Prozess zur Auswahl angemessener Sicherungsmaßnahmen (ZAWAS)

Präsentation zur Praxishilfe
Version 1.0 – Erprobungsfassung

Stand 30. November 2018

Stefan Mierowski
- Referat 4 -

Die Landesbeauftragte für den Datenschutz Niedersachsen

Inhalt

Art. 5 DSGVO
„Grundsätze für die Verarbeitung“

(1) Personenbezogene Daten müssen …

lit. f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

→ Verpflichtung, angemessene Sicherheit der Verarbeitung zu gewährleisten

→ Dokumentation für Nachweisbarkeit

Art. 24 (1) DSGVO
„Verantwortung des für die Verarbeitung Verantwortlichen“

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.

→ Berücksichtigung von Rahmenbedingungen der Verarbeitung
→ Verpflichtung zur risikobasierten Vorgehensweise
→ Dokumentation für Nachweisbarkeit und Prüfbarkeit

Art. 25 (1) DSGVO
„Datenschutz durch Technikgestaltung“

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 … um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

- → angemessene Sicherungsmaßnahmen
- → Berücksichtigung von Rahmenbedingungen der Verarbeitung
- → Verpflichtung zur risikobasierten Vorgehensweise
- → im Rahmen von Planung/Entwicklung und Betrieb

Art. 32 (1) DSGVO „Sicherheit der Verarbeitung“

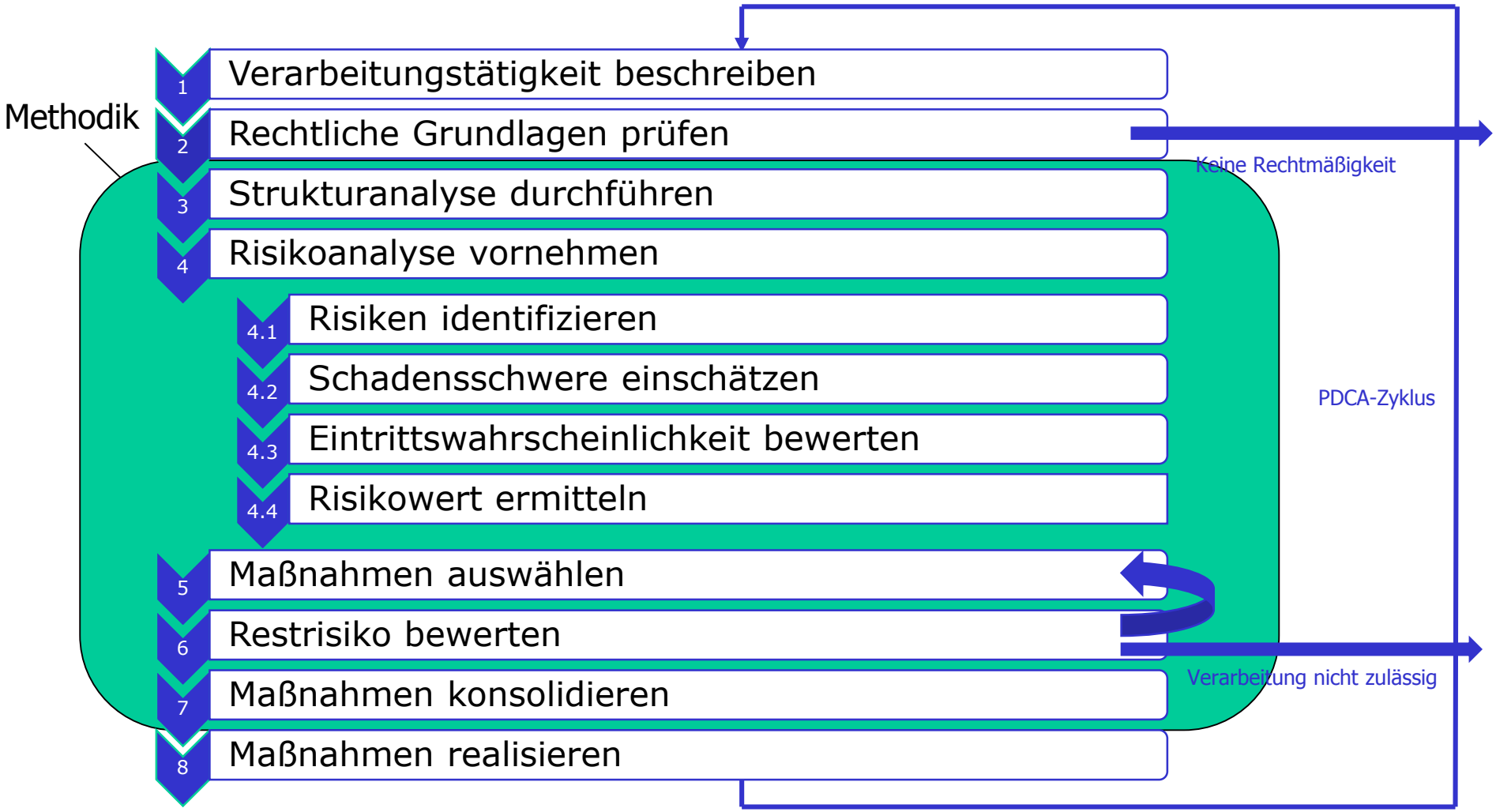
Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche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

…

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- → angemessene Sicherungsmaßnahmen
- → Berücksichtigung von Rahmenbedingungen der Verarbeitung
- → Verpflichtung zur risikobasierten Vorgehensweise
- → Implementierung einer zyklischen und standardisierten Vorgehensweise

Prozess zur Auswahl angemessener Sicherungsmaßnahmen – Version 1.0



1 Verarbeitungstätigkeit beschreiben

- Verfolgte Zwecke aufführen
- Ablauf der Verarbeitungstätigkeit darstellen
- Genutzte und erzeugte Daten benennen
- Technische Ausgestaltung beschreiben
- Verzeichnis der Verarbeitungstätigkeiten heranziehen
- Abgrenzen, was kein Bestandteil der Prüfung ist
- Ggf. Schnittstellen zu anderen Verarbeitungstätigkeiten darstellen

2 Rechtliche Grundlagen prüfen

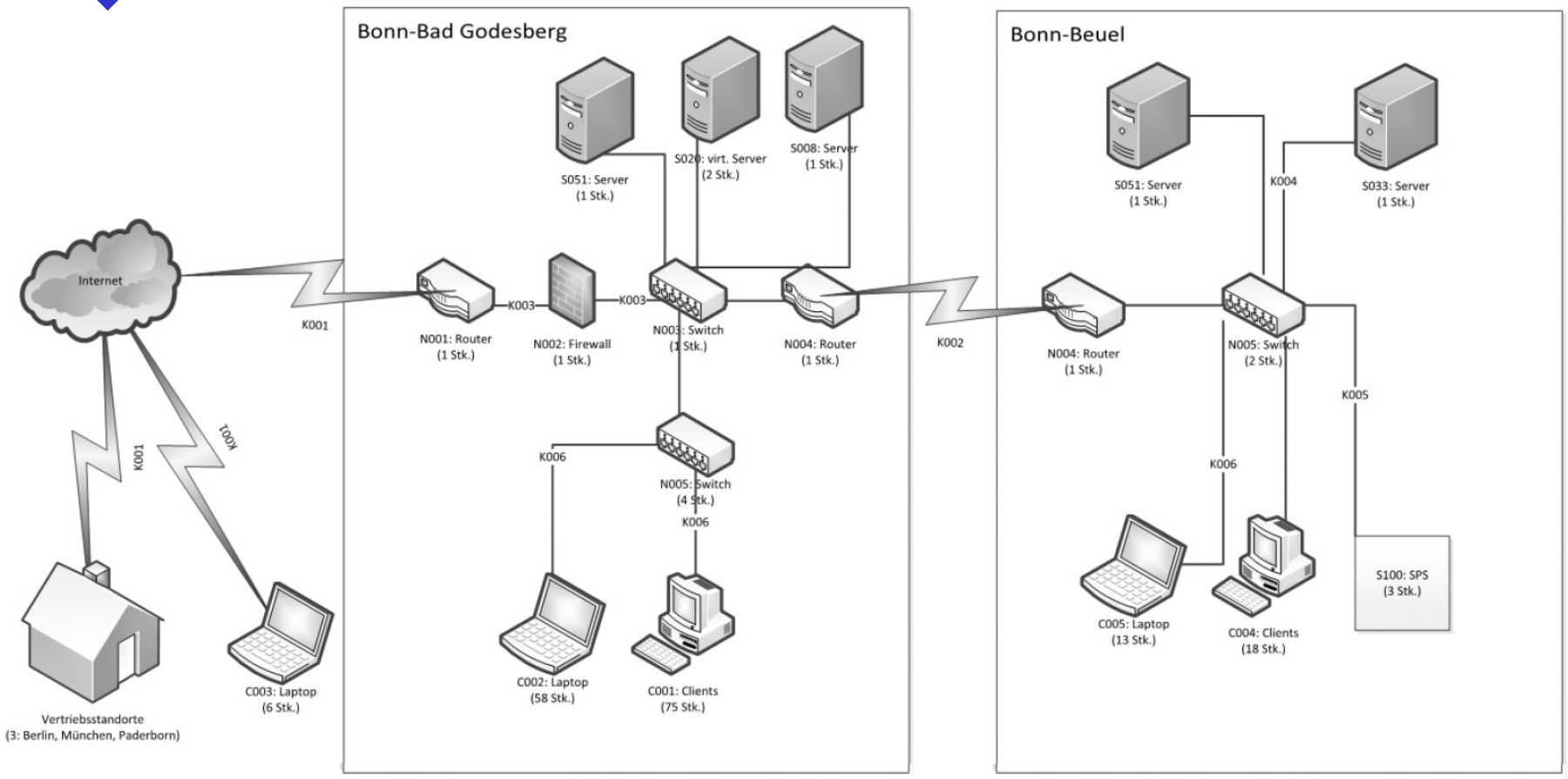
Grundsatz der Rechtmäßigkeit	Art. 6 DSGVO
Grundsatz der Zweckbindung	Art. 5 (1) lit. b DSGVO
Grundsatz der Datenminimierung	Art. 5 (1) lit. c DSGVO
Wahrung der Rechte Betroffener	Art. 12 ff DSGVO
Erforderlichkeit einer DSFA	Art. 35 DSGVO
ggf. Rechtmäßigkeit der Auftragsverarbeitung	Art. 28 + 29 DSGVO
ggf. Rechtmäßigkeit der Übermittlung(en)	Art. 44 ff DSGVO

-> nur wenn Rechtmäßigkeit der Verarbeitung vorliegt weitere Prüfung

3 Strukturanalyse durchführen

- Ermittlung und Beschreibung der zu schützenden Objekte der Verarbeitungstätigkeit (Geschäftsprozess)
  - Dienste (Fachapplikationen: z. B. Buchhaltung, Textverarbeitung, E-Mail)
  - Systeme (z. B. Server, Clients, Drucker)
  - Räume
  - Kommunikationsbeziehungen
  - Daten
- Darstellung der Objektbeziehungen

3 Strukturanalyse durchführen



Netzplan aus: BSI-Standard 200-2

4.1 Risiken identifizieren

Aus der DS-GVO abgeleitete Gewährleistungsziele:

- Datenminimierung (übergreifende Anforderung),
- Vertraulichkeit,
- Integrität,
- Verfügbarkeit,
- Transparenz,
- Nichtverkettung und
- Intervenierbarkeit.

4.1 Risiken identifizieren

IT-Grundschutz-Gefährdungskatalog (alt):

- höhere Gewalt: Hochwasser, Feuer, Blitzschlag, …
- organisatorische Mängel: fehlende/mangelhafte Zuständigkeiten, Konzeptionen, Schulungen, Dokumentationen,…
- menschliche Fehlhandlungen: Unwissenheit, Bequemlichkeit, Fahrlässigkeit, …
- technisches Versagen: Soft- oder Hardwareausfall, Stromausfall, …
- vorsätzliche Handlungen: Manipulation, Diebstahl, Vandalismus, …

4.1 Risiken identifizieren

Elementare Gefährdungen

- G 0.1 Feuer
- G 0.2 Ungünstige klimatische Bedingungen
- G 0.3 Wasser
- G 0.4 Verschmutzung, Staub, Korrosion
- G 0.5 Naturkatastrophen
- G 0.6 Katastrophen im Umfeld
- G 0.7 Großereignisse im Umfeld
- G 0.8 Ausfall oder Störung der Stromversorgung
- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.10 Ausfall oder Störung von Versorgungsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistern
- G 0.12 Elektromagnetische Störstrahlung
- G 0.13 Abfangen kompromittierender Strahlung
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.24 Zerstörung von Geräten oder Datenträgern
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktionen von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.33 Personenausfall
- G 0.34 Anschlag
- G 0.35 Nötigung, Erpressung oder Korruption
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.39 Schadprogramm
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.41 Sabotage
- G 0.42 Social Engineering
- G 0.43 Einspielen von Nachrichten
- G 0.44 Unbefugtes Eindringen in Räumlichkeiten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen
- G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

4.1 Risiken identifizieren

Risiko:

- „Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.“[1]
- EG 76:

  „Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden.“
- Das Risiko hat zwei Dimensionen: Erstens die Eintrittswahrscheinlichkeit und zweitens die Schwere eines möglichen Schadens.[1]

[1] Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürliche Personen

4.2 Schadensschwere einschätzen

Was könnte bei der Bewertung eine Rolle spielen:

- Das Kurzpapier Nr. 18[1] sieht bei der Ermittlung der Schwere eines möglichen Schadens vier Abstufungen vor
  - geringfügig
  - überschaubar
  - substantiell
  - groß.
- Art der Verarbeitung
- Umstände der Verarbeitung
- Zwecke der Verarbeitung
- Lässt sich auf Schutzstufenkonzept der LfD Niedersachsen wie folgt übertragen:

[1] Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürliche Personen

4.2 Schadensschwere einschätzen

Schutz-stufe	Personenbezogene Daten,	zum Beispiel	Schwere des möglichen Schadens
A	die von den Betroffenen frei zugänglich gemacht wurden.	Telefonverzeichnis, Wahlvorschlagsverzeichnisse, eigene freizugänglich gemachte Webseite, frei zugängliche soziale Medien	geringfügig
B	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht, nicht frei zugängliche soziale Medien	

4.2 Schadensschwere einschätzen

Schutz-stufe	Personenbezogene Daten,	zum Beispiel	Schwere des möglichen Schadens
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen").	Einkommen, Grundsteuer, Ordnungswidrigkeiten	überschaubar
D	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz").	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Arbeitszeugnisse, Gesundheitsdaten, Schulden, Pfändungen, Sozialdaten, Daten besonderer Kategorien nach Art. 9 DS-GVO	substantiell

4.2 Schadensschwere einschätzen

Schutz-stufe	Personenbezogene Daten,	zum Beispiel	Schwere des möglichen Schadens
E	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm	groß

4.3 Eintrittswahrscheinlichkeit bewerten

Eintrittswahrscheinlichkeit

Das Kurzpapier Nr. 18 sieht bei der Ermittlung der Eintrittswahrscheinlichkeit vier Abstufungen vor

- geringfügig
- überschaubar
- substantiell
- groß.

4.3 Eintrittswahrscheinlichkeit bewerten

Was könnte bei der Bewertung der Eintrittswahrscheinlichkeit eine Rolle spielen?

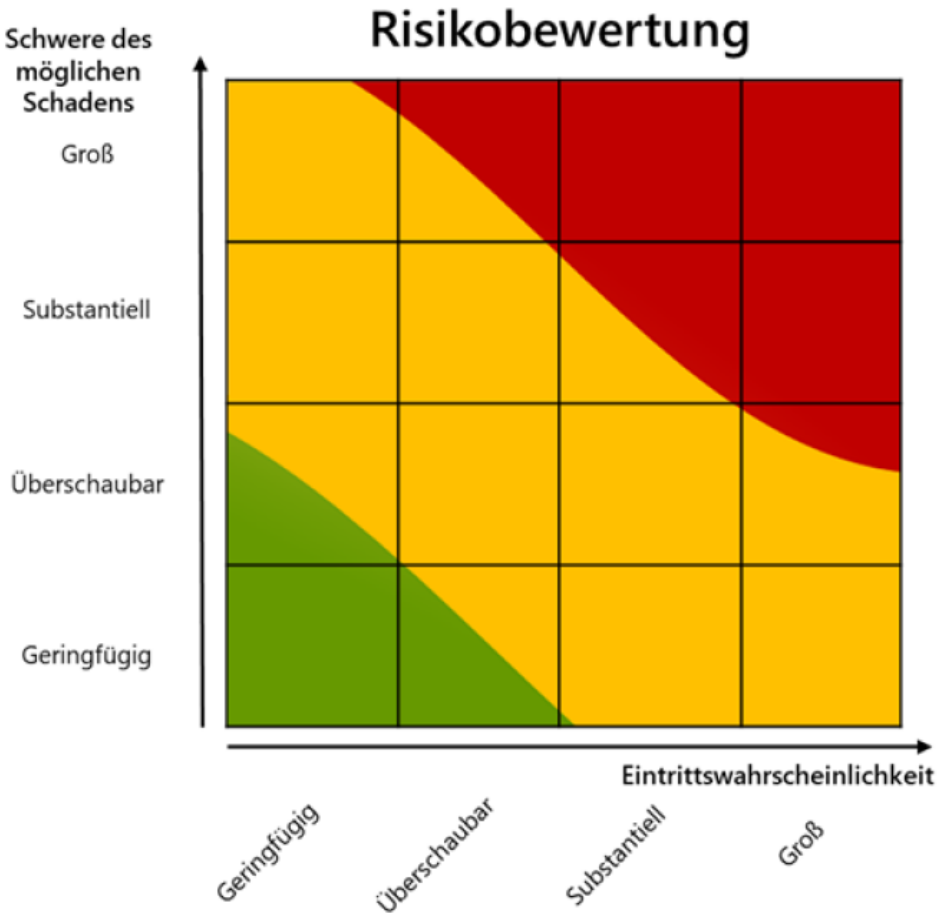
- Umfang der Verarbeitung
- Präsenz von Gefährdungslagen
- statistische Erhebungen / Studien
- Missbrauchsinteresse eines Schädigers
- Aufwand, um Schäden herbeizuführen
- Risiko, beim Missbrauch entdeckt zu werden

4.4 Risikowert ermitteln

Der Risikowert ergibt sich aus der Eintritts-wahrscheinlichkeit und der Schwere des möglichen Schadens:

Risikowert:

- geringes Risiko
- (normales) Risiko
- hohes Risiko



5 Maßnahmen auswählen

Art. 25 (1) und Art. 32 (1) DS-GVO:

Die Auswahl der Maßnahmen erfolgt unter Berücksichtigung:

- Des Risikowertes
- Des Stands der Technik
- Der Implementierungskosten

5

Maßnahmen auswählen

Art. 25 (1) und Art. 32 (1) DS-GVO:

Stand der Technik berücksichtigen

„Bei der Formel vom Stand der Technik gestaltet sich die Feststellung und Beurteilung der maßgeblichen Tatsachen für Behörden und Gerichte allerdings schwieriger. Sie müssen in die Meinungsstreitigkeiten der Techniker eintreten, um zu ermitteln, was technisch notwendig, geeignet und vermeidbar ist.“[1]

Davon unterschieden:

„§ 7 Abs. 2 Nr. 3 AtomG geht schließlich noch einen Schritt weiter, indem er auf den Stand der Wissenschaft und Technik abstellt.“ [1]

[1] BVerfG, Beschluss vom 08.08.1978 – 2 BvL 8/77

5 Maßnahmen auswählen

Art. 25 (1) und Art. 32 (1) DS-GVO:

Stand der Technik berücksichtigen

Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionalität von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.[2]

[2] Gesetzesbegründung zu § 8a BSIG, BT-Drucks. 18/4096, S. 26

5 Maßnahmen auswählen

Art. 25 (1) und Art. 32 (1) DS-GVO:

Implementierungskosten berücksichtigen

Gesamtkostenbetrachtung:

- Einmalige und laufende Kosten,
- Personal- und Sachkosten und
- Konzeptionskosten, Investitionskosten und Betriebskosten.

5 Maßnahmen auswählen

Wo finde ich Maßnahmen (Auswahl)?

- DS-GVO: z. B. Verschlüsselung, Pseudonymisierung (Art. 32 Abs. 1)
- Standard-Datenschutzmodell (SDM) - generische Maßnahmen im SDM Kapitel 7
- BSI – IT-Grundschutz-Kompendium
- BSI - Grundschutzmaßnahmen (alt)
- ISO 27001 generische Maßnahmen
- SDM – Maßnahmenkatalog (erste Bausteine von einzelnen Aufsichtsbehörden in Erprobung)
- IT-Grundschutz-Profile
- Eigene Aufstellung

5 Maßnahmen auswählen

Der Katalog der Maßnahmen

- enthält detaillierte Beschreibungen der zu treffenden technischen Maßnahmen und
- beschreibt, welche organisatorischen Regelungen für die sichere Einführung bzw. den weiteren Betrieb der betrachteten Verarbeitungstätigkeit erforderlich sind.

6 Restrisiko bewerten

- Beschreibung der Restrisiken, die sich aus der gewählten Lösung ergeben und nicht durch weitergehende technische oder organisatorische Sicherungsmaßnahmen reduziert werden können.
- Evtl. geprüfte und verworfene Lösungen aufzeigen und erläutern, warum diese nicht zum Tragen kommen.
- Fazit zur Durchführbarkeit / Nichtdurchführbarkeit des geplanten Verfahrens aus datenschutzrechtlicher Sicht. Soweit noch hohe Risiken bestehen oder das verbleibende Restrisiko aus anderen Gründen nicht übernommen werden kann, darf die Verarbeitungstätigkeit nicht produktiv eingesetzt werden.

7 Maßnahmen konsolidieren

Maßnahmen werden im Zusammenhang betrachtet und geprüft,

- ob einzelne Maßnahmen überflüssig werden, weil andere zu realisierende Maßnahmen einen mindestens gleichwertigen Schutz für das jeweilige Ziel bewirken und
- welche Maßnahmen noch konkretisiert und an die individuellen Gegebenheiten der Institution angepasst werden müssen.

Ziel ist es, durch Streichung der überflüssigen und Konkretisierung der verbleibenden Maßnahmen den erforderlichen finanziellen und personellen Realisierungsaufwand auf das notwendige Maß zu begrenzen.

Ergebnis ist eine auf die jeweilige Institution zugeschnittene und konkretisierte Liste.

8 Maßnahmen realisieren

- Aufgaben und Verantwortlichkeiten zuweisen
- Überprüfung der Umsetzung (Review)
- Fortschreibung des Gesamtsicherheitskonzeptes der Dienststelle
- Priorisierung, wenn Budget und/oder Personal knapp
  - Sachlogische Zusammenhänge beachten
  - Maßnahmen mit Breitenwirkung vorrangig
  - Wenn Bereiche betroffen sind, in denen viele Maßnahmen fehlen
- Dokumentation der Priorisierung