Universität ist eine Institution der wissenschaftlichen Lehre, Forschung und Dienstleistung. Sie erfüllt ihre Aufgaben im Dienst der Allgemeinheit und achtet die Würde des Menschen und der Kreatur. »)* ***Umso unspezifischer die gesetzliche Grundlage für die Datenbearbeitung ist, umso wichtiger ist das Beachten der Verhältnismässigkeit und im Zusammenhang mit Forschungsprojekten reicht es nicht aus, sich nur auf den Forschungsauftrag der Universität abzustützen, dieser erlaubt einfach, dass man grundsätzlich Datenbearbeitungen vornehmen darf. Für die konkrete Datenbearbeitung ist ergänzend eine Einwilligung mit Angabe (vgl. Ziff. 5.1.) des konkreten Zwecks erforderlich***
- Humanforschungsgesetz

5.2. Zweckbindung:

- eine Datenbearbeitung muss immer zu einem **bestimmten Zweck** erfolgen

5.3. Verhältnismässigkeit

- ist ein Grundprinzip des öffentlichen Rechts und gilt auch für die Bearbeitung von Personendaten. Danach dürfen Personendaten nur bearbeitet werden, wenn:
    - dies **für einen bestimmten Zweck objektiv geeignet und tatsächlich erforderlich** ist und
    - die Datenbearbeitung für die betroffene Person sowohl hinsichtlich ihres Zwecks als auch hinsichtlich ihrer Mittel **zumutbar ist** (vereinfacht gesagt, muss zwischen dem Bearbeitungszweck und der damit zusammenhängenden Beeinträchtigung der Persönlichkeit der betroffenen Person ein vernünftiges Verhältnis bestehen)

Beispiele für fehlende Verhältnismässigkeit

- Sammeln von Daten ohne direkten Zusammenhang zum Zweck
- Sammeln von Daten auf Vorrat (z.B. im Sinn von «ev. könnte man diese Daten mal noch brauchen…»)

5.4. Richtigkeit (Integrität):

- wer Personendaten bearbeitet, hat sich zu vergewissern, dass die Daten richtig sind
- bei Personendaten im Sinne von Tatsachenfeststellungen, sind diese richtig, wenn sie die Tatsache in Bezug auf die betroffene Person und in Bezug auf den Verwendungszweck der Daten sachgerecht wiedergeben
- bei Werturteilen gibt es logischerweise keine Richtigkeit
- es handelt sich immer um eine relative Richtigkeit, d.h. keine abstrakte Richtigkeit, sondern auf den konkreten Fall bezogene

Beispiel für Richtigkeit von Daten (bzw. Anspruch der betroffenen Person auf allfällige Korrektur falscher Daten)

- das Geschlecht einer Person muss richtig angegeben werden, das führt dazu, dass ein entsprechender Eintrag in einer Datensammlung nach einer Geschlechtsumwandlung korrigiert werden muss (je nach Fall erfolgt die Berichtigung entsprechend einem Begehren der betroffenen Person oder z.B. im Fall des Spitals, wo die Geschlechtsumwandlung vorgenommen wurde, muss das Spital das Patientendossier von sich aus korrigieren)

5.5. Erkennbarkeit der Datenbearbeitung:

- für die betroffene Person muss transparent erkennbar sein, dass sie betreffende Personendaten erhoben und bearbeitet werden

5.6. Transparenz:

- die betroffenen Personen müssen ausreichend informiert werden über die Datenbearbeitung, so dass sie verstehen können, was mit ihren Daten zu welchem Zweck gemacht wird
- zudem haben die betroffenen Personen jederzeit und ohne Angabe von Gründen das Recht Auskunft über ihre Daten zu erfragen

6. Wann ist eine Einwilligung erforderlich? Wann reicht eine Einwilligung als Rechtfertigungsgrund? Muss eine Einwilligung schriftlich erfolgen?

- Ob eine Einwilligung zwingend oder allenfalls ergänzend zu einer gesetzlichen Grundlage erforderlich ist bzw. als Rechtfertigungsgrund (vgl. Ziff. 5.1.) ausreichend ist, hängt von dem anzuwendenden Datenschutzrecht ab. **Sowohl nach dem IDG/BS wie nach dem KDSG/BE reicht eine Einwilligung nicht, es bedarf immer auch einer gesetzlichen Grundlage**.
- Auch ob eine Einwilligung mündlich oder schriftlich erfolgen kann, regelt das anzuwendende Recht. Einwilligungen können mehrere Funktionen erfüllen, unter anderem auch die Information (Transparenzgrundsatz, vgl. Ziff. 5.6.) der betroffenen Personen und im Weiteren kann sie eine sehr generell gehaltene gesetzliche Grundlage präzisieren (vgl. Ziff. 3).

➢ **Empfehlung: bei Forschungsprojekten empfiehlt sich das Einholen einer Einwilligung und aus Beweisgründen, wenn möglich in schriftlicher Form oder allenfalls als Tonaufnahme**.

7. Welche Gesetze sind bei Datenbearbeitungen zu beachten?

7.1. Zu unterscheiden ist, ob eine private Person (natürlich oder juristisch) oder eine Behörde (eidgenössisch, kantonal, kommunal) bzw. eine öffentliche Institution eine Datenbearbeitung vornimmt

a. Das Datenschutzrecht in der Schweiz teilt sich in Bundesrecht und kantonales Recht auf
b. **Bundesdatenschutzgesetz** gilt für die Datenbearbeitung durch **den Bund** (neben den Bundesbehörden auch für die ETH & EPFL) **und Private** (Achtung: Forschende, die ihre Forschung im Rahmen ihrer Anstellung an einer Universität betreiben gelten nicht als Private)
c. **Kantonales Datenschutzgesetz** gilt für **kantonale und kommunale Behörden, für kantonale öffentliche Institutionen** (z.B. Universitäten, öffentliche Spitäler) und für Private, die im Auftrag eines Kantons Datenbearbeiten

7.2. Im Weiteren ist im Falle eines **Auslandsbezugs** (Datenerhebung im Ausland, Datenlieferung ins Ausland etc.) zu prüfen, ob allenfalls ausländisches Datenschutzrecht (insbesondere EU-DSGVO) anzuwenden ist? Bei einem Auslandsbezug empfiehlt sich immer **juristischen Rat einzuholen**, ob die EU-DSGVO oder allenfalls ein anderes ausländisches Gesetz zur Anwendung kommt, ist schwierig zu beurteilen und bedarf der Einzellfallanalyse.

8. Wer ist verantwortlich für die korrekte Datenverarbeitung?

- Bei Forschungsarbeiten im Rahmen der universitären Anstellung kommt das entsprechende kantonale Datenschutzrecht zur Anwendung und entsprechend trägt die Universität als kantonale Institution mit öffentlichem Auftrag die Verantwortung
- Bei Forschungsarbeiten an der ETH und der EPFL kommt Bundesdatenschutzgesetz zur Anwendung und damit trägt die ETH bzw. die EPFL die Verantwortung

➢ **Zu beachten:** Universitätsinterne Richtlinien, Reglemente über die Nutzung von Informatikmittel, Umgang mit (Forschungs-)daten, Integritätsordnungen und andere Erlasse, die die Verantwortung für den korrekten Umgang mit Daten zusätzlich regeln

- Bei privater Forschung kommt das Bundesdatenschutzgesetz (DSG) zur Anwendung und die Verantwortung trägt die private, datenverarbeitende Person.

9. Was heisst Anonymisierung, Pseudonymisierung, Verschlüsselung, etc.?
    - **Anonymisierung** bedeutet, dass der Personenbezug **irreversibel** (= endgültig) so aufgehoben wird, dass ohne unverhältnismässigen Aufwand keine Rückschlüsse auf Personen mehr möglich sind. Anonymisierte Daten gelten nicht mehr als Personendaten.
    - Unter **Pseudonymisierung** versteht man die Aufhebung des Personenbezugs, wobei ein bestimmter Schlüssel (also eine Tabelle mit der Übersetzung Pseudonym zu Person) zur **Re-Personifizierung** der Informationen erhalten bleibt. Werden Daten pseudonymisiert, sind die Bedingungen zu regeln, unter denen eine Person identifiziert werden darf und wie der Schlüssel aufbewahrt wird (Schlüsselmanagement). Anders als bei den anonymisierten Daten bleiben pseudnoymisierte Daten Personendaten.

    - **Achtung:** in diesem Abschnitt geht es nur um Verschlüsselung im juristischen Sinn, davon zu unterscheiden ist die Verschlüsselung im technischen und methodischen Sinn