Modul 1, 13. September 2016

Webinar@Weblaw: DSGVO – Geltungsbereich, Bearbeitungsgrundsätze, Informationspflichten.

Nicolas Passadelis

Bearbeitungsgrundsätze: Personendaten, Datensparsamkeit, Privacy by Design und Privacy by Default bei eigenen Produkten und Dienstleistungen.

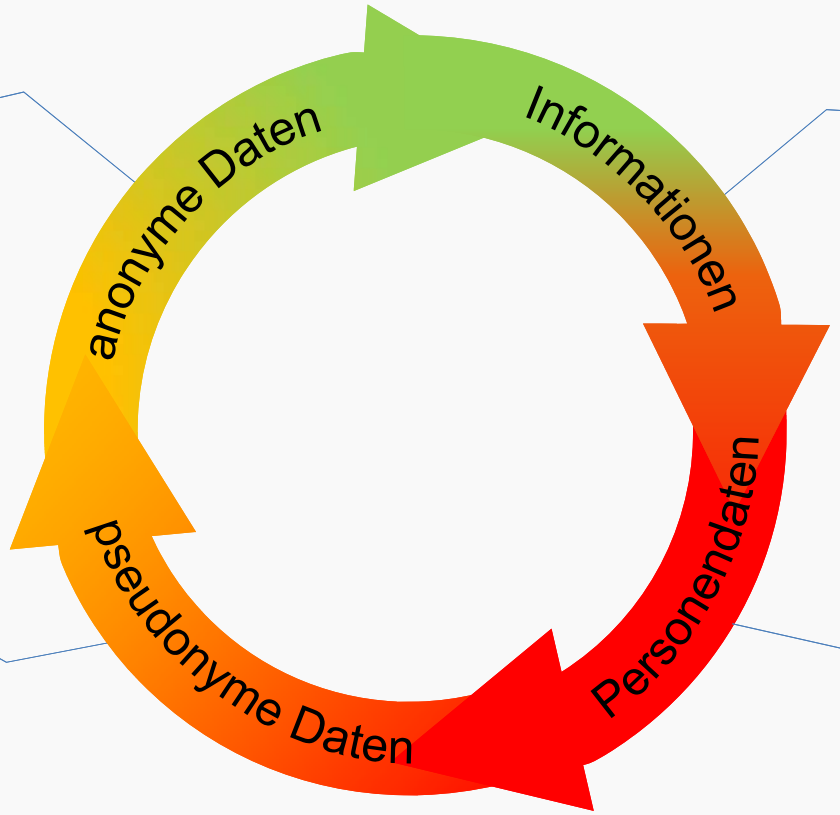
Inhaltsverzeichnis.

1. Personenbezogene Daten – Definition und Bedeutung.

- Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 I Ziff. 1 DSGVO)
- Verarbeitung von personenbezogenen Daten definiert den sachlichen Anwendungsbereich der DSGVO:
  - bei ganz oder teilweise automatisierter (elektronischer) Verarbeitung personenbezogener Daten
  - bei nicht-automatisierter Verarbeitung nur, sofern die Daten in einem Datensystem gespeichert sind oder werden sollen (Art. 2 I 1 DSGVO).

2. Informationskategorien unter der DSGVO.

Personenbezogene Daten in einer Weise bearbeitet, dass betroffene Person nicht oder nicht mehr identifiziert werden kann (Erw. 26 DSGVO)



Informationen ohne jeglichen Personenbezug.

Personenbezogene Daten können ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer Person zugeordnet werden (Art. 4 Ziff. 5 DSGVO)

Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Ziff. 1 DSGVO)

3. Neue Datenkategorien.

Genetische Daten (Art. 3 Ziff. 13 DSGVO

- Daten zu genetischen Eigenschaften einer Person
- eindeutige Informationen zu Physiologie oder Gesundheit
- Körperproben

Biometrische Daten (Art. 3 Ziff. 14 DSGVO

- Daten zu körperlichen, psychischen oder verhaltenstypischen Merkmalen
- erlauben eindeutige Identifikaton der Person
- durch technische Verfahren gewonnen

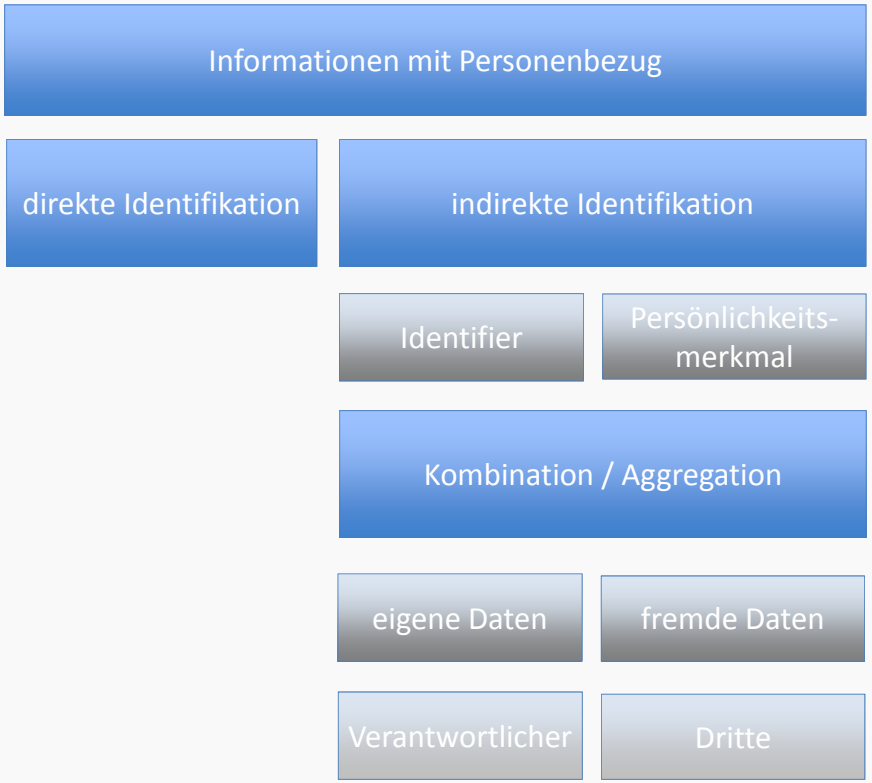
Gesundheitsdaten (Art. 3 Ziff. 15 DSGVO)

- Daten beziehen sich auf körperliche oder geistige Gesundheit
- enthalten Informationen zum Gesundheitszustand

Gleichstellung mit den sensitiven Daten (Art. 9 I DSGVO)

4. Personenbezogene Daten.

- Informationen ohne jeglichen Personenbezug von der DSGVO nicht erfasst *(Bsp. Materialliste)*. Ebenso Daten mit Bezug auf jur. Personen und Verstorbene (Erw. 27)
- Entscheidend ist die Möglichkeit der Identifikation auf der Basis eines Datums (Personenbezug)
- Identifikation kann direkt aus dem Datum selbst *(z.B. Name, Vorname, Foto, Bild)* oder indirekt über Identifier *(z.B. Kundennummer, User ID, Geräte ID, Cookie ID)* bzw. Persönlichkeitsmerkmale *(z.B. Beruf, Sprachkenntnisse)* erfolgen
- Indirekte Identifikation insbesondere durch Kombination mit anderen Daten aus eigenen Beständen oder Beständen Dritter *(Bsp. Identifikation über Geräte ID bei späterer Registrierung)*
- Identifikation auch erst durch Übermittlung an Dritte oder spätere Datenerhebung durch den Verantwortlichen denkbar



5. Wahrscheinlichkeit der (indirekten) Identifikation.

- Feststellung der direkten Identifizierbarkeit einer ist in der Praxis unproblematisch
- Mehr Schwierigkeiten bereitet die Festellung der indirekten Identifizierbarkeit

  Testfrage: Wie wahrscheinlich ist die Identifizierung durch den Verantwortlichen oder Dritten nach allgemeinem Ermessen?

- Der Wahrscheinlichkeitstest wurde unter der DSGVO vermutlich etwas erleichtert (vgl. Stellungnahme WP 216: "*identification reasonably impossible*")
- Durchführung einer Risikoanalyse. Dabei sind zu berücksichtigen:
  - Mittel, welche der Verantwortliche oder ein Dritter für Identifizierung einsetzen könnte
  - Kosten, Zeitaufwand, verfügbare Technologien, technische Entwicklungen *(NB: kriminelle Energie reicht nicht aus!)*
  - Sachliche, zeitliche und persönliche sowie örtliche Risiken
- Wahrscheinlichkeit der Identifikation kann durch Pseudonymisierung und Anonymisierung beeinflusst werden

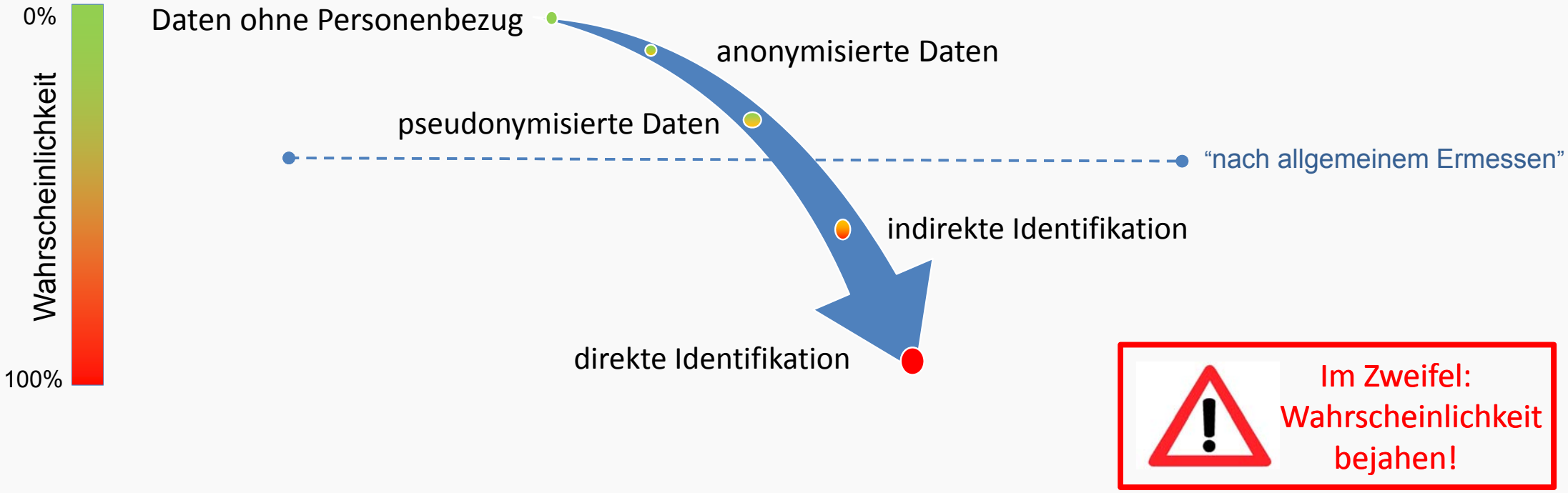
6. Pseudonymisierung.

- Neue Kategorie unter der DSGVO (Art. 5 Ziff. 5 DSGVO).
- DSGVO privilegiert die Pseudonymisierung. Erleichterung von Big Data *(→ David Rosenthal, Modul 4)*
- Bei der pseudonymisierten Verarbeitung von personenbezogenen Daten ist eine Identifikation der verarbeiteten Daten ohne Beizug von Zusatzinformationen faktisch nicht möglich
- Für die Pseudonymisierung sind zwei grundlegende Massnahmen erforderlich:
  1. Daten, welche direkte Identifikation zulassen (Identifiers) werden entfernt oder maskiert *(Bsp. Name wird durch eine nach dem Zufallsprinzip generierte Nummer ersetzt)*
  2. Zusatzinformationen, die eine Identifikation erlauben, sind durch technische und organisatorische Sicherheitsmassnahmen dem Verarbeiter der personenbezogenen Daten wirksam entzogen (vgl. Art 31 I lit. a DSGVO)
- Pseudonymisierung verringert die Wahrscheinlichkeit einer indirekten Identifikation
- Identifikation wäre durch Kombination bzw. Aggregation mit anderen Daten einfach möglich, wird aber durch Sicherheitsmassnahmen verhindert *(Test: Verschafft sich ein Hacker oder ein ungetreuer Mitarbeiter Zugang zu den pseudonymisierten Daten und dem Schlüssel, verfügt er wieder über personenbezogene Daten)*

7. Anonymisierung.

- Beiläufige Erwähnung in der DSGVO (Erw. 26 DSGVO)
- Informationen, die keinen Personenbezug aufweisen
- Personenbezogene Daten, die so verändert wurden, dass die betroffene Person nicht oder mehr identifiziert werden
- Um die Identifikation zu verhindern, braucht es keine weiteren Massnahmen oder Sicherungen (Abgrenzung zu pseudonymisierten Daten)
- Ist eine Identifikation nach allgemeinem Ermessen wahrscheinlich, so liegt keine (erfolgreiche) Anonymisierung vor, sondern “bloss” eine Pseudonymisierung
- Ist die Identifikation nach allgemeinem Ermessen unwahrscheinlich, so sind die Daten anonymisiert
- Im Zweifel ist davon auszugehen, dass die Daten “bloss” pseudonymisiert sind. Schutzpflichten und Pseudonymisierungsprivileg bleiben dann bestehen

8. Wahrscheinlichkeit im Überblick.



Im Zweifel: Wahrscheinlichkeit bejahen!

9. Grundsätze der Bearbeitung.

Rechtmässigkeit
(Art. 1 I lit. a DSGVO)
(→ Bühlmann, Modul 2)

Treu & Glauben
(Art. 1 I lit. a DSGVO)

Transparenz
(Art. 1 I lit. a DSGVO)
(→ Schneider, Modul 1)

Zweckbindung
(Art. 1 I lit. b DSGVO)

Datenminimierung
(Art. 1 I lit. c DSGVO)

Speicherbegrenzung
(Art. 1 I lit. e DSGVO)

Integrität
(Art. 1 I lit. f DSGVO)
(→ Rosenthal, Modul 3)

Rechenschaftspflicht
(Art. 5 II DSGVO)
(→ Rosenthal, Modul 4)

Allgemeiner Teil DSGVO / Auslegungshilfen

10. Zweckbindung.

- Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden. Eine (spätere) Weiterverarbeitung in einer mit diesen Zwecken unvereinbaren Weise ist unzulässig (Art. 5 I lit. b DSGVO)
- Ausnahme: Vereinbarkeit statistischer Zwecke nach De-Personalisierung (vgl. 89 I DSGVO)
- Regelung weitgehend identisch mit Art. 6 I lit. b DS-RL
- Konkretisierung der Vereinbarkeit bisher durch Stellungnahme WP 203 ("Compatibility Assessment")
- Erwägungsgrund 50 übernimmt die von der WP 29 entwickelten Vereinbarkeitsprinzipien
- Ausdifferenzierung durch Datenschutzbehörden und Gerichte erfolgen. Keine mitgliedstaatliche Gesetzgebungskompetenz mehr
- Beispiele:

  Bei einem Verkauf erhobene Daten werden für weitere Bestellungen bzw. Lieferungen verarbeitet ☑

  Bei einem Verkauf erhobene Daten werden für Direktmarketing verwendet ☒

11. Datenminimierung.

- Die Verarbeitung von personenbezogenen Daten muss dem verfolgten Zweck, erheblich und auf das notwendige Mass beschränkt sein (Art. 5 I lit. c DSGVO) (DSG: Verhältnismässigkeit)

So viel wie nötig und so wenig wie möglich!

- Heiliger Gral des Datenschutzes. In vielen anderen Bestimmungen der DSGVO verkörpert
- Erfasst werden alle Verarbeitungsparameter über den gesamten Lebenszyklus von Daten!
- Konkret müssen im Rahmen der Verhältnismässigkeit z.B. begrenzt werden:
  - Art der erhobenen Daten: Bei Neuerhebungen muss jede Datenkategorie auf ihre Erforderlichkeit geprüft werden (nur Must-Haves)
  - Umfang der erhobenen Daten: Datenerhebung auf noch nicht bekannte, aber denkbare Verarbeitungszwecke ist nicht zulässig (keine Vorratsspeicherung). Beschränkung von Big Data-Anwendungen
  - Zahl der Personen mit Zugriff zu Daten: Zugriff muss entsprechend der Funktion gewährt werden (Need-to-know)
  - Speicherorte: beliebige Vervielfältigung von Daten in vielen Datenbanken ist unverhältnismässig

12. Speicherbegrenzung.

- Identifikation der gespeicherten Personen ist nur solange zulässig, wie dies zur Erfüllung des Zwecks erforderlich ist (Art. 5 I lit. b DSGVO)
- Ausfluss des Prinzips der Datenminimierung
- Ist der Zweck erreicht, so müssen die personenbezogenen Daten gelöscht werden.
- Ausnahme: Verarbeitung zu statistischen Zwecken nach erfolgter De-Personalisierung der Daten z.B. durch Pseudonymisierung (Art. 89 I DSGVO)
- Beispiel:

  Transaktionsdaten und Nutzungsdaten eines verlorenen Kunden können gespeichert und zu statistischen Zwecken verarbeitet werden, so lange der Kunde aufgrund dieser Daten nicht identifiziert werden kann

13. Privacy by Design.

- Privacy by Design (Datenschutz durch Technikgestaltung) bezeichnet die Pflicht des Verantwortlichen, bei der Festlegung der Verarbeitungsmittel wie auch der Verarbeitung selbst die erforderlichen Massnahmen zu ergreifen, um die Datenschutzgrundsätze umzusetzen zu können (Art. 25 I DSGVO)
- Regelungsgehalt ergibt sich aus den allgemeinen Grundsätzen, wurde bislang aber vor allem bei der Festlegung der Verarbeitungsmittel zu wenig beachtet
- Bei Evaluation bzw. Entwicklung von eigenen Produkten und Verfahren gehört der Datenschutz ins Pflichtenheft (Beispiel: Datenbank-Software lässt Löschung nicht zu)
- Besonderes Augenmerk ist auf Speicherbegrenzung, Datenminimierung, Zugriffsberechtigungen, Sicherheit, Löschmöglichkeit richten (Beispiel: Datenerhebung des Kühlschranks lässt sich abstellen)
- Möglichkeit einer Selbstadministration der Datenschutzeinstellungen durch betroffene Personen ist datenschutzfreundlich und effizient, sofern Informatiksysteme entsprechend konzipiert sind
- Bei grösseren Projekten ist Durchführung eines Privacy Impact Assessments (Datenschutzfolgen-Abschätzung) empfehlenswert, selbst wenn rechtlich nicht zwingend *(→ David Vasella, Modul 3)*

14. Privacy by Default.

- Privacy by Default (datenschutzfreundliche Voreinstellung) bezeichnet die Pflicht des Verantwortlichen, bei der Festlegung der Verarbeitungsmittel wie auch der Verarbeitung selbst die erforderlichen Massnahmen zu ergreifen, um die Datenschutzgrundsätze umzusetzen zu können (Art. 25 I DSGVO)
- Regelungsgehalt ebenfalls wenig griffig. Ergibt sich bereits aus dem Verhältnismässigkeitsprinzip (Datenminimierung / Datensparsamkeit)
- Beispiele:
  - Internet-Browser ist nach der Installation so eingestellt, dass Cookies nicht akzeptiert werden
  - Social Media Account ist standardmässig auf «nicht öffentlich» eingestellt

15. Take Aways.

1. Mit Bezug auf Datenkategorien und Bearbeitungsgrundsätze bringt die DSGVO keine wesentlichen Neuerungen. Neu sind die rechtlichen Risiken, welche die Strategie einer “wohlwollenden Gleichgültigkeit” nach sich ziehen kann
2. Die (weitgehende) Einhaltung der Bearbeitungsgrundsätze erfordert ausreichend genaue Kenntnisse und Kontrolle über die Verarbeitung von personenbezogenen Daten im Unternehmen über den gesamten Lebenszyklus von personenbezogenen Daten. Datenschutz-Compliance wird eine Daueraufgabe werden
3. Datenschutz-Governance und Sensibilisierung der Organisation werden unerlässlich
4. Pseudonymisierung von personenbezogenen Daten wird in der Praxis an Bedeutung gewinnen. Der damit einhergehende Aufwand erfordert aber die Bereitstellung der notwendigen Ressourcen

Besten Dank für Ihre Aufmerksamkeit!

Baker & McKenzie Zürich
Dr. iur. Nicolas Passadelis
Holbeinstrasse 30
8034 Zürich
Tel. +41 44 384 12 09
Nicolas.Passadelis@bakermckenzie.com
www.bakermckenzie.com