Datenschutzrisiken erkennen und bewerten

Benjamin Bremert,
Felix Bieker

ULD-Sommerakademie 2019

Risiko nach DSGVO: Rechte und Freiheiten

(75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

(75) Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer

(94) Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung bei Fehlen von Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung des Risikos ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen würde, und ist der Verantwortliche der Auffassung, dass das Risiko nicht durch in Bezug auf verfügbare Technologien und Implementierungskosten vertretbare Mittel eingedämmt werden kann, so sollte die Aufsichtsbehörde vor Beginn der Verarbeitungstätigkeiten konsultiert werden. Ein solches hohes Risiko ist wahrscheinlich mit bestimmten Arten der Verarbeitung und dem Umfang und der Häufigkeit der Verarbeitung verbunden, die für natürliche Personen auch eine Schädigung oder eine Beeinträchtigung der persönlichen Rechte und Freiheiten mit sich bringen können. Die Aufsichtsbehörde sollte das Beratungsersuchen innerhalb einer bestimmten Frist beantworten. Allerdings kann sie, auch wenn sie nicht innerhalb dieser Frist reagiert hat, entsprechend ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen eingreifen, was die Befugnis einschließt, Verarbeitungsvorgänge zu untersagen. Im Rahmen dieses Konsultationsprozesses kann das Ergebnis einer im Hinblick auf die betreffende Verarbeitung personenbezogener Daten durchgeführten Datenschutz-Folgenabschätzung der Aufsichtsbehörde unterbreitet werden; dies gilt insbesondere für die zur Eindämmung des Risikos für die Rechte und Freiheiten natürlicher Personen geplanten Maßnahmen.

Art. 8 GRCh: Grundrecht auf Datenschutz

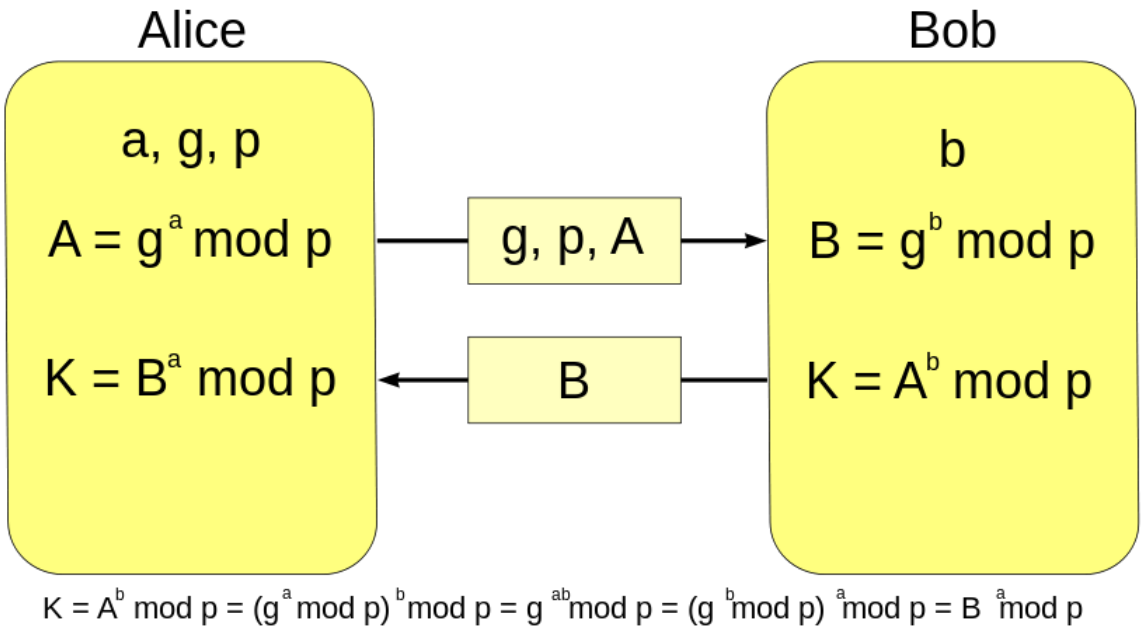
- Datenschutz ist auf Verfassungsebene verankert
- Nicht nur Privatsphäre
- Schützt alle personenbezogenen Daten
- Verarbeitung von Daten ist Eingriff (Beeinträchtigung)
  - Muss gerechtfertigt sein
  - Eingriff so mild wie möglich

Weitere relevante Rechte

- Artikel 7: Recht auf Schutz des Privatlebens (privacy)
- Artikel 11: Meinungsfreiheit
- Artikel 12: Versammlungsfreiheit
- Artikel 21: Nichtdiskriminierung
- Artikel 47: wirksamer Rechtsbehelf
- Und weitere, je nach Kontext

- Auch einfache Rechte umfasst, z.B. Betroffenenrechte

Datenschutz: weiter als IT-Sicherheit



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

IT-Sicherheit: Die Angreiferin ist Eve (oder Mallory).

Datenschutz: Der Angreifer ist Bob!
(Zumindest auch.)

Definition Risiko

- Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses,
  - das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder
  - zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.

Definition Risiko

Risiko im Sinne der DSGVO hat zwei Dimensionen:

1. die Schwere des möglichen Schadens und
2. die Wahrscheinlichkeit,

dass das Ereignis und Folgeschäden eintreten.

Anforderungen an das Team

a) Dokumentation und Verständnis der konkreten Datenverarbeitung
b) Dokumentation und Verständnis des Umfelds der konkreten Datenverarbeitung
c) Kenntnis möglicher Rechte und Freiheiten
d) Problembewusstsein hinsichtlich der Arten möglicher Eingriffe in Rechte und Freiheiten

- Anwendung der Punkte a) – d) auf die konkrete Datenverarbeitung

I. Risikoerkennung
- Welche Schäden können entstehen?
- Durch welche Ereignisse können Schäden entstehen?
- Durch welche Handlungen/Umstände können Ereignisse eintreten (Risikoquellen)?

II. Abschätzung von
- Eintrittswahrscheinlichkeit
- Schwere möglicher Schäden

III. Zuordnung zu Risikoabstufungen

Risikoerkennung

- **Welche Schäden können entstehen?**
  - Negative Folgen der Verarbeitung selbst (Schäden/Beeinträchtigungen)
  - Negative Folgen von Abweichungen der geplanten Verarbeitung (zB unbefugte Zugriffe, Offenlegung, Vernichtung, unbeabsichtigt/vorsätzlich unbefugt)
  - Beispiele aus ErwGr. 75 DSGVO:
    - Diskriminierung
    - Identitätsdiebstahl/Rufschädigung
    - Erschwerung der Rechtsausübung/Kontrolle
    - Profilerstellung
    - ...

- Welche Schäden können entstehen?
- **Durch welche Ereignisse können Schäden entstehen?**
  - Verletzung der DS-Grundsätze & Betroffenenrechte
    - Unbefugte oder unrechtmäßige Verarbeitung
    - Intransparente Verarbeitung
    - Verweigerung der Betroffenenrechte
    - Verwendung der Daten durch die Verantwortliche zu inkompatiblen Zwecken
    - ...

- Welche Schäden können entstehen?
- Durch welche Ereignisse können Schäden entstehen?
- **Durch welche Handlungen / Umstände können Ereignisse eintreten (Risikoquellen)?**
  - Verantwortliche/Auftragsverarbeiter
  - Unbefugte Angreifer („Cyber-“Kriminelle, der Staat)
  - Technische Fehlfunktionen/äußere Einflüsse

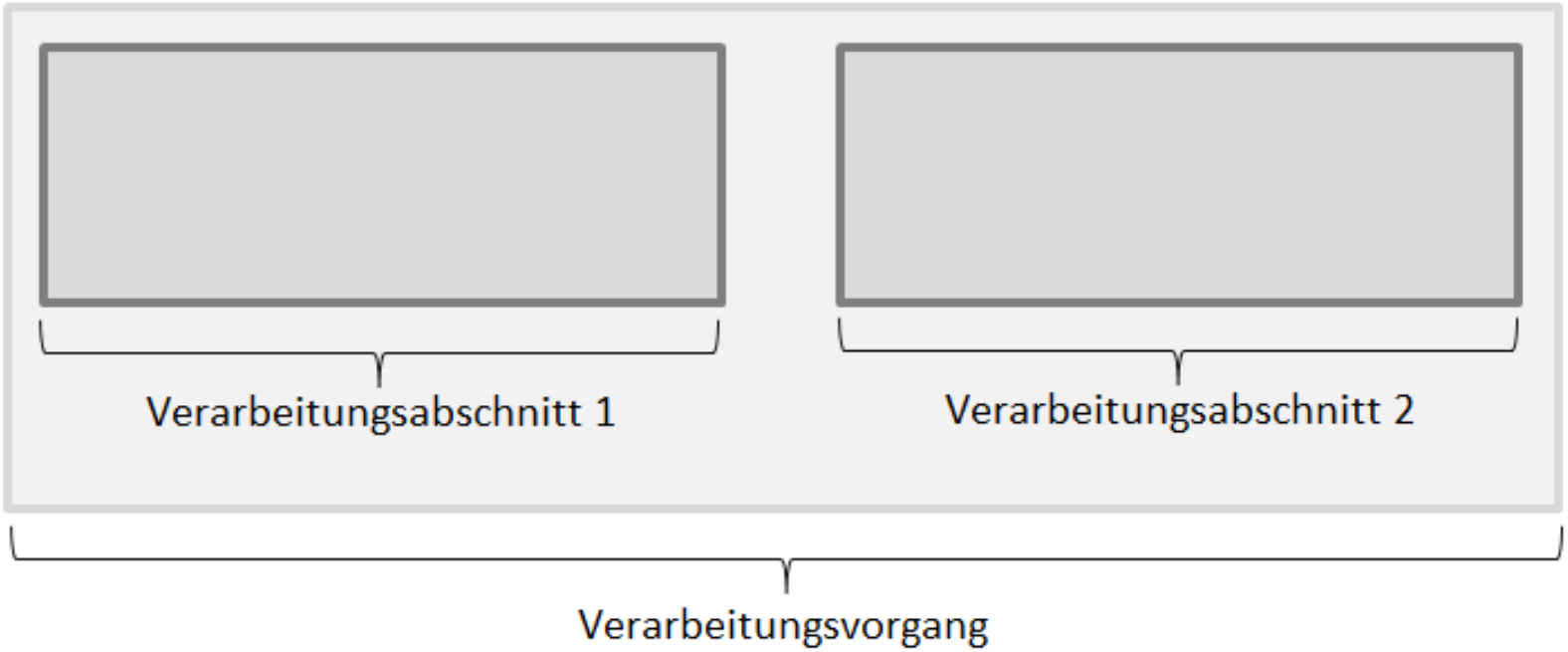
Unterteilung des Verarbeitungsvorgangs

Ein Verarbeitungsvorgang ist nach logischer und technischer Betrachtung in Abschnitte zu trennen.

Logische Trennbarkeit ist in der Regel dort anzunehmen, wo in der Gesamtverarbeitung eine räumliche, zeitliche oder funktionelle Zäsur vorzufinden ist.

Eine zeitliche Zäsur ist an der Länge der jeweiligen Unterbrechung im Verhältnis zur Länge der Gesamtdatenverarbeitung zu beurteilen.

Abschnitte des Verarbeitungsvorgangs

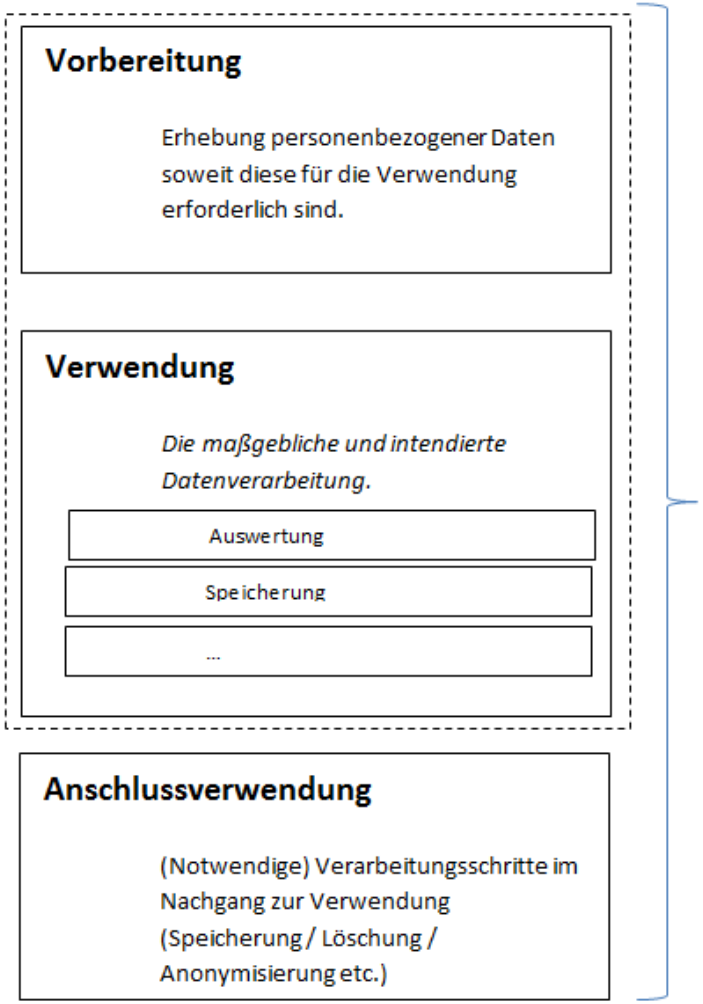


Phasen der Verarbeitungsabschnitte

- Zweck:
  - Zur Abbildung komplexer Verarbeitungsabschnitte
  - Sichtbarkeit vermeintlich unproblematischer
    - Neben- oder Hilfsverarbeitungsschritte
    - aus denen sich spezifische Risiken ergeben

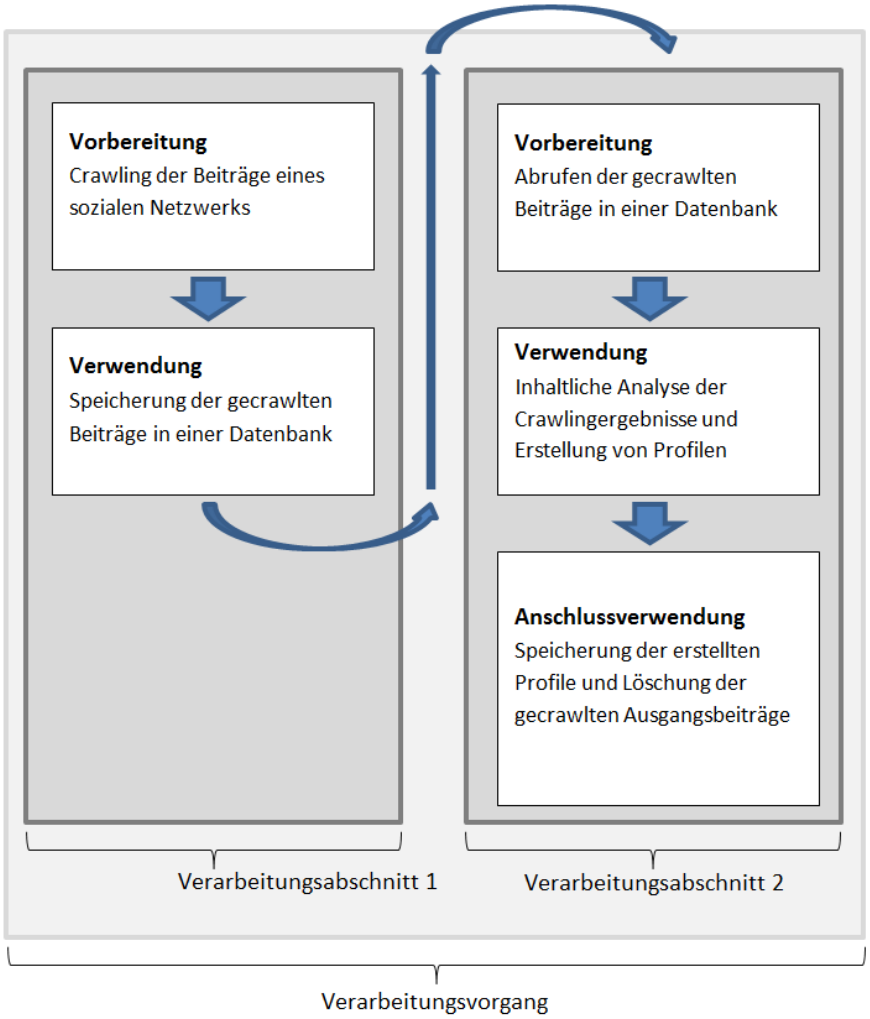
Phasen der Verarbeitungsabschnitte

Je nach intendierter Datenverarbeitung sind lediglich Vorbereitung und Verwendung. relevant, etwa wenn Daten gesammelt und gespeichert (aber nicht gelöscht) werden.

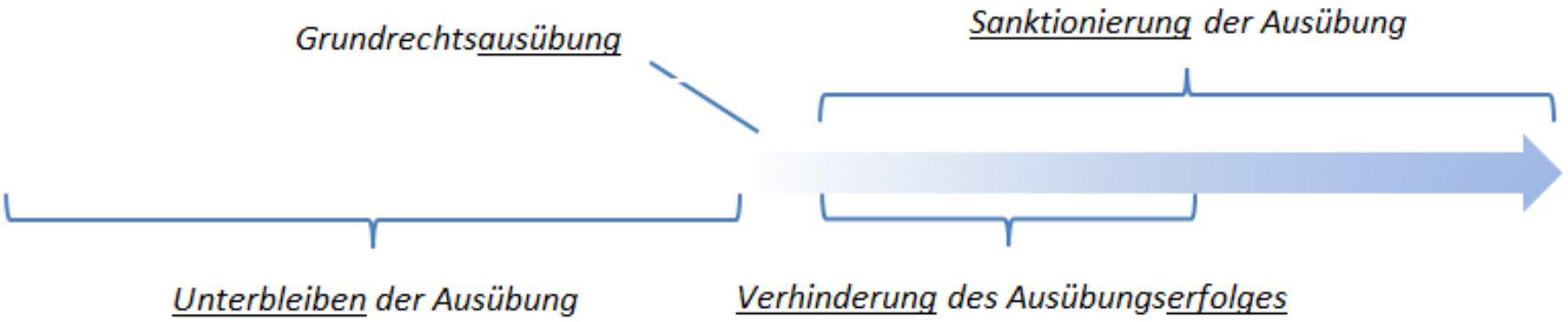


Verarbeitung i.S.v. Art. 4 Abs. 2 DSGVO

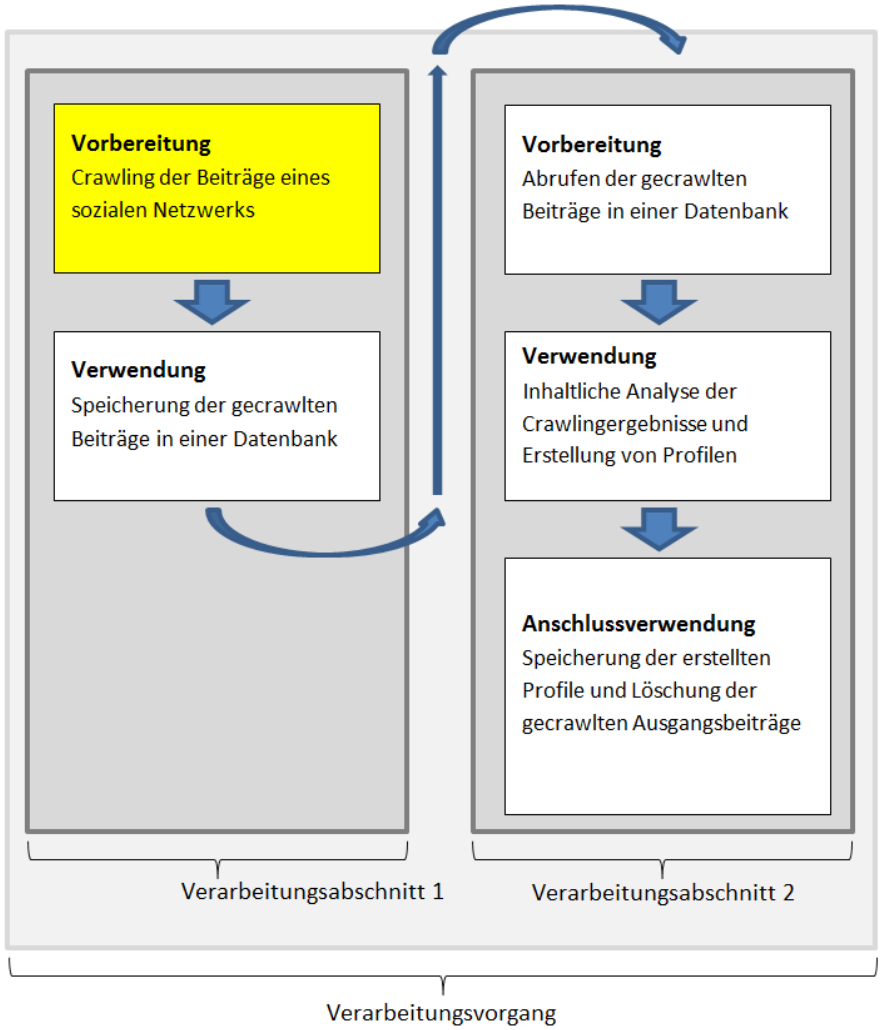
Gesamtverarbeitungsvorgang



Zeitlicher Ablauf der Beeinträchtigung

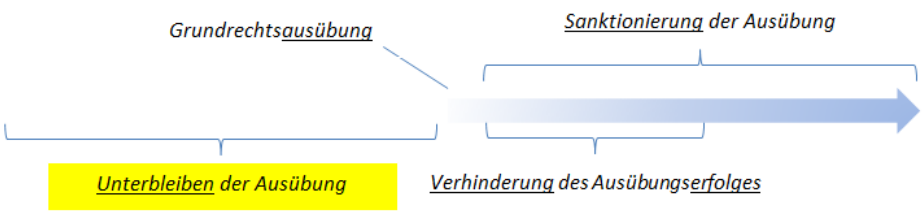


Erkennung Einzelrisiken (Art. 8 GrCh)

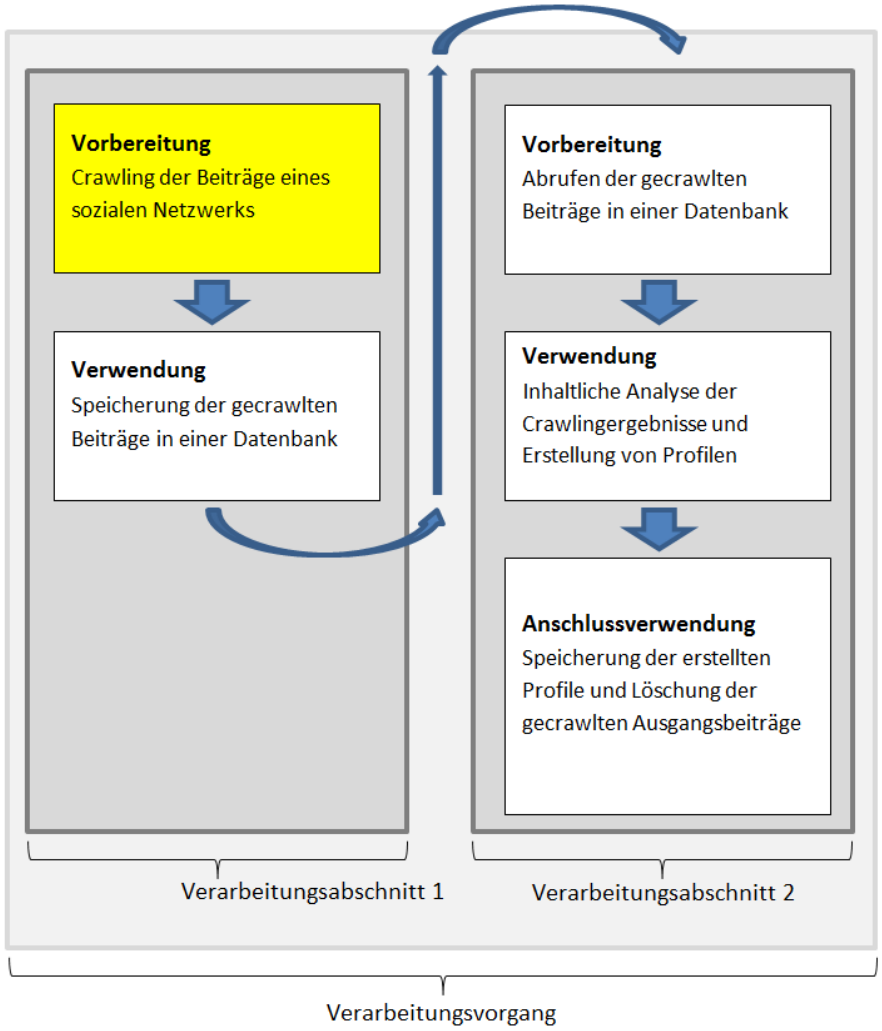


Intervenierbarkeit

- Fehlende Implementierung der Geltendmachung von Betroffenenrechten
- Fehlende Erfüllung der Transparenzpflichten ggü. der betroffenen Person (iVm Transparenz)

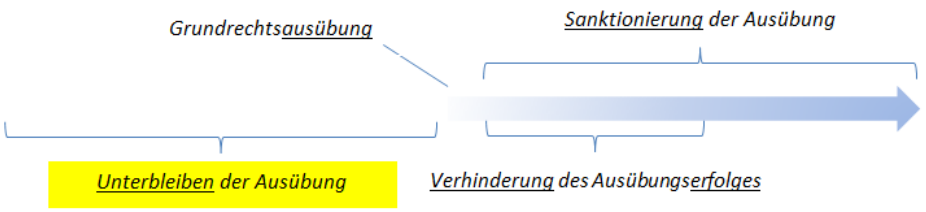


Erkennung Einzelrisiken (Art. 8 GrCh)

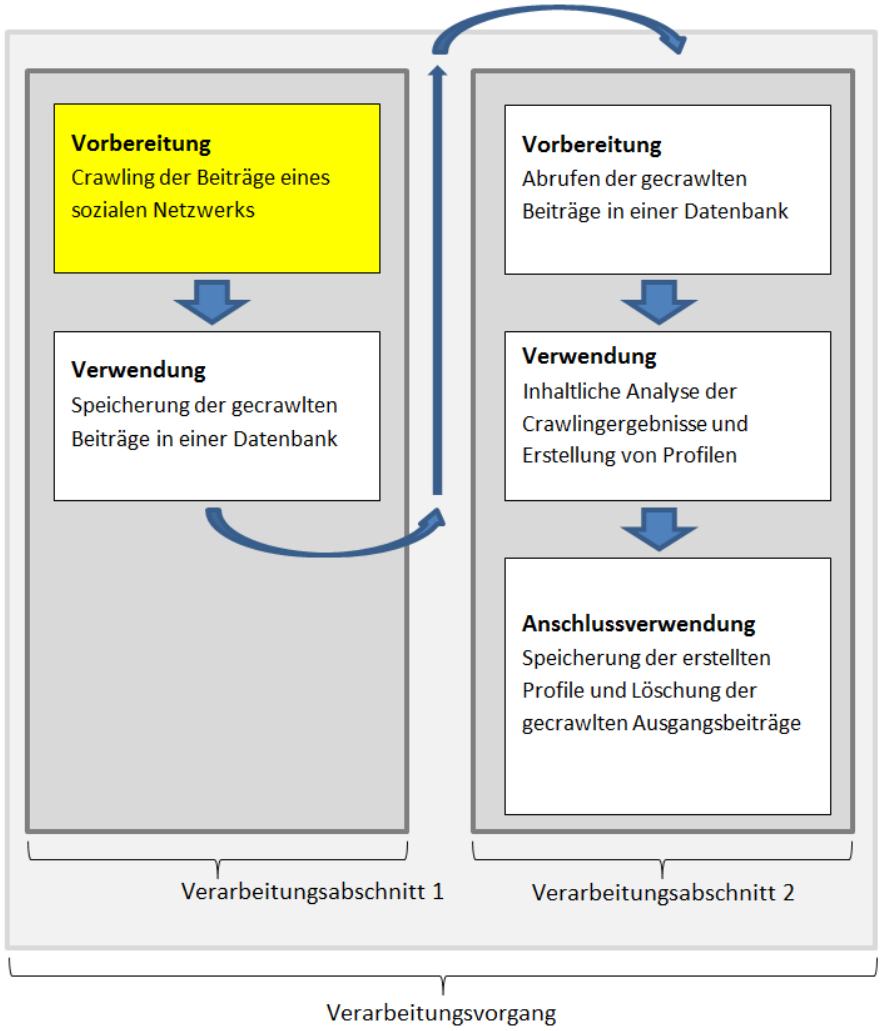


Datenminimierung

- Fehlende Beschränkung oder Eingrenzung der während des Crawlings erhobenen personenbezogenen Daten
- Fehlender Schutz der gecrawlten Daten gegen die Möglichkeit der Kenntnisnahme

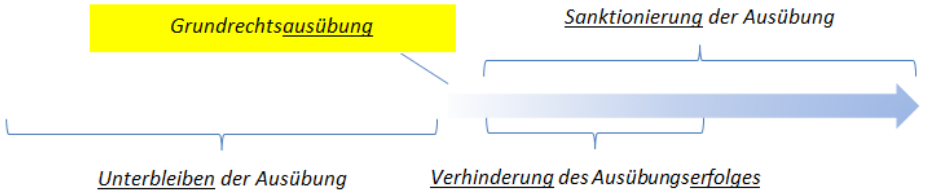


Erkennung Einzelrisiken (Art. 8 GrCh)



Intervenierbarkeit

- Fehlende Berücksichtigung berechtigter Widersprüche (-> fehlende Rechtsgrundlage des Verantwortlichen)



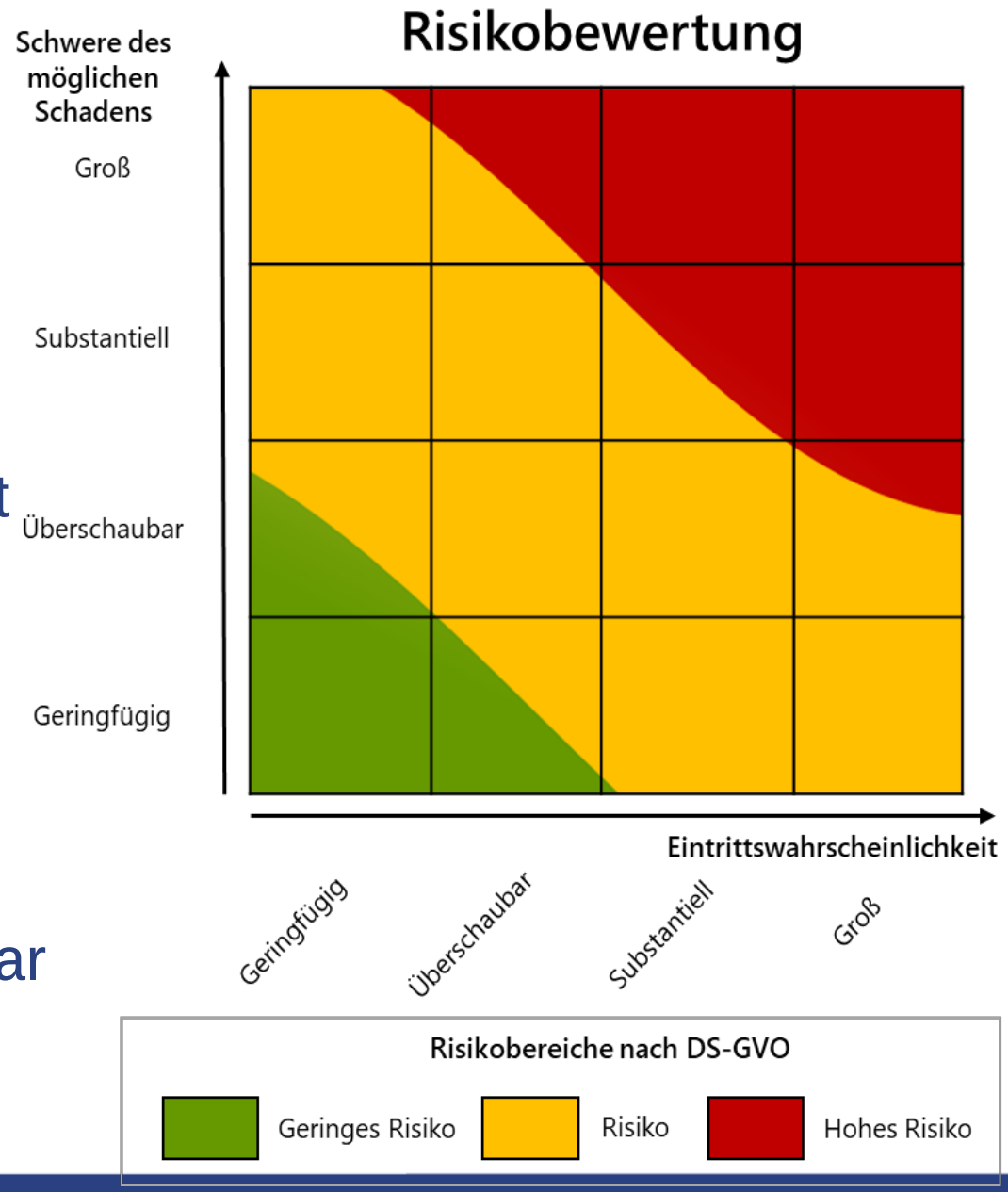
Risikoabschätzung

- Nicht quantifizierbar, aber objektive Begründung und Abstufungen
  - Eintrittswahrscheinlichkeit: beschreibt „mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt und mit welcher weiteren Wahrscheinlichkeit es zu Folgeschäden kommen kann.“

- Schwere möglicher Schäden
  - Wertungen des Gesetzgebers:
    - Schützenswerte Personen/Daten (Kinder, Beschäftigte, Artt. 9, 10 DSGVO)
    - Eindeutig identifizierende Daten, z.B. PKZ
    - Profiling
    - Reversibilität des Schadens und Interventionsmöglichkeiten
    - Systematische Überwachung
    - Anzahl der Personen, Datensätze, Merkmale in Datensatz oder geographische Abdeckung

Risiko -abstufungen

- Kategorisierung als Vorschlag
- Kurven sind Feature: verdeutlicht Grenzfället
  - Verantwortung für Entscheidung bei Verantwortlicher
  - Muss sachlich begründet/ dokumentiert/prüfbar sein



Anwendungsfälle

Erkennung und Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen

- Art. 24 Abs. 1 DSGVO (Verantwortlichkeit)
- Art. 25 Abs. 1 DSGVO (Datenschutz by Design & Default)
- Art. 32 Abs. 1 DSGVO (Sicherheit der Verarbeitung)
- Art. 33 Abs. 1 DSGVO (Meldung von Datenpannen)
- Art. 34 Abs. 1 DSGVO (Benachrichtigung nach Datenpannen)
- Art. 35 Abs. 1 DSGVO (Datenschutz-Folgenabschätzung)

Vielen Dank für Ihre Aufmerksamkeit!