

Die Identifizierung von Risiken für die Rechte und Freiheiten natürlicher Personen

Felix Bieker

Sommerakademie
10. September 2018



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Macht-
asymmetrie



Datenschutz
notwendig

Wichtig:

Perpektive des
Individuums



Bild: nextvoyage via Pixabay

I. Rechte und Freiheiten natürlicher Personen

Artikel 1

Gegenstand und Ziele

- (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- (3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

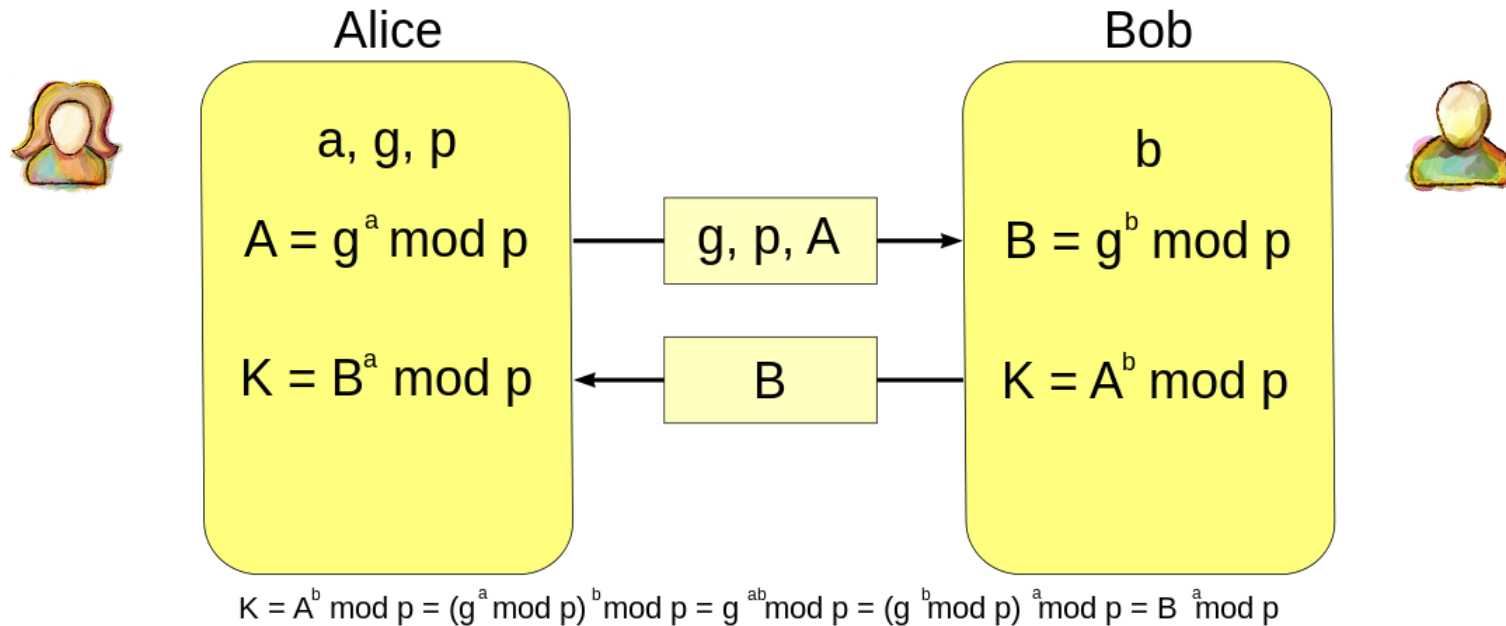
Art. 8 GRCh: Grundrecht auf Datenschutz

- 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



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

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

II. Risiko für 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 Sicherungsmaßnahmen 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.
- (76) Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

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 Schadens** und
 2. die **Wahrscheinlichkeit**,
dass das Ereignis und die Folgeschäden eintreten.

Risiko nach DSGVO

- (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 **Sicherungsmaßnahmen 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 Beratungersuchen 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.

Beeinträchtigungen

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

Bsp.: Eintrag in Hausverbotsdatei, falsche Einstufung der Kreditwürdigkeit, „chilling effects“

Schaden

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

III. Risikobeurteilung

1. Risikoidentifikation

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

2. Abschätzung von

- Eintrittswahrscheinlichkeit
- Schwere möglicher Schäden

3. Zuordnung zu Risikoabstufungen

III. Risikobeurteilung

1. Risikoidentifikation

- **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:
 - Diskriminierung
 - Identitätsdiebstahl/Rufschädigung
 - Erschwerung der Rechtsausübung/Kontrolle
 - Profilerstellung
 - ...

III. Risikobeurteilung

1. Risikoidentifikation

- 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
 - ...

III. Risikobeurteilung

1. Risikoidentifikation

- 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

III. Risikobeurteilung

2. Abschätzung

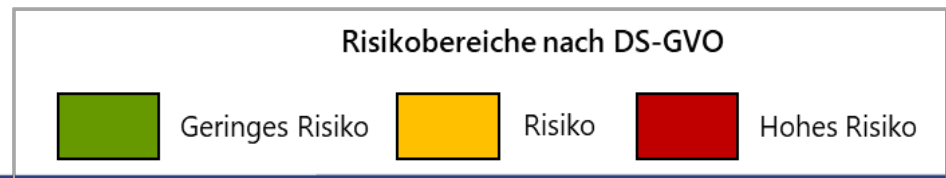
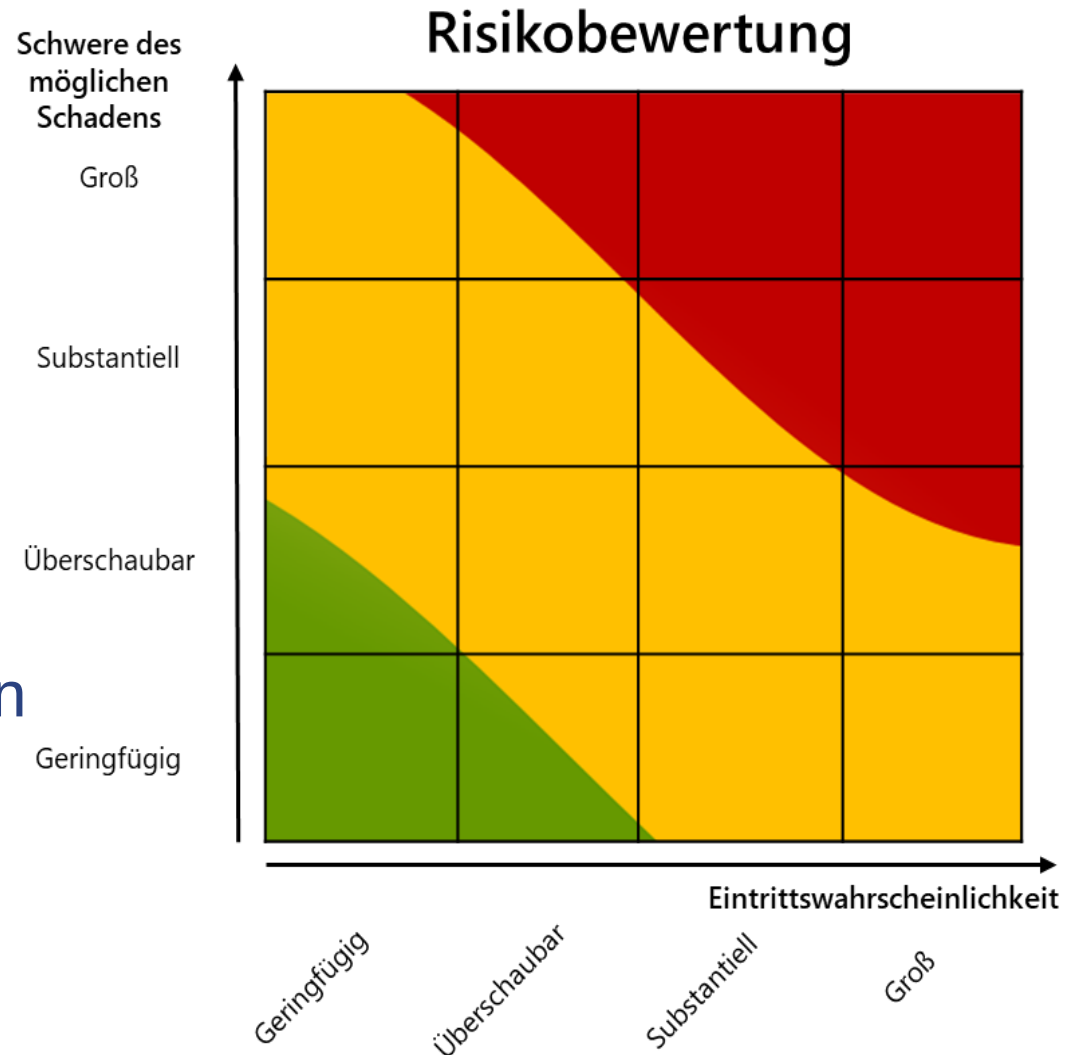
- Nicht quantifizierbar, aber objektive Begründung und Abstufungen
 - Eintrittswahrscheinlichkeit: beschreibt „mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt und mit welcher weiteren Wahrscheinlichkeit es zu Folgeschäden kommen kann.“

III. Risikobeurteilung

- 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

3. Zuordnung zu Risikoabstufungen

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



V. Eindämmung des Risikos/ Restrisiko

- Abhilfemaßnahmen der Verantwortlichen, die angemessenes Schutzniveau herstellen + IT-Sicherheit aus Betroffenenensicht
- Restrisiko
 - Nach Umsetzung der Abhilfemaßnahmen verbleibend
 - Verantwortliche muss beurteilen, dokumentieren, testen, überwachen

VI. Anwendungsfälle

Artikel 35

Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

VI. Anwendungsfälle

Artikel 35

Datenschutz-Folgenabschätzung

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen **Risiken für die Rechte und Freiheiten natürlicher Personen** trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

VI. Anwendungsfälle

Artikel 35

Datenschutz-Folgenabschätzung

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der **Risiken für die Rechte und Freiheiten natürlicher Personen** geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

VI. Anwendungsfälle

Artikel 35

Datenschutz-Folgenabschätzung

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

Artikel 32

Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des **Risikos für die Rechte und Freiheiten natürlicher Personen** treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

VI. Anwendungsfälle

Artikel 35

Datenschutz-Folgenabschätzung

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

Artikel 32

Sicherheit der Verarbeitung

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.

VII. Fazit

- **Risiko** nicht für Organisationen, sondern **für Individuen**
- Muss durchgängig analysiert werden
- Risiken müssen
 - identifiziert und
 - beurteilt werden, damit ein
 - **angemessenes Schutzniveau** für Betroffene erreicht wird

→ **Datenschutz-Management-System** nach SDM



Referenzen

- Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen (2018)
<https://www.datenschutzzentrum.de/artikel/1225-.html>
- Bieker/Hansen/Bremert: Die Risikobeurteilung nach der DSGVO, DuD 8/2018, S. 492
- Bieker: Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, DuD 1/2018, S. 27
- Forum Privatheit: White Paper Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz (3. Auflage 2017)
[https://www.forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums.php](https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums.php)
- Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Das Standard-Datenschutzmodell, V.1.1 – Erprobungsfassung (2017)
https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf



Vielen Dank für die Aufmerksamkeit!

Felix Bieker, LL.M. (Edinburgh)

fbieker@datenschutzzentrum.de

0049 431 988 1200

<https://www.datenschutzzentrum.de>



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein