Risiken erkennen und bewerten

– Der Risikobegriff in der DSGVO und wie man mit ihm arbeitet –

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz

DuD-Konferenz 2019
Berlin, 4. Juni 2019

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

- Der Risikobegriff in der DSGVO
- Arbeiten mit der Risikomatrix
- Beispiele
  - IT-Sicherheit Art. 32 DSGVO
  - Datenschutz durch Gestaltung Art. 25 DSGVO
  - Datenschutz-Folgenabschätzung Art. 35 DSGVO
  - Datenpannen Art. 33f. DSGVO
- Fazit

Risikobegriff der DSGVO

- Ein 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.

- Zwei Dimensionen des Risikos:
  1. die Schwere des Schadens
  2. die Wahrscheinlichkeit, dass das Ereignis und etwaige Folgeschäden eintreten

- Kategorien:
  - (Nahezu) kein Risiko Art. 33 DSGVO
  - Risiko Art. 33 DSGVO
  - Hohes Risiko
    Artt. 34, 35, 36 DSGVO

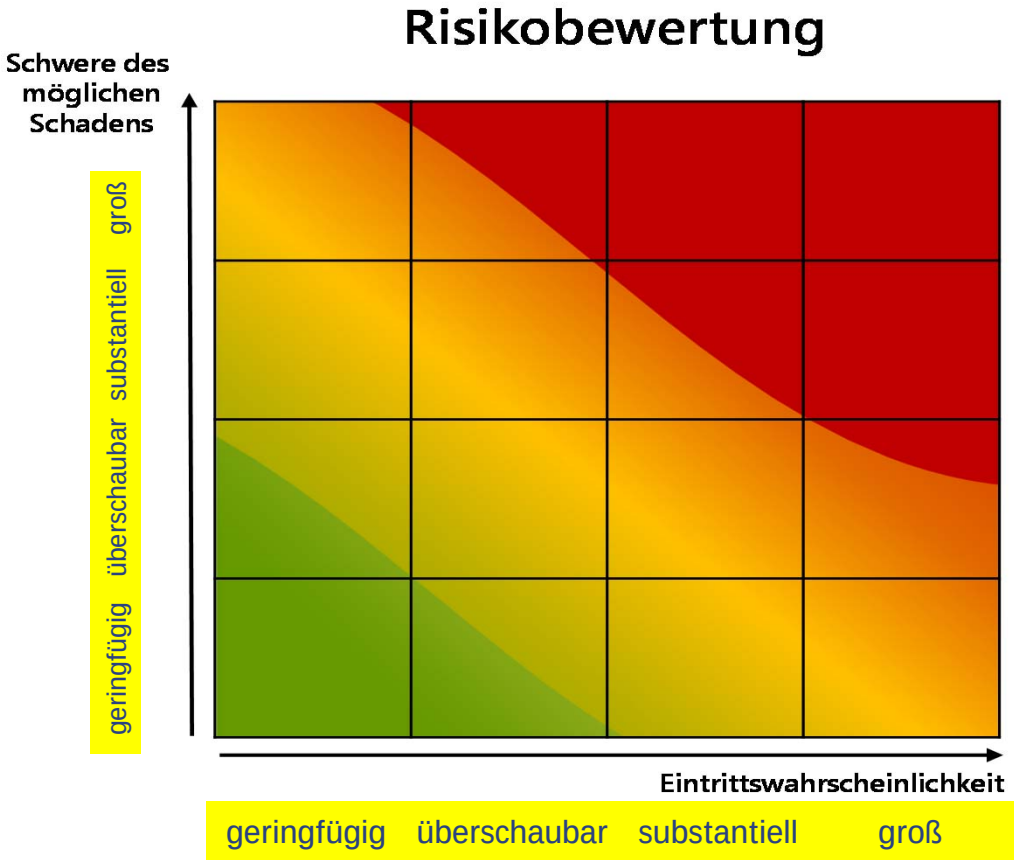
https://www.datenschutzzentrum.de/artikel/1225-.html

Risikobegriff der DSGVO

- Risiko = Schwere möglicher Schäden x Eintrittswahrscheinlichkeit
- Lässt sich nicht völlig quantifizieren
- Kann aber objektiv bestimmt werden

- Risiken für Rechte müssen mit technischen und organisatorischen Maßnahmen eingedämmt werden

→ Artt. 24, 25, 32, 35 DSGVO



Überblick

- Der Risikobegriff in der DSGVO
- Arbeiten mit der Risikomatrix
- Beispiele
  - IT-Sicherheit Art. 32 DSGVO
  - Datenschutz durch Gestaltung Art. 25 DSGVO
  - Datenschutz-Folgenabschätzung Art. 35 DSGVO
  - Datenpannen Art. 33f. DSGVO
- Fazit

Inkl. Beeinträchtigungen der Rechte und Freiheiten ErwGr. 94

Wesentliche Fragen

- Welche Schäden*) können für die natürlichen Personen auf der Grundlage der zu verarbeitenden Daten bewirkt werden?

  physischer, materieller oder immaterieller Natur ErwGr. 75

- Wodurch, d.h. durch welche Ereignisse, kann es zu dem Schaden kommen?

  Nichteinhaltung der Datenschutz-Grundsätze Art. 5 DSGVO inkl. der Betroffenenrechte Artt. 12 ff. DSGVO

- Wie, d.h. durch welche Handlungen und Umstände, kann es zum Eintritt dieser Ereignisse kommen?

  Risikoquellen: intern/extern; vorsätzlich/fahrlässig; Security/Safety oder Datenschutz

Nicht irgendwelche Schäden ...

(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.

Vom IT-Grundschutz lernen

4.4 Szenarien bilden

Im Rahmen einer Risikoanalyse kann unter Umständen eine sehr große Anzahl an möglichen Risiken in Betracht gezogen werden. Für die weitere Behandlung der identifizierten Risiken ist es jedoch wenig praktikabel, jedes einzelne identifizierte Risiko gesondert zu behandeln. Daher sollten die relevanten Risiken gruppiert werden. Hierfür bieten sich zwei Strategien an:

- Sie fassen alle Risiken zusammen, die auf einen Prozess wirken,
- Sie gehen von den Ressourcen aus, beispielsweise dem Personal oder einem technischen System wie einer Produktionsanlage, und gruppieren die Risiken entsprechend.

In der Praxis hat es sich bewährt, einem Notfallplan eine überschaubare Anzahl von **Risikoszenarien** zugrunde zu legen. Beispiele für solche Szenarien sind:

- der Ausfall zentraler Computersysteme,
- der Zusammenbruch der Netzinfrastruktur,
- die Zerstörung wichtiger Gebäude,
- der Wegfall wichtiger Lieferanten oder
- ein erheblicher Ausfall von Mitarbeitern.

Szenario-Technik erleichtert realistische Notfallvorsorge

Mit Hilfe der Szenario-Technik können Sie analysieren, welche Auswirkungen solche Vorfälle auf die Geschäftsprozesse haben können. Dabei sollten Sie den Ablauf eines Notfalls plastisch durchdenken. Bedenken Sie nicht nur extrem negative Entwicklungen ("Worst-Case"-Szenarien). Auch möglicherweise weniger gravierende oder sogar positive Auswirkungen können wertvolle Hinweise für die zu entwickelnden Notfallkonzepte liefern. Da dieses Verfahren sehr aufwändig ist, sollten Sie maximal 15 Notfallszenarien beschreiben und den Schwerpunkt auf solche Szenarien legen, die hohe und realistische Risiken enthalten (= hohes Schadensausmaß, nicht zu geringe Eintrittswahrscheinlichkeit).

IT-Grundschutz-Schulung

Online-Kurs IT-Grundschutz
Online-Kurs: Notfallmanagement
Startseite Webkurs
Einführung
Notfallmanagement initiieren
Business Impact analysieren
Risiken analysieren
Risiken identifizieren
Risikenbewerten
› **Szenarien bilden**
Strategien wählen
Risikoanalyse dokumentieren
Test
Strategien entwickeln
Konzepte einführen
Notfälle bewältigen
Notfälle üben
Notfallmanagement verbessern
Glossar

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/4_RisikenAnalysieren/3_Szenarien%20bilden/SzenarienBilden_node.html

Hilfreich für Szenario-Technik

Auswirkungen auf betroffene Person prüfen:
physisch (Leib & Leben), materiell (Finanzen, Aufwand), immateriell (Ruf, gesellschaftlich)

Achtung:

- Wenn der Schaden nicht oder kaum reversibel ist

oder

- die betroffene Person nur wenige oder beschränkte Möglichkeiten hat,
  - die Verarbeitung selbst zu prüfen oder gerichtlich prüfen zu lassen

  oder
  - sich dieser Verarbeitung zu entziehen, etwa, weil sie von der Verarbeitung gar keine Kenntnis hat.


DSK

Kurzpapier Nr. 18

Risiko für die Rechte und Freiheiten natürlicher Personen

Eintrittswahrscheinlichkeit

- Im Bereich der IT-Sicherheit:
  - Teilweise Statistiken, z.B. Personalausfall- oder Störfallzahlen
  - Aber: *„Exakte quantitative Angaben zu Eintrittswahrscheinlichkeiten sind […] in der Regel nicht möglich.“* [BSI]

- Hilfreiche Überlegungen
  - Bei Vorsatz:
    - Interesse an dem Eintritt des Ereignisses?
    - Aufwand für das Herbeiführen des Ereignisses?
    - Risiko, entdeckt zu werden?
    - Häufigkeit der Vorgänge, bei denen ein Ereignis möglich ist?
  - Bei Fahrlässigkeit: Bewusstsein der Beschäftigten? Ausstattung?
  - Bei Naturereignissen o.ä.: Indikatoren?

Work in Progress (Quelle: beh. DSB in S-H)

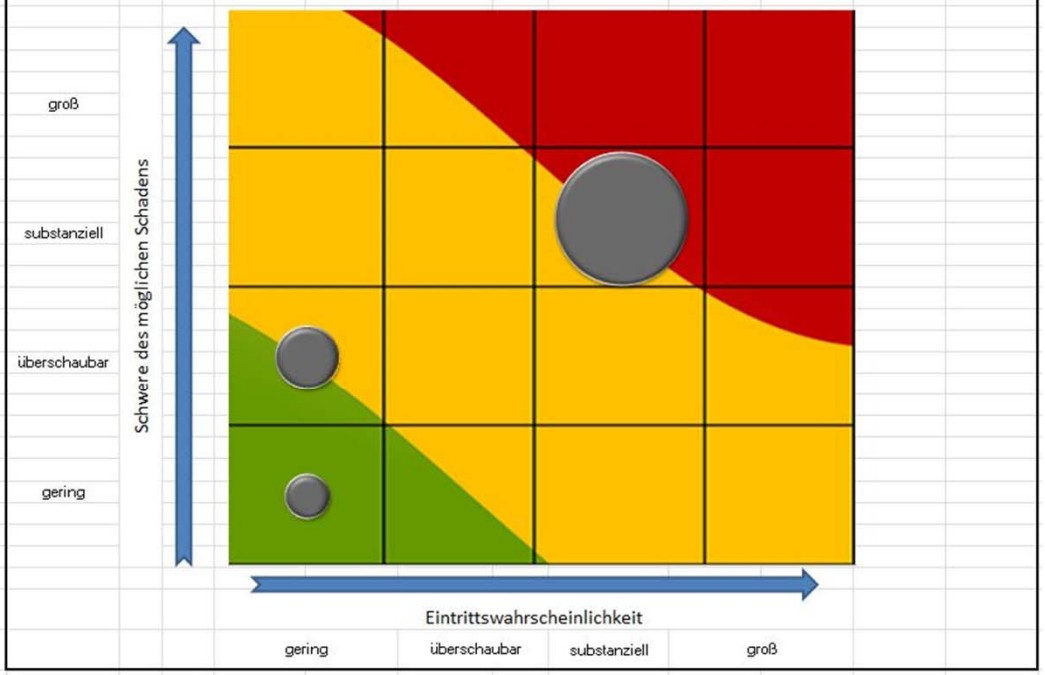
A2 fx Produktphase

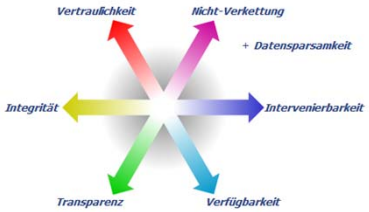
Produktphase

Rechnerische Darstellung

		Eintrittsw.	Schaden	Produkt
Datenminierung		1	1	1
Verfügbarkeit	Daten	1	1	1
	Systeme	1	2	2
	Prozesse	1	2	2
Integrität	Daten	1	2	2
	Systeme	3	3	9
	Prozesse	1	1	1
Vertraulichkeit	Daten	1	2	2
	Systeme	1	2	2
	Prozesse	1	2	2
Transparenz	Daten	1	1	1
	Systeme	1	1	1
	Prozesse	1	1	1
Nichtverkettbarkeit	Daten	1	1	1
	Systeme	1	1	1
	Prozesse	1	1	1
Intervenierbarkeit	Daten	1	1	1
	Systeme	1	1	1
	Prozesse	1	1	1

Grafische Darstellung





Überblick

- Der Risikobegriff in der DSGVO
- Arbeiten mit der Risikomatrix
- Beispiele
  - IT-Sicherheit Art. 32 DSGVO
  - Datenschutz durch Gestaltung Art. 25 DSGVO
  - Datenschutz-Folgenabschätzung Art. 35 DSGVO
  - Datenpannen Art. 33f. DSGVO
- Fazit

Art. 32 DSGVO: Sicherheit
Art. 25 DSGVO: Datenschutz durch Gestaltung

- „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 [... Maßnahmen ...]“ [Artt. 32 (1) u. Art. 25 (1) DSGVO]

- Maßnahmen: angemessen und geeignet, um die Risiken für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen so weit einzudämmen, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird

- Menge von Standardrisiken

z.B. Admin-Zugriffe, automatisches Update, Vernetzung, Dienstleister

- Auch speziellere Risiken, z.B. Aufdeckung einer Pseudonymisierung, Diskriminierung, ...

Art. 35 DSGVO: DSFA [WP248rev0.1]
Art. 36: DSGVO: Vorherige Konsultation

Kriterien zur Schwellwertanalyse der DSFA

1. Bewerten oder Einstufen (Profiling, Scoring) [Erw.Gr. 71, 91]
2. Automatisierte Entscheidungsfindung mit Rechtswirkung o.ä. [Art. 35 Abs. 3 Buchst. a DSGVO]
3. Systematische Überwachung [Art. 35 Abs. 3 Buchst. c DSGVO]
4. Vertrauliche oder höchstpersönliche Daten [Artt. 9 und 10 DSGVO]
5. Großer Umfang [Erw.Gr. 91]
6. Abgleichen oder Zusammenführen von Datensätzen (unterschiedliche Zwecke/Verantwortliche – über die Erwartungen hinausgehend)
7. Daten zu schutzbedürftigen Betroffenen [Erw.Gr. 75]
8. Innovative Nutzung oder neue Lösungen [Art. 35 Abs. 1 DSGVO, Erw.Gr. 89, 91]
9. Hinderung an der Ausübung eines Rechts [Art. 22 DSGVO, Erw.Gr. 91]

Risiko aus Sicht der betroffenen Person!

Art. 33 DSGVO: Meldung von Datenpannen
Art. 34 DSGVO: Benachrichtigung [WP250rev0.1]

Fall (immer pbD)	Melden	Benachr.	Bemerkung
USB-Stick verloren mit verschlüsseltem Backup	Nein	Nein	Solange die Verschlüsselung funktioniert
Hacker-Angriff auf Server mit Datenabfluss	Ja	Bei Risiko*)	*) „severity of likely consequences“: high
Wg. Stromausfalls kurz kein Zugriff auf pbD	Nein	Nein	Aber dokumentieren nach Art. 33 Abs. 5 DSGVO
Ransomware ohne Backup	Ja	Ja	Mit Backup ggf. „nein“
Einzelfehlzustellung	Ja	Bei Risiko	Wirklich Einzelfall?
Patientenakten im Krankenhaus für 30 h nicht verfügbar	Ja	Ja	
Studentendaten an falschen Mailverteiler gesandt	Ja	Bei Risiko	
E-Mails an TO statt BCC	Ja*)	Ja*)	*) Ggf. nicht, wenn keine sensiblen Daten und geringe Zahl

Überblick

- Der Risikobegriff in der DSGVO
- Arbeiten mit der Risikomatrix
- Beispiele
  - IT-Sicherheit Art. 32 DSGVO
  - Datenschutz durch Gestaltung Art. 25 DSGVO
  - Datenschutz-Folgenabschätzung Art. 35 DSGVO
  - Datenpannen Art. 33f. DSGVO
- Fazit

Fazit

Bild: Andrew Martin via Pixabay

- Risikobestimmung „work in progress“:
  - In der Wissenschaft [z.B. KI; Chilling] & Politik
  - In der IT-Sicherheit
  - Im Datenschutz
- Im Datenschutzmanagement
  - vor Betrieb
  - dann regelmäßig und anlassbezogen
- Bewusstsein über Risiko wichtig für Maßnahmen [auch beim Personal]
- Deren Wirksamkeit wichtig für ausreichende Eindämmung des Risikos [Restrisiken!]
- Informationen und Maßnahmen einfordern von Dienstleistern und Zulieferern