DSB-5seenland.de

Grundlagen der DSGVO

Risiko- & Schutzbedarf

Risikoansatz bsi-Grundschutz

Schutzziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Schutzobjekte:

Alle Hard- und Softwarekomponenten, mit denen Informationen im Unternehmen verarbeitet werden.

Methodik:

Bsi-Grundschutzmodell

Risikoansatz DSGVO-Datenschutz

Schutzziele (Gewährleistungsziele gem. SDM3.0):

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Datenminimierung
- Nichtverkettung (von Zwecken)
- Transparenz
- Intervenierbarkeit

Schutzobjekte:

Rechte und Freiheiten natürlicher (betroffener) Personen

Methodik:

Standard-Datenschutzmodell 3.0 (SDM3.0)

Bewertungsmethoden

Informationssicherheit:

- Mathematisch auf Basis statistischer Auswertungen
- Mathematisch/Finanziell bei eingetretenen Schäden

Datenschutz:

Qualitativer Ansatz, da z.B. Faktoren wie:

- „Missbrauchsinteresse“,
- „Entdeckungsrisiko“
- „Risiko der unberechtigten Offenlegung“

Können nicht mathematisch erfasst werden, sondern müssen in Kategorien eingestuft werden.

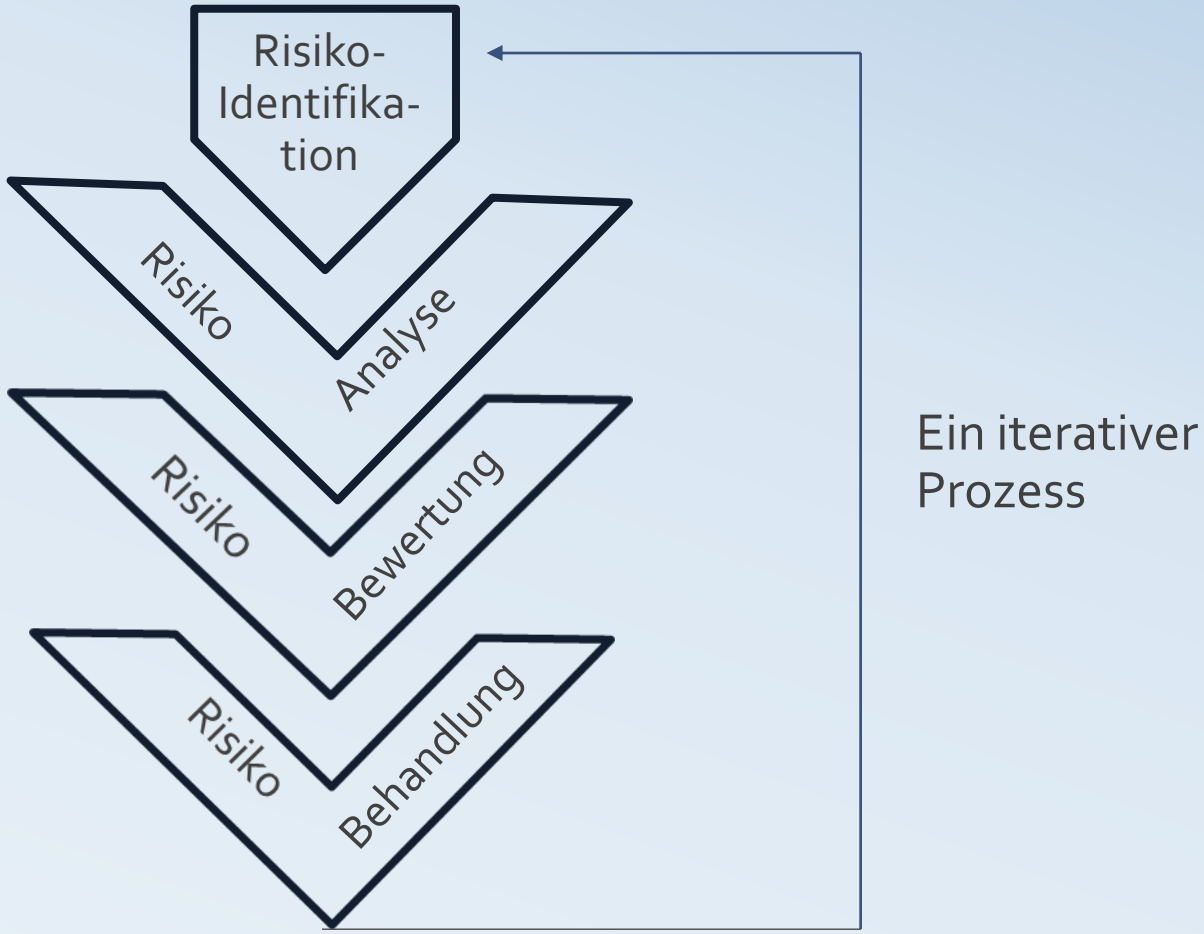
Risiken

DSB-5seenland.de

- Nach der DSGVO ist es nicht zulässig, auf die Behandlung von Anforderungen insbesondere der Umsetzung der Grundsätze aus Art. 5 DSGVO gänzlich zu verzichten und die daraus resultierenden Risiken in Kauf zu nehmen.
- Die aus dem Bereich der Informationssicherheit bekannten Instrumente der Risikoakzeptanz oder des Risikotransfers stehen im datenschutzrechtlichen Kontext dem Verantwortlichen nicht zur Verfügung.
- Spielraum besteht bei der Auswahl und der Art und Weise der Umsetzung von Anforderungen mit Hilfe von technischen und organisatorischen Maßnahmen, die in einem angemessenen Umfang gefordert werden.
- Dazu müssen bestehende Risiken für die Rechte und Freiheiten natürlicher Personen analysiert und abgesichert werden.
- Erst wenn ein angemessenes Schutzniveau erreicht wurde und somit die Interessen der Betroffenen angemessen berücksichtigt wurden, können die verbleibenden Restrisiken durch den Verantwortlichen akzeptiert werden.

Risikoanalyse - Vorgehen

DSB-5seenland.de



Ein iterativer Prozess

Risikoanalyse - Schwellwertanalyse

DSB-5seenland.de

Schwellwertanalyse

Voraussetzung für eine Risikoanalyse ist die Durchführung einer Schwellwertanalyse. In der Schwellwertanalyse wird geprüft, ob eine Verarbeitungstätigkeit ein vermutlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, also ob eine Datenschutzfolgeabschätzung (DSFA) durchgeführt werden muss.

Risikoanalyse - Schwellwertanalyse

Das SDM 3.0 schlägt ein 4-stufiges Prüfungsverfahren vor:

1. Ist die betroffene Verarbeitung in der „DSFA-MUSS-Liste" der Aufsichtsbehörden enthalten?
2. Zählt sie zu den besonders riskanten Verarbeitungen gem. Art. 35, Abs.3 DSGVO?
3. Treffen mind. 2 Eigenschaften der u.g. Aufzählung auf die Verarbeitungstätigkeit zu (WP248 des EDSA)
   a) Bewerten oder Einstufen („Evaluation or scoring")
   b) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung („Automated-decision making with legal or similar significant effect")
   c) Systematische Überwachung („Systematic monitoring")
   d) Vertrauliche Daten oder höchst persönliche Daten („Sensitive data or data of a highly personal nature")
   e) Datenverarbeitung in großem Umfang („Data processed in a large scale")
   f) Abgleichen oder Zusammenführen von Datensätzen („Matching or combining datasets")
   g) Daten zu schutzbedürftigen Betroffenen (Data concerning vulnerable data subjects")
   h) Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen („Innovative use or applying new technological or organisational solutions")
   i) Betroffene werden an der Ausübung ihres Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages gehindert („When the processing in itself prevents data subjects from exercising a right or using a service or a contract")
4. Prüfen, ob Art, Umfang, Umstände oder Zwecke (ErwGr. 76 DS-GVO) der Verarbeitungstätigkeit das Risiko für betroffene Personen erhöhen. Hierfür ist es ratsam, entsprechende Praxiserfahrungen und konkretisierende Gerichtsurteile in die Prüfung eines eventuell bestehenden hohen Risikos einzubeziehen.

Risikoidentifikation

Fragestellung:

a. Welche Schäden können für die natürlichen Personen auf der Grundlage der zu verarbeitenden Daten bewirkt werden?

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

c. Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?

Es müssen alle denkbaren negativen Folgen der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen, ihre wirtschaftlichen, finanziellen und immateriellen Interessen, ihren Zugang zu Gütern oder Dienstleistungen, für ihr berufliches und gesellschaftliches Ansehen, für ihren gesundheitlichen Zustand und für alle ihre sonstigen legitimen Interessen betrachtet werden.

Risikoidentifikation

Im Erwägungsgrund 75 zur DSGVO werden beispielhaft genannt:

- Diskriminierung,
- Identitätsdiebstahl,
- finanzieller Verlust, z.B. durch Betrug,
- Rufschädigung,
- wirtschaftliche oder gesellschaftliche Nachteile,
- Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen,
- Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten,
- Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte,
- körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter oder offengelegter Daten.

Risikoidentifikation

Welche Ereignisse können zu den Schäden führen:

- Unbefugte oder unrechtmäßige Verarbeitung
- Verarbeitung wider Treu und Glauben
- Intransparente Verarbeitung
- Unbefugte Offenlegung von und Zugang zu Daten
- Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten
- Verweigerung der Betroffenenrechte
- Verwendung der Daten durch den Verantwortlichen zu inkompatiblen Zwecken
- Verarbeitung nicht vorhergesehener Daten
- Verarbeitung nicht richtiger Daten
- Verarbeitung über die Speicherfrist hinaus

Risikoidentifikation

Aus welchen Quellen können die Schadenereignisse kommen:

- Beschäftigte des Verantwortlichen oder des Auftragsverarbeiters, könnten bewusst oder unbeabsichtigt den für die Verarbeitung vorgesehenen Rahmen überschreiten (z. B. eine Vertriebsabteilung, die die Zweckbindung von Kundendaten ändern könnte, etwa um eine Zielvorgabe zum Umsatz zu erfüllen)
- unbefugte Angreifer wie Cyberkriminelle
- staatliche Stellen, die sich unbefugt Zugang verschaffen
- Kommunikationspartner, mit denen personenbezogene Daten befugt ausgetauscht werden
- Hersteller und Dienstleister, die Informationstechnik einschließlich der mit ihr verwendeten Software, die für die Verarbeitung personenbezogener Daten oder in ihrem Umfeld eingesetzt wird, bereitstellen oder pflegen
- technische Fehlfunktionen und äußere Einflüsse, z.B. durch höhere Gewalt

Risikoanalyse

Die Eintrittswahrscheinlichkeit eines Risikos 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.

Eintrittswahrscheinlichkeit	Mögliche zukünftige Häufigkeit	Erfahrung der Vergangenheit
Sehr gering (1)	Ereignis kann ausgeschlossen werden	bisher noch nie eingetreten
Gering (2)	Ereignis tritt frühestens in 6 Jahren oder später ein	vor über 6 Jahren eingetreten
Mittel (3)	Ereignis tritt in den nächsten 4-6 Jahren ein	in den letzten 4-6 Jahren eingetreten
Häufig (4)	Ereignis tritt in den nächsten 1-3 Jahren ein	in den letzten 1-3 Jahren eingetreten
Sehr häufig (5)	Ereignis tritt im nächsten Jahr ein	im letzten Jahr eingetreten

Risikoanalyse- Schutzbedarfsanalyse

Die Schwere eines möglichen Schadens muss in jedem Einzelfall insbesondere unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung bestimmt werden. Wesentliche Faktoren sind insbesondere:

- Die Verarbeitung besonders geschützter Daten im Sinne von Art. 9 und 10 DSGVO, bei denen die DSGVO ausdrücklich eine gesteigerte Schutzbedürftigkeit vorsieht.
- Verarbeitung von Daten schützenswerter Personengruppen (z. B. Kinder, Beschäftigte).
- Verarbeitung nicht veränderbarer und eindeutig identifizierenden Daten wie z. B. eindeutigen Personenkennzahlen im Vergleich zu pseudonymisierten Daten.
- Automatisierte Verarbeitungen, die eine systematische und umfassende Bewertung persönlicher Aspekte (z. B. Profiling) beinhalten und auf deren Grundlage dann Entscheidungen mit erheblichen Rechtswirkungen für betroffene Personen getroffen werden (vgl. Art. 35 Abs. 3 lit. a DSGVO).
- 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.
- Wenn die Verarbeitung eine systematische Überwachung ermöglicht.
- Die Anzahl der betroffenen Personen, die Anzahl der Datensätze und die Anzahl der Merkmale in einem Datensatz sowie die geographische Abdeckung, die mit den verarbeiteten Daten erreicht wird.

Risikoanalyse - Qualitative Schutzstufen

DSB-5seenland.de

Die Landesaufsichtsbehörde Niedersachsen hat daher ein Schutzstufenmodell entwickelt, das inzwischen weit anerkannt ist. Daraus wird der Schutzbedarf ermittelt:

- **Stufe A (1)**: Personenbezogene Daten, die die betroffenen Personen frei zugänglich gemacht haben
- **Stufe B (2)**: Personenbezogene Daten, deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber die betroffenen Personen nicht frei zugänglich gemacht haben
- **Stufe C (3)**: Personenbezogene Daten, deren unsachgemäße Handhabung eine betroffene Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigen könnte(„Ansehen“)
- **Stufe D (4)**: Personenbezogene Daten, deren unsachgemäße Handhabung eine betroffene Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz“)
- **Stufe E (5)**: Personenbezogene Daten, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit der betroffenen Person beeinträchtigen könnte

Risiko

Um eine Risikohöhe oder einen Schutzbedarf sowie die entsprechenden TOM's festlegen zu können, muss erst die Risikoschwere bewertet werden.

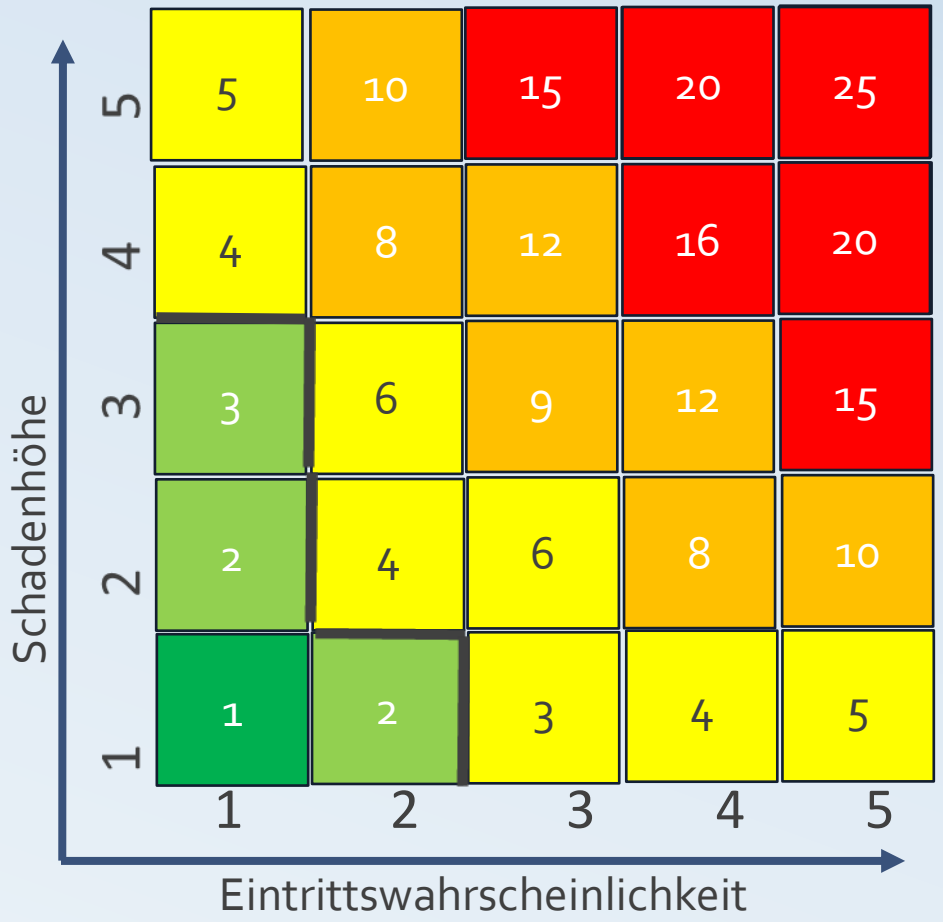
Ausmaß	X	Eintrittswahr-scheinlichkeit	=	Risikoschwere

Bewertung der Risikoschwere qualitativ (Beispiel):

Unwesentlich (Stufe A)	1
Gering (Stufe B)	2
Mittel (Stufe C)	3
Beherrschbar (Stufe D)	4
Kritisch (Stufe E)	5

Risikoanalyse - Risikomatrix

DSB-5seenland.de



Schutzbedarfsstufen

Unwesentlich	1
Gering	2-3
Mittel	4-6
Hoch	7-12
Kritisch	>12

Akzeptables Risiko:
Alle Risiken deren Risikoschwere >4 ist

Alle anderen müssen mit entsprechenden Maßnahmen gesichert werden

Risikoanalyse - Bewertung

DSB-5seenland.de

Verarbeitung	Risiko	Eintrittswahrs.	Schwere	Auswirkung
Personalverwaltung	ID-Diebstahl	3	5	15
	Diskriminierung	4	2	8
	Finanzielle Schäden	2	4	8
	Rufschädigung	5	3	15
	Körperlicher Schaden	1	4	4
Kundendaten	Rufschädigung	5	4	20
	Wirtschaftliche Nacht.	4	5	20
	Finanzielle Nachteile	4	4	16
	Erschwerung Rechtsausübung	1	4	4
	Kontrollverlust	5	2	10
	Profiling	2	1	2

Unwesentlich	1
Gering	2
Mittel	3
Beherrschbar	4
Kritisch	5

Schutzbedarfsstufen

Unwesentlich	1
Gering	2-3
Mittel	4-6
Hoch	7-12
Kritisch	>12

Die Einstufung richtet sich immer nach dem höchsten Einzelrisiko

Risikoanalyse

Als Risiko der Verarbeitung insgesamt ist grundsätzlich die höchste Risikoschwere der Einzelrisiken anzunehmen.

Risikoanalyse - Risikobehandlung

Zur Minimierung der Datenschutzrisiken werden dem Stand der Technik entsprechende TOM's eingesetzt.

Diese müssen der Art und Schwere des Risikos angemessen sein und ergeben sich aus der Schutzbedarfsanalyse. Zur Auswahl stehen bspw.:

Kategorien der TOM:

- Zutrittskontrolle – Schutzziel Vertraulichkeit
- Zugangskontrolle – Schutzziel Vertraulichkeit
- Zugriffskontrolle – Schutzziel Vertraulichkeit
- Pseudonymisierung/Anonymisierung - Schutzziel Vertraulichkeit
- Weitergabekontrolle – Schutzziel Integrität
- Eingabekontrolle – Schutzziel Integrität
- Verfügbarkeitskontrolle – Schutzziel Verfügbarkeit
- Regelmäßige Überprüfung und Aktualisierung durch Datenschutzmanagement