

BETROFFENENRECHTE & RISIKO & WIEDERHOLUNG

Benjamin Bremert <benjamin@bremert.de>

Christian-Albrechts-Universität zu Kiel

6. Juli 2026

Rechtsauffassungen sind solche der jeweiligen Referent:innen.

AUFBAU

- Wiederholungsfälle
- Risiko
- Datenpannen
- Betroffenenrechte
 - Grundsätze
 - Informationspflichten der Verantwortlichen, Artt. 13, 14 DSGVO
 - Einzelne Betroffenenrechte

KLAUSURFALL

In welchen Fällen gilt die DSGVO auch für die nichtautomatisierte Verarbeitung personenbezogener Daten?

KLAUSURFALL

Fällt jede private Veröffentlichung mit personenbezogenen Daten im Internet unter die Haushaltsausnahme, sodass die DSGVO keine Anwendung mehr findet?

KLAUSURFALL

Die S Ltd. mit Sitz in Lima, Peru betreibt einen Dienst zur zielgerichteteren Ausspielung von Online-Werbung. Hierfür werden Profile über das Surfverhalten von NutzerInnen (auch innerhalb der EU) angelegt. Ist die DSGVO auf die von der S Ltd. verantwortete Datenverarbeitung anwendbar und wieso?

KLAUSURFALL

- Wie lauten die Kriterien zur Bestimmung des Verantwortlichen, über welche Aspekte der Datenverarbeitung muss ein Verantwortlicher entscheiden? Nennen Sie jeweils ein konkretes Beispiel für jedes Kriterium.
- Müssen im Falle der gemeinsamen Verantwortlichkeit alle Verantwortlichen gleichermaßen über die Kriterien entscheiden oder darf es hier Unterschiede zwischen dem Maß an Mitbestimmung der Verantwortlichen geben?

KLAUSURFALL

Beschreibung Sie die Stellung der Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DSGVO im Gefüge der Rechtsgrundlagen.

Wie ist der Aufbau der Prüfung eines berechtigten Interesses?

KLAUSURFALL

Nennen Sie ein konkretes Beispiel für ein sicher nicht berechtigtes Interesse im Rahmen der Rechtsgrundlage des berechtigten Interesses (Art. 6 Abs. 1 lit. f DSGVO), also einen Fall in dem es nicht mehr auf die Interessenabwägung ankommt.

KLAUSURFALL

Der R. e.V. ist ein Sportverein mit einer Tennissparte. Er ist Mitglied im Tennis-Landesverband S.-H.T. e.V.. Die Mitglieder des R. e.V. sind nur Mitglieder im R. e.V., nicht aber im S.-H.T. e.V. Für die Punktspiele der durch den S.-H.T. e.V. betriebenen Tennisligen müssen die jeweiligen Begegnungen durch den R. e.V. an den S.-H.T. e.V. gemeldet werden. Nach dem jeweiligen Spiel muss das Ergebnis über eine Online-Plattform eingetragen werden. Die Ergebnisse, Begegnungen und Kurzprofile (Leistungsklasse, Ergebnisse etc. auf Personenebene) sind im Internet frei abrufbar.

Welche Datenverarbeitungen werden hier durch wen vorgenommen und auf welcher Rechtsgrundlage könnte das geschehen?

KLAUSURFALL

Die A GmbH pflegt eine Kundenkartei mit den Daten anderer Unternehmen. Für jedes Unternehmen sollen dabei auch die Kontaktdaten der zuständigen MitarbeiterInnen im Unternehmen erfasst und hinterlegt (und damit verarbeitet) werden. Kann sich die A GmbH dabei als Rechtsgrundlage auf den Vertrag mit dem Kunden (Unternehmen) berufen?

KLAUSURFALL

Was soll das Merkmal der Erforderlichkeit innerhalb der Rechtsgrundlagen sicherstellen? Welcher Grundsatz der DSGVO enthält das Merkmal der Erforderlichkeit und wo ist er geregelt?

KLAUSURFALL

Die S möchte eine der R GmbH erteilte Einwilligung in die Verarbeitung personenbezogener Daten widerrufen. Welche Wirkung hat der Widerruf, berührt er auch die Rechtmäßigkeit der bereits erfolgten Datenverarbeitung?

RISIKO & DATENPANNEN

DEFINITION RISIKO I

- 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 II

- Risiko im Sinne der DSGVO hat zwei Dimensionen:
 1. die **Schwere des Schadens** und
 2. die **Wahrscheinlichkeit**,
dass das Ereignis und die Folgeschäden eintreten.

BEEINTRÄCHTIGUNG

- Grundrechtseingriff ist Beeinträchtigung
- Beeinträchtigung ist nach ErwGr. 75 Schaden, wenn sie nicht gerechtfertigt ist
 - Explizit von Begriff Schadensereignis erfasst

Bsp.: Falsche Einstufung der Kreditwürdigkeit, „chilling effects“ etc.

SCHADEN

- Ergibt sich aus
 - der geplanten Verarbeitung selbst,
 - eigenverantworteten und
 - fremdverursachten Abweichungen (security + safety)

RISIKOBEURTEILUNG

- Identifikation der Risiken
 - Welche Schäden können entstehen?
 - Durch welche Ereignisse können Schäden entstehen?
 - Durch welche Handlungen und Umstände können Ereignisse eintreten (Risikoquellen)?
- Abschätzung von ...
 - Eintrittswahrscheinlichkeit
 - Schwere möglicher Schäden

RISIKOIDENTIFIKATION

- Negative Folgen der Verarbeitung
- Negative Folgen von Abweichungen der geplanten Verarbeitung (z.B. unbefugte Zugriffe, Offenlegung, Vernichtung etc.)

Beispiele:

- Diskriminierung
- Identitätsdiebstahl/Rufschädigung
- Erschwerung der Rechtsausübung/Kontrolle

RISIKOIDENTIFIKATION II

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

RISIKOIDENTIFIKATION III

- Was sind mögliche Risikoquellen?
 - Verantwortliche und Auftragsverarbeiter
 - Unbefugte Angreifer („Cyber-“Kriminelle, der Staat)
 - Technische Fehlfunktion / äußere Einflüsse

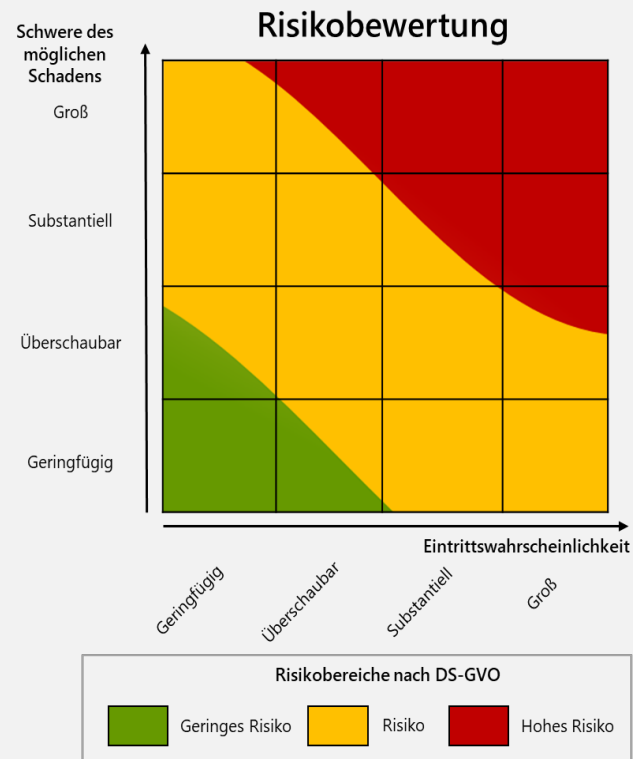
RISIKOBEURTEILUNG I

- Abschätzung ist nicht quantifizierbar, bedarf aber einer objektiven Begründung und Abstufungen
- Eintrittswahrscheinlichkeit: beschreibt „mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt und mit welcher Wahrscheinlichkeit es zu Folgeschäden kommen kann“.

RISIKOBEURTEILUNG II

- Schwere möglicher Schäden
 - Wertung des Gesetzgebers
 - Besonders schützenswerte Personen und Daten (Kinder, Beschäftigte, Daten nach Artt. 9, 10 DSGVO)
 - Eindeutig identifizierbare Daten (z.B. Personenkennziffer)
 - Profiling
 - Reversibilität des Schadens und Interventionsmöglichkeiten
 - Systematische Überwachung
 - Anzahl der Personen, Datensätze, Merkmale in Datensatz oder geographische Abdeckung

RISIKOBEURTEILUNG III



Aus: Kurzpapier Nr. 18, DSK

EINDÄMMUNG DES RISIKOS

- Abhilfemaßnahmen der Verantwortlichen, die ein angemessenes Schutzniveau herstellen + IT-Sicherheit aus Betroffenen Sicht
- Restrisiko:
 - Nach Umsetzung der Abhilfemaßnahmen verbleibendes Risiko
 - Verantwortlichen obliegt die Beurteilung, sie müssen dokumentieren, testen und überwachen.

ZUSAMMENFASSEND

- Die Risikobestimmung dient nicht den Organisationen, sondern den Individuen
- Das Risiko muss durchgängig analysiert werden
- Risiken müssen
 - Identifiziert und
 - Beurteilt werden, damit
 - **angemessenes Schutzniveau** für betroffene Personen erreicht wird.

DATA BREACHES

- Ein „Data Breach“ ist ein Vorfall, der die Verletzung des Schutzes personenbezogener Daten zur Folge hat.
- Verursacht in der Regel durch die Verletzung der Sicherheit.
- Der Vorfall führt z.B. zur Vernichtung, Verlust, Veränderung, Offenlegung oder Zugang von/zu personenbezogenen Daten.
- Verletzung der klassischen Schutzziele der IT-Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit).

DATA BREACHES

In der Regel ist jede Verletzung des Schutzes personenbezogener Daten auch gleichzeitig eine IT-Sicherheitsvorfall, umgekehrt resultiert aber nicht jeder IT-Sicherheitsvorfall in einem Datenschutzvorfall.

DATA BREACHES

- **Auslöser:**
 - Unfall oder höhere Gewalt
 - Vorsatz
 - Fahrlässigkeit
- **Folgen:**
 - Kontrollverlust
 - Einschränkung von Rechten
 - Diskriminierung
 - Identitätsdiebstahl oder –betrug
 - Aufhebung von Pseudonymisierung
 - ...

MELDUNG EINES VORFALLS (AN DIE AUFSICHTSBEHÖRDE)

Artikel 33

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

- (1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.
- (2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.
- (3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:
 - a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- (4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.
- (5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

MELDUNG EINES VORFALLES (AN DIE AUFSICHTSBEHÖRDE)

Wann wird gemeldet?

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

MELDUNG EINES VORFALLES (AN DIE AUFSICHTSBEHÖRDE)

Wer meldet wem?

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten **meldet der Verantwortliche** unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem **Auftragsverarbeiter** eine Verletzung des Schutzes personenbezogener Daten bekannt wird, **meldet er diese dem Verantwortlichen** unverzüglich.

MELDUNG EINES VORFALLES (AN DIE AUFSICHTSBEHÖRDE)

Wann?

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

KLAUSURFALL

Ein Verantwortlicher stellt am Freitag um 14 Uhr eine meldepflichtige Datenpanne fest, bis wann müsste er diesen Vorfall (im Regelfall) spätestens der Aufsicht melden?

MELDUNG EINES VORFALLES (AN DIE AUFSICHTSBEHÖRDE)

Was wird gemeldet?

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

BENACHRICHTIGUNG (DER BETROFFENEN PERSONEN)

Artikel 34

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

BENACHRICHTIGUNG (DER BETROFFENEN PERSONEN)

Wann wird benachrichtigt?

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

BENACHRICHTIGUNG (DER BETROFFENEN PERSONEN)

Wer benachrichtigt wann?

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so **benachrichtigt der Verantwortliche** die betroffene Person **unverzüglich** von der Verletzung.

BENACHRICHTIGUNG (DER BETROFFENEN PERSONEN)

Was enthält die Benachrichtigung?

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

BENACHRICHTIGUNG (DER BETROFFENEN PERSONEN)

Was enthält die Benachrichtigung?

- (3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:
- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 - b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 - c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 - d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

BENACHRICHTIGUNG (DER BETROFFENEN PERSONEN)

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

- a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
- b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;
- c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

RISIKO EINES DATENSCHUTZVORFALLES

- Hohes und sehr hohes Risiko
 - z.B. ernste Folgen (Gefahr Leib, Leben Gesundheit; Stellenwert des Dienstes für die betroffenen Personen, sensible Daten (nicht *nur* besondere Kategorien personenbezogener Daten)), keine Interventionsmöglichkeiten oder Sicherungsmaßnahmen möglich
- Meldung an Aufsichtsbehörde
- Benachrichtigung der betroffenen Person(en)

RISIKO EINES DATENSCHUTZVORFALLES

- Risiko
 - Schaden absehbar
 - Schadensbegrenzung möglich
- Meldung an Aufsichtsbehörde

RISIKO EINES DATENSCHUTZVORFALLES

- Kein Risiko
 - Schäden verhindert
 - Risiko wurde beseitigt

BETROFFENENRECHTE

GRUNDSÄTZE I

- Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist, Art. 11 DSGVO
 - Ist eine Identifizierung für die Zwecke der Verarbeitung nicht erforderlich, so muss der Verantwortliche zur bloßen Einhaltung der DSGVO keine zusätzlichen Informationen verarbeiten, um die betroffene Person zu identifizieren, Art. 11 Abs. 1 DSGVO.
 - Im Falle der Ausübung von Betroffenenrechten, informiert der Verantwortliche die betroffene Person darüber, wenn er nicht in der Lage ist, sie zu identifizieren, Art. 11 Abs. 2 Satz 1 DSGVO. Die betroffene Person kann dann zusätzliche Informationen bereitstellen, die eine Identifizierung ermöglichen, Art. 11 Abs. 2 Satz 2 DSGVO.

GRUNDSÄTZE II

- Transparenzregelungen
 - Der Verantwortliche muss alle Informationen nach Artt. 13 und 14 DSGVO sowie alle Mitteilungen nach Artt. 15 – 22 sowie 34 DSGVO in
 - **präziser,**
 - **transparenter,**
 - **verständlicher** und
 - **leicht zugänglicher Form**
 - **in klarer und einfacher Sprache**übermitteln (Genauigkeits- und Verständlichkeitsgebot).

GRUNDSÄTZE III

- Form der Informationserteilung
 - Proaktive Informationspflichten: Entscheidung liegt grundsätzlich bei den Verantwortlichen, danach ist sowohl eine schriftliche als auch elektronische Informationserteilung zulässig (Umkehrschluss Art. 12 Abs. 1 Satz 3 DSGVO).
 - „Reaktive“ Informationspflichten: Liegen teilweise zur Disposition der betroffenen Person. Wird der Antrag elektronisch gestellt, so muss der Verantwortliche grundsätzlich in derselben Form antworten (Art. 12 Abs. 3 Satz 4 DSGVO). Die betroffene Person kann – sofern ihre Identität nachgewiesen ist – auch eine mündliche Information verlangen (Art. 12 Abs. 1 Satz 3 DSGVO).

GRUNDSÄTZE IV

- Frist für die Betroffenenrechte
 - Entsprechende Anträge nach Artt. 15 bis 22 DSGVO sind **unverzüglich** zu bearbeiten, **in jedem Fall innerhalb eines Monats** (Art. 12 Abs. 3 Satz 1 DSGVO). Diese Frist **kann auf zwei Monate verlängert** wenn, wenn die Komplexität des Falles oder die Anzahl von Anträgen dies erfordert (Art. 12 Abs. 3 Satz 2 DSGVO). Über die Fristverlängerung ist die betroffene Person innerhalb des Monats mit den Gründen für die Fristverlängerung zu informieren (Art. 12 Abs. 3 Satz 3 DSGVO).

GRUNDSÄTZE V

- Die Informationen sind grundsätzlich kostenlos zu erteilen, Art. 12 Abs. 5 Satz 1 DSGVO.
- Bei offenkundig unbegründeten oder exzessiven Anträgen (insb. häufige Wiederholung), kann entweder a) ein angemessenes Entgelt verlangt werden oder b) der Antrag verweigert werden.
 - Grundsätzlich sind die Ausnahmen der Betroffenenrechte eng zu sehen. Ein exzessiver Antrag liegt vor, wenn ein Antrag rechtsmissbräuchlich gestellt wird, etwa bei häufiger Wiederholung der Anträge oder mit Schädigungsabsicht.
 - Eine Wiederholung kann aber auch berechtigt sein, insbesondere wenn zwischen den Anfragen Änderungen im Datenbestand eintreten.

GRUNDSÄTZE VI

- Das Vorliegen eines Ausnahmefalles hat der Verantwortliche zu nachzuweisen.
- Vor der Weigerung (schwerere Folge) sollte der Verantwortliche ein angemessenes Entgelt für Auskunftserteilung (mildere Folge) fordern. Eine unmittelbare Weigerung könnte sich sonst als ermessensfehlerhaft herausstellen und wäre dann auch bußgeldbewehrt. Dabei ist der jeweilige Verwaltungsaufwand für die Erteilung der Auskunft bzw. Durchführung der Maßnahme zu berücksichtigen.
- In jedem Fall ist eine Negativauskunft (z.B. keine Daten vorhanden) zu erteilen.

INFORMATIONSPFLICHTEN DER VERANTWORTLICHEN

- Bei Artt. 13 und 14 DSGVO handelt es sich um proaktive Informationspflichten der Verantwortlichen.
- Man differenziert nach der Art der Datenerhebung:
 - Datenerhebung bei der betroffenen Person (sie selbst als unmittelbare Datenquelle, sog. „Direkterhebung“)
 - Informationserteilung nach Art. 13 DSGVO
 - oder:
Datenerhebung nicht bei der betroffenen Person (etwa öffentlich zugängliche Daten oder Dritte)
 - Informationserteilung nach Art. 14 DSGVO

ZU ERTEILENDE INFORMATIONEN I

Art. 13 DSGVO

Name und Kontaktdaten der Verantwortlichen sowie ggfs. der Vertreter

Kontaktdaten der Datenschutzbeauftragten

Zwecke, zu denen die pbD verarbeitet werden sollen + Rechtsgrundlagen

Wenn Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO beruht: Die berechtigten Interessen, die von den Verantwortlichen oder Dritten verfolgt werden.

Kategorien pbD, die verarbeitet werden

Empfänger oder Kategorien von Empfängern der pbD

Ggfs. die Absicht der Verantwortlichen, die pbD an ein Drittland oder eine internationale Org. zu übermitteln, das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses sowie ein Verweis auf geeignete oder angemessene Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist oder wo sie verfügbar sind.

ZU ERTEILENDE INFORMATIONEN II

Art. 13 DSGVO

Art. 14 DSGVO

Dauer der Speicherung der pbD oder die Kriterien für die Festlegung der Dauer

Bestehen der Betroffenenrechte

Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde

Wenn Verarbeitung auf Art. 6 Abs. 1 lit. a DSGVO beruht: Bestehen des Widerrufsrechtes

Ob die Bereitstellung der pbD gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und welche möglichen Folgen eine Nichtbereitstellung hätte

Ggfs. Bestehen einer automatisierten Entscheidungsfindung und dann aussagekräftige Informationen über die involvierte Logik sowie Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betr. Person

ZU ERTEILENDE INFORMATIONEN III

Art. 13 DSGVO

Andere Verarbeitungszwecke, die von den Zwecken zum Zeitpunkt der Erhebung abweichen

Art. 14 DSGVO

Quellen der pbD

EMPFÄNGER

- Sind nach Art. 4 Nr. 9 DSGVO:
„Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.
- Solche Empfänger, die im Zeitpunkt der Erhebung schon absehbar sind.
- Entweder (konkrete) Empfänger oder Kategorien von Empfängern, wobei wohl kein Wahlrecht des Verantwortlichen besteht (strittig!). Somit müssen konkrete Informationen erteilt werden, wenn diese bekannt sind.

ZEITPUNKT DER INFORMATIONSERTEILUNG

- Art. 13 DSGVO: Zum Zeitpunkt der Erhebung.
- Art. 14 DSGVO (Abs. 3):
 - Unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Erlangung der pbD, längstens jedoch innerhalb eines Monats.
 - Falls die pbD zur Kommunikation verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung.
 - Falls die pbD an andere Empfänger offengelegt werden sollen, spätestens zum Zeitpunkt der ersten Offenlegung.

AUSNAHMEN DER INFORMATIONSERTEILUNG I

- Art. 13 Abs. 4 DSGVO:
 - Keine Anwendbarkeit der Abs. 1, 2 und 3, wenn die betroffene Person bereits über die Informationen verfügt.
- Art. 14 Abs. 5 DSGVO:
 - Keine Anwendbarkeit der Abs. 1 - 4, wenn die betroffene Person bereits über die Informationen verfügt.
 - Wenn die Erteilung dieser Informationen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde (Art. 14 Abs. 5 lit. b DSGVO), dies gilt insbesondere für
 - die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke,

AUSNAHMEN DER INFORMATIONSERTEILUNG II

- wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (vorbehaltlich der in Art. 89 Abs. I DSGVO genannten Bedingungen und Garantien),
- Fälle, in denen die Pflicht zur Informationserteilung die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt (temporäre Ausnahme).

=> In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person, **einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit.**

- Die Erlangung oder Offenlegung durch Rechtsvorschrift der Union oder der Mitgliedsstaaten ausdrücklich geregelt ist.
- Die Personenbezogenen Daten gemäß dem Unionsrecht oder dem mitgliedsstaatlichen Recht dem Berufsgeheimnis unterliegen und daher vertraulich behandelt werden müssen.

AUSKUNFT I

ART. 15 DSGVO

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

- a) die Verarbeitungszwecke;
- b) die Kategorien personenbezogener Daten, die verarbeitet werden;
- c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Der erste Teil des Auskunftsanspruchs aus Art. 15 DSGVO entspricht weitestgehend den (proaktiven) Informationspflichten der DSGVO.

AUSKUNFT II

ART. 15 DSGVO

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

In Abs. 3 findet sich das sog. „Recht auf Datenkopie“:

- Umfasst die vollständigen auf die betroffene Person bezogenen Daten, wie sie beim Verantwortlichen im Zeitpunkt der Auskunftserteilung vorliegen.
- Keine Grenze für das Recht auf Datenkopie sind Begehren, die einem datenschutzfremden Zweck dienen, etwa der Informationsbeschaffung für einen Zivilprozess (so teilweise deutsche Gerichte unter Verweis auf Rechtsmissbrauch, § 242 BGB). Die betroffene Person muss das Begehren nicht begründen.
- Beschränkt durch Abs. 4 (Rechte und Freiheiten Dritter).