Der Bayerische Landesbeauftragte
für den Datenschutz

Risikoanalyse und Datenschutz-Folgenabschätzung

Systematik, Anforderungen, Beispiele

Herausgeber:

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18
Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de
https://www.datenschutz-bayern.de

Bearbeiter:

Dr. Christoph Wambsganz
unter Mitwirkung von Oliver Brunner,
Corina Scheiter und Dr. Matthias Stief

Version 1.0 | Stand: 1. Mai 2022

Dieses Arbeitspapier wird ausschließlich in elektronischer Form bereitgestellt. Es kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „DSFA“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Vorwort

Der rationale Umgang mit Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten ist ein Kernanliegen des Datenschutzrechts. In einer Risikoanalyse werden Risiken identifiziert und bewertet. In vielen Fällen genügt dies nicht: Dann müssen Verantwortliche technisch-organisatorische Maßnahmen treffen, um eine Verarbeitung datenschutzkonform durchführen zu können – oder diese Verarbeitung gar einmal unterlassen, wenn das Risiko auch mit solchen Maßnahmen nicht auf ein grundrechtsverträgliches Niveau abgesenkt werden kann. Eine Risikoanalyse ist nicht nur Kern jeder Datenschutz-Folgenabschätzung. Der Verantwortliche wird eine Risikoanalyse oftmals auch vorzunehmen haben, um seine Verpflichtungen aus Art. 24, Art. 25 und Art. 32 Datenschutz-Grundverordnung (DSGVO) adäquat erfüllen zu können.

Die Orientierungshilfe „Risikoanalyse und Datenschutz-Folgenabschätzung" stellt Methode und Bausteine einer datenschutzrechtlichen Risikoanalyse vor, erläutert die Erarbeitung technisch-organisatorischer Maßnahmen und gibt Praxishinweise für die Durchführung von Risikoanalysen. Besonderen Wert legt das Papier auf den Gedanken der Skalierung: Risikoanalysen müssen nicht in jedem Fall aufwändig sein; je nach Anlass sind verschiedene „Ausbaustufen" möglich. Das wird an mehreren konkreten Anwendungsfällen dargestellt.

Bayerische öffentliche Stellen erhalten so das nötige Wissen, um Risikoanalysen selbst erfolgreich planen und durchführen zu können sowie erforderliche technisch-organisatorische Maßnahmen entwickeln und implementieren zu können. Wer sich mit dem Thema „Risikoanalyse" auseinandersetzen möchte, dem sei für die erste Orientierung – auch zum Aufbau dieser Orientierungshilfe sowie zum Überblick über die weiterhin bereitgestellten Materialien – zunächst die Lektüre der Einführung (ab Seite 7) empfohlen.

Bitte beachten Sie außerdem folgende **Benutzungshinweise**:

- In der Orientierungshilfe zitierte Veröffentlichungen des Bayerischen Landesbeauftragten für den Datenschutz sind – soweit nicht anders angegeben – auf der Homepage https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018" abrufbar.
- Wenn Sie Rückfragen oder Verbesserungsvorschläge haben, nutzen Sie bitte das dafür eingerichtete Postfach **orientierungshilfen@datenschutz-bayern.de**.

Inhaltsverzeichnis

Vorwort ... 3

Inhaltsverzeichnis ... 4

I. Einführung ... 7

II. Kontext der Risikoanalyse ... 10

1. Zweck, Rechtsgrundlage und Mittel ... 10
2. Betriebsmittel ... 12
3. Aufwand ... 13

III. Methode der Risikoanalyse ... 15

1. Gegenstand der Risikoanalyse ... 17
2. Gewährleistungsziele ... 18
3. Risikoanalyse der SDM-Datensicherheitsziele ... 21
4. Risikoanalyse der SDM-Schutzbedarfsziele ... 24
5. Durchführung der Gesamtbewertung ... 26

IV. Bausteine einer Risikoanalyse ... 28

1. Schwachstelle ... 29
   a) Verfügbarkeit ... 29
   b) Vertraulichkeit ... 30
   c) Integrität ... 31
      aa) Datenintegrität ... 31
      bb) Konzepteinhaltung ... 31
      cc) Richtigkeit ... 32
   d) Datenminimierung ... 32
   e) Intervenierbarkeit ... 32
   f) Transparenz ... 33
   g) Nichtverkettung ... 33
2. Risiko- und Gefährdungsquellen ... 33
3. Szenario ... 34
4. Bewertung der Risiken ... 36
5. Technische und organisatorische Maßnahmen (TOMs) ... 37

V. Systematik der TOMs ... 38

1. Anforderungen an TOMs ... 39
   a) Umfassende Betrachtung ... 39
   b) Risikoorientierung ... 41
   c) Datenschutz durch Technikgestaltung ... 42

d) Datenschutzfreundliche Voreinstellungen ... 42
e) Stand der Technik und Organisation ... 42
f) Zeitpunkt der Umsetzung ... 44
g) Wirksamkeitsüberwachung ... 45
h) TOMs als Verarbeitungsvorgang ... 46
i) Adressaten der Umsetzungspflicht ... 46
2. Quellen und Fundstellen von TOMs ... 46
a) Vorgaben ... 46
b) Risikoanalyse ... 47
c) Herausgeber von TOM-Katalogen ... 48
3. Weitere Besonderheiten von TOMs ... 48
a) Schadensverhinderung oder Schadensminimierung ... 48
b) Implementierungskosten ... 49
c) Beschäftigtendatenschutz ... 49

VI. Praxishinweise für Risikoanalysen ... 50

1. Adressatengerechte Gestaltung ... 50
2. Organisation der Durchführung ... 51
a) Team ... 51
b) Dokumentation, Verweisung und Maßnahmenmanagement ... 52
3. Typische Optimierungspotenziale ... 53
a) Unnötige Komplexität vermeiden ... 53
aa) Bausteinbildung für mehrfach genutzte Betriebsmittel ... 53
bb) Gruppierung von TOMs ... 54
cc) Elementare Szenarien ... 54
b) Abgrenzung zur IT-Sicherheit ... 55
c) Weitere Optimierungspotenziale ... 57
4. Skalierbarkeit ... 58
5. Verteilte Risikoanalyse ... 60
6. Aktualisierung ... 63

VII. Anwendungsfall 1: Datenschutz-Folgenabschätzung (DSFA) ... 64

1. Einführung ... 64
2. Erforderlichkeitsprüfung ... 65
3. Durchführung ... 66
a) Mindestanforderungen und Vorgehensschritte ... 67
b) IT-Unterstützung für den DSFA-Bericht ... 68
c) IT-Unterstützung für das Maßnahmenmanagement ... 70
4. Zusammenspiel DSFA und Verzeichnis von Verarbeitungstätigkeiten ... 70
5. Weitere Aspekte zur DSFA ... 71
a) Zusammengesetzte DSFA ... 71
b) Gesetzliche DSFA ... 71

VIII. Anwendungsfall 2: „Risikoanalyse-Allgemein“ 74

1. Vergleich Risikoanalyse-Allgemein und DSFA 74
2. Durchführung 75

IX. Arbeitshilfen und Beispiele 77

X. Glossar 78

I. Einführung

Der Begriff →Risikoanalyse kommt in zahlreichen, ganz unterschiedlichen Anwendungsbereichen vor, in denen es ein hohes Gut zu schützen gilt.[1] Auf den datenschutzrechtlichen Kontext bezogen bedeutet dies, dass der →Verantwortliche analysieren und beurteilen muss, welche Risiken durch seine Verarbeitung von →personenbezogenen Daten für die betroffenen Personen entstehen und mit welchen Folgen für diese natürlichen Personen bei Risikoeintritt zu rechnen ist. Damit ist es jedoch nicht getan. Denn nach der Erkenntnis, dass eine Verarbeitung mit Risiken für betroffene Personen verbunden ist, müssen angemessene Schutzmaßnahmen ergriffen werden. Hintergrund hierfür ist, dass jede Verarbeitung personenbezogener Daten einen Eingriff in das unionale Datenschutzgrundrecht und gegebenenfalls das nationale Grundrecht auf informationelle Selbstbestimmung mit sich bringt. Da es vollständig risikolose Verarbeitungen nicht geben kann,[2] muss der Verantwortliche durch die wirksame Umsetzung technischer und organisatorischer Maßnahmen (→TOMs) ein dem Risiko angemessenes Schutzniveau gewährleisten und nachweisen.

Im Datenschutz kann die Risikoanalyse in unterschiedlichen Zusammenhängen zur Anwendung kommen. Bei der Prüfung, ob für einen Verarbeitungsvorgang eine Datenschutz-Folgenabschätzung (→DSFA, siehe Art. 35 DSGVO) erforderlich ist, wird die Risikoanalyse grundsätzlich in der speziellen Form einer sogenannten **Schwellwertanalyse** durchgeführt (vgl. Punkte VII. 2. und VIII. 1.). In der DSFA selbst ist ebenfalls eine Risikoanalyse als wichtige Komponente enthalten, die im Folgenden als „**Risikoanalyse-DSFA**“ bezeichnet wird (vgl. Punkt VII.). Aber auch wenn eine DSFA für einen bestimmten Verarbeitungsvorgang nicht erforderlich sein sollte, kann mit einer allgemeinen Risikoanalyse (im Folgenden bezeichnet als „**Risikoanalyse-Allgemein**“) der Nachweis erbracht werden, dass der Verantwortliche die erforderlichen Schutzmaßnahmen getroffen hat (vgl. Punkt VIII.).

Bereits vor der Datenschutzreform 2018 waren die bayerischen öffentlichen Stellen verpflichtet, technische und organisatorische Maßnahmen zu treffen, um Risiken bei der Verarbeitung personenbezogener Daten entgegenzuwirken.[3] Nun ist nach der DSGVO jeder Verantwortliche (und grundsätzlich auch jeder →Auftragsverarbeiter) verpflichtet, mittels der wirksamen Umsetzung von TOMs ein dem Verarbeitungsrisiko angemessenes Schutzniveau zu gewährleisten und hierbei grundsätzlich eine risikobasierte Methodik (das heißt insbesondere eine Bewertung von Eintrittswahrscheinlichkeit und Schwere des Schadens) zu wählen. Welche TOMs dem Risiko entsprechend wirksam umgesetzt werden müssen, richtet sich nach der jeweiligen Risikoanalyse.

1 Z. B. eine IT-Risikoanalyse auf der Basis von IT-Grundschutz oder eine Gefährdungsbeurteilung nach dem Arbeitsschutzgesetz.

2 Vgl. Datenschutzkonferenz, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, S. 3, Internet: https://www.datenschutzkonferenz-online.de/kurzpapiere.html.

3 Vgl. Art. 7 Bayerisches Datenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung.

I. Einführung

In dieser Orientierungshilfe wird zusammen mit weiteren Arbeitshilfen (siehe Punkt IX.) eine Vorgehensweise zur Durchführung solcher Risikoanalysen unter Anwendung der folgenden **Leitgedanken** aufgezeigt:

- **Verwendung bestehender Standards.** – Ziel bei der Erstellung dieser Orientierungshilfe ist es, schon Bestehendes zu nutzen, eventuell existierende Lücken zu schließen und notwendige Konkretisierungsschritte zu ergänzen. Wesentliche Basis der folgenden Ausführungen sind somit schon bestehende relevante Standards, Empfehlungen und Veröffentlichungen.
- **Praxisorientierung.** – Ein Schwerpunkt wurde darauf gelegt, eine praxiserprobte Lösung für eine effektive und effiziente Durchführung der datenschutzrechtlichen Risikoanalyse und DSFA darzustellen. Dabei wurde konsequent der organisatorische Grundsatz „Unnötige Komplexität vermeiden!“ beachtet.
- **Risikoorientierung.** – Wie ein roter Faden zieht sich das Prinzip der Risikoorientierung durch die gesamte DSGVO. Dadurch geprägt werden im Einzelfall die Mindestanforderungen und die mögliche Skalierbarkeit einer Risikoanalyse.
- **Umfassende Darstellung.** – Die Erfahrung hat gezeigt, dass bestimmte Einzelaspekte in der einen oder anderen Konstellation eine hohe Bedeutung gewinnen können. Daher wurde auf die Behandlung aller für bayerische öffentliche Stellen relevanten Aspekte geachtet.
- **Mindestanforderungen.** – Diese Orientierungshilfe fokussiert die Mindestanforderungen. Ein „Mehr“ ist in vielen Bereichen möglich.
- **Empfehlungscharakter.** – Nicht wenige der im Folgenden dargestellten Bereiche sind im Datenschutzrecht relativ unbestimmt und abstrakt geregelt. Daher sind die Ausführungen grundsätzlich als Empfehlung zu verstehen, die allerdings auf Praxiserfahrungen basieren.

Obwohl bei der folgenden Darstellung der Fokus unter anderem auf das Wesentliche, die Mindestanforderungen und auf eine möglichst hohe Verständlichkeit gelegt wird, kann eine gewisse Komplexität, die der Thematik innewohnt, nicht vermieden werden.

Um einen **raschen Überblick** und ein klares Verständnis von der Thematik zu erhalten, wird die folgende Herangehensweise mit fünf aufeinander aufbauenden **Schritten** zur Nutzung dieser Orientierungshilfe empfohlen:

▶ **1 Beispiele sichten**
Unter dem Punkt IX. wird auf anschauliche Beispiele verwiesen. Nach dem Erfahrungsgrundsatz „Lernen am Beispiel“ lohnt es sich daher, in einem ersten Schritt die veröffentlichen Beispiele näher zu betrachten.

▶ **2 Unklarheiten nachschlagen**
Sollten bei den Beispielen Unklarheiten oder Fragen auftauchen, können diese durch Nachschlagen in den relevanten Bereichen dieser Orientierungshilfe beantwortet werden. Dies ist sehr einfach möglich, da insbesondere unter Punkt IV. alle einzelnen Bausteine der Risikoanalyse übersichtlich beschrieben werden.

- **3 Anwendungsfälle unterscheiden**
  Je nach der zu bewertenden Verarbeitung kann eine Risikoanalyse-Allgemein (vgl. Punkt VIII.) ausreichen oder eine Risikoanalyse-DSFA (vgl. Punkt VII.) erforderlich sein.

- **4 Unterschiedliche Ausbaustufen berücksichtigen**
  Vor der ersten Durchführung einer Risikoanalyse scheint der „abschreckend hohe" Aufwand ein nicht zu unterschätzendes Hindernis in der Praxis zu sein (siehe Punkt II. 3.). Risikoanalysen-Allgemein und Risikoanalysen-DSFA können unterschiedlich umfangreich und aufwändig sein. Mit Hilfe dieser Orientierungshilfe können diese Risikoanalysen in den drei Ausbaustufen „S–Small", „M–Medium" und „L–Large" durchgeführt werden. Dies wird unter dem Punkt VI. 4. konzeptionell und durch unterschiedliche Beispiele (vgl. Punkt IX.) anschaulich dargestellt.

- **5 (Typische) Fehler vermeiden**
  In der Beratungspraxis konnten schon typische Optimierungspotenziale bei der Durchführung von Risikoanalysen identifiziert werden, die schwerpunktmäßig unter Punkt VI. 3. beschrieben werden.

Diese Orientierungshilfe ersetzt vollständig die folgenden schon zuvor veröffentlichten Arbeitshilfen:

- „Datenschutz-Folgenabschätzung – Methodik und Fallstudie" und
- „Die Datenschutz-Grundverordnung (DSGVO) – Anforderungen an Technik und Sicherheit der Verarbeitung".

Wer sich bisher schon intensiver mit diesen Arbeitshilfen beschäftigt hat, für den werden insbesondere die folgenden neuen Aspekte von besonderem Interesse sein:

- Systematisierung der Schwachstellen bei digitalisierten Verarbeitungen (vgl. Punkt IV. 1.),
- umfassende Beleuchtung der TOMs (vgl. Punkt V.),
- Beschreibung der Risikoanalyse-Allgemein (vgl. Punkt VIII.),
- Darstellung der gesetzlichen DSFA (vgl. Punkt VII. 5. b)) sowie
- diverse operative Hinweise, die sich bislang aus einer umfangreichen Beratungspraxis ergeben haben (z. B. Skalierbarkeit der Risikoanalyse, zweigeteilte Risikoanalyse, typische Fehler usw., vgl. Punkt VI.).

Fachbegriffe und Abkürzungen werden im Glossar näher erläutert. Im Glossar befindliche Fachbegriffe sind in der Regel im Text bei ihrer ersten Nennung mit einem Pfeil markiert (z. B. →Fachbegriff).

Aus Gründen der Lesbarkeit wird im Folgenden auf das Gendern von Personengruppen verzichtet. Die Verwendung des generischen Maskulinums schließt ausdrücklich alle Geschlechterformen mit ein.

II. Kontext der Risikoanalyse

1. Zweck, Rechtsgrundlage und Mittel

Bevor eine Risikoanalyse durchgeführt wird, sind zwei Zulässigkeitsvoraussetzungen zu prüfen, die der Risikoanalyse vorgelagert sind. Denn bei der Beantwortung der Frage, ob eine bestimmte Verarbeitung personenbezogener Daten datenschutzkonform ist, müssen die drei folgenden Bereiche als unverzichtbare Säulen des Datenschutzes genauer geprüft und voneinander unterschieden werden.

Zuerst ist ein Blick auf den **Zweck** einer Verarbeitung zu werfen, also warum Daten von natürlichen Personen überhaupt verarbeitet werden sollen (vgl. Art. 5 Abs. 1 Buchst. b DSGVO). Dieser Zweck kann vom Verantwortlichen selbst festgelegt oder beispielsweise auch durch Gesetz vorgegeben werden. Der hinreichend bestimmte Zweck muss legitim sein und hat Auswirkungen auf diverse wichtige Verarbeitungsaspekte, etwa auf die Identifizierung des datenschutzrechtlichen Verantwortlichen (vgl. Art. 4 Nr. 7 DSGVO), auf die Datenbandbreite, also welche personenbezogenen Daten für die Verarbeitung erforderlich sind (vgl. Art. 5 Abs. 1 Buchst. c DSGVO), und auf den Zeitraum, während dem die personenbezogenen Daten verarbeitet werden dürfen (vgl. Art. 5 Abs. 1 Buchst. e DSGVO).

Als nächste Säule der Verarbeitung ist neben dem Zweck eine tragfähige **→Rechtsgrundlage** für die Verarbeitung zu identifizieren, welche die Verarbeitung umfassend abdeckt und trägt. Fehlt einem Verarbeitungsvorgang die Rechtsgrundlage, so ist die Verarbeitung nicht rechtmäßig.[4]

Als dritte Säule sind die **→Mittel**, also die Art und Weise der Verarbeitung zu betrachten. Hierzu gibt es im Datenschutzrecht zahlreiche Anforderungen, die größtenteils als Grundsätze für die Verarbeitung in Art. 5 DSGVO zu finden sind. Das Standard-Datenschutzmodell (→SDM)[5] strukturiert diese datenschutzrechtliche Anforderungen in einen Katalog von sieben →SDM-Gewährleistungsziele (siehe Punkt III. 2.). Aus den Ausführungen im SDM geht hervor, dass der Kanon der SDM-Gewährleistungsziele vollständig alle DSGVO-Anforderungen im Hinblick auf das „Wie" der Verarbeitung abdeckt.

Insgesamt können die drei Säulen „Zweck", „Rechtsgrundlage" sowie „Art und Weise" anschaulich als „Dreiklang des Datenschutzes" aufgefasst werden. Die Prüfung der Rechtsgrundlage (Rechtmäßigkeit) und des Zwecks sind einer datenschutzrechtlichen Risikoanalyse vorgelagert und damit nicht originärer Inhalt einer Risikoanalyse.

[4] Vgl. Art. 6 Abs. 1 UAbs. 1 Satz 1 DSGVO; zudem wird die „Rechtmäßigkeit" parallel zu anderen Grundsätzen der Verarbeitung in Art. 5 Abs. 1 Buchst. a DSGVO genannt.

[5] Das Standard-Datenschutzmodell beschreibt eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele; weiterführende Informationen zu diesem Modell sind zu finden unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell.

Die drei Hauptaspekte der datenschutzrechtlichen Rechtskonformitätsprüfung werden in der Abbildung 2 dargestellt, wobei dort nur der Bereich für die „Art und Weise“ weiter aufgegliedert und damit in seiner inneren Struktur sichtbar wird.

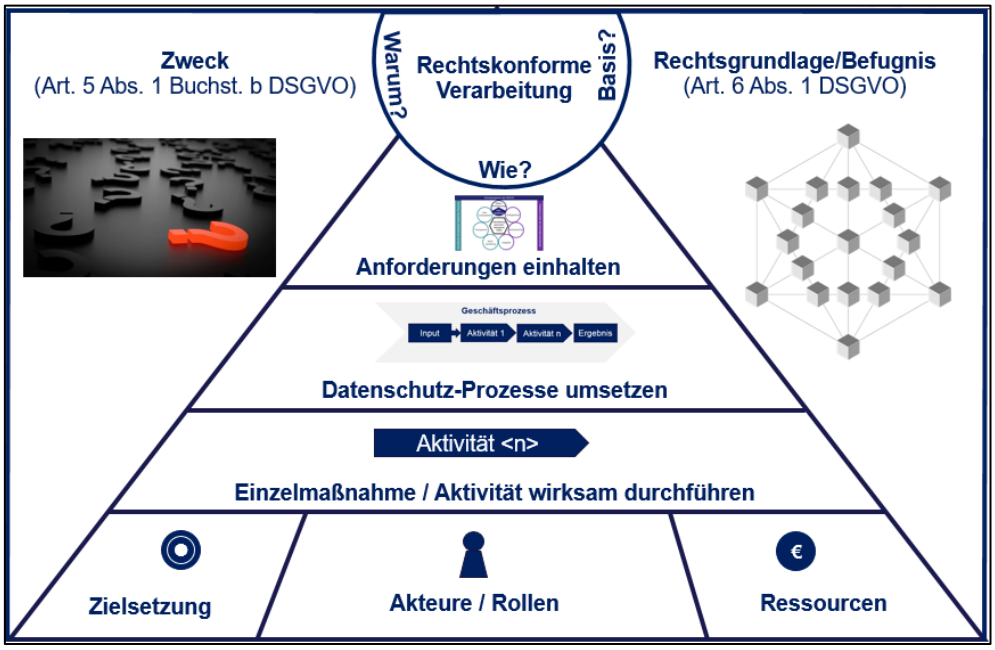


Abb. 1: Zweck, Rechtsgrundlage und Mittel als Dreiklang der datenschutzrechtlichen Rechtskonformitätsprüfung

Methodisch kann die Umsetzung einer DSGVO-Anforderung zum Mittel, also dem „Wie“, in Form von Datenschutz-Prozessen dargestellt werden. Der Begriff „Mittel der Verarbeitung“ umfasst insbesondere den Umfang der Datenverarbeitung, die Speicherdauer, die genutzten Betriebsmittel usw., ist also relativ weit zu verstehen. Alle diese Einzelaspekte müssen festgelegt und wirksam umgesetzt werden. Beides, die Festlegung sowie die Umsetzung, erfolgt in organisatorischen Abläufen, die mittels Prozessen beschrieben und dokumentiert werden können. Jeder Prozess hat zu Beginn einen Auslöser („Input“), daran anschließend beliebig viele Aktivitäten und führt am Ende zu einem Ergebnis.

Beispiel: Macht eine →betroffene Person ihren nach Art. 15 DSGVO zustehenden Auskunftsanspruch gegenüber einem Verantwortlichen geltend, so ist das Auskunftsersuchen der Auslöser. Die einzelnen Schritte, die der Verantwortliche anschließend durchführt (z. B. Identitätsfeststellung der antragstellenden Person, Angebot eines Dialogs zur Konkretisierung, Zusammenstellung der relevanten Informationen) stellen die Aktivitäten dar, die zur Beantwortung des Auskunftsersuchen führen. Die finale Beantwortung des Auskunftsersuchens stellt das abschließende Ergebnis des Auskunftsprozesses dar.

Diese Sichtweise orientiert sich am sogenannten →Geschäftsprozessmanagement, das eine praxiserprobte Methode insbesondere für die Dokumentation, zielgerichtete Steuerung und Überwachung von Prozessen und der gesamten Ablauforganisation einer Institution darstellt. Die einzelne Aktivität in einem Prozess besitzt eine klare Zielsetzung, wird durch Akteure (z. B. Personen, IT-Systeme, Dienste) durchgeführt und benötigt für ihre Durchführung bestimmte Ressourcen.

Die Implementierung der Datenschutz-Prozesse, die für eine Institution notwendig sind, gewährleisten insbesondere der datenschutzrechtliche Verantwortliche und gegebenenfalls der Auftragsverarbeiter.

Die einzelnen Anforderungen der DSGVO und die davon ableitbaren Datenschutz-Prozesse sind teilweise mit unterschiedlichen Abstraktionsniveaus in der DSGVO verankert. Besonders detailliert ist etwa die Benennung eines Datenschutzbeauftragten festgelegt (siehe Art. 37 DSGVO). Deutlich abstrakter und unbestimmter sind hingegen die Durchführung einer DSFA und die Auswahl geeigneter technischer und organisatorischer Maßnahmen (siehe Punkt V.) geregelt.

2. Betriebsmittel

Wie gerade dargestellt (siehe Punkt II. 1.), sind die Mittel, die für eine Verarbeitung genutzt werden, eine wesentliche Komponente der Verarbeitung. Zu den Mitteln der Verarbeitung gehören insbesondere die Organisation für die Verarbeitung, die Unterstützung durch Technik (Betriebsmittel) sowie die konkrete Festlegung des verarbeiteten Datenbestands (Datenbasis).

Technische Betriebsmittel können unverzichtbar für eine Verarbeitungstätigkeit sein und diese **unmittelbar** unterstützen (z. B. IT-gestützter Arbeitsplatz, E-Mail-System) oder in der Umsetzung von technischen und organisatorischen Maßnahmen der Verarbeitungstätigkeit **mittelbar** dienen, indem sie diese hinsichtlich bestehender Risiken absichern (z. B. Backup-System, Firewall, Anti-Schadsoftware-System).

Einige Betriebsmittel verarbeiten ihrerseits eigene personenbezogene Daten (**spezifische Betriebsmitteldaten**).

Beispiel: Das Videokonferenzsystem einer bayerischen Stadt verarbeitet die IP-Adressen der Endgeräte von den an einer Videokonferenz teilnehmenden Personen sowie im Rahmen der Benutzerverwaltung die Daten der Administratoren (z. B. Daten im Benutzerkonto, automatisierte Protokollierung der Systemzugriffe).

Bei der Auswahl angemessener Mittel sind unter anderem auch der Verarbeitung zugrunde liegende Zweck und die Rechtsgrundlage zu berücksichtigen. Insgesamt ergibt sich somit folgendes Gesamtbild.

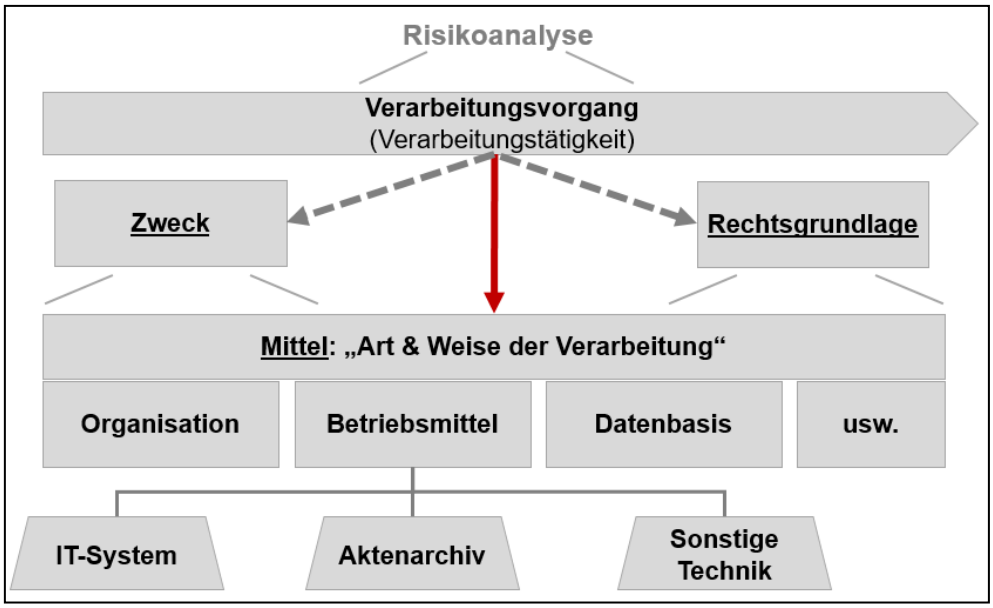


Abb. 2: Betriebsmittel als Gegenstand einer datenschutzrechtlichen Risikoanalyse

Betriebsmittel, die von unterschiedlichen Verarbeitungstätigkeiten genutzt werden, bieten sich für eine „Bausteinbildung“ besonders gut an (vgl. Punkt VI. 3. a) aa)).

3. Aufwand

Der erforderliche Aufwand für die erstmalige Durchführung sowie die gegebenenfalls anschließenden Aktualisierungen einer Risikoanalyse ist eine viel diskutierte Frage und kann mit der nötigen Klarheit regelmäßig nur im Einzelfall beantwortet werden. Denn auch wenn die unterschiedlichen Ausbaustufen und Skalierungen für die Risikoanalyse beachtet und optimal angewendet werden (vgl. Punkt VI.4), gibt es weitere Faktoren, die im Einzelfall aufwandssenkend oder aufwandserhöhend wirken können.

Generell **aufwandssenkende Faktoren** sind insbesondere:

- **Synergien nutzen.** – Es existiert bereits eine „vorgefertigte“ DSFA oder Risikoanalyse-Allgemein, die der Verantwortliche als eigene übernehmen oder einfach an seine Bedürfnisse anpassen kann. Dieser Optimierungsfaktor entsteht bei der gesetzlichen DSFA (vgl. Punkt VII. 5. b)), dem Aufteilen der Risikoanalyse (vgl. Punkte VI. 5. und VII.5.a)) sowie dem Nutzen sonstiger möglicher Synergien (vgl. Punkt VI. 3. c)).
- **Organisation optimieren.** – Bei der Durchführung einer Risikoanalyse sind die allgemein gültigen organisatorischen Grundsätze anwendbar. So sind etwa ein nachvollziehbares und systematisches Vorgehen, eine fortgeschrittene Standardisierung, die Bereitstellung des benötigten Know-how, ein gut funktionierendes →Maßnahmenmanagement, eine geeignete Förderung durch die Behördenleitung sowie eine bedarfsgerechte Digitalisierung mögliche Optimierungspotenziale.

– **Dokumentation geeignet durchführen**. – Da eine sachgerechte Dokumentation für die Nachweiserbringung unverzichtbar ist, sollte von Beginn an ein möglichst hoher Reifegrad für die Dokumentation verwendet werden (vgl. auch Punkt VI. 2. b)). Hinweise hierzu sind auch in den Beispielen enthalten (siehe Punkt IX.).

Generell **aufwandserhöhende Faktoren** sind insbesondere:

– **Erhöhtes Risiko.** – Für die Risikohöhe existieren im Datenschutz die drei Stufen „geringes Risiko", „(normales) Risiko" und „hohes Risiko" (vgl. Punkt III. 3.). Nach dem DSGVO-Grundsatz des risikoorientierten Vorgehens gehen Verarbeitungen mit einem höheren Verarbeitungsrisiko grundsätzlich mit einem höheren Durchführungsaufwand einher. Ausdruck dieses Grundsatzes ist die DSFA, die bei Hochrisikoverarbeitungen verpflichtend ist und mittels erhöhten Mindestanforderungen (vgl. Punkte VIII. 1. und VII. 3. a)) durchgeführt sowie nachgewiesen werden muss.

– **Erhöhte Komplexität.** – Eine erhöhte Komplexität der jeweils betrachteten Verarbeitung führt grundsätzlich zu einer erweiterten Risikobetrachtung und damit zu einem erhöhten Durchführungsaufwand (vgl. Punkt VI. 4.).

– **Lücken schließen.** – In der Beratungspraxis gibt es nicht wenige Fälle, in denen durch die systematische und umfassende Analyse etwa bei einer DSFA-Durchführung bestehende Lücken identifiziert und geschlossen werden mussten (z. B. unzureichendes Löschkonzept, unzureichendes Berechtigungsmanagement, fehlende oder lückenhafte Dokumentationen). Diese Aufwandspositionen können erheblich sein, sollten aber nicht dem originären Aufwand der Risikoanalyse zugeschlagen werden. Denn durch die Durchführung einer Risikoanalyse sind solche Handlungsbedarfe, die unabhängig von einer Risikoanalyse nicht bestehend dürften, nur aufgedeckt worden.

Dem zu erbringenden Aufwand gegenüber stehen die Erfüllung der Nachweispflicht sowie weitere wichtige Vorteile. Neben der Erfüllung der gesetzlichen Anforderungen ist besonders die deutliche Erhöhung der Wahrscheinlichkeit zu nennen, potenzielle Datenschutzverstöße erst gar nicht zu ermöglichen bzw. diese bereits vor ihrem Entstehen zu erkennen und zu verhindern. Zudem werden mittels der Risikoanalyse wichtige eigene Prozesse qualitätsgesichert und insbesondere Schutzmaßnahmen systematisch auf Vollständigkeit und Wirksamkeit überprüft.

III. Methode der Risikoanalyse

Ein wichtiger Aspekt, der mit der DSGVO im Datenschutz verankert wurde, ist die im Vergleich zur Zeit vor der Datenschutzreform 2018 deutlich umfangreichere Rechenschafts- und Nachweispflicht (vgl. Art. 5 Abs. 2 DSGVO). Diese Pflicht liegt primär beim Verantwortlichen (vgl. Art. 5 Abs. 2 und 24 DSGVO). Vor diesem Hintergrund stellt sich die Frage, wie der Verantwortliche die ordnungsgemäße Art und Weise seiner Verarbeitungsvorgänge datenschutzkonform nachweisen kann.

Der Nachweis für eine datenschutzkonforme und damit angemessene Mittelauswahl besteht darin, dass der jeweils betrachtete Verarbeitungsvorgang die gesetzlichen Anforderungen, die durch die sieben SDM-Gewährleistungsziele strukturiert werden, durchgängig erfüllt. Dieser Brückenschlag zwischen den DSGVO-Vorgaben („Soll" der Verarbeitung) und der tatsächlichen Durchführung („Ist" der Verarbeitung) kann – wie in der folgenden Abbildung dargestellt – auf unterschiedliche Art und Weise erfolgen.

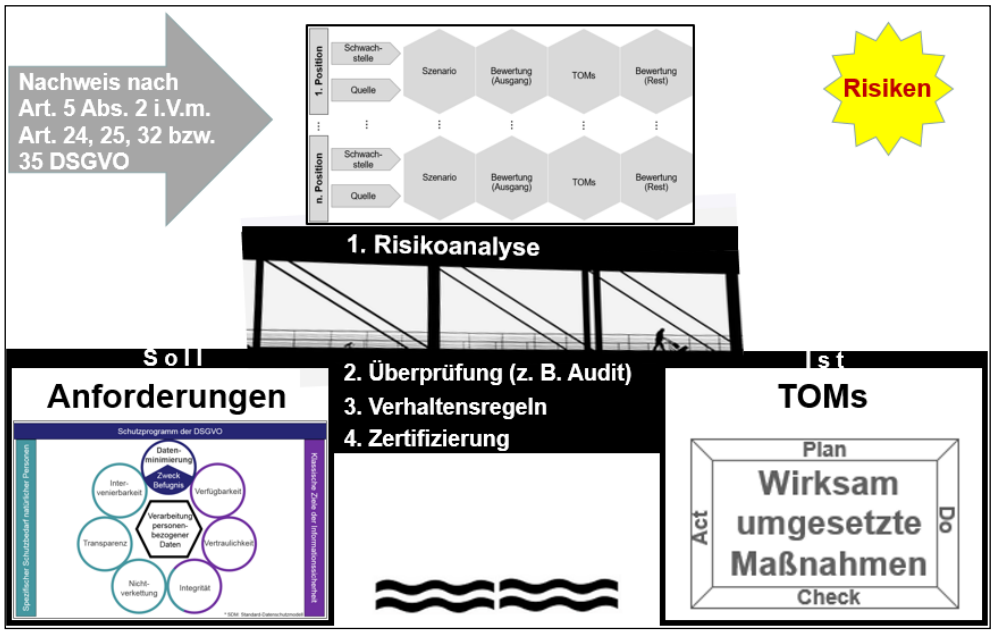


Abb. 3: Nachweismöglichkeiten für die rechtskonforme Art und Weise eines Verarbeitungsvorgangs

Zum einen kann die Erfüllung der SDM-Gewährleistungsziele durch eine Überprüfung etwa im Rahmen eines Audits[6] nachgewiesen werden, das beispielsweise durch eine interne Stelle (z. B. Datenschutzbeauftragter, interne Revision) oder durch einen externen Spezialisten

6 Ein Audit in diesem Sinn ist eine Prüfung mit einem Abschlussbericht, mittels der untersucht wird, ob eine bestimmte Verarbeitung in den untersuchten Bereichen datenschutzkonform ist.

durchgeführt werden kann. In aller Regel ist diese Nachweisform jedoch nur punktuell und anlassbezogen.

Zum anderen können Zertifizierungsverfahren (vgl. Art. 24 Abs. 3 DSGVO) als Gesichtspunkte herangezogen werden, dass ein Verantwortlicher seine datenschutzrechtlichen Pflichten erfüllt. Da auch diese Nachweismöglichkeiten derzeit nur punktuell genutzt werden, ist der Blick wie folgt auf das Standard-Instrument der DSGVO zu richten, das dem Verantwortlichen für seine Nachweiserbringung immer zur Verfügung steht.

Die DSGVO stellt die Rechte und Freiheiten der betroffenen Personen – also derjenigen, deren personenbezogene Daten verarbeitet werden – in den Vordergrund der Sicherheitsbetrachtungen.

Art. 24 Abs. 1 Satz 1 und Art. 32 Abs. 1 DSGVO legen jeweils fest, dass die Erforderlichkeit von TOMs unter Berücksichtigung „der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken (bzw. des Risikos) für die Rechte und Freiheiten natürlicher Personen" geprüft werden muss. Ein Risiko ist dabei ein datenschutzwidriges →Szenario mit seinen Konsequenzen für die betroffenen Personen, das grundsätzlich bezüglich seiner Eintrittswahrscheinlichkeit und seiner Schwere beurteilt wird.[7]

Ähnlich wie im Bereich der IT-Sicherheit[8] muss daher regelmäßig bei der Einführung einer neuen Verarbeitung eine Risikoanalyse durchgeführt werden. Kriterien für die Risikoanalyse lassen sich vor allem den Erwägungsgründen 75 und 76, 89 bis 91 sowie 94 der DSGVO entnehmen.

Der Begriff „Risikoanalyse" bezeichnet in einschlägigen Empfehlungen[9] jedoch oft nur einen Schritt im Rahmen einer „Risikobeurteilung", die regelmäßig aus den folgenden Schritten besteht:

- Identifikation von Risiken (Risk Identification),
- Analyse von Risiken (Risk Analysis),
- Evaluation oder Bewertung von Risiken (Risk Evaluation).

Im deutschen Sprachgebrauch hat sich allerdings der Begriff „Risikoanalyse" für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert.[10] Daher wird in dieser

[7] Vgl. Artikel 29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt, WP 248 Rev. 01, S. 6; die vom Europäischen Datenschutzausschuss gebilligten Leitlinien sind im Internet auf https://www.datenschutz-bayern.de unter der Rubrik „DSFA" abrufbar.

[8] Z. B. eine IT-Risikoanalyse auf der Basis von IT-Grundschutz oder eine Gefährdungsbeurteilung nach dem Arbeitsschutzgesetz.

[9] Z. B. ISO-Normen.

[10] Vgl. Bundesamt für Sicherheit in der Informationstechnik, Risikoanalyse auf Basis von IT-Grundschutz, Standard 200-3, Kapitel 1.3, Internet: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html.

Orientierungshilfe – wie auch im IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (→BSI) –weiterhin der Begriff „Risikoanalyse“ für den umfassenden Prozess benutzt.

Die Festlegung der Methode, die für die Durchführung der Risikoanalyse Anwendung findet, ist ein besonders wichtiger Schritt. Die DSGVO nennt an mehreren Stellen (vgl. Art. 24 Abs. 1, 25 Abs.1, 32 Abs.1 und 35 Abs. 7 DSGVO) hinsichtlich dieser Methode nur die beiden Bausteine „unterschiedliche Eintrittswahrscheinlichkeit und Schwere“ der Risiken (Risikobewertung) und „geeignete technische und organisatorische Maßnahmen“ (TOMs). Daher ist die Methode anhand der Zielsetzung der datenschutzrechtlichen Risikoanalyse vor einer Durchführung weiter zu konkretisieren.

1. Gegenstand der Risikoanalyse

Gegenstand einer Risikoanalyse ist ein hinreichend beschriebener und von anderen Verarbeitungsvorgängen klar abgegrenzter Verarbeitungsvorgang (im Folgenden als „→**Zielverarbeitung**“ bezeichnet). Die Zielverarbeitung kann jede Form einer Verarbeitung von personenbezogenen Daten haben, also insbesondere sein

- eine →Verarbeitungstätigkeit im Sinne des Art. 30 Abs. 1 DSGVO,
- mehrere ähnliche, zusammengefasste Verarbeitungstätigkeiten,
- die Verarbeitung von personenbezogenen Daten durch ein Betriebsmittel (vgl. Punkt II.2),
- eine Vorgangsreihe nach Art. 4 Nr. 2 DSGVO oder
- Teilverarbeitungen aus den zuvor genannten Verarbeitungsformen.

Beim Zuschnitt der Zielverarbeitung ist stets zu gewährleisten, dass keine Lücken und damit „blinde Flecken“ hinsichtlich der notwendigen Risikobetrachtung entstehen. Eine Prüfung auf Vollständigkeit der Risikoanalyse setzt zum einen voraus, dass alle Verarbeitungen – inklusive die spezifische Verarbeitungen von Betriebsmitteln (siehe Punkt II.2 und Punkt VI. 3. a) aa)) – im Verzeichnis von Verarbeitungstätigkeiten dokumentiert sind. Zum anderen muss jede Verarbeitungstätigkeit von einer Risikobetrachtung vollständig umfasst sein und damit eine Zuordnung der einzelnen Verarbeitungstätigkeit zu der bzw. den einschlägigen Risikoanalyse(n) klar und eindeutig möglich sein.

Trotz des grundsätzlich bestehenden hohen Freiheitsgrads bei der Auswahl und dem Zuschnitt der Zielverarbeitung sind folgende Rahmenbedingungen zu beachten:

- **Transparenz.** – Immer zu gewährleisten ist, dass die Risikoanalyse transparent bleibt, also auch für Dritte verständlich und nachvollziehbar ist. Einen wichtigen Einfluss auf die Transparenz hat die Komplexität der Zielverarbeitung.
- **Ähnlichkeit.** – Eine Zielverarbeitung kann auch mehrere, voneinander unabhängige Verarbeitungsvorgänge bündeln, die hinreichend ähnlich sind. Diese Ähnlichkeit bezieht sich beispielsweise auf die durch die Zielverarbeitung verarbeiteten Daten, auf die dort gelten-

den speziellen rechtlichen Schutzanforderungen sowie auf die dort vorhandenen Verarbeitungsrisiken. In aller Regel sind dabei Grenzziehungen zu beachten, die sich schon aus dem Zuschnitt von Geschäftsprozessen, der Festlegung von „Produkten" für die Leistungserbringung oder aus anderen einheitlichen Lebenssachverhalten ergeben.

2. Gewährleistungsziele

Die Grundsätze des Art. 5 DSGVO sowie weitere, diese Grundsätze konkretisierende DSGVO-Anforderungen können in einzelne Datenschutz-Ziele überführt werden. Dies macht etwa das **Standard-Datenschutzmodell** (SDM)[11], indem es datenschutzrechtliche Anforderungen in einen Katalog von insgesamt sieben SDM-Gewährleistungszielen abbildet. Das SDM ist als Standard-Methode im Datenschutz anerkannt und wird insbesondere von folgenden Stellen zitiert:

- **Europäischer Datenschutzausschuss (EDSA)**. – Die vom Europäischen Datenschutzausschuss gebilligten „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt'"[12](im Folgenden: Leitlinien) wird das SDM im Anhang 1 als Beispiel von Rahmenbestimmungen für DSFAs genannt.
- **Bundesamt für Sicherheit in der Informationstechnik (BSI).** – Im Baustein „CON.2: Datenschutz" des IT-Grundschutz-Kompendiums ist die SDM-Methodik als Basisanforderung formuliert.[13]
- **IT-Planungsrat.** – Der →IT-Planungsrat empfiehlt seinen Mitgliedern, das SDM bei Planung, Einführung und Betrieb von personenbezogenen Verarbeitungen anzuwenden.[14]

Aus den Ausführungen im SDM geht hervor, dass der Kanon der SDM-Gewährleistungsziele vollständig alle technischen und organisatorischen Anforderungen der DSGVO abdecken. Damit ist der Erfüllungsgrad der sieben Gewährleistungsziele hinsichtlich der Zielverarbeitung eine anerkannte „Messmethode" für den Nachweis, dass der Mitteleinsatz bei einer Verarbeitung die DSGVO-Anforderungen einhält.

[11] Siehe hierzu Fn. 5.

[12] Siehe hierzu Fn. 7.

[13] Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_2_Datenschutz_Edition_2021.html.

[14] Internet: https://www.it-planungsrat.de/beschluss/beschluss-2020-06.

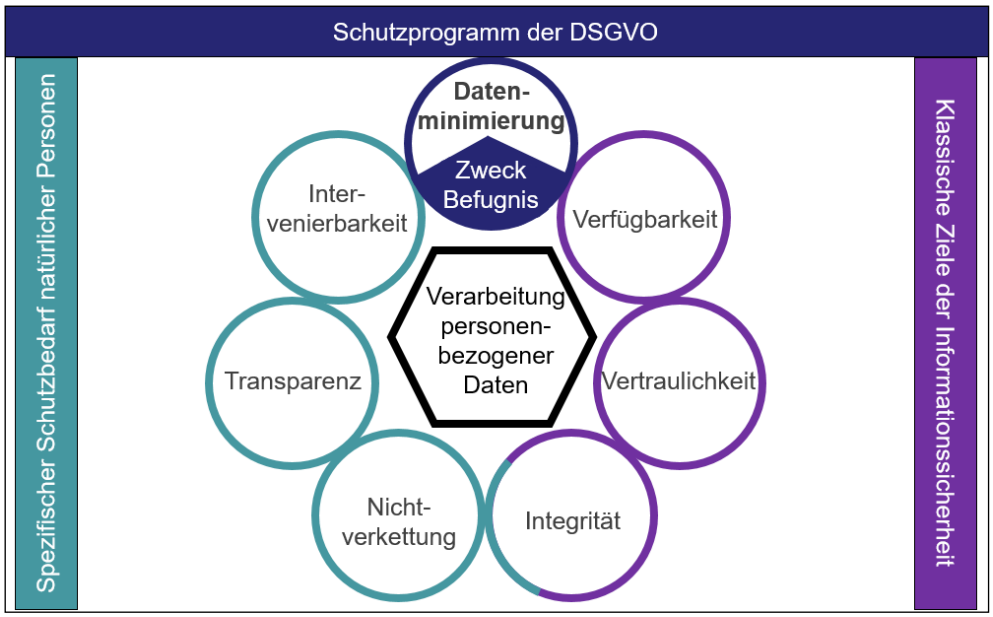


Abb. 4: Die sieben SDM-Gewährleistungsziele

Die sieben SDM-Gewährleistungsziele besitzen in aller Kürze und auf das Wesentliche reduziert folgenden inhaltlichen Umfang:

- **Datenminimierung:** „Nur benötigte personenbezogene Daten verarbeiten!"
- **Verfügbarkeit:** „Personenbezogene Daten müssen relevante Geschäftsprozesse ermöglichen!"
- **Vertraulichkeit:** „Personenbezogene Daten nur für befugte Personen (Kenntnis und Veränderung)!"
- **Integrität:** „Personenbezogene Daten unversehrt, aktuell, richtig und nach Konzeption verarbeiten!"
- **Nichtverkettung:** „Keine rechtswidrige Zweckentfremdung bei der Datenverarbeitung!"
- **Transparenz:** „Verarbeitung ist erkennbar, nachvollziehbar und prüfbar!"
- **Intervenierbarkeit:** „Betroffenen können die ihnen zustehenden Datenschutzrechte wirksam ausüben!"

Das SDM-Gewährleistungsziel **„Integrität"** spielt eine Sonderrolle, da es nach dem SDM folgende Teilaspekte besitzt:[15]

- **Datenintegrität:** Anforderung, dass Korrektheit/Unversehrtheit von Informationen/personenbezogenen Daten und die korrekte Funktionsweise von Systemen sichergestellt ist.

[15] Vgl. SDM (Fn. 5), S. 32.

- **Konzeptionseinhaltung:** Anforderung, dass Prozesse und Systeme die für sie gültigen Vorgaben kontinuierlich einhalten (Gleichklang von Betrieb als Ist und der Konzeption als Soll).
- **Richtigkeit:** Anforderung, dass zwischen der rechtlich normativen Anforderung und dem Betrieb eine hinreichende Deckung besteht.

Die Risikoanalyse weist die Erfüllung der SDM-Gewährleistungsziele nach und ist somit Basis für die Beantwortung der Frage, ob die eingesetzten Mittel der Zielverarbeitung die Anforderungen der DSGVO einhalten.

Die SDM-Gewährleistungsziele der klassischen Informationssicherheit „Verfügbarkeit", „Vertraulichkeit" und den Teilaspekt „Datenintegrität" des SDM-Gewährleistungsziels „Integrität" verweist Art. 32 Abs. 1 DSGVO mit „Eintrittswahrscheinlichkeit und Schwere des Risikos" auf die klassische **Risikomanagementmethode**. Folglich wird für diese drei Ziele, die im Folgenden als „→**SDM-Datensicherheitsziele**" bezeichnet werden, grundsätzlich das klassische Risikomanagement als Methode für die Risikoanalyse empfohlen (siehe Punkt III. 3.).

Für die vier anderen SDM-Gewährleistungsziele „Datenminimierung", „Intervenierbarkeit", „Transparenz" und „Nichtverkettung" sowie der Teilaspekte „Konzepteinhaltung" und „Richtigkeit" des SDM-Gewährleistungsziels „Integrität" werden im Folgenden als „→**SDM-Schutzbedarfsziele**" bezeichnet. Diese Ziele können als „fundamentale Rechte und Prinzipien"[16] verstanden werden, die insbesondere unabhängig von der Eintrittswahrscheinlichkeit und der Schwere nicht Bestandteil von Abstufungen sein können.

Vor diesem Hintergrund kommt für die Risikoanalyse der SDM-Schutzbedarfsziele ein spezielles **Zielerfüllungsmanagement** zur Anwendung (siehe Punkt III. 4.), woraus sich folgendes Gesamtbild ergibt:[17]

[16] Siehe Commission Nationale de l'Informatique et des Libertés, Privacy Impact Assessment (PIA) – Methodology, Stand Februar 2018, S. 3, im Internet abrufbar unter https://www.cnil.fr/en/PIA-privacy-impact-assessment-en.

[17] Vgl. Bitkom e. V., Risk Assessment & Datenschutz-Folgenabschätzung, Leitfaden, 2017, S. 8.

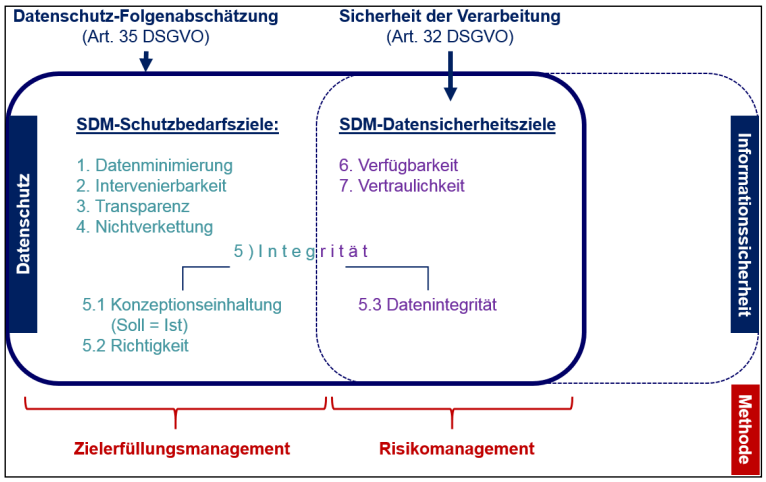


Abb. 5: Die SDM-Schutzbedarfs- und die SDM-Datensicherheitsziele mit jeweiligen Risikoanalysemethoden

Die Aufspaltung in unterschiedliche Risikoanalysen birgt auf der Maßnahmen-Ebene nicht die Gefahr, dass gleiche TOMs in beiden Risikobereichen parallel und gegebenenfalls unterschiedlich behandelt werden müssten. Denn beide Bereiche erfordern grundsätzlich unterschiedliche Maßnahmen zur Risikoeindämmung.

3. Risikoanalyse der SDM-Datensicherheitsziele

Beim klassischen Risikomanagement für den Datenschutz werden die Risiken aus Sicht der betroffenen Personen betrachtet. Dieselbe Methode wird oft auch im Bereich der IT-Sicherheit mit dem wichtigen Unterschied eingesetzt, dass dort primär der Schwerpunkt auf die Risiken für die jeweilige Institution gelegt wird (siehe Punkt VI. 3. b)).

Zu jedem relevanten Einzelrisiko werden erfasst:

- die →Schwachstelle,
- die →Risikoquelle,
- das Risiko-Szenario,
- die Risikoindexierung (Eintrittswahrscheinlichkeit, Schwere/Schaden, ampelfarbener Risikoindex) ohne TOMs,
- die TOMs sowie
- der ampelfarbene, mit Freitext begründete Risikoindex bei Wirksamkeit der TOMs.

Folglich kann die Risikoanalyse mittels klassischen Risikomanagements wie folgt schematisch dargestellt werden:

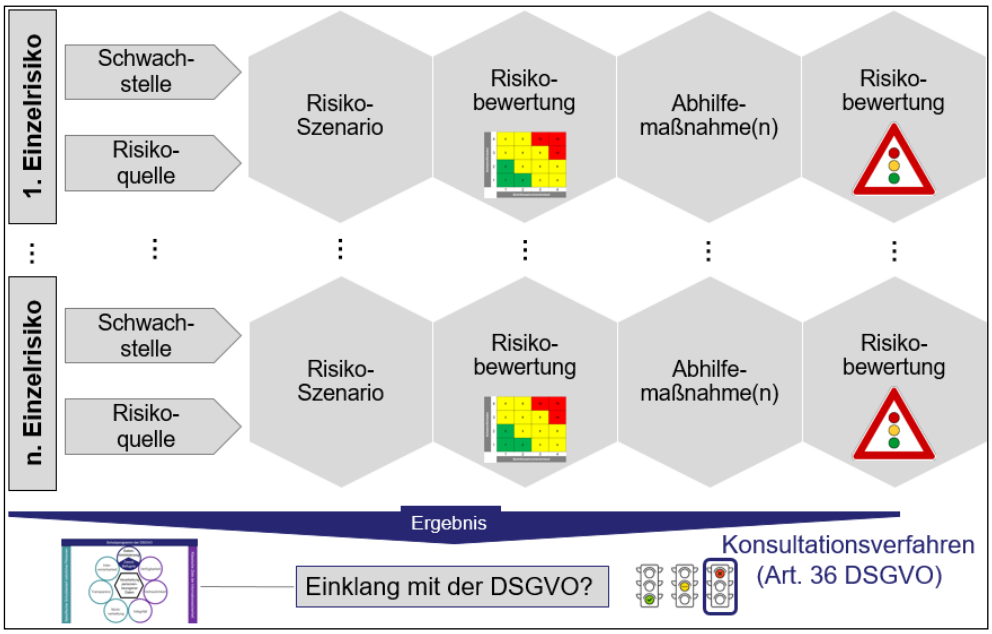


Abb. 6: Risikoanalyse der SDM-Datensicherheitsziele

Aus der Abbildung geht hervor, dass das Risiko-Szenario der eigentliche Gegenstand für die Risikobewertung ist. In jedem Szenario wird möglichst differenziert ein Ereignis beschrieben, durch das der betrachtete Verarbeitungsvorgang den normativen DSGVO-Rahmen verlassen würde und das es daher zu vermeiden gilt.

Für eine einfachere Herleitung aller relevanten Risiko-Szenarien dient die Betrachtung der Schwachstellen und der Risikoquellen (siehe Punkt IV. 3.). Schwachstellen sind dabei als Eigenschaften des betrachteten Verarbeitungsvorgangs definiert, die geeignet sind, bei hinzutreten einer bestimmten Risikoquelle ein Szenario mit Schadwirkung für die Rechte und Freiheiten natürlicher Personen auszulösen. Das Zusammenspiel der vier Aspekte Schwachstelle, Risikoquelle, Risiko-Szenario und Risikoindexierung soll kurz an einem Beispiel des Alltags veranschaulicht werden:

Beispiel: Falls das Alter der Reifen eines Autos mehr als zehn Jahre beträgt, sind die Reifen eine Schwachstelle des Autos. Solange das Auto etwa nur auf einem Schrottplatz steht, stellen die alten Reifen mit verschlechterten Grip-Eigenschaften kein Risiko dar. Wird das Auto aber gefahren und tritt „Regen“ als Risikoquelle zur Schwachstelle hinzu, so stellt der Sachverhalt „Auto fährt mit alten Reifen im Regen“ ein Risiko-Szenario dar, das hinsichtlich Eintrittswahrscheinlichkeit und prognostizierten Schadensausmaß, also insgesamt mit dem Risikoindex „hoch“ bewertet werden kann.

Ein Risiko im Sinne der DSGVO ist folglich das Bestehen der Möglichkeit des Eintritts eines Szenarios, 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.

Beim Risikomanagement hat ein Risiko grundsätzlich zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.[18]

Bei der hier empfohlenen Risikobewertung werden die Eintrittswahrscheinlichkeit und die Schwere/der Schaden wie folgt abgestuft:

Grad	Bezeichnung des Grads	Eintrittswahrscheinlichkeit	
		Beschreibung	Beispiel
1	geringfügig	Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.	Befall durch Schadsoftware bei einem Stand-Alone Rechner, der an keinem Netzwerk angeschlossen ist und an dem keine weiteren Medien angeschlossen werden können.
2	überschaubar	Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und nur mit einem BSI zertifizierten Firmennetzwerk verbunden ist.
3	substanziell	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und direkt mit dem Internet verbunden ist.
4	groß	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem veralteten Windows-XP Rechner ohne Antivirensoftware, der direkt mit dem Internet verbunden ist.

Abb. 7: Möglicher Grad der Eintrittswahrscheinlichkeit

Grad	Bezeichnung des Grads	Schwere der Folgen / möglicher Schaden	
		Beschreibung	Beispiel
1	geringfügig	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.	**immateriell:** leichte Verärgerung **materiell:** Zeitverlust **physisch:** vorübergehende Kopfschmerzen
2	überschaubar	Betroffene erleiden eventuell signifkante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.	**immateriell:** geringe, aber objektiv nachweisbare psychische Beschwerden **materiell:** deutlich spürbarer Verlust an privatem Komfort **physisch:** minderschwere körperliche Schäden (z. B. leichte Krankheit)
3	substanziell	Betroffene erleiden eventuell signifkante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	**immateriell:** schwere psychische Beschwerden **materiell:** finanzielle Schwierigkeiten **physisch:** schwere körperliche Beschwerden
4	groß	Betroffene erleiden eventuell signifkante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.	**immateriell:** dauerhafte, schwere psychische Beschwerden **materiell:** erhebliche Schulden **physisch:** dauerhafte, schwere körperliche Beschwerden

Abb. 8: Möglicher Grad der Schwere/des Schadens

[18] Vgl. Fn. 2, S. 1.

III. Methode der Risikoanalyse

Die Eintrittswahrscheinlichkeit kann folglich durch die vorliegenden Gegebenheiten, eigene Erfahrungen sowie Erfahrungen anderer und auch durch Statistiken unterstützt werden. Bei Statistiken muss allerdings beachtet werden, unter welchen Randbedingungen sie entstanden sind, da auch Statistiken für einen speziellen Anwendungszweck erstellt worden sind und daher nicht ohne Weiteres auf die speziellen Belange der Institution übertragen werden können. Außerdem ist die Interpretation von statistischen Ergebnissen prinzipiell mit Unsicherheiten behaftet.[19]

Aus den festgelegten Einstufungen für die Eintrittswahrscheinlichkeit und für die Schwere der Auswirkung ergibt sich im Ergebnis folgende Risikomatrix, die im Wesentlichen der Empfehlung der Datenschutzkonferenz folgt:[20]

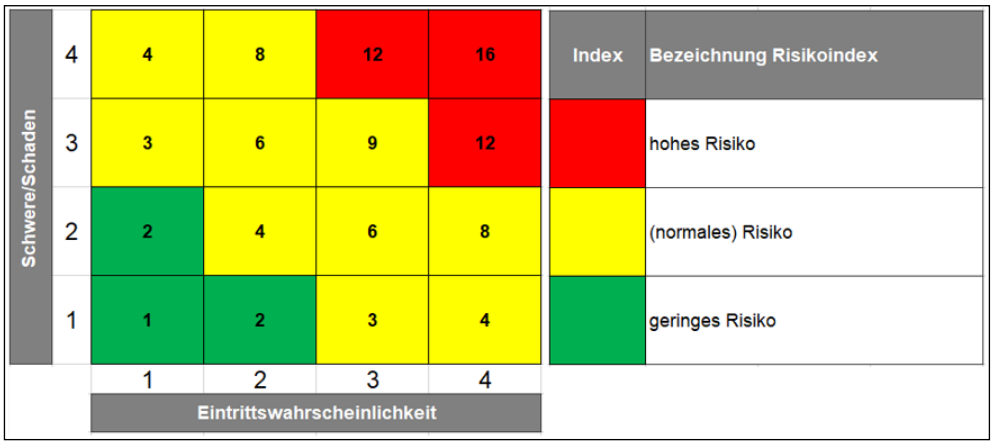


Abb. 9: Risikomatrix und Risikoindex

Für den Risikoindex existieren im Datenschutz genau drei Stufen. Denn die DSGVO kennt die Begriffe „Risiko“ und „hohes Risiko“, wobei „Risiko“ auch als „normales Risiko“ bezeichnet werden kann. Daneben verwendet die DSGVO die Formulierung „voraussichtlich nicht zu einem Risiko“ führend (Art. 27 Abs. 2 Buchst. a und Art. 33 Abs. 1 DSGVO). Da es vollständig risikolose Verarbeitungen nicht geben kann, wird die Formulierung „nicht zu einem Risiko“ von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko“ führend verstanden.[21]

4. Risikoanalyse der SDM-Schutzbedarfsziele

Bei der Risikoanalyse der SDM-Schutzbedarfsziele steht das Risiko im Vordergrund, dass ein fundamentales DSGVO-Prinzip nicht vollständig eingehalten werden kann. Um Vermischun-

[19] Vgl. des BSI-Standard 200-3 (Fn. 11), Kapitel 5.1

[20] Vgl. Datenschutzkonferenz, Risiko für die Rechte und Freiheiten natürlicher Personen (Fn. 2).

[21] Vgl. Fn. 2.

gen mit dem Risikomanagement zu vermeiden, wird im Folgenden von der Gefährdung gesprochen, dass ein Zielerfüllungsgrad von 100% nicht dauerhaft erreicht werden kann. Somit ergibt sich folgendes Bild:

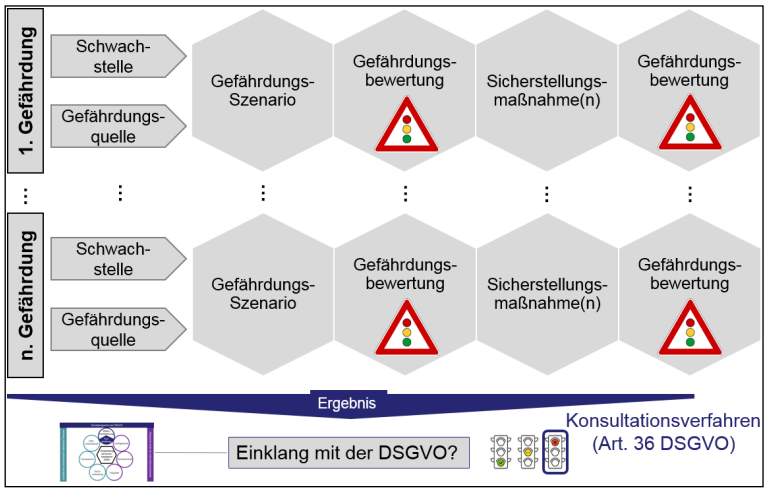


Abb. 10: Risikoanalyse der SDM-Schutzbedarfsziele

Wie in der Risikoanalyse der SDM-Datensicherheitsziele ist das einzelne Gefährdungs-Szenario der eigentliche Gegenstand für die Gefährdungsbewertung. In jedem Szenario wird möglichst differenziert ein Ereignis beschrieben, durch das der betrachtete Verarbeitungsvorgang den normativen DSGVO-Rahmen verlassen würde und das es daher zu vermeiden gilt.

Für eine einfachere Herleitung aller relevanten Gefährdungs-Szenarien dient die Betrachtung der Schwachstellen und der Gefährdungsquellen. Schwachstellen sind dabei als Eigenschaften des betrachteten Verarbeitungsvorgangs definiert, die geeignet sind, bei hinzutreten einer bestimmten Gefährdungsquelle die vollständige Zielerreichung zu verhindern.

Folgende Unterschiede zur Risikoanalyse der SDM-Datensicherheitsziele (vgl. Abb. 6: Risikoanalyse der SDM-Datensicherheitsziele) sind erkennbar:

- **1 Gefährdung**
  Anstelle einzelner Risiken werden im Abstrahierungsgrad grundsätzlich frei wählbare Gefährdungen der SDM-Schutzbedarfsziele betrachtet. Naheliegend für das SDM-Gewährleistungsziel „Intervenierbarkeit“ wäre etwa ein Gefährdungsprofil, das sich aus den Gefährdungen im Hinblick auf die einzelnen DSGVO-Betroffenenrechte (Auskunft, Löschung, Berichtigung usw.) zusammensetzt.

- **2 Gefährdungsbewertung**
  Die Gefährdungsbewertung, ebenfalls in Ampelfarbe kodiert, kann abgestuft folgende Ergebnisse haben:

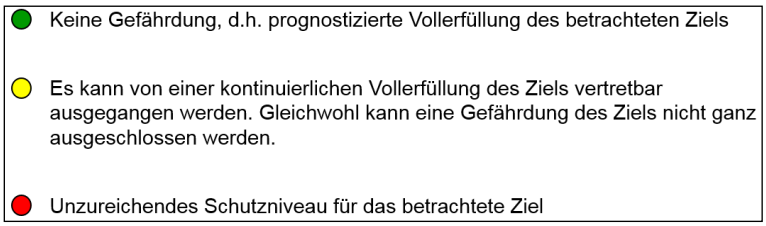


Abb. 11: Mögliche Ergebnisse der Gefährdungsbewertung

▶ **3 Sicherstellungsmaßnahme**

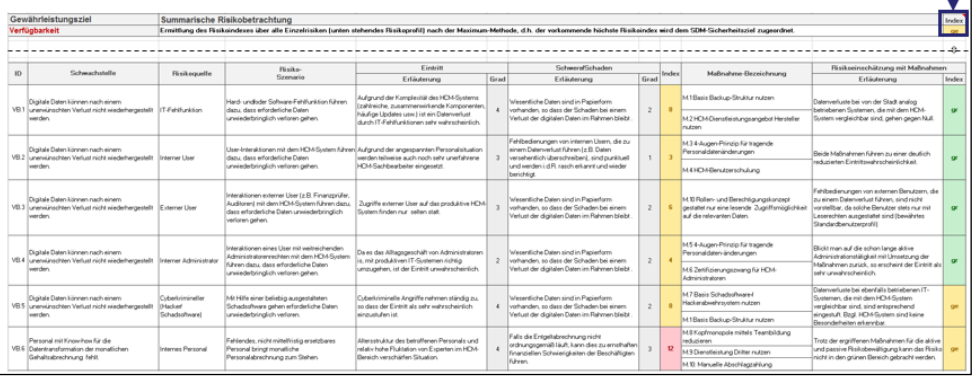
Anstelle des Begriffs „Abhilfemaßnahme" wird hier der Begriff „Sicherstellungsmaßnahme" verwendet. Aus der unterschiedlichen Maßnahmenbezeichnung soll nur hervorgehen, dass im Kontext des Zielerfüllungsmanagements die Maßnahmen dazu dienen, die vollständige Erfüllung des betroffenen Ziels lückenlos sicherzustellen. Da beim klassischen Risikomanagement die Maßnahmen das Einzelrisiko auf ein vertretbares Maß reduzieren bzw. ganz beseitigen, wurden die Maßnahmen dort – wie in der DSGVO – als Abhilfemaßnahmen bezeichnet. Letztendlich dienen beide Maßnahmentypen dem gleichen Ziel, als TOMs das Risiko für die Rechte und Freiheiten natürlicher Personen im Rahmen der DSGVO zu halten.

Die Aspekte Schwachstelle, Gefährdungsquelle und Gefährdungs-Szenario besitzen die gleiche Grundbedeutung wie unter Punkt III. 3. dargestellt.

5. Durchführung der Gesamtbewertung

Jedes SDM-Gewährleistungsziel (siehe Abb. 5: Die SDM-Schutzbedarfs- und die SDM-Datensicherheitsziele mit jeweiligen Risikoanalysemethoden) besitzt nach Durchführung der Risikoanalysen mehrere bewertete Einzelrisiken (SDM-Datensicherheitsziele) bzw. mehrere bewertete Gefährdungen (SDM-Schutzbedarfsziele). Wie in der folgenden Abbildung dargestellt, werden die einzelnen Bewertungen in der Form auf das jeweilige SDM-Gewährleistungsziel aufsummiert, indem der höchste Risikoindex bzw. die höchste Gefährdungsbewertung für das Gesamtergebnis des SDM-Ziels übernommen wird (sog. Maximum-Ansatz):

Jedes einzelne SDM-Gewährleistungsziel wird auf der Basis eines Risikos- bzw. Gefährdungsprofil summarisch in Ampelfarben bewertet. Die summarische Gesamtbewertung über alle Einzelbewertungen der SDM-Gewährleistungsziele beantwortet zusammen mit den anderen Angaben, ob die betrachtete Verarbeitung im „Einklang mit der DSGVO“ steht.



Gewährleistungsziel	Summarische Risikobetrachtung	Index
Verfügbarkeit	Ermittlung des Risikoindexes über alle Einzelrisiken (unten stehendes Risikoprofil) nach der Maximum-Methode, d.h. der vorkommende höchste Risikoindex wird dem SDM-Sicherheitsziel zugeordnet.	

ID	Schwachstelle	Risikoquelle	Risiko-Szenario	Eintritt		SchwereSchaden		Index	Maßnahme-Bezeichnung	Risikoeinschätzung mit Maßnahmen	
				Erläuterung	Grad	Erläuterung	Grad			Erläuterung	Index
VB.1	Digitale Daten können nach einem unerwünschten Verlust nicht wiederhergestellt werden.	IT-Fehlfunktion	Hard- und/oder Software-Fehlfunktion führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Aufgrund der Komplexität des HDM-Systems (zahlreiche, zusammenwirkende Komponenten, häufige Updates usw.) ist ein Datenverlust durch IT-Fehlfunktionen sehr wahrscheinlich.	4	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt.	2	8	M.1 Basis Backup-Struktur nutzen M.2 HDM-Dienstleistungsangebot Hersteller nutzen	Datenverluste bei von der Stadt analog betriebenen Systemen, die mit dem HDM-System vergleichbar sind, gehen gegen Null.	gr
VB.2	Digitale Daten können nach einem unerwünschten Verlust nicht wiederhergestellt werden.	Interner User	User-Interaktionen mit dem HDM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Aufgrund der angespannten Personalsituation werden teilweise auch noch sehr unerfahrene HDM-Sachbearbeiter eingesetzt.	3	Fehlbedienungen von internen Usern, die zu einem Datenverlust führen (z.B. Daten versehentlich überschrieben), sind punktuell und werden i.d.R. rasch erkannt und wieder berichtigt.	1	3	M.3 4-Augen-Prinzip für tragende Personaldatenänderungen M.4 HDM-Benutzerschulung	Beide Maßnahmen führen zu einer deutlich reduzierten Eintrittswahrscheinlichkeit.	gr
VB.3	Digitale Daten können nach einem unerwünschten Verlust nicht wiederhergestellt werden.	Externer User	Interaktionen externer User (z.B. Finanzprüfer, Auditoren) mit dem HDM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Zugriffe externer User auf das produktive HDM-System finden nur selten statt.	3	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt.	2	6	M.10 Rollen- und Berechtigungskonzept gestattet nur eine lesende Zugriffsmöglichkeit auf die relevanten Daten.	Fehlbedienungen von externen Benutzern, die zu einem Datenverlust führen, sind nicht vorstellbar, da solche Benutzer stets nur mit Leserechten ausgestattet sind (bewährtes Standardbenutzerprofil)	gr
VB.4	Digitale Daten können nach einem unerwünschten Verlust nicht wiederhergestellt werden.	Interner Administrator	Interaktionen eines User mit weitreichenden Administratorenrechten mit dem HDM-System führen dazu, dass erforderliche Daten unwiederbringlich verloren gehen.	Da es das Alltagsgeschäft von Administratoren is, mit produktiven IT-Systemen nichtig umzugehen, ist der Eintritt unwahrscheinlich.	2	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt.	2	4	M.5 4-Augen-Prinzip für tragende Personaldaten-änderungen M.6 Zertifizierungszwang für HDM-Administratoren	Blickt man auf die schon lange aktive Administrationstätigkeit mit Umsetzung der Maßnahmen zurück, so erscheint der Eintritt als sehr unwahrscheinlich.	gr
VB.5	Digitale Daten können nach einem unerwünschten Verlust nicht wiederhergestellt werden.	Cyberkrimineller (Hacker/ Schadsoftware)	Mit Hilfe einer beliebig ausgestalteten Schadsoftware gehen erforderliche Daten unwiederbringlich verloren.	Cyberkriminelle Angriffe nehmen ständig zu, so dass der Eintritt als sehr wahrscheinlich einzustufen ist.	4	Wesentliche Daten sind in Papierform vorhanden, so dass der Schaden bei einem Verlust der digitalen Daten im Rahmen bleibt.	2	8	M.7 Basis Schadsoftware/ Hackerabwehrsystem nutzen M.1 Basis Backup-Struktur nutzen	Datenverluste bei ebenfalls betriebenen IT-Systemen, die mit dem HDM-System vergleichbar sind, sind entsprechend eingestuft. Bzgl. HDM-System sind keine Besonderheiten erkennbar.	gr
VB.6	Personal mit Know-how für die Datentransformation der monatlichen Gehaltsabrechnung fehlt.	Internes Personal	Fehlendes, nicht mittelfristig ersetzbares Personal bringt monatliche Personalabrechnung zum Stehen.	Altersstruktur des betroffenen Personals und relativ hohe Fluktation von Experten im HDM-Bereich verschärfen Situation.	4	Falls die Entgeltabrechnung nicht ordnungsgemäß läuft, kann dies zu ernsthaften finanziellen Schwierigkeiten der Beschäftigten führen.	3	12	M.8 Kopfmonopole mittels Teambildung reduzieren M.9 Dienstleistung Dritter nutzen M.10 Manuelle Abschlagszahlung	Trotz der ergriffenen Maßnahmen für die aktive und passive Risikobewältigung kann das Risiko nicht in den grünen Bereich gebracht werden.	gr

Abb. 12: Ermittlung der Bewertung eines SDM-Gewährleistungsziels mittels des Maximum-Ansatzes

Um einen Zweifel an der gleichen Aussagekraft der Ergebnisse der beiden verwendeten Methoden (Risikomanagement für die SDM-Datensicherheitsziele und Zielerfüllungsmanagement für die SDM-Schutzziele) erst gar nicht aufkommen zu lassen, sollten die Bewertungsergebnisse der beiden unterschiedlichen Methoden nicht mittels des Maximal-Ansatzes „zusammengerechnet“ werden.

IV. Bausteine einer Risikoanalyse

Werden die Bausteine der beiden Methoden Risikomanagement und Zielerfüllungsmanagement übereinander gelegt und miteinander verglichen, so ergeben sich schematisch die Gemeinsamkeiten, wie sie in der folgenden Abbildung dargestellt sind.

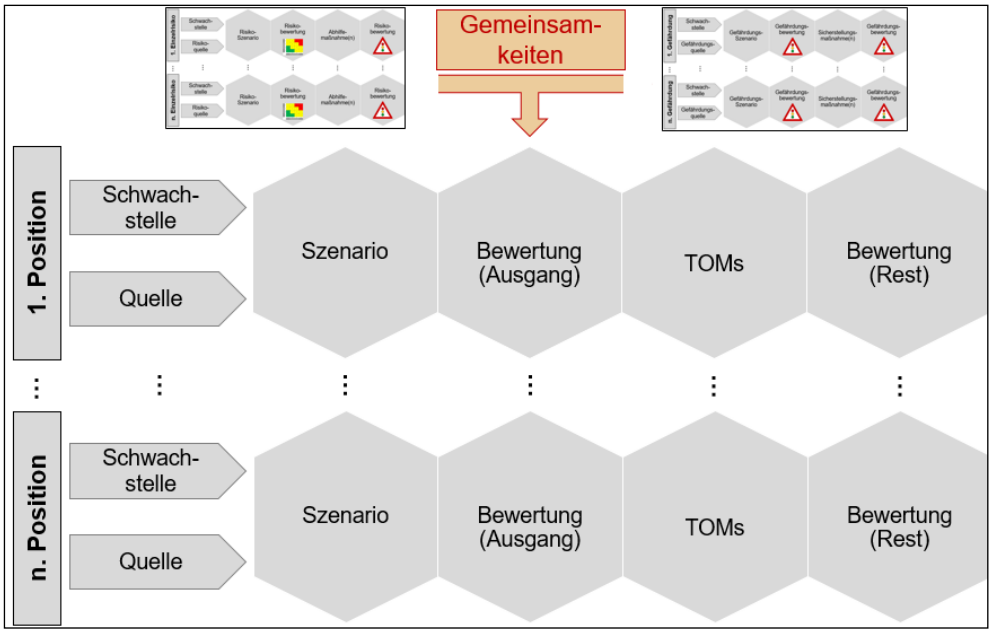


Abb. 13: Elementare Bausteine einer datenschutzrechtlichen Risikoanalyse

Zu jedem relevanten Einzelrisiko bzw. Einzelgefährdung werden somit erfasst:

- die Schwachstelle, die dem Szenario zugrunde liegt,
- die Quelle(n), die zusammen mit der Schwachstelle das konkret betrachteten Szenario verursacht/en,
- das Szenario, also das Ereignis oder der Zustand, der bei der Verarbeitung zu vermeiden ist,
- die Bewertung des einzelnen Szenarios ohne die Berücksichtigung von TOMs (→Ausgangsrisiko[22] bzw. →Ausgangsgefährdung),
- die geplanten und vor Durchführung der Zielverarbeitung wirksam umgesetzten TOMs, die das Ausgangsrisiko bzw. die Ausgangsgefährdung auf ein vertretbares und angemessenes Niveau reduzieren, sowie

[22] Siehe Datenschutzkonferenz, Risiko für die Rechte und Freiheiten natürlicher Personen (Fn. 2).

– die Bewertung des einzelnen Szenarios, bei der die wirksame Umsetzung der zugeordneten TOMs unterstellt wird (Restrisiko bzw. Restgefährdung).

Vor diesem Hintergrund werden die elementaren Bausteine einer Risikoanalyse genauer beschrieben.

1. Schwachstelle

Bei Verarbeitungsvorgängen, die durch IT-Systeme unterstützt werden, existieren typische Schwachstellen, die sich für eine generelle Betrachtung anbieten. Schwachstellen sind dabei als Eigenschaften des betrachteten Verarbeitungsvorgangs definiert, die geeignet sind, bei hinzutreten einer bestimmten Quelle eine Schadwirkung für die Rechte und Freiheiten natürlicher Personen zu entfalten. Diese Schwachstellen können den SDM-Gewährleistungszielen wie folgt zugeordnet werden.

a) Verfügbarkeit

Hinsichtlich der Verfügbarkeit („personenbezogene Daten müssen relevante Geschäftsprozesse ermöglichen!“) sind insbesondere die beiden folgenden Schwachstellen relevant.

– **Datenverlust.** – In IT-Systemen können – wie auch in der papiergebundenen Bearbeitung – personenbezogene Daten unerwünscht verloren gehen.

– **Störung von Ressourcen.** – Jeder Verarbeitungsvorgang benötigt für seine Durchführung Ressourcen, das heißt menschliches Tätigwerden und/oder technische Unterstützung, insbesondere in der Form von Betriebsmitteln. Diese Abhängigkeit von Ressourcen ist oft Ursache dafür, dass schon bei einem Fehler oder einer sonstigen Störung von nur einer Ressource der Verarbeitungsvorgang eingeschränkt oder überhaupt nicht mehr durchgeführt werden kann. In der Vergangenheit konnte nicht selten beobachtet werden, dass ein kleinerer Fehler oder Störung die gesamte Zielverarbeitung für einen längeren Zeitraum lahmlegte. Diese Anfälligkeit gegenüber Fehlern und sonstigen Störungen ist teilweise auf die immer noch wachsende Komplexität von IT-Systemen zurückzuführen. Daher lohnt sich der Blick auf Einzelressourcen, die typischerweise zu berücksichtigen sind (siehe Abbildung 14).

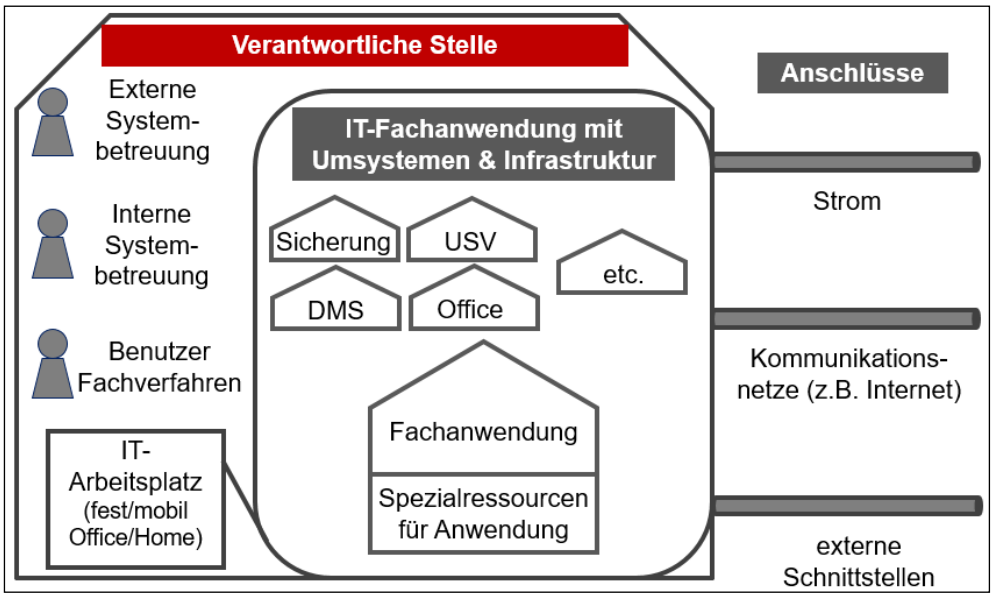


Abb. 14: Typische Ressourcen bei einer IT-unterstützten Verarbeitung

Die IT-Fachanwendung (z. B. Personalwirtschafts-, Finanzwirtschafts- oder Beihilfesystem) steht regelmäßig im Mittelpunkt der Betrachtung und ist mit anderen IT-Anwendungen sowie weiteren IT-Systemen verbunden. Dabei bestehen insbesondere Verbindungen und Schnittstellen zu allgemeinen IT-Anwendungen (siehe Punkt V. 1. a), z. B. Office-Anwendungen, Dokumentenmanagementsystem [DMS], elektronische Akte) und zur IT-Infrastruktur (z. B. internes Netzwerk, Datensicherung, unterbrechungsfreie Stromversorgung [USV], Firewall). Daneben kann eine IT-Fachanwendung auch bei Bedarf auf für sie eingerichtete Spezialsysteme (z. B. Spezial-Scanner und -Drucker) zugreifen.

IT-Systeme haben zudem Personen, die sie nutzen und betreuen. Der Zugriff auf die IT-Systeme erfolgt grundsätzlich über die eingerichteten IT-Arbeitsplätze. Da IT-Systeme zum Beispiel nicht ohne elektrischen Strom auskommen und in aller Regel auch mit der Außenwelt – etwa über das Internet – vernetzt sind, sind die verwendeten Anschlüsse ebenfalls zu berücksichtigen.

b) Vertraulichkeit

Schwachstellen für die Vertraulichkeit (Kenntnis und Weitergabe von personenbezogenen Daten nur für befugte Personen) stellen in der Praxis zumeist einen Schwerpunkt der Betrachtung dar. Auch in diesem Bereich können typische Schwachstellen unter die folgenden vier Gesichtspunkte subsumiert werden.

– **Arbeitsplatz.** – Personenbezogene Daten können über den Arbeitsplatz unbefugt verarbeitet werden, indem beispielsweise der Rechner am Arbeitsplatz erfolgreich durch eine Schadsoftware angegriffen wird oder am Arbeitsplatz abgelegte Unterlagen unbefugt eingesehen werden.

- **Datenübermittlung.** – Personenbezogene Daten können über digitale Schnittstellen, physikalischen Transport oder mündlich übermittelt und dabei von unbefugten Personen verarbeitet werden.
- **Datenauslagerung.** – Digitale personenbezogene Daten können aus dem IT-System, in dem die fachliche Verarbeitung laufend durchgeführt wird, auch ohne Übermittlungsabsicht exportiert und ausgelagert werden (z. B. Datenausdruck auf Papier oder Export auf digitale Medien, wie etwa Datensicherungsbänder, USB-Stick, Laptop und Log-Datei) und danach durch Zugriff auf den Auslagerungsort unbefugt verarbeitet werden.
- **Direktzugriff auf technischen Speicherort.** – Unbefugte Personen können einen bestehenden Zugriffsschutz umgehen und mittels des damit erlangten direkten Zugriffs auf den technischen Speicherort (z. B. Datenbank) personenbezogene Daten verarbeiten.

c) Integrität

aa) Datenintegrität

Die Datenintegrität („personenbezogene Daten nur rechtskonform ändern!“) kann insbesondere aufgrund folgender Schwachstellen verletzt werden.

- **Änderung Dokument.** – Digitale Dokumente mit personenbezogenen Daten können – wie papiergebundene Dokumente – unerwünscht geändert werden.
- **Änderung Datensatz.** – Bei der Bearbeitung eines einzelnen Datensatzes können digitale personenbezogene Daten unerwünscht geändert werden.
- **Änderungsabfrage.** – Durch eine einzelne Änderungsabfrage können massenhaft digitale personenbezogene Daten unerwünscht geändert werden.
- **Änderung Datenformat.** – Durch die Änderung eines Datenfeld-Formats können digitale personenbezogene Daten unerwünscht und massenhaft geändert werden.
- **Darstellung berechneter Daten.** – Datenabfragen mit integrierten Berechnungen können fehlerhaft sein, ohne dass die ausgewertete Datenbasis selbst unerwünscht verändert wurde (z. B. Formel, die auf Basis des gespeicherten Geburtsdatums das Lebensalter zu einem bestimmten Zeitpunkt im Rahmen einer Datenabfrage berechnet, ist fehlerhaft).

bb) Konzepteinhaltung

Die Anforderung, dass Prozesse und IT-Systeme die für sie gültigen Vorgaben kontinuierlich einhalten (Gleichklang von Betrieb als „Ist“ und der Konzeption als „Soll“), führt zu folgenden Schwachstellen.

- **Einhaltung der Vorgaben.** – Die Prozesse und sie unterstützende IT-Systeme, welche die Verarbeitung der personenbezogenen Daten unterstützen, können von den einschlägigen Vorgaben unerwünscht abweichen.

- **Aktualität der Konzepte.** – Die einschlägigen Vorgaben für die Prozesse und sie unterstützende IT-Systeme, die für die Verarbeitung der personenbezogenen Daten genutzt werden, können veralten und damit nicht mehr gültig sein.

cc) Richtigkeit

Für die Anforderung, dass die von einer Verarbeitung betroffenen personenbezogenen Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen, sind folgende Schwachstellen von Relevanz.

- **Sachliche Richtigkeit.** – Daten können nicht den sachlichen Anforderungen an die Richtigkeit entsprechend erhoben und weiter verarbeitet werden.
- **Aktualität.** – Notwendige Änderungen von personenbezogenen Daten können unberücksichtigt bleiben und dadurch zu einer unerwünschten Alterung von personenbezogenen Daten führen.
- **Unvollständigkeit.** – Unvollständige personenbezogene Daten können dann unrichtig sein, wenn durch das Fehlen die Verarbeitung nicht ordnungsgemäß durchgeführt werden kann.
- **Falsche Metadaten.** – Metadaten können die richtige Interpretation von personenbezogenen Daten verhindern, beispielsweise können Feld- und Spaltenbezeichnungen für die personenbezogenen Daten bei deren Darstellung falsch sein.

d) Datenminimierung

Der wichtige Grundsatz, dass nur die für die Zielverarbeitung erforderlichen personenbezogenen Daten verarbeitet werden dürfen (Datensparsamkeit), kann durch zwei Schwachstellen konterkariert werden.

- **Datenüberhang.** – Es können personenbezogene Daten verarbeitet werden, deren Verarbeitung von vornherein nicht erforderlich ist.
- **Fehlende Datenlöschung.** – Es können personenbezogene Daten verarbeitet werden, die insbesondere seit dem schon erfolgten Wegfall oder der Erreichung des Verarbeitungszwecks bereits gelöscht sein müssten.

e) Intervenierbarkeit

Betroffenen Personen müssen die ihnen zustehenden Datenschutzrechte bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden. Schwachstellen sind demnach in der Verhinderungsmöglichkeit der Rechtsausübung zu suchen.

- **Auskunft.** – Betroffene Personen können ihr Recht auf Auskunft nicht wahrnehmen (Art. 15 DSGVO).
- **Berichtigung.** – Betroffene Personen können ihr Recht auf Berichtigung nicht wahrnehmen (Art. 16 DSGVO).

- **Löschung.** – Betroffene Personen können ihr Recht auf Löschung nicht wahrnehmen (Art. 17 Abs. 1 DSGVO).
- **Einschränkung.** – Betroffene Personen können ihr Recht auf Einschränkung der Verarbeitung nicht wahrnehmen (Art. 18 DSGVO).
- **Datenübertragbarkeit.** – Betroffene Personen können ihr Recht auf Datenübertragbarkeit nicht wahrnehmen (Art. 20 DSGVO beachte Art. 20 III S. 2 DSGVO für öffentliche Stellen).
- **Widerspruch.** – Betroffene Personen können ihr Recht auf Widerspruch nicht wahrnehmen (Art. 21 Abs. 1 Satz 1 DSGVO).
- **Automatisierte Entscheidung.** – Betroffene Personen können ihr Recht auf Abwehr automatisierter Entscheidungen im Einzelfall nicht wahrnehmen (Art. 22 DSGVO).
- **Benachrichtigung.** – Betroffene Personen werden vom Verantwortlichen trotz bestehender Pflicht nicht benachrichtigt (Art. 34 DSGVO).

f) Transparenz

Ein Verarbeitungsvorgang muss für die betroffenen Personen als solcher erkennbar, nachvollziehbar und prüfbar sein. Aus dieser Anforderung können folgende Schwachstellen abgeleitet werden.

- **Information.** – Die Informationspflichten nach Art. 13, 14 DSGVO werden nicht (vollständig) erfüllt.
- **Dokumentationslücke.** – Die Dokumentationspflichten werden nicht (vollständig) erfüllt, das heißt insbesondere kann nicht (vollständig) dargelegt werden, welche Daten zu welchem Zweck durch welche Betriebsmittel mit welcher Verantwortlichkeit und mit welchen Empfängern verarbeitet werden.
- **Geschäftsprozess.** – Datenschutzrechtlich relevante Aspekte des Geschäftsprozesses, in dem der Verarbeitungsvorgang integriert ist, sind nicht hinreichend bekannt bzw. nicht ausreichend dokumentiert.

g) Nichtverkettung

Im Hinblick auf die Nichtverkettung existiert die Schwachstelle, dass personenbezogene Daten rechtswidrig für andere als für den Verarbeitungsvorgang festgelegte Zwecke verarbeitet werden können.

2. Risiko- und Gefährdungsquellen

Risiko- und Gefährdungsquellen sind insbesondere Akteure oder Umweltereignisse, die aufgrund einer der Zielverarbeitung innewohnenden Schwachstelle zu einem unerwünschten

Szenario führen können. Somit sind Quellen zum einen als „Angriffe auf den Verarbeitungsvorgang“ durch Personen (z. B. Straftäter, Besucher, Beschäftigte des Verantwortlichen) oder durch die Umwelt (z. B. Unwetter, Überschwemmung, Streiks) zu verstehen. Zum anderen können Quellen aber auch nur Fehler sein, bei denen Menschen oder Technik von den einschlägigen Vorgaben abweichen; auf den Vorsatz von Individuen kommt es dabei nicht an. Auch die Möglichkeit einer bloßen Unbedachtheit kann zu berücksichtigen sein.

Zusammenfassend können Risiko- bzw. Gefährdungsquellen, wie in der folgenden Abbildung gezeigt, systematisch strukturiert werden. Dabei bezieht sich das Strukturierungsmerkmal der „Einflussnahme“ darauf, wie einfach der Verantwortliche das menschliche Verhalten der genannten Personengruppen grundsätzlich beeinflussen kann.

		Risiko-/Gefährdungsquellen:
Menschliches Verhalten	Hohe Einflussnahme	- Personal (Verantwortlicher; Führungskraft; Sachbearbeitung usw.) - IT-User (Interner/Externer User; Administrator/Anwender/Entwickler usw.) - Dienstleister (Auftragsverarbeiter; Lieferant; Reinigungsdienst usw.) - Besucher
	Geringe Einflussnahme	- Externer Vorgangsbeteiligter (Bürger/Wirtschaft; Antragsteller usw.) - Dritter (Empfänger Falschversand; Finder; Strafverfolgung usw.) - Straftäter (Cyberkrimineller; Einbrecher; Dieb usw.)
Umwelt	IT-Gesamtsystem	IT-Fehlfunktion (Software-/Hardwarefehler; Hitze/Kälte/Staub usw.)
	Elemente	- Wasser - Feuer - Blitz - Sturm - Erdbeben
	Anschlüsse	- Strom - Internet
	Weitere Umwelteinflüsse	- Großereignis - Naturkatastrophe

Abb. 15: Systematische Strukturierung der Quellen

Im Bereich „menschliches Verhalten“ können die Quellen noch detaillierter unterteilt und beschrieben werden. In diesem Bereich können durch eine weitergehende Analyse der verschiedenen Angreiferkategorien (z. B. Straftäter, interner Mitarbeiter, Besucher, Geheimdienst) verschiedene Aspekte dieser Kategorien, wie etwa „Attraktivität eines unbefugten Datenzugriffs“ und „zur Verfügung stehende Ressourcen“, in einem sogenannten Angreifermodell vertieft dargestellt und Rückschlüsse auf das bei diesen Quellen bestehende Risiko hergeleitet werden. Ein Angreifer ist dabei eine Institution oder Person, welche absichtlich eine unbefugte Verarbeitung anstrebt, die beim beabsichtigten Erfolg zur Verletzung der Sicherheit der Verarbeitung führt. Ein Angreifermodell beschreibt daher neben den Attributen angenommener Angreifer insbesondere auch die zu erwartenden Angriffswerkzeuge und -modalitäten.

3. Szenario

Ein Szenario kann während der Durchführung der Zielverarbeitung eintreten und ist die Beschreibung für ein denkbares Ereignis oder einen denkbaren Zustand. Jedes Szenario führt zu einer (zeitweisen) Nichterfüllung von DSGVO-Anforderungen hinsichtlich der Art und

Weise der Verarbeitung und ist daher im Zusammenhang mit der Zielverarbeitung unerwünscht und zu vermeiden. Beim Eintritt eines Szenarios liegt regelmäßig ein Datenschutzverstoß mit potenziellen Schaden für betroffene Personen vor, der je nach seiner konkreten Ausprägung auch eine meldepflichtige Verletzung des Schutzes personenbezogener Daten sein kann (vgl. Art. 33 DSGVO).

Das Szenario ohne Berücksichtigung von TOMs ist Gegenstand für die Bewertung des Ausgangsrisikos. Das Szenario mit den hierzu wirksam umgesetzten TOMs ist Gegenstand für die Bewertung des Restrisikos (siehe Punkt IV. 4.).

Nach dem Erfahrungssatz „Gefahr erkannt – Gefahr gebannt" ist unverzichtbar, dass alle für den Zielvorgang relevanten Szenarien identifiziert und einer anschließenden Bewertung zugeführt werden. In der Vergangenheit haben diverse Datenpannen gezeigt, dass nicht selten einzelne Szenarien, die vom Verantwortlichen übersehen wurden und damit nicht mit geeigneten TOMs abgesichert waren, später Ursache für einen schwerwiegenden Datenschutzverstoß waren.

Für eine systematische Herleitung von relevanten Szenarien dient die Betrachtung der Schwachstellen und der Quellen als Arbeitshilfe. Das Zusammenspiel der drei Aspekte Schwachstelle, Quelle und Szenario soll kurz an einem Beispiel des Alltags veranschaulicht werden.

Beispiel: Das Dach eines Hauses hat eine begrenzte Dachtraglast, die als generelle Schwachstelle von Häusern verstanden werden kann. Nur wenn starker Schneefall oder Sturm als mögliche Quellen hinzukommen und auf diese Schwachstelle einwirken, ergibt sich das Szenario „Dach stürzt wegen zu großer Schnee- bzw. Windlast ein." Die Bewertung des Ausgangsrisikos für dieses Szenario wird insbesondere nach der geografischen Lage des Hauses unterschiedlich ausfallen und kann etwa mit der Maßnahme reduziert werden, dass ab einer bestimmten Schneelast der Schnee vom Dach entfernt wird.

Durch die Kombination der unter Punkt IV. 1. aufgeführten Schwachstellen mit den unter Punkt IV. 2. genannten Quellen können systematisch Szenarien gebildet und deren Relevanz bezüglich des Zielvorgangs anschließend beurteilt werden.

Beispiel: So können sich beispielsweise zur **Schwachstelle „Datenverlust"** durch Kombination unterschiedlicher Quellen folgende Szenarien ergeben:

- **Benutzer** überschreibt unerwünscht bei der Datensatzbearbeitung ein Datum, das dadurch verloren geht.
- **Schadsoftware** verschlüsselt personenbezogene Daten, so dass diese nicht mehr zugreifbar sind.
- **Administrator** (interner Beschäftigter/Dienstleister) wechselt im zentralen elektronischen Datenspeichersystem (Network Attached Storage-/NAS-System) einen falschen Datenträger aus, wodurch Daten verloren gehen.

Die Detaillierung und Granularität der Szenarien sollten sich insbesondere an dem verbundenen Ausgangsrisiko und der vorliegenden Verarbeitungskomplexität orientieren. Somit können Zielverarbeitungen unterschiedliche Analyseschwerpunkte erfordern.

Beispiel: Ist für eine Zielverarbeitung etwa eine einfach operationalisierbare und kurze Aufbewahrungsfrist zu beachten, wodurch eine automatisierte Löschung als TOM einfach umsetzbar ist, muss das Gewährleistungsziel „Datenminimierung" in dieser Hinsicht nicht so vertieft behandeln werden wie bei einer Zielverarbeitung mit einem komplexen, teilweise mit manuellen Tätigkeiten ausgestalteten Löschkonzept und langer Speicherdauer.

Die Strukturierung und Sortierung der Szenarien ist mit besonderer Rücksicht auf die gegebene Komplexität, die Verständlichkeit sowie die Transparenz zu wählen. So kann sich die Struktur der Szenarien orientieren

- an den Gewährleistungszielen,
- bei Verarbeitungsvorgängen, die sich aus wichtigen, gut abgrenzbaren Teilverarbeitungsvorgängen zusammensetzen, an diesen Teilverarbeitungsvorgängen oder
- absteigend an der Höhe der bestehenden Ausgangsrisiken.

Bei einer Strukturierung der Szenarien nach den Gewährleistungszielen ist zu beachten, dass nicht alle Szenarien sich auf genau einen Bereich eines Gewährleistungsziels abbilden lassen. Vielmehr gibt es Szenarien, die mehreren Gewährleistungszielen gleichzeitig zugeordnet werden können.

Beispiel: Ein erfolgreicher Schadsoftware-Angriff kann sowohl Auswirkungen auf die Vertraulichkeit, Verfügbarkeit und Datenintegrität haben. In einem solchen Fall sollte das betroffene Einzelszenario nur einmal in der Risikoanalyse gegebenenfalls mit entsprechenden Verweisungen behandelt werden, um insbesondere die Gefahr von Inkonsistenzen und von unnötiger Komplexität in der Risikoanalyse zu vermeiden (siehe Punkt VI. 3. a) bb)).

Bei den unterschiedlich denkbaren Strukturierungen der Szenarien wird jedoch die Trennung der Szenarien nach ihrer jeweiligen Bewertungsmethode (z. B. Risiko- und Zielerfüllungsmanagement) in aller Regel durchgehend erhalten bleiben.

4. Bewertung der Risiken

Gegenstand einer einzelnen Risikobewertung ist ein Szenario, für welches das Risiko abgeschätzt wird. Dabei wird das Szenario zum einen ohne Berücksichtigung der TOMs als sogenanntes Ausgangsrisiko und zum anderen mit Berücksichtigung der TOMs als sogenanntes Restrisiko bewertet.[23] Mögliche Methoden für die Ermittlung dieser beiden Risiken wurden schon unter den Punkten III. 3. und III. 4. vorgestellt.

Arten einer datenschutzrechtlichen Risikobewertung können folgendermaßen unterschieden werden (die Risikobewertung im Rahmen einer DSFA-Erforderlichkeitsprüfung, siehe Punkt VII. 2., ist einbezogen):

[23] Siehe Datenschutzkonferenz, Risiko für die Rechte und Freiheiten natürlicher Personen (Fn. 2).

Risiko-Art	Input	Methode	Risikostufe	Zweck
Schwellwert-risiko	Verarbeitungs-vorgang (abstrakt)	DSFA-Kriterien	Hoch Nicht hoch	DSFA-Erforderlichkeit
Ausgangs-risiko	Szenario ohne Schutzmaßnahmen	Risiko- oder Zielerfüllungs-management	Hoch Normal Gering	Bedarf Schutz-maßnahmen identifizieren
Restrisiko	Szenario mit wirksamen Schutzmaßnahmen	Risiko- oder Zielerfüllungs-management	Hoch Normal Gering	Angemessenes Schutzniveau gewährleisten

Abb. 16: Unterscheidung wichtiger Risiko-Arten mit ihren Eigenschaften

Das Schwellwertrisiko wird grundsätzlich im Rahmen der DSFA-Erforderlichkeitsprüfung (siehe Punkt VII. 2.) ermittelt und hat als Analysegegenstand einen Verarbeitungsvorgang, der relativ abstrakt und losgelöst von Schutzmaßnahmen betrachtet wird. Die Methode der „DSFA-Kriterien" zur Ermittlung, ob bei diesem Verarbeitungsvorgang ein hohes Risiko vorliegt, wird nicht in dieser Arbeitshilfe, sondern in den Leitlinien[24] beschrieben und ausführlich in meiner Orientierungshilfe „Datenschutz-Folgenabschätzung" für die bayerischen öffentlichen Stellen erläutert und konkretisiert.[25]

5. Technische und organisatorische Maßnahmen (TOMs)

Erst durch die wirksame Umsetzung der TOMs, die durch die Risikoanalyse ermittelt wurden, wird für die Zielverarbeitung ein dem Risiko angemessenes Schutzniveau gewährleistet. TOMs reduzieren Risiken auf ein angemessenes Niveau bzw. gewährleisten, dass Gewährleistungsziele dauerhaft erfüllt werden. Im Datenschutz ist nur eine Risikoreduktion bis hin zu angemessenen Restrisiken oder Risikovermeidung, also insbesondere kein Transfer von Risiken – etwa auf Versicherungen – möglich.

Obwohl die Auswahl potenzieller TOMs für viele, insbesondere auch die IT-Sicherheit betreffende Bereiche groß ist, bleibt die besondere Herausforderung, für eine konkrete Zielverarbeitung risikoorientiert effektive Einzelmaßnahmen zu identifizieren und einen geeigneten Abstrahierungsgrad für das Maßnahmenprofil zu finden.

Da das wesentliche Ziel der datenschutzrechtlichen Risikoanalyse darin besteht, auf Basis der gewonnenen Erkenntnisse geeignete TOMs nachhaltig umzusetzen, werden weitere Aspekte zu den TOMs ihrer Bedeutung entsprechend im nächsten Kapitel behandelt.

[24] Siehe Fn. 8.

[25] Die Orientierungshilfe ist auf https://www.datenschutz-bayern.de in der Rubrik „DSFA" abrufbar.

V. Systematik der TOMs

TOMs sind an verschiedenen Stellen der DSGVO verankert. So finden sich an folgenden Stellen Aussagen dazu:

- Art. 5 Abs. 1 Buchst. f DSGVO „Grundsätze für die Verarbeitung personenbezogener Daten“,
- Art. 24 DSGVO „Verantwortung des für die Verarbeitung Verantwortlichen“,
- Art. 25 DSGVO „Datenschutz durch Technikgestaltung und durch datenschutz-freundliche Voreinstellungen“,
- Art. 32 DSGVO „Sicherheit der Verarbeitung“,
- Art. 35 DSGVO „Datenschutz-Folgenabschätzung“ und
- Art. 36 DSGVO „Vorherige Konsultation“.

Nach diesen Vorgaben müssen TOMs durch den Verantwortlichen und/oder den Auftragsverarbeiter wirksam umgesetzt werden und sind dazu bestimmt, dauerhaft ein dem Risiko angemessenes Schutzniveau bei jeder Verarbeitung personenbezogener Daten zu gewährleisten. Damit die TOMs dieser Bestimmung nachkommen können, müssen sie verschiedene Anforderungen erfüllen.

Die TOMs können entsprechend ihrer Bezeichnung grundsätzlich in folgende zwei Gruppen unterteilt werden.

Technische Maßnahmen entfalten die beabsichtigte Schutzwirkung für die Verarbeitung im Wesentlichen durch Technik, also durch physische und softwaretechnische Komponenten. Dabei ist jedoch zu beachten, dass viele Maßnahmen in diesem Bereich auch einen organisatorischen Anteil haben.

Beispiel: Bei einer Alarmanlage, einem Backup-System und einem Anti-Schadsoftware-System oder auch nur bei einer Datenverschlüsselung genügt nicht die bloße technische Einrichtung. Diese Techniksysteme müssen für ihre dauerhafte Wirksamkeit dauerhaft regelkonform betreut und gemanagt werden (z. B. Benutzerverwaltung, Überwachung, Aktualisierung).

Organisatorische Maßnahmen sind hingegen im Wesentlichen in der Ablauforganisation verankert und gestalten durch Regelungen sowie Vorgaben die Rahmenbedingungen einer oder mehrerer Verarbeitungen. Bei organisatorischen Maßnahmen spielen technische Aspekte – falls überhaupt – eine untergeordnete Rolle.

Beispiel: Die Regelung in einer Dienstanweisung, bestimmte Daten nicht mündlich an Dritte zu kommunizieren, sowie die Schulung oder andere Sensibilisierung von Beschäftigten sind organisatorische Maßnahmen.

Folglich existieren Bereiche, in denen TOMs nicht durch Technik abgesichert werden können und damit ausschließlich organisatorische TOMs implementierbar sind. Da der Begriff „technische und organisatorische Maßnahmen“ jedoch beider Ausgestaltungsformen der TOMs umfasst, gehört die Abgrenzung regelmäßig nicht zu den wesentlichen Herausforderungen bei einer Risikoanalyse.

1. Anforderungen an TOMs

a) Umfassende Betrachtung

Bei **digitalisierten Verarbeitungsvorgängen** werden personenbezogene Daten durch unterschiedliche Komponenten verarbeitet. Das Standard-Datenschutzmodell (SDM) unterscheidet dabei die drei Komponenten „Daten“, technische „Systeme und Dienste“ sowie technische, organisatorische und personelle „Prozesse“ der Verarbeitung.[26] Diese Unterscheidung berücksichtigend können die unterschiedlich möglichen Anknüpfungspunkte von TOMs im Folgenden schematischen Schichtenmodell identifiziert werden, bei dem die einzelnen Schichten von unten nach oben aufeinander aufbauen.

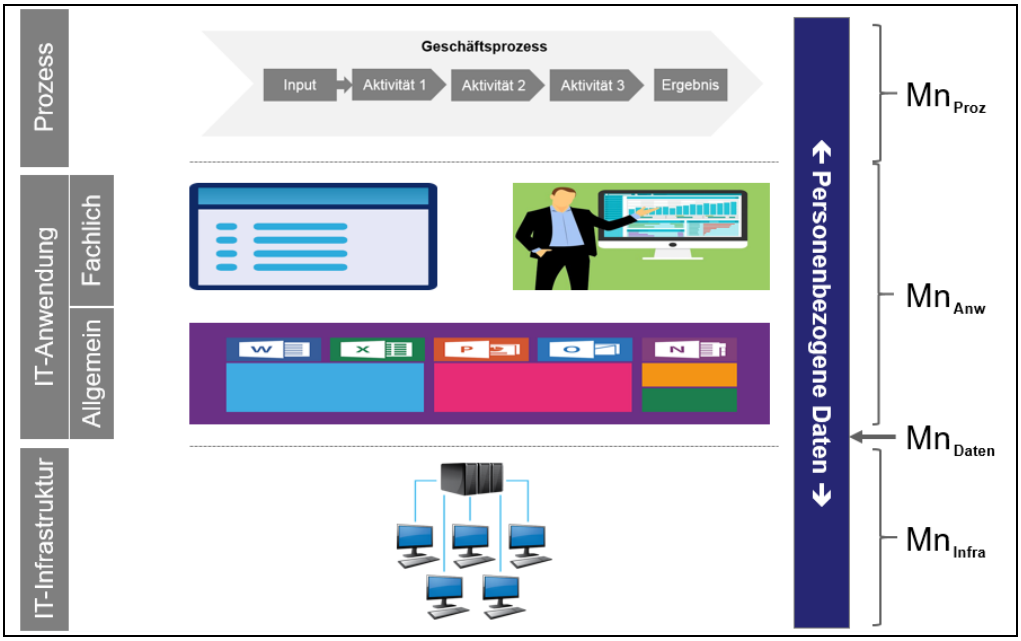


Abb. 17: Mögliche TOM-Anknüpfungspunkte bei digitalisierten Verarbeitungen

Mit der systematischen Betrachtung und Dokumentation von **Geschäftsprozessen** kann die Ablauforganisation einer Institution lückenlos und mit einem beliebigen Detailierungsgrad dargestellt werden. Die Verarbeitungsvorgänge sind in der Ablauforganisation integriert und können auch innerhalb der Geschäftsprozessmodellierung umfassend dargestellt werden. Die vollständige Darstellung der Geschäftsprozesse in einer Prozesslandkarte ist dabei ein

[26] Vgl. SDM (Fn. 5), S. 14.

V. Systematik der TOMs

Instrument, um den Überblick über alle Geschäftsprozesse einer Institution bzw. Stelle und damit auch über alle in den Geschäftsprozessen integrierten Verarbeitungstätigkeiten zu schaffen.

Eine vollständige Prozessorganisation muss gewährleisten, dass Geschäftsprozesse auf ihren Hauptzweck hin ausgerichtet sind. Aufgrund der ebenfalls gebotenen Orientierung von Verarbeitungstätigkeiten nach ihrem Verarbeitungszweck sind Verarbeitungstätigkeiten in der Regel deckungsgleich mit Geschäftsprozessen.[27]

Beispiel: TOMs, die auf der Ebene des Geschäftsprozesses „Personal verwalten" verankert sind, sind beispielsweise
- die Anweisungen, beim Verlassen des Büros die Zimmertür abzusperren, und
- Personen, die keinen Dienstausweis in der Dienststelle tragen, nach ihrem Zielort zu fragen.

Bei IT-unterstützten Verarbeitungen können die genutzten **IT-Anwendungen** weiter in die IT-Fachanwendungen (z. B. Personalwirtschafts-, Finanzwirtschafts- und Einwohnermeldesystem) und allgemeine, übergreifende IT-Anwendungen (z. B. Textverarbeitungs-, Tabellenkalkulations-, E-Mail-, Videokonferenz- und E-Aktensystem) unterteilt werden. IT-Anwendungen können insbesondere mittels eigener IT-Systeme und eigener IT-Infrastruktur oder aber auch mittels IT-Diensten (z. B. Cloud-Computing in der Form als Software-as-a-Service oder Platform-as-a-Service) betrieben werden.

Beispiel: TOMs, die an IT-Anwendungen anknüpfen, sind zum Beispiel
- ein Rollen- und Berechtigungsmanagement für eine IT-Anwendung und
- die Deaktivierung von Export- und Makro-Funktionen in einer IT-Anwendung.

Die **IT-Infrastruktur** mit ihren Rechnern, Servern, Netzwerken, Diensten aus der Cloud (z. B. Infrastructure-as-a-Service) usw. ist die Basis des IT-Gesamtsystems.

Beispiel: In der IT-Infrastruktur knüpfen TOMs an
- die Verwendung von Firewalls und
- den Schutz von Schadsoftware.

Personenbezogene Daten werden in allen diesen Schichten verarbeitet.

Beispiel: TOMs, die unmittelbar an den personenbezogenen Daten anknüpfen, sind beispielsweise
- die Verschlüsselung von personenbezogenen Daten und
- die Pseudonymisierung von personenbezogenen Daten (vgl. Art. 32 Abs. 1 DSGVO).

Es gibt TOMs, die genau einer Schicht zugeordnet werden können (z. B. Festplattenverschlüsselung als TOM auf der Ebene IT-Infrastruktur), und andere TOMs, die auf mehreren Schichten Wirkung entfalten und daher relevant sind.

Beispiel: Auf mehreren Schichten einsetzbar sind etwa

[27] Vgl. Baustein 51 „Zugriff auf Daten, Systeme und Prozesse erteilen" des Standard Datenschutzmodells (SDM, Fn. 5) .

- eine Sensibilisierung/Schulung,
- eine Protokollierung der Zugriffe auf personenbezogene Daten und
- ein Änderungs- und Zugriffsmanagement.

Bei der Betrachtung des schematischen Schichtenmodells geht es im Wesentlichen um die Vermeidung von Analyselücken. Indem für die jeweilige Zielverarbeitung alle relevanten Verarbeitungsmittel in jeder Verarbeitungsschicht ermittelt und betrachtet werden, wird erst ein durchgängiger Schutz der personenbezogenen Daten über alle Schichten hinweg gewährleistet.

b) Risikoorientierung

Das Risiko einer Verarbeitung muss mittels TOMs auf ein angemessenes Niveau reduziert werden. Die Auswahl geeigneter TOMs richtet sich dabei nach dem Risiko, das einer Zielverarbeitung noch ohne Berücksichtigung von Schutzmaßnahmen innewohnt. Das Ausgangsrisiko wird insbesondere durch die verarbeiteten Daten, die weiteren Umständen der Verarbeitung und die sich daraus ergebenden risikobehafteten Szenarien geprägt. Die Geeignetheit von TOMs bemisst sich danach, ob nach einer wirksamen Umsetzung der TOMs das verbleibende Restrisiko bezüglich des betrachteten Szenarios angemessen ist.

Die Identifikation geeigneter TOMs erfolgt in der Regel schrittweise und iterativ. Bei diesem Vorgehen sind insbesondere folgende Fragestellungen und Prüfungen zu berücksichtigen:

- Werden alle Einzelaspekte des betrachteten Szenarios durch die zugeordneten TOMs abgedeckt?
- Ist die einzelne TOM geeignet für die beabsichtigte Risikoreduzierung?
- Ergibt sich durch das Zusammenwirken der TOMs ein wirksames Ganzes?
- Stehen einzelne TOMs im Widerspruch zueinander oder sind sie inkonsistent?

Ungeeignete TOMs sollten verworfen und noch fehlende angemessene TOMs ergänzt werden.

Zu jeder TOM muss grundsätzlich auch ihr Wirkmechanismus, mittels dessen jeweils die Risikominderung erreicht werden soll, verständlich in der Risikoanalyse dargestellt werden. Bei einer Überprüfung des Wirkmechanismus vergleichbarer TOMs kann risikoorientiert diejenige TOM angemessen und auszuwählen sein, die bei Berücksichtigung des Stands der Technik (vgl. Punkt V. 1. e)) den auf dem Markt wirkungsvollsten Schutz bietet.

Die bloße Nennung von Begriffskategorien, wie z. B. „Einsatz von Verschlüsselung“, genügt nicht. Denn hierbei fehlen etwa die Angaben zu der Verschlüsselungsart (z. B. Transportverschlüsselung, Ende-zu-Ende-Verschlüsselung), zum Verschlüsselungsalgorithmus sowie die Beschreibung der Verschlüsselungsparameter, wie beispielsweise die Schlüssellänge und Methoden zur sicheren Verwahrung privater Entschlüsselungsschlüssel.

Zudem muss aus der Maßnahmenbeschreibung ebenfalls hervorgehen, auf welche Komponente(n) die TOM wirkt (z. B. Virusschutz für Client, Virusschutz für Server). Insgesamt muss

plausibilisiert werden, inwiefern die identifizierten TOMs geeignet sind, die Risiken so zu mindern, dass nur noch ein angemessenes Restrisiko übrigbleibt.

c) Datenschutz durch Technikgestaltung

Fragen des Datenschutzes müssen bereits bei der Konzipierung von Verarbeitungsmitteln berücksichtigt werden (Art. 25 Abs. 1 DSGVO). Dies betrifft etwa die Punkte Gestaltung von Eingabefeldern (z. B. Datenminimierung beachten bei Feldkonfiguration als Pflichtfeld, Auswahlliste oder Freitextfeld), unmittelbarer Schutz von personenbezogenen Daten (z. B. Pseudonymisierung, Verschlüsselung), Möglichkeiten zur Datenlöschung und Funktionsumfang von Berechtigungskonzepten. Der Datenschutz durch Technikgestaltung ist insbesondere schon bei der Beschaffung[28] von IT-Systemen, welche die Verarbeitung von personenbezogenen Daten unterstützen, zu berücksichtigen.

d) Datenschutzfreundliche Voreinstellungen

Die Voreinstellungen von datenschutzrechtlich relevanten Funktionen der Betriebsmittel und anderen Einstellungen der Verarbeitungsmittel sollten so gestaltet sein, dass sie die Grundprinzipien des Datenschutzes und der IT-Sicherheit von vornherein berücksichtigen (Beispiele: Eingabe von schwachen Standard-Passwörtern nicht möglich, Verschlüsselung aktiviert, Beschränkung der Berechtigungen von Benutzern, Ortungsdienste ausgeschaltet).

e) Stand der Technik und Organisation

Bei der Auswahl der TOMs ist gemäß Art. 25 und 32 DSGVO der „Stand der Technik" zu beachten, der jedoch gesetzlich nicht näher definiert wird. Wie bisher auch ist es daher sinnvoll, sich an öffentlich zugänglichen Standards zu orientieren, wie etwa an den Technischen Richtlinien (BSI-TR) und sonstigen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie den Richtlinien und Leitfäden des Landesamts für Sicherheit in der Informationstechnik (LSI).

Diese gesetzliche Anforderung ist auch auf den organisatorischen Aspekt von TOMs auszuweiten, so dass die TOMs insbesondere auch den Stand der Organisation zu berücksichtigen haben. Im Hinblick auf die Organisation, bei der insbesondere durch „good practice" in bestimmten Bereichen ebenfalls von einem „Stand der Organisation" ausgegangen werden kann, existieren zwar nicht annähernd so viele Hinweise wie zum Stand der Technik.[29] Im Hinblick auf bestehende Beschreibungen und Bedeutung rein organisatorischer Maßnahmen (z. B. Sensibilisierung von Beschäftigten) ist aber auch hier ein entsprechender Maßstab anzulegen.

[28] Beispielsweise im Rahmen des Vergabeverfahrens.

[29] Siehe jedoch beispielsweise das Arbeitspapier „Datenschutz bei der Nutzung von Telefax-Diensten", das den Stand der Organisation beim Faxen darstellt und das auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018" abrufbar ist.

Da das Sicherheitsniveau „Stand der Technik und Organisation“ in der DSGVO nicht weitergehend konkretisiert wird, lohnt sich ein Blick auf die Rechtsprechung. Nach der Rechtsprechung wird beim Stand der Technik nach nationalem Verständnis der rechtliche Maßstab für das Gebotene an das neuere Angebot der technischen Entwicklung verlagert, da die allgemeine Anerkennung und die praktische Bewährung allein für den Stand der Technik nicht ausschlaggebend sind. Nicht hingegen umfasst sind Maßnahmen, die neusten Entwicklungen aus Laboren und Forschung entspringen.[30]

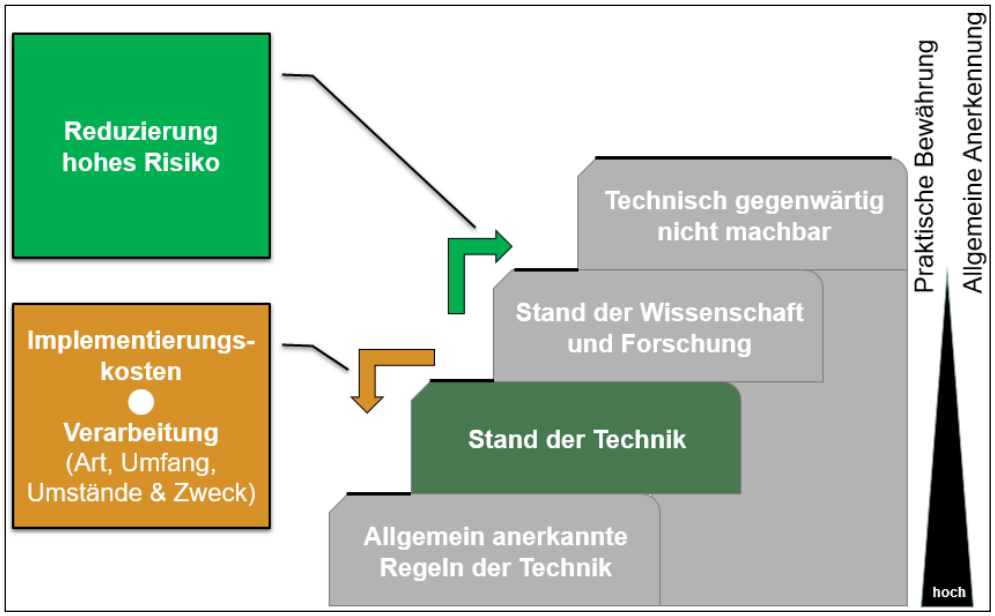


Abb. 18: Drei-Stufen-Theorie für die Anforderungen an die Technik nach Kalkar-Entscheidung

Für die Prüfung, ob eine konkrete technische und organisatorische Maßnahme angemessen ist, müssen grundsätzlich die Implementierungskosten mit den Ergebnissen der Risikoanalyse abgewogen werden (siehe Abbildung 18). Je sensibler die personenbezogenen Daten[31] und je höher die Risiken für die betroffenen Personen sind, desto umfassendere TOMs sind regelmäßig angemessen. In Einzelfällen ist auch denkbar, dass nur TOMs nach dem Stand der Wissenschaft und Forschung ein bestehendes hohes Verarbeitungsrisiko auf ein angemessenes Niveau reduzieren können.

Bestehende Orientierungshilfen zum Stand der Technik verdeutlichen, dass das Festlegen eines Mindeststandards für eine bestimmte Branche von vielen einzelnen Faktoren abhängt. Eine genaue Bestimmung des Mindeststandards muss daher vor dem Hintergrund eventuell

30 Vgl. die drei gerichtlichen Abstufungen „allgemein anerkannten Regeln der Technik“, „Stand der Technik“ und „Stand von Wissenschaft und Technik“ in BVerfGE 49, 89, 1978, „Kalkar I“.

31 Siehe etwa besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO.

bestehender spezialgesetzlicher Regelungen und anhand der individuellen Voraussetzungen vorgenommen werden.[32]

Der Stand der Technik ist dynamisch und muss laufend auf neue Entwicklungen und Reifegrade hin überprüft werden. Relativiert wird diese Anforderung allerdings insbesondere durch die grundsätzlich zu berücksichtigenden Implementierungskosten für die Maßnahmen[33] und die Ausprägung sowie das Ausgangsrisiko der Zielverarbeitung. So erfordert die Auswahl der TOMs im Einzelfall eine nachvollziehbare Abwägung der im Art. 32 DSGVO genannten Aspekte, die gesondert zu dokumentieren ist.

f) Zeitpunkt der Umsetzung

Der Verantwortliche muss bereits zum Zeitpunkt der Festlegung der Mittel als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete TOMs treffen (Art. 25 Abs. 1 DSGVO – Datenschutz durch Technikgestaltung). Bei einer Verarbeitung mit einem voraussichtlichen hohem Risiko muss die dann erforderliche DSFA (siehe Punkt VII.), die auch die zur Bewältigung der Risiken geplanten TOMs mit umfasst (Art. 35 Abs. 7 DSGVO), **vorab** durchgeführt bzw. nachgewiesen werden (Art. 35 Abs. 1 DSGVO).

Diese Pflicht, dass der Verantwortliche vor der eigentlichen Verarbeitung sich mit deren genauen Ausgestaltung beschäftigen muss, hat zum einen das Ziel, möglichst zeitnah erkennen zu können, ob eine Verarbeitung trotz geplanter TOMs ein hohes Risiko zur Folge hat. In einem solchen Fall muss der Verantwortliche vor der Verarbeitung die zuständige Datenschutz-Aufsichtsbehörde konsultieren (Art. 36 Abs. 1 DSGVO).

Zum anderen benötigen manche TOMs für ihre wirksame Umsetzung längere Zeiträume (z. B. Netztrennung, indem interne IT-Netzsegmente restriktiv mit Netzwerkkomponenten voneinander getrennt werden). Zudem führt die rechtzeitige Analyse und Vorplanung einer Verarbeitung auch dazu, dass auf dem Weg bis hin zur eigentlichen Durchführung der Verarbeitung wichtige Aspekte und TOMs nicht vergessen werden.

Beispiel: Bei der Beschaffung eines neuen IT-Systems, das die Verarbeitung unterstützen soll, können sogenannte Ausschlusskriterien bei der Durchführung der Vergabe aus dem Datenschutz stammen. In diesem Zusammenhang zu denken wäre beispielsweise an unverzichtbare Löschfunktionen und die Umsetzbarkeit des erforderlichen Zugriffsschutzes. Bei der Beschaffung vergessene und später auch nicht anderweitig umsetzbare Funktionen können im schlechtesten Fall dazu führen, dass ein beschafftes IT-System nicht datenschutzkonform betrieben werden kann.

[32] Vgl. Bundesverband IT-Sicherheit e.V. (TeleTrusT), IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik", Technische und organisatorische Maßnahmen, Internet: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/.

[33] Im Zusammenhang mit der DSFA ist der Aspekt der Implementierungskosten bzgl. der TOMs nicht ausdrücklich genannt, vgl. Punkt VIII.1.

g) Wirksamkeitsüberwachung

Nachdem die erforderlichen TOMs zumeist iterativ in mehreren Schritten festgelegt wurden (siehe Punkt V. 2.), müssen diese wirksam umgesetzt werden, das heißt sie müssen beauftragt, umgesetzt und dauerhaft aktiviert werden. Diese Umsetzung kann, je nach Komplexität der Maßnahme, auch in Form eines Vorhabens oder Projekts durchgeführt werden. Nach der Umsetzung sind die TOMs erforderlichenfalls hinsichtlich ihrer Wirksamkeit zu überprüfen und gegebenenfalls zu aktualisieren (vgl. Art. 24 Abs. 1 Satz 2, Art. 25 Abs. 1, 32 Abs. 1 Buchst. d, 35 Abs. 11 DSGVO).

Die Wirksamkeit einer TOM muss von ihrer Wirkungsweise und Schutzwirkung schon begrifflich unterschieden werden. Die Wirksamkeit einer TOM liegt vor, wenn die TOM genauso, wie sie spezifiziert wurde, dauerhaft umgesetzt ist.

Die Wirkungsweise und Schutzwirkung hingegen gehören zu der Spezifikation einer TOM, also zu der Fragestellung, ob die TOM überhaupt geeignet ist, dass für sie einschlägige Verarbeitungsrisiko angemessen zu reduzieren (siehe Punkt V. 1. b)).

Die Prüfung der Wirksamkeit von TOMs kann unterschiedlich aufwändig sein.

Beispiel: So kann die IT-gestützte Überwachung einer festgelegten Mindestkomplexität von Passwörtern deutlich einfacher auf Wirksamkeit überprüft werden als die Wirksamkeit eines komplexen Datensicherungssystems, bei dem etwa regelmäßige Wiederherstellungstests für die Wirksamkeitsprüfung durchgeführt werden müssen.

Folgende Teilaspekte sollten bei der Wirksamkeitsüberwachung mit berücksichtigt werden:

- Sind die TOMs für die Mitarbeiter und andere Adressaten leicht verständlich und transparent?
- Sind die implementierten TOMs tolerant gegenüber Bedienungs-und Betriebsfehlern (die hohe Benutzerfreundlichkeit einer TOM unterstützt deren Wirksamkeit)?
- TOMs, die von den Adressaten nicht akzeptiert werden, werden oft „umgangen". Es sollten praktikable Lösungen erarbeitet werden, die die Adressaten möglichst wenig einschränken oder behindern.
- Wie leicht können Adressaten von TOMs diese umgehen?
- Ist zeitnah ersichtlich, wenn eine TOM ausfällt und damit nicht mehr wirksam ist?

Ein systematisches Maßnahmenmanagement, das auch für andere Maßnahmenbereiche einer Organisation (z. B. IT-Sicherheit, Arbeitssicherheit) genutzt werden kann, kann dabei helfen, die DSGVO-Anforderungen an TOMs effizient zu erfüllen (vgl. Punkt VI. 2. b)).

h) TOMs als Verarbeitungsvorgang

Es gibt TOMs, die als eigenständige Verarbeitungsvorgänge – insbesondere in der Form von Betriebsmitteln – selbst spezifische personenbezogene Daten verarbeiten. Da für alle Verarbeitungen der Einklang mit der DSGVO nachzuweisen ist, müssen auch die spezifischen TOM-Daten im Rahmen einer Risikoanalyse mit betrachtet werden (siehe Punkt VI. 3. a) aa)).

Beispiel: Die Datensicherung als wichtige TOM verarbeitet regelmäßig sowohl die personenbezogenen Daten des Verarbeitungsvorgangs, dessen Daten gesichert werden, als auch spezifische Betriebsmitteldaten, wie z. B. Protokollierungsdaten und Daten zu den Benutzern des Backup-Systems (Benutzerverwaltung).

i) Adressaten der Umsetzungspflicht

Die DSGVO verpflichtet Verantwortliche und Auftragsverarbeiter dazu, die Verarbeitung und die hierfür eingesetzte Technik und Organisation im Hinblick auf die Gewährleistung des grundrechtlichen Schutzes der Rechte der betroffenen Personen auszugestalten (Art. 25, 28, 32 DSGVO). Zur Minderung der entstehenden Risiken sind der Verantwortliche und der Auftragsverarbeiter dazu verpflichtet, auch die dafür angemessenen TOMs zu implementieren.

Werden ausnahmsweise Dritte als ausführende Akteure für risikomindernde TOMs benannt, so ist dies nur möglich, wenn ein vertragliches oder sonstiges Weisungs- und Kontrollrecht besteht, mittels dessen der Verantwortliche bzw. der Auftragsverarbeiter die Durchsetzung der TOMs gewährleisten kann.

2. Quellen und Fundstellen von TOMs

TOMs können aus unterschiedlichen Quellen hergeleitet werden, die wie folgt unterschieden werden können.

a) Vorgaben

In den für die Institution einschlägigen Normen und Vorgaben können bestimmte TOMs ausdrücklich festgelegt und eine Implementierung gefordert werden.

- **1 Rechtsvorschriften**
  Die DSGVO und andere Normen, wie Fachgesetze mit Rechtsgrundlagen für die Verarbeitung von Daten, geben bestimmte TOMs teilweise verbindlich oder nur empfehlend vor. Die DSGVO sieht zwar keine Auflistung von Datensicherheitsmaßnahmen mehr vor, wie sie Art. 7 BayDSG in der bis zum 24. Mai 2028 geltenden Fassung enthielt („Zehn Gebote"). Insbesondere in Art. 25 und Art. 32 DSGVO werden jedoch einige Maßnahmen und Schutzziele in Bezug auf die Technik und Sicherheit der Datenverarbeitung aufgeführt. Diese beziehen sich teils unmittelbar auf die Daten, teils aber auch auf die IT-Systeme, die im Zusammenhang mit der Datenverarbeitung eingesetzt werden (vgl. insbesondere Art. 32 Abs. 1 DSGVO).

Beispiel: Als Beispiele hierfür sind die Richtlinie der Kassenärztliche Bundesvereinigung nach § 75b Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (SGB V) über die Anforderungen zur Gewährleistung der IT-Sicherheit zu nennen.

- **2 Selbstregulierung**
  Zudem sind TOMs in Verhaltensregeln (Art. 40 DSGVO), sonstigen Vorgaben und Mindeststandards, die von gesellschaftlichen Gruppen, Verbänden und Organisationen für ihren Wirkungskreis geschaffen werden, verankert.[34] Zu beobachten ist, dass berufsspezifische Verhaltensregeln immer häufiger genutzt werden bzw. deren Erstellung gesetzlich vorgesehen werden.

  Beispiel: Als Beispiele genannt werden können die geplanten und noch in Abstimmung befindlichen Verhaltensregeln der Bundesnotarkammer zu technischen und organisatorischen Maßnahmen der Notarinnen und Notare im Hinblick auf deren elektronische Aufzeichnungen und Hilfsmittel nach § 6 Notar-Akten- und Verzeichnisse-Verordnung.

- **3 Interne Vorgaben**
  Viele Institutionen bzw. Stellen geben sich im Rahmen ihres Datenschutzmanagement selbst weitere interne Vorgaben etwa in der Form einer „Datenschutz-Geschäftsordnung", die auch TOMs enthalten.[35]

- **4 Anweisungen einer Aufsichtsbehörde**
  Anweisungen von zuständigen Aufsichtsbehörden können ebenfalls Vorgaben zu TOMs enthalten (vgl. beispielsweise Art. 58 Abs. 2 Buchst. d DSGVO).

b) Risikoanalyse

TOMs sind zudem vom Verantwortlichen im Rahmen der jeweils notwendigen Risikoanalyse selbst herzuleiten (vgl. zum Beispiel Art. 35 Abs. 7 Buchst. d DSGVO). Die Risikoanalyse ist entweder im Kontext einer Risikoanalyse-Allgemein (siehe Punkt VIII.) oder im Kontext einer Risikoanalyse, die im Zusammenhang mit einer DSFA stets durchgeführt wird (Risikoanalyse-DSFA, siehe Punkt VII.), ein wichtiger Generator für TOMs.

Die Risikoanalyse-DSFA und die Risikoanalyse-Allgemein haben als wesentliches Ziel, geeignete TOMs für die Zielverarbeitung zu identifizieren und wirksam umzusetzen, um ein dem Verarbeitungsrisiko angemessenes Schutzniveau zu gewährleisten.

[34] Z. B. Deutsche Krankenhausgesellschaft, Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, Internet: https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/.

[35] Beispielsweise hat das Bayerische Staatsministerium des Innern, für Sport und Integration ein Muster für eine Datenschutz-Geschäftsordnung unter https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen veröffentlicht.

c) Herausgeber von TOM-Katalogen

Zahlreiche Institutionen geben für unterschiedliche Fach- und Lebensbereiche teilweise sehr umfangreiche „Kataloge", „Orientierungshilfen", „Positionspapiere", „Bausteine", „Tätigkeitsberichte", „Empfehlungen" usw. heraus, die wichtige übergreifende und spezielle, auf eine bestimmte Zielverarbeitung abzielende TOMs enthalten. Folgende Herausgeber können als kleine Auswahl exemplarisch hier genannt werden:

- **Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK).** – Neben dem SDM mit seinem Maßnahmenkatalog (z. B. "Baustein 60: Löschen und Vernichten") veröffentlicht die DSK zahlreiche weitere Unterlagen, in denen TOMs-Kataloge enthalten sind.
- **Datenschutz-Aufsichtsbehörden.** – Auf den Webauftritten der deutschen und europäischen unabhängigen Datenschutz-Aufsichtsbehörden finden sich zahlreiche Aussagen zu TOMs.[36]
- **Behörden für die IT-Sicherheit.** – Im Bereich der TOMs für die IT-Sicherheit sind die Veröffentlichungen des BSI und des LSI zu nennen.

Neben den oft zu findenden TOM-Katalogen, die teilweise unterschiedliche Zeitstände und sehr unterschiedliche Konkretisierungsgrade bezüglich der Beschreibung der einzelnen TOMs aufweisen, wurden auch Arbeitshilfen für die Herleitung von TOMs veröffentlicht.[37]

3. Weitere Besonderheiten von TOMs

a) Schadensverhinderung oder Schadensminimierung

Bei der Methode des Risikomanagements wird das Risiko grundsätzlich durch die beiden Dimensionen Eintrittswahrscheinlichkeit und Schadenshöhe ermittelt (siehe Punkt III. 3.). Zur Reduzierung eines Risikos müssen folglich die TOMs entweder die Eintrittswahrscheinlichkeit oder/und die Schadenshöhe reduzieren. Es ist wichtig, dass dem Verantwortlichen beide Wirkungsweisen von TOMs bewusst sind und der Schwerpunkt nicht nur auf eine Wirkungsrichtung gesetzt wird.

Beispiel: Die Verschlüsselung von personenbezogenen Daten ist eine Schutzmaßnahme mit dem typischen Hauptziel, die Wahrscheinlichkeit eines unbefugten Datenzugriffs zu reduzieren. Die Umsetzung eines Notfallkonzepts hingegen ist eine Maßnahme, die nach einer aufgetretenen Datenpanne auf die Minderung des Schadens und der Folgen für die betroffenen

[36] Siehe etwa Zentralarchiv für Tätigkeitsberichte der Bundes- und der Landesdatenschutzbeauftragten sowie der Aufsichtsbehörden für den Datenschutz (ZafTDa), Internet: https://www.zaftda.de/.

[37] Z. B. Prozess zur Auswahl angemessener Sicherungsmaßnahmen (ZAWAS), Internet: https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/zawas/praxisnahe-hilfe-zum-technisch-organisatorischen-datenschutz-173395.html.

Personen abzielt. Je nach Gestaltung der Schulung von Beschäftigten, die an Verarbeitungen beteiligt sind, kann diese Sensibilisierung kombiniert sowohl die Eintrittswahrscheinlichkeit als auch die Schadenshöhe reduzieren.

b) Implementierungskosten

Die einzelnen TOMs sind unter der Berücksichtigung von mehreren Aspekten einzurichten. Davon umfasst sind auch grundsätzlich[38] die Implementierungskosten (vgl. Art. 32 Abs. 1 DSGVO). Zu diesen Kosten gehören die Kosten für die Einrichtung und Umsetzung einer TOM sowie die Kosten für deren Betrieb und späteren Deaktivierung. Obwohl die Implementierungskosten ein Auswahlkriterium für angemessene TOMs sind, werden mit bloßen Kostenargumenten keine unzureichenden TOMs zu rechtfertigen sein.

Wie beim Abwägungsaspekt „Stand der Technik" (siehe Punkt V.1.e)) handelt es sich auch bei den Kosten um einen Faktor, der in die Einzelfallabwägung zum Feststellen der Verhältnismäßigkeit und Angemessenheit einer bestimmten TOM eingeht. Art. 24 Abs. 1 DSGVO, der einen wichtigen Maßstab für den Handlungsbedarf des Verantwortlichen regelt, nennt die Implementierungskosten jedoch nicht. Der Verantwortliche könnte sich also bei einem Verzicht auf angemessene TOMs nicht darauf berufen, dass ihm die finanziellen oder personellen Mittel fehlen: Er muss stets in der Lage sein, seiner Verantwortung nach Art. 24 Abs. 1 DSGVO sowie seiner Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO nachzukommen.[39]

c) Beschäftigtendatenschutz

Da durch TOMs regelmäßig auch etwa Benutzerdaten als spezifische Betriebsmitteldaten verarbeitet werden (siehe Punkt V. 1. h)), ist im Fall der Verarbeitung von Beschäftigtendaten der Beschäftigtendatenschutz sowie gegebenenfalls die Wahrung der Mitbestimmungsrechte der Personalvertretung zu beachten.

[38] Im Zusammenhang mit der DSFA ist der Aspekt der Implementierungskosten bzgl. der TOMs nicht ausdrücklich genannt, vgl. Punkt VIII.1.

[39] Vgl. Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 32 DSGVO Rn. 26.

VI. Praxishinweise für Risikoanalysen

1. Adressatengerechte Gestaltung

Eine Risikoanalyse sollte adressatengerecht gestaltet werden.

Die „Rechenschaftspflicht" trifft den Verantwortlichen (vgl. auch Punkt V. 1. i)). Dieser muss nachweisen können, dass eine Verarbeitung gemäß den Vorgaben der DSGVO erfolgt (vgl. insbesondere Art. 5 Abs. 2, Art. 24 Abs. 1 Satz 1 DSGVO). Im Rahmen dieses Nachweises kann auf eine Risikoanalyse-Allgemein zurückgegriffen werden (siehe Punkt VIII.). Im Rahmen einer DSFA ist eine Risikoanalyse gemäß Art. 35 Abs. 7 Buchst. c und d DSGVO verpflichtend (siehe Punkt VII.).

Adressat einer durchgeführten DSFA bzw. einer Risikoanalyse-Allgemein ist zunächst die verantwortliche Stelle selbst. So müssen beispielsweise alle für die Wirkung von TOMs unverzichtbaren Informationen an die relevanten Beschäftigten und sonstigen Personen weitergegeben werden. Dabei ist zu gewährleisten, dass diese Informationen dauerhaft, also auch bei einem Wechsel von Zuständigkeiten und nach längerem Zeitablauf ohne Anwendung dieser Informationen, in der Organisation fest verankert bleiben und gelebt werden. Die Informationsweitergabe muss daher adressatengerecht (z. B. Checklisten, Schulung, Einzelanweisung) und in Teilbereichen auch wiederholend erfolgen.

Ferner ist die jeweils zuständige Datenschutz-Aufsichtsbehörde potenzieller Adressat einer durchgeführten DSFA bzw. einer Risikoanalyse-Allgemein. Denn auf Grundlage ihrer allgemeinen Untersuchungsbefugnisse hat sie einen Anspruch auf Einsichtnahme in die datenschutzrechtlich relevanten Nachweisunterlagen des Verantwortlichen und des Auftragsverarbeiters (vgl. insbesondere Art. 58 Abs. 1 DSGVO). Daher sind die Risikoanalysen so zu gestalten, dass eine Aufsichtsbehörde sie schnell und ohne unnötigen Einarbeitungsaufwand (z. B. klare und nachvollziehbare Aufbausystematik, Verwendung anerkannter Methoden) nachvollziehen und beurteilen kann.

Die Rechte und Freiheiten betroffener Personen stehen zwar im Mittelpunkt der datenschutzrechtlichen Risikoanalyse. Dieser Personenkreis hat jedoch allenfalls bei Erfüllung bestimmter Bedingungen ein Einsichtsrecht in die Risikoanalyse, da insbesondere ein solches nicht allgemein in Art. 15 DSGVO verankert ist. In tatsächlicher Hinsicht können jedoch DSFAs und allgemeine Risikoanalyse vollständig oder zumindest auszugsweise

– als vertrauensbildende Maßnahme,[40]

[40] Siehe z. B. den Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland unter https://www.coronawarn.app/de/#privacy.

- in Form einer gesetzlichen DSFA als Teil der Gesetzesbegründung[41] (vgl. auch Punkt VII. 5. b)) und
- zur Umsetzung der TOMs an die betroffenen Beschäftigten

kommuniziert werden.

Bei der Offenlegung einer Risikoanalyse können Bedenken des Verantwortlichen bezüglich der Sicherheit der Verarbeitung aufkommen. Neben einer auszugsweisen Offenlegung ist auch an die Möglichkeiten zu denken, die unter dem Schlagwort „Spannungsverhältnis zwischen Nachweispflicht und Sicherheit" unter dem Punkt VI. 5. dargestellt werden.

2. Organisation der Durchführung

a) Team

Bayerische öffentliche Stellen sollten frühzeitig entscheiden, welche Methodik für die Risikoanalyse verwendet wird. Nach der Festlegung des methodischen Ansatzes kann es auch sinnvoll sein, organisatorische Rahmenbedingungen für die Durchführung von Risikoanalysen zu bestimmen. Diese Rahmenbedingungen werden insbesondere durch die Größe der verantwortlichen Stelle, die Komplexität der jeweils betrachteten Zielverarbeitung sowie die bestehenden Nutzungsmöglichkeiten von Standardisierungen und Synergien (vgl. Punkt VI. 3. c)) beeinflusst. Daher kann die organisatorische Spannweite im Einzelfall von „eine Person führt die DSFA bzw. die Risikoanalyse-Allgemein durch" bis hin zur „Durchführung im Rahmen eines (Teil-)Projekts durch ein interdisziplinäres Team" reichen.

Bei digitalisierten Verarbeitungen sind grundsätzliche folgende Personen potenzielle Kandidaten für das interdisziplinäre Team, das die DSFA bzw. die Risikoanalyse-Allgemein durchführt:

Festes Teammitglied ist zunächst ein Vertreter des Verantwortlichen, der die Risikoanalyse durchführt (vgl. z. B. Art. 24 Abs. 1 DSGVO). Weitere Teammitglieder sollten Fachkunde für die Themen „Prozesse der Verarbeitung", „technische Systeme" sowie „verarbeitete personenbezogene Daten" einbringen. Daher sollten vertreten sein: das Sachgebiet, das den betroffenen Geschäftsprozess inklusive der darin verarbeiteten personenbezogenen Fachdaten verantwortet, das Sachgebiet, das für die IT-Unterstützung des betroffenen Geschäftsprozesses zuständig ist, sowie gegebenenfalls ein Sachgebiet mit besonderer Fachkunde im Datenschutzrecht. Soweit im Einzelfall – besonders zu prüfen bei der Durchführung einer DSFA (vgl. Art. 35 Abs. 9 DSGVO) – angebracht, sollten auch Beschäftigte mit nutzbringender Fachkunde, betroffene Personen, ihre Vertreter (dies umfasst auch die Personalvertretung und weitere Interessenvertretungen) und externe Experten befragt bzw. beteiligt werden.

[41] Siehe z. B. Gesetz zur digitalen Modernisierung von Versorgung und Pflege (DVPMG), Anlage zu § 307 Absatz 1 Satz 3 SGB V.

Der behördliche Datenschutzbeauftragte kann im Einzelfall ein Mitglied des Teams sein oder nur bei Bedarf zugezogen werden. Dabei kann seine Beratungsleistung unterschiedlich ausgeprägt sein. Zu beachten ist, dass der behördliche Datenschutzbeauftragte entsprechend seines gesetzlichen Auftrags nur eine Beratungsleistung erbringt. Die Arbeit eines Risikoanalyse-Teams darf nicht darauf hinauslaufen, dass der behördliche Datenschutzbeauftragte die für eine Risikoanalyse erforderlichen Dokumente entwirft und die übrigen Teammitglieder nur Meinungsäußerungen dazu abgeben. Die Risikoanalyse ist Sache des Verantwortlichen; die Mitwirkung des behördlichen Datenschutzbeauftragten dient der Qualitätssicherung. Davon abgesehen ist der behördliche Datenschutzbeauftragte bei entsprechenden offenen Fragestellungen Verbindungsperson zur jeweils zuständigen Datenschutz-Aufsichtsbehörde (vgl. Art. 39 Abs. 1 Buchst. d und e DSGVO).

b) Dokumentation, Verweisung und Maßnahmenmanagement

Wie dargelegt, genügt es nicht, TOMs im Rahmen einer Risikoanalyse zu identifizieren und zu dokumentieren. Die TOMs müssen zudem umgesetzt und dauerhaft wirksam sein (siehe Punkt V. 1. g)). Diese Umsetzung stellt in aller Regel den deutlich größten Aufwand einer Risikoanalyse dar und wird naheliegender Weise im Rahmen eines allgemeinen Maßnahmenmanagement erfolgen, das in einer Institution in aller Regel bereits implementiert ist (vgl. Punkt VII. 3. c)).

Daher ist es wichtig, die in einem Bericht zur Risikoanalyse dokumentierten TOMs mit den entsprechenden Maßnahmen im Maßnahmenmanagement zu verbinden. Dies kann beispielsweise mittels eindeutigen Maßnahmen-Identifikatoren erfolgen, die jeweils sowohl im Risikoanalyse-Bericht als auch im Maßnahmenmanagement für die TOMs verwendet werden.

Für eine eindeutige Bezugnahme sollten auch weitere zentrale Komponenten eindeutig gekennzeichnet werden. Hierzu können ebenfalls eindeutige **Identifikatoren** genutzt werden (z. B. Dok-ID für Dokumente, Szenario-ID für Szenarien). In den Arbeitshilfen zu dieser Orientierungshilfe wird die Verwendung solcher Identifikatoren anschaulich gezeigt (siehe Punkt IX.).

Die Dokumentation einer TOM kann einzeln, aber auch im Rahmen von anderen TOMs zusammengefasst in umfangreicheren Unterlagen oder Spezifikationen erfolgen („**TOM-Kompendium**“, wie z. B. Sicherheitskonzept, Konzept der IT-Infrastruktur, Schulungskonzept). Im Bericht zur Risikoanalyse (siehe Punkte VII. 3. b)) kann es daher notwendig sein, bei einer TOM auf eine oder mehrere Unterlagen zu verweisen. Bei solchen Verweisen sollten die im jeweiligen TOM-Kontext relevanten Abschnitte der verwiesenen Unterlage konkret referenziert werden, damit etwa bei verteilten Risikoanalysen bei Bedarf der Verantwortliche berechtigte weitergehende Informationen zu TOMs gezielt von der Stelle, welche die Zentral-Risikoanalyse verwaltet, zielgerichtet einholen kann (siehe Punkt VI. 5)).

Im Hinblick auf die Dokumentation ist allgemein zu beachten, dass derselbe Aspekt nur an einer Stelle der Gesamtdokumentation („**Ankerstelle**“) genauer beschrieben und erläutert

werden sollte. Sollte der Aspekt auch in anderen Bereichen der Gesamtdokumentation relevant sein, so sollte grundsätzlich aus Konsistenzgründen dort nur auf die Ankerstelle verwiesen werden.

Die Transparenz und das Verständnis fördern zudem die konsequente Verwendung **einheitlicher Begriffe**, wobei die Verwendung von Glossaren hilfreich sein kann.

Zudem muss die Dokumentation **adressatengerecht** sein (siehe Punkt VI. 1).

3. Typische Optimierungspotenziale

Aus der langjährigen Beratungstätigkeit zu Risikoanalysen und den damit gemachten Erfahrungen werden im Folgenden einige Gesichtspunkte dargestellt, in denen typischerweise oft noch Optimierungspotenziale realisierbar sind.

a) Unnötige Komplexität vermeiden

aa) Bausteinbildung für mehrfach genutzte Betriebsmittel

Eine Verarbeitungstätigkeit, die etwa einen fachlichen Geschäftsprozess repräsentiert, kann von unmittelbaren und mittelbaren Betriebsmitteln unterstützt werden (siehe Punkt II. 2.). Aus Effizienzgründen kann es naheliegend sein, für Betriebsmittel, die parallel für unterschiedliche Verarbeitungstätigkeiten genutzt werden, separate Risikoanalysen zu erstellen. Die Verarbeitungstätigkeiten, die diese Betriebsmittel einsetzen, können dann bausteinartig auf diese Betriebsmittel zusammen mit den schon durchgeführten Risikoanalysen verweisen.

Beispiel: Bei der Verarbeitungstätigkeit „Bewerbungsmanagement durchführen“ kann ein Videokonferenzsystem als unmittelbares Betriebsmittel für Online-Bewerbungsgespräche und ein Backupsystem als TOM sowie mittelbares Betriebsmittel zur Gewährleistung der Verfügbarkeit verwendet werden. Da sowohl das Videokonferenz- als auch das Backupsystem regelmäßig auch für andere Verarbeitungstätigkeiten zum Einsatz kommen, liegt es aus Effizienzgründen nahe, sowohl für das Videokonferenzsystem als auch für das Backupsystem eigene Risikoanalysen durchzuführen bzw. spezifische Teilbereiche in einer beide Betriebsmittel umfassenden Risikoanalyse zu erstellen.

Hilfreich bei der Durchführung von Risikoanalysen separat für Betriebsmittel ist, bei diesen Risikoanalysen zusätzlich die berücksichtigten Verarbeitungskonstellationen als schon „geprüfte und berücksichtigte Anwendungsfälle“ für das jeweilige Betriebsmittel mit anzugeben. Durch die Angabe derartiger Anwendungsfälle kann, wenn eine Verarbeitungstätigkeit ein neues Betriebsmittel nutzen soll, rasch entschieden werden, ob ein bereits existierendes relevantes Betriebsmittel ohne Anpassung seiner Risikoanalyse verwendet werden kann.

bb) Gruppierung von TOMs

Für eine bessere Übersichtlichkeit und Fokussierung auf die jeweiligen Besonderheiten einer Zielverarbeitung kann in einer Risikoanalyse eine TOM-Gruppierung hilfreich sein. Eine solche Gruppierung kann sich beispielsweise auf den Spezialisierungsgrad der einzelnen TOM beziehen und wie folgt durchgeführt werden:

- **Gruppe der „speziellen TOMs".** – Darunter sind TOMs zu verstehen, deren Implementierung (fast) nur bei der betrachteten Zielverarbeitung sinnvoll ist. Bei neuartigen Zielverarbeitungen können zeitnahe Veröffentlichungen dieser speziellen TOMs für verantwortliche Stellen eine große Hilfe beispielsweise bei der Beschaffung neuer IT-Systeme sein.

  Beispiel: Bei der Zielverarbeitung „Videokonferenz durchführen" sind insbesondere die TOMs „Virtuellen Hintergrund nutzen" und „Moderationsfunktionen nutzen" spezielle TOMs.

- **Gruppe der „adaptiven TOMs".** – Darunter sind TOMs zu verstehen, die für mehrere Zielverarbeitungen nach einer verarbeitungsspezifischen Ausgestaltung geeignet sind, das Risiko angemessen zu reduzieren. Der Nutzen dieser Gruppe ist darin zu sehen, dass bei den adaptiven, also immer wieder erneut anzupassenden und umzusetzenden TOMs eine Standardisierung, beispielsweise durch Erstellung von Mustern mit Vorgabe der Mindestinhalte und einer Basisstruktur, angeraten sein kann.

  Beispiel: Bei vielen digitalen Zielverarbeitungen sind insbesondere die TOMs „Technisches Rollen und Berechtigungskonzept implementieren", „Protokollierungskonzept implementieren", „Testkonzept implementieren" und „Löschkonzept implementieren" adaptive TOMs.

- **Gruppe der „übergreifenden TOMs".** – Darunter sind TOMs zu verstehen, die für zahlreiche Zielverarbeitungen ohne nennenswerte Anpassung an die jeweilige Zielverarbeitung geeignet sind, das Risiko angemessen zu reduzieren. In diesem Kontext ist es regelmäßig sinnvoll, diese TOMs jeweils in separaten Unterlagen zu spezifizieren und nachzuweisen. Die einzelne Risikoanalyse braucht damit nur noch auf diese entsprechenden Unterlagen zu verweisen.

  Beispiel: Solche übergreifende TOMs sind etwa „Ein Datenschutz-Management betreiben" und „Im Rahmen eines Informationssicherheitsmanagementsystems ein Informationssicherheitskonzept nach IT-Grundschutz des BSI umsetzen".

cc) Elementare Szenarien

In der Risikoanalyse sollten nur Szenarien behandelt werden, die unmittelbar mit der Zielverarbeitung verknüpft sind, und die insgesamt zu einem klaren, widerspruchsfreien Szenarien-Profil führen. Hierfür sind insbesondere folgende Aspekte zu berücksichtigen:

- **Wirksamkeit von TOMs.** – Szenarien, die überwiegend Aspekte der Unwirksamkeit von TOMs beinhalten (z. B. fehlende, unzureichende Implementierung oder Störung von TOMs), sollten nicht in die Risikoanalyse mit aufgenommen werden. Die Risiken der un-

zureichenden Wirksamkeit von TOMs müssen im Maßnahmenmanagement zu jeder einzelnen TOM behandelt und gegebenenfalls mit spezifischen Wirksamkeitsmaßnahmen reduziert werden (z. B. Aktivierung und laufende Kontrolle der Monitorfunktionen eines Schadsoftware-Abwehr-Systems).

- **Schadensposition als Szenario.** – Mögliche Schadenspositionen, z. B. der Erpressungsversuch nach einem unbefugten Zugriff auf sehr vertrauliche Daten, sollten in die Bewertung des Schadens bzw. der Folgen eines Szenarios und nicht als eigene Szenarien in die Risikoanalyse einfließen.
- **Überschneidende Szenarien.** – Szenarien, die sich inhaltlich überscheiden oder sogar ganz entsprechen, sollten vermieden werden. Ist im Einzelfall eine Mehrfachnennung von Szenarien oder anderen Komponenten unverzichtbar, so sollte auf den Bereich verweisen werden, in dem sich schon die ausführliche Beschreibung befindet (Ankerstelle, siehe Punkt VI. 2. b)).

b) Abgrenzung zur IT-Sicherheit

Nicht selten wird Datenschutz mit IT-Sicherheit gleichgesetzt. IT-Sicherheit ist ein Bereich der Informatik, der sich mit dem Schutz von IT-Systemen und den damit verarbeiteten Informationen in allen ihren Erscheinungsformen beschäftigt. Das (EU-)Datenschutzrecht bezieht sich allerdings (alleine) auf den „Schutz von natürlichen Personen bei der Verarbeitung personenbezogener Daten", vgl. Art. 1 DSGVO. Datenschutzrecht soll die Rechte und Freiheiten natürlicher Personen gewährleisten, die von Datenverarbeitungen konkret betroffen sind.[42] Zwischen IT-Sicherheit und der Sicherheit der Verarbeitung im Datenschutz bestehen sowohl Berührungspunkte als auch Bereiche, in denen deutliche Unterschiede bestehen und sogar Spannungsverhältnisse auftreten.[43] In aller Regel sind solche Spannungsverhältnisse jedoch nach entsprechenden Analysen und Prüfungen im Sinn der beiden berührten Bereiche auflösbar.

Die IT-Sicherheit unterstützt zwar in wesentlichen Bereichen die Datenschutzanforderungen. Es gibt aber auch Fälle, in denen Schutzmaßnahmen aus der IT-Sicherheit datenschutzrechtliche Probleme aufwerfen. Während die IT-Sicherheit die IT-Systeme und Daten unabhängig von einem Personenbezug zu schützen versucht, stehen im Datenschutz natürliche Personen und deren personenbezogene Daten im Fokus.

Beispiel: Beim klassischen Beispiel der TOM „Protokollierung von IT-Benutzeraktivitäten" ist es oft Ziel der IT-Sicherheit, möglichst langfristig und umfangreiche Protokolldaten zu verarbeiten, um die IT-Systeme stabil betreiben und Fehler finden zu können. Der Datenschutz fragt hingegen konsequent mit Blick auf die von der Protokollierung betroffenen Personen insbesondere nach der Erforderlichkeit und der Nichtverkettung.

Weitere wesentliche Unterschiede finden sich in der folgenden Abbildung.

[42] Vgl. Thomas Petri, Kai Engelbrecht: „Meine Daten, die Verwaltung und ich", S. 1, 2019, veröffentlicht unter https://www.datenschutz-bayern.de/info/.

[43] Vgl. Kapitel „E1 Zusammenwirken von SDM und BSI-Grundschutz" im SDM (Fn. 5).

VI. Praxishinweise für Risikoanalysen

Aspekt	Datenschutz	IT-Sicherheit	Anmerkung
Schutzgegenstand	Verarbeitung von personenbezogenen Daten (pbDaten)	IT-Systeme und deren verarbeiteten Daten (IT)	IT-Sicherheit ist ein Teil der Informationssicherheit
Schutzadressat	Natürliche betroffene Personen mit ihren Rechten und Freiheiten	Institutionen, die ihre IT rechtmäßig einsetzen	Datenschutz ist Grundrechtsschutz
Hauptgefährdung	Stelle, die (auch rechtskonform) pbDaten verarbeitet	Interne und externe Angreifer	
Zielsetzung	Bei legitimen Zweck und tragfähiger Rechtsgrundlage müssen die 7 SDM-Gewährleistungsziele erfüllt sein	Die mit IT-Systemen verarbeiteten Daten sollen integer, vertraulich und verfügbar bleiben	SDM-Gewährleistungsziele enthalten auch Integrität, Vertraulichkeit und Verfügbarkeit
Spezielle Aufsicht	Unabhängige behördliche Datenschutzaufsicht	Punktuell behördliche Aufsicht (z. B. KRITIS)	

Abb. 19: Wichtige Unterschiede zwischen Datenschutz und IT-Sicherheit

Mit Blick auf die Risikoanalyse, wie diese das BSI in seinem Standard „200-3: Risikoanalyse auf Basis von IT-Grundschutz“ beschreibt, existieren folgende **Berührungspunkte**:

- **Grundwerte.** – Die drei Gewährleistungsziele „Vertraulichkeit“, „Verfügbarkeit“ und „Datenintegrität“ entsprechen grundsätzlich den drei Grundwerten der IT-Sicherheit.
- **Methode.** – Im Datenschutz wie auch in der IT-Sicherheit kann grundsätzlich die Methode des Risikomanagements im Rahmen der Risikoanalysen eingesetzt werden.
- **Szenarien.** – In der Sicherheit der Verarbeitung und der IT-Sicherheit sind die betrachteten Szenarien, die das BSI begrifflich als „Gefährdungen“[44] bezeichnet, größtenteils deckungsgleich.
- **Eintrittswahrscheinlichkeit.** – Die Wahrscheinlichkeit des Eintritts eines Szenarios bzw. einer Gefährdung wird in beiden Gebieten auf gleiche Art und Weise ermittelt.
- **Ausgangs- und Restrisiko.** – Auf beiden Gebieten wird in einem ersten Schritt das Ausgangsrisiko und nach Zuordnung der einschlägigen TOMs das Restrisiko bestimmt.[45]
- **TOMs.** – TOMs, die identifizierten Szenarien zugeordnet sind, sind der eigentliche Antrieb für die beiden Gebiete Sicherheit der Verarbeitung und IT-Sicherheit. Bei den TOMs besteht grundsätzlich ein sehr hoher Überdeckungsgrad, auch wenn bestimmte TOMs aus Datenschutzgründen anders ausgestaltet werden müssen (z. B. restriktivere Aufbewahrungsdauer von Protokollierungen).

Diese Berührungspunkte haben bereits die eine oder andere Institution dazu gebracht, eine Risikoanalyse der IT-Sicherheit auch als datenschutzrechtliche Risikoanalyse ohne Beachtung der folgenden wesentlichen **Unterschiede** zu verwenden:

[44] Der im BSI verwendete Begriff „Gefährdung“ ist nicht deckungsgleich mit dem im Zusammenhang des Zielerfüllungsmanagements genutzten, gleichlautenden Begriff (vgl. Punkt III.4).

[45] Vgl. BSI-Standard 200-3 (Fn. 11), S. 34 und Kapitel 6.2.

- **Fokussierung des Schutzes.** – Die datenschutzrechtliche Risikoanalyse hat die Rechte und Freiheiten natürlicher Personen, die von der Zielverarbeitung betroffen sind, im Fokus. Die Risikoanalyse in der IT-Sicherheit hat hingegen die Interessen der Institution oder der Person, die IT-Systeme rechtmäßig betreiben und nutzen, im Fokus. Hierin liegt ein wesentlicher Unterschied zwischen den Risikoanalysen beider Gebiete.

- **Schutzgegenstand.** – In der IT-Sicherheit sind alle Objekte von Interesse, die im Zusammenhang mit der IT-Nutzung stehen. Im Datenschutz ist die Verarbeitung von personenbezogenen Daten der Schutzgegenstand der Risikoanalyse.

- **Gewährleistungsziele.** – Der Datenschutz spannt mit seinen sieben Gewährleistungszielen einen Schutzschirm auf, der weit über die drei Grundwerte „Vertraulichkeit", „Verfügbarkeit" und „Integrität" der IT-Sicherheit hinausreicht.

- **Höhe des Schadens.** – Die Folgen beim Eintritt eines Szenarios bzw. einer Gefährdung und damit auch die Schadenshöhe sind aufgrund einer anderen Schutzausrichtung unterschiedlich zu betrachten und nicht selten unterschiedlich zu bewerten. Allerdings sind relevante Schadenspositionen im Sinn des Datenschutzes, die durch IT-Systeme verursacht wurden, stets auch mit relevanten Folgen für die IT-Sicherheit verbunden. Denn technische Datenschutzpannen beeinflussen zumindest auch das Image einer Institution.

  Beispiel: Ein „Imageverlust der Institution" kann zwar als Schadensposition bei einer Risikoanalyse für die IT-Sicherheit aufgeführt werden. Bei der datenschutzrechtlichen Risikoanalyse mit dem Blick auf betroffene Personen stellt der Imageverlust der Institution jedoch keine Schadensposition dar.

- **Risikoindex.** – Im Datenschutz gibt es die drei folgenden Risikoabstufungen: „geringes Risiko", „normales Risiko" und „hohes Risiko" (siehe Punkt III. 3.). In der IT-Sicherheit schlägt beispielsweise das BSI einen vierstufigen Risikoindex mit dem Hinweis vor, diesen bei Bedarf auf die eigenen Bedürfnisse anzupassen.[46]

Auch wenn deutliche Unterschiede zwischen der datenschutzrechtlichen Risikoanalyse und der Risikoanalyse der IT-Sicherheit bestehen, sind grundsätzlich nicht wenige Komponenten und Bereiche, wie etwa Szenarien, deren Eintrittswahrscheinlichkeit und die wirksam umgesetzten TOMs, wiederverwendbar bzw. für Verweisungen nutzbar.

c) Weitere Optimierungspotenziale

Bei datenschutzrechtlichen Risikoanalysen können insbesondere folgende Optimierungspotenziale und Fehler beobachtet werden:

- **Gemeinsames Vorgehensmodell.** – Grundsätzlich ist es naheliegend, dass in einer Institution die Methode für das Risikomanagement unterschiedlicher Anwendungsbereiche (z. B. Datenschutz, IT-Sicherheit, Arbeitsschutz) soweit wie möglich vereinheitlicht wird.

[46] Vgl. BSI-Standard 200-3 (Fn. 11), S. 27.

Dazu sollten sich die betroffenen Bereiche – eventuell unter Einsatz einer intern koordinierenden Stelle – hinsichtlich der verwendeten Grundmethode und dem konkreten Vorgehen abstimmen.

- **Auswahl eines Pilotbereichs.** – Sollte erstmalig eine DSFA oder Risikoanalyse-Allgemein durchgeführt werden, kann es ratsam sein, mit einer Zielverarbeitung zu beginnen, deren Komplexität möglichst niedrig und überschaubar ist. Denn dann kann der Schwerpunkt bei der Durchführung auf die Methode der Risikoanalyse gelegt werden und diese durch Praxiserfahrungen besonders rasch selbst erfahren und gefestigt werden. Zudem kann der Start mit einer fachlichen Organisationseinheit, die im Umfeld von Risikomanagement bereits Know-how besitzt oder bei der ein besonderer Handlungsbedarf besteht, für eine erste Pilotdurchführung hilfreich sein.
- **Synergien nutzen.** – Falls Institutionen sehr ähnliche und vergleichbare Verarbeitungsvorgänge haben, liegt es nahe, sich miteinander abzustimmen und effiziente Wege für die Durchführung der entsprechenden Risikoanalysen zu suchen.

  Beim Angebot von „good practice"-Unterlagen, Vorlagen und sonstigen Mustern würde ein besonders hoher Mehrwert geschaffen werden, wenn TOMs eingebettet in einer datenschutzrechtlichen Risikoanalyse dargestellt werden. Denn dann bräuchten Verantwortliche diese Muster nur noch auf ihre konkrete Zielverarbeitung anpassen und verifizieren sowie die Risikoanalyse um die Risiken ergänzen, die für die jeweilige verantwortliche Stelle technik- und organisationsspezifisch sind.
- **Hersteller und Lieferanten mit einbinden.** – Bei Beschaffungen können Zuarbeiten zu den Risikoanalysen durch die Lieferanten als Leistungspositionen ausdrücklich vereinbart werden. In besonderen Konstellationen ist sogar eine formale Aufteilung der Risikoanalyse denkbar (siehe Punkt VI. 5.).
- **Ausgangsrisiken mit Berücksichtigung von TOMs.** – Nicht selten werden fälschlicherweise bei der Bewertung des Ausgangsrisikos zugehörige TOMs schon risikomindernd mit berücksichtigt (siehe Punkt IV. 4.).
- **Konsistenz durch Ankerstellen gewährleisten.** – Häufig werden dieselben Aspekte an mehreren Textstellen unterschiedlich und damit inkonsistent dargestellt. Daher sind die unter dem Punkt VI. 2. b) schon gegebenen Empfehlungen besonders wichtig.

4. Skalierbarkeit

Nach Art. 24, 25 und 32 DSGVO bzw. Art. 35 DSGVO trifft den Verantwortlichen die Pflicht, für grundsätzlich alle Verarbeitungsvorgänge nachzuweisen, dass ein dem Risiko angemessenes Schutzniveau bei der Verarbeitung besteht. Da sich Zielverarbeitungen insbesondere mit Blick auf ihr Risikoprofil und auf ihr jeweils angemessenes Schutzniveau deutlich unterscheiden können, stellt sich die Frage, ob und, wenn ja, wie eine Risikoanalyse entsprechend ihrem Kontext unterschiedlich tiefgehend gestaltet und skaliert werden kann.

Wie ein roter Faden zieht sich das Prinzip der Risikoorientierung durch die gesamte DSGVO (vgl. Punkt V. 1. b)). Die Risikoorientierung hat grundsätzlich auch Einfluss auf die Mindestanforderungen der zu erbringenden datenschutzrechtlichen Nachweise. Folglich steigen die Mindestanforderungen an die Risikoanalyse zusammen mit der jeweiligen Höhe des Ausgangsrisikos. Da eine Risikoanalyse zudem hinreichend klar, verständlich, systematisch und für ihre Adressaten (siehe Punkt VI. 1.) auch gut nachvollziehbar sein muss, hat die jeweilige Komplexität sowohl der Zielverarbeitung als auch der Risikoanalyse-Bausteine ebenfalls Einfluss auf die Mindestanforderungen.

Bei jeder Risikoanalyse müssen das Ausgangsrisiko, eventuell auch in zusammenfassender, genereller Form, die betrachteten Szenarien, die Risikobewertungen und TOMs klar erkennbar sein sowie deren Vollständigkeit und Plausibilität von den Adressaten der Risikoanalyse nachvollzogen werden können.

Nach einer solchen Rahmensetzung können Risikoanalysen und deren Mindestanforderungen wie folgt in die drei Ausbaustufen „S–Small“, „M–Medium“ und „L–Large“ unterteilt werden.

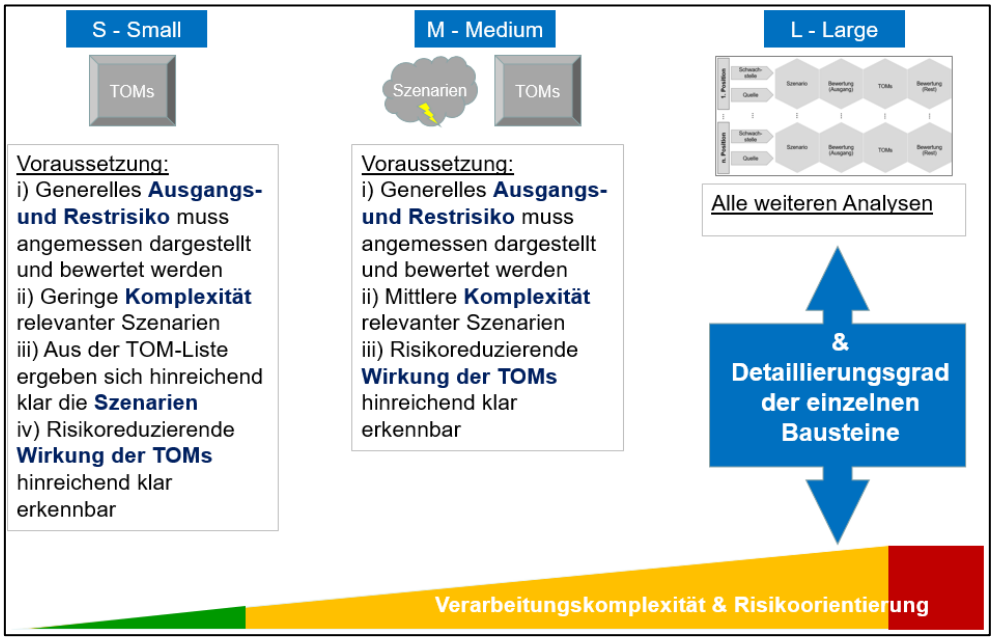


Abb. 20: Ausbaustufen und Skalierbarkeit einer Risikoanalyse

Die **Ausbaustufe „L–Large“** ist jedenfalls dann zu wählen, wenn hohe Ausgangsrisiken bestehen und/oder die Zielverarbeitung und/oder die zu betrachtenden Szenarien eine hohe Komplexität aufweisen. Bei der Ausbaustufe „L–Large“ enthält die Risikoanalyse alle fünf schon beschriebenen Bausteine (siehe Punkt IV.). Daher kann die Risikoanalyse dieser Ausbaustufe durch den inhaltlichen Detaillierungsgrad der einzelnen Bausteine punktuell vergröbert und verfeinert werden sowie durch weitere optionale Bausteine (z. B. „Angreifermodell“, vgl. Punkt IV. 2.) ergänzt werden.

VI. Praxishinweise für Risikoanalysen

Die Auswahl der Granularität der Bausteininhalte ist ein Skalierungsmittel, das stets risiko- und komplexitätsorientiert genutzt werden sollte und bei allen Risikoanalysen in jeder Ausbaustufe zur Verfügung steht. Ein Beispiel hierfür ist die Aggregation im Einzelfall zusammenhängend zu betrachtender Einzelszenarien zu einem Hauptszenario, etwa im Bereich der Intervenierbarkeit das Szenario „Betroffenenrechte können insbesondere aufgrund interner Organisationsabläufe nicht rechtzeitig und wirksam ausgeübt werden". Bei effektiver Nutzung dieser Skalierungsmöglichkeit kann eine Risikoanalyse ohne unnötigen Dokumentationsaufwand erstellt werden. Denn die in den Bausteinen dokumentierbaren Inhalte sind grundsätzlich unverzichtbarer Analyseschritte bei jeder Risikoanalyse. Insbesondere bei größeren Institutionen kann aus Einheitlichkeitsgründen angeraten sein, alle Risikoanalysen in dieser Ausbaustufe zu erstellen.

Bei den beiden kleineren Ausbaustufen „M–Medium" und „S–Small" muss das Ausgangsrisiko der Zielverarbeitung so dargestellt werden, dass daraus auch die getroffene Wahl der Ausbaustufe begründet und plausibel wird.

Bei der **Ausbaustufe „M–Medium"** werden nur das generelle Ausgangs- und Restrisiko sowie die relevanten Szenarien zusammen mit den ihnen zugeordneten TOMs dargestellt. Dabei dürfen die einschlägigen Szenarien sowie die Zielverarbeitung maximal eine mittlere Komplexität aufweisen und die risikoreduzierende Wirkungsweise der jeweils zugeordneten TOMs klar erkennbar und einschätzbar sein.

Bei der **Ausbaustufe „S–Small"** werden nur das generelle Ausgangs- und Restrisiko sowie die TOMs dargestellt (diese können etwa bei der Beschreibung der Verarbeitungstätigkeit im Bereich „Allgemeine Beschreibung der TOMs" gemäß Art. 32 Abs. 1 DSGVO aufgelistet und konkretisiert werden). Diese deutliche Verkürzung der Dokumentation darf nur erfolgen, wenn die einschlägigen Szenarien sowie die Zielverarbeitung eine geringe Komplexität aufweisen und die risikoreduzierende Wirkungsweise der jeweils zugeordneten TOMs klar erkennbar und einschätzbar sein. Zudem müssen auf Grundlage der beschriebenen TOMs klar und eindeutig die Szenarien hervorgehen, die bei der Risikoanalyse berücksichtigt wurden.

5. Verteilte Risikoanalyse

Wirken bei einer Verarbeitungstätigkeit oder bei einer sonstigen, in einem engen fachlichen Sachzusammenhang stehenden Verarbeitung mehrere Stellen unmittelbar oder nur mittelbar zusammen, kann die formale Aufteilung der Risikoanalyse nach Wissens- und Zuständigkeitssphären sowie aus Effizienz-, Konsistenz- und Aktualitätsgründen im Einzelfall sinnvoll sein. Ein solches Zusammenwirken kann insbesondere bei einem Verantwortlichen-Auftragsverarbeiter-, bei einem Verantwortlichen-Hersteller-Verhältnis und bei einer gemeinsamen Verantwortlichkeit beobachtet werden. Derartigen Konstellationen zeichnen sich oft dadurch aus, dass verwendete Verarbeitungsmittel von einer der beteiligten Stelle besonders aus faktischen oder wissensbasierten Gründen betreut, weiterentwickelt und „beherrscht" werden.

IT-Systeme werden immer komplexer und ändern nicht selten dynamisch ihre Unterstützung von Verarbeitungen (z. B. agile Softwareentwicklung). Zudem entfernen sich IT-Systeme, etwa in der Form von Cloud-Diensten, immer weiter weg aus dem direkten Einflussbereich

des Verantwortlichen. Daher liegt nahe, das relevante, oft sehr spezielle Know-how externer IT-Systemhersteller, IT-Systembetreiber und IT-Diensteanbieter direkt in die Risikoanalyse mit einfließen zu lassen.

Bei zentralen IT-Systemen, die mehrere Verantwortliche gleichzeitig einsetzen, kann zudem aus Effizienz-, Konsistenz- und Aktualitätsgründen eine sachgerechte Aufteilung der Risikoanalyse geboten sein.

Typischerweise kann die Risikoanalyse in solchen Konstellationen in zwei Teile aufgeteilt und diese Teile mit entsprechenden Verweisungen fest miteinander verbunden werden.

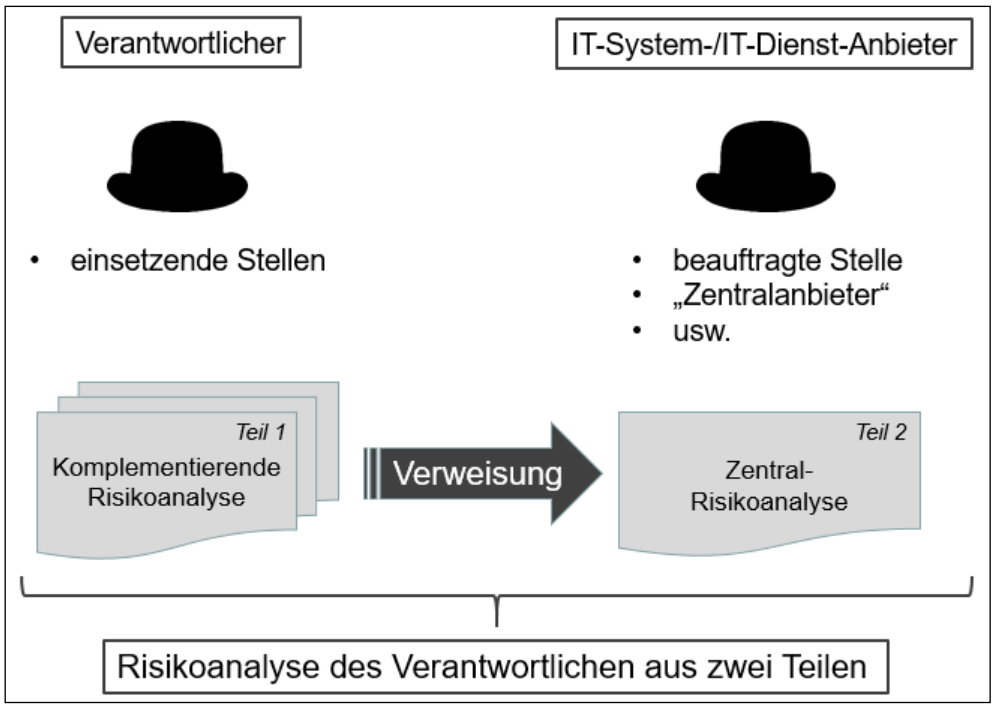


Abb. 21: Schematische Übersicht einer verteilten Risikoanalyse

Die „Zentral-Risikoanalyse“ (Teil 2 der Risikoanalyse) betrachtet und umfasst die Risiken des zentralen IT-Systems bzw. der Verarbeitungsmittel, für deren Risikoanalyse nach entsprechender Vereinbarung der Hersteller von genutzten Verarbeitungsmitteln oder der Systembetreiber zuständig ist.

Die Zentral-Risikoanalyse wird durch den Teil der Risikoanalyse, den der Verantwortliche selbst erstellt und pflegt (Teil 1 der Risikoanalyse), ergänzt. Darin behandelt der Verantwortliche insbesondere die bei ihm spezifisch vorliegenden Risiken, die sich aus den vom Verantwortlichen dezentral genutzten Betriebsmitteln (z. B. IT-unterstützte Arbeitsplätze, Drucker) und aus seiner Organisation (z. B. Ausprägung der Geschäftsprozesse) ergeben.

Der Teil 1 muss eindeutig auf den Teil 2 der Risikoanalyse verweisen, um beide Teile zur vollständigen Risikoanalyse zusammensetzen zu können.

VI. Praxishinweise für Risikoanalysen

Auch bei einer verteilten Risikoanalyse muss der Verantwortliche den Nachweis in Form einer DSFA oder einer Risikoanalyse-Allgemein gesamtheitlich erbringen (vgl. Art. 24 Abs. 1 und Art. 35 Abs. 1 DSGVO). Daher ist immer zu gewährleisten, dass der Verantwortliche bedarfsgerechten Zugriff auch auf die Zentral-Risikoanalyse, und zwar sowohl auf deren Dokumentation (Risikoanalyse-Bericht) als auch auf die Information hat, aus der sich die wirksame Umsetzung aller darin enthaltenen TOMs ergibt.

Bei einer solchen Offenlegung der Zentral-Risikoanalyse gegenüber im Einzelfall denkbar zahlreichen einsetzenden Stellen können Bedenken der Ersteller der Zentral-Risikoanalyse bezüglich Sicherheit und Geschäftsgeheimnissen aufkommen. Zwar sollte jeder Produktlieferant und jeder Auftragsverarbeiter dem Verantwortlichen und anderen relevanten Beteiligten hilfreiche Informationen bereitstellen. Dabei sollte aber darauf geachtet werden, keine Geheimnisse preiszugeben und insbesondere durch die Offenlegung von Schwachstellen keine Sicherheitsrisiken, insbesondere keine größere Angriffsfläche zu verursachen.[47]

Der Verantwortliche bleibt jedoch verantwortlich. Das gilt auch dann, wenn er sich Leistungen in der Form einer Risikoanalyse von Anbietern zunutze macht. Die Gesamtdokumentation muss daher so beschaffen sein, dass der Verantwortliche seiner Rechenschaftspflicht nachkommen kann. Zumindest gegenüber der Datenschutz-Aufsichtsbehörde können Geschäftsgeheimnisse die Kontrolldichte nicht verringern.[48]

Dieses **Spannungsverhältnis** zwischen der gesetzlichen **Nachweispflicht** des Verantwortlichen und der **Sicherheit** sowie dem Interesse des Zentral-Risikoanalyse-Erstellers am Schutz seiner Geschäftsgeheimnisse kann beispielsweise im Einzelfall wie folgt aufgelöst werden:

- **Granularität und Verweisung.** – Der Bericht zur Zentral-Risikoanalyse stellt die Bausteine zwar vollständig und nachvollziehbar, aber in einem Detaillierungsgrad dar, der keine Bedenken bezüglich der Wahrung von Geschäftsgeheimnissen auslöst. Dabei muss allerdings auf die weiterführenden Unterlagen des Zentral-Risikoanalyse-Erstellers so verwiesen werden, dass im Fall eines überwiegenden berechtigen Interesses des Verantwortlichen die relevanten und eindeutig zitierten Unterlagen diesem zur Verfügung gestellt werden können (siehe Punkt VI. 2. b)).
- **Besondere Maßnahmen zur Vertraulichkeit.** – Kann der Verantwortliche ein Interesse, das im Einzelfall höher als das Interesse am Schutz von Geschäftsgeheimnissen zu werten ist, gegenüber dem Zentral-Risikoanalyse-Erstellers nachweisen, so können risikoorientiert begleitende Schutzmaßnahmen bei der zur Verfügungsstellung der einschlägigen TOM-Unterlagen ergriffen werden (z. B. Verschwiegenheitsvereinbarung, Zugriff nur für zur Verschwiegenheit verpflichtete Beschäftigter des Verantwortlichen, Einsatz eines Treuhänders).

Vor dem dargestellten Hintergrund sollte vor IT-Beschaffung grundsätzlich die sachgerechte Zuarbeit zur Risikoanalyse der künftigen Auftragnehmer betrachtet und gegebenenfalls diese

[47] Siehe WP 248 (Fn. 8) S. 8.

[48] Eine Grenze gibt es hier allenfalls bei Art. 16 Abs. 2 Satz 2 BayDSG, der aber keine Geschäfts-, sondern Staatsgeheimnisse betrifft.

Zuarbeit als Leistungsposition inklusive des Regelungsrahmens ausdrücklich in die Leistungsbeschreibung mit aufgenommen werden.

6. Aktualisierung

Eine Risikoanalyse ist nicht statisch, sondern muss dynamisch bei wesentlichen Änderungen der Zielverarbeitung oder ihres Kontextes angepasst werden (vgl. insbesondere Art. 24 Abs. 1 Satz 2 DSGVO).

Darüber hinaus erfordert die Überprüfungs- und Aktualisierungspflicht, auch bestehende IT-Systeme regelmäßig in Augenschein zu nehmen, insbesondere im Hinblick auf geänderte Rechtsvorschriften, auf wesentliche Verfahrensänderungen (etwa durch Hinzunahme neuer Datenarten), auf veränderte Zuständigkeiten sowie auch auf Weiterentwicklungen hinsichtlich des Standes der Technik (beispielsweise geänderte Anforderungen an Verschlüsselungsverfahren). Der notwendige regelmäßige Überprüfungsturnus – also nicht anlassbezogen – ist risikoorientiert zu bestimmen, jedoch spätestens als Zwei- bis Fünf-Jahres-Rhythmus auszugestalten. Die insoweit durchgeführten Prüfungen müssen schriftlich dokumentiert werden.

VII. Anwendungsfall 1: Datenschutz-Folgenabschätzung (DSFA)

1. Einführung

Als ersten Anwendungsfall für die vorgestellte Methode einer datenschutzrechtlichen Risikoanalyse wird die Risikoanalyse für Verarbeitungsvorgänge betrachtet, die (voraussichtlich) eine Hochrisikoverarbeitung darstellen. Denn bei Verarbeitungsvorgängen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen ist die DSFA (Art. 35 DSGVO) das vorgegebene Nachweis-Instrument. Mit Hilfe der DSFA sind Verarbeitungsvorgänge, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen mit sich bringen, grundsätzlich vor ihrem Beginn auf ihr mögliches Schadenspotenzial zu prüfen und zu bewerten. Wesentliches Ziel der DSFA ist es, auf Basis der gewonnenen Erkenntnisse geeignete technische und organisatorische Maßnahmen (TOMs) nachhaltig umzusetzen, um die ermittelten Risiken auf ein angemessenes Maß zu reduzieren.

Im Unterschied zu der Risikoanalyse-Allgemein (siehe Punkt VIII.) ist die DSFA nach der Konzeption der DSGVO ein spezielles und formalisiertes Verfahren für Hochrisikoverarbeitungen. Dies bedeutet, dass der Verantwortliche grundsätzlich[49] eine DSFA für jeden Verarbeitungsvorgang nachweisen muss, der voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Generelle Ausführungen zur DSFA, wie etwa die Erforderlichkeit einschließlich eines Prüfschemas, sind ausführlich in meiner Orientierungshilfe „Datenschutz-Folgenabschätzung“ dargelegt.[50]

Nach der Sichtung bereits bestehender DSFA-Methoden folgte die Erkenntnis, dass die Kombination verschiedener, schon bestehender DSFA-Ansätze zielführend erscheint.

Die DSFA-Methodik „Privacy Impact Assessment“ (→PIA) der französischen Datenschutz-Aufsichtsbehörde CNIL wird als methodische Grundlage verwendet und punktuell in nicht widersprüchlichen Bereichen mit Komponenten des SDM sowie mit dem DSFA-Papier[51] und dem Risikomanagement[52] der Datenschutzkonferenz kombiniert. Der aufgezeigte Lösungsweg sollte auch für Befürworter einer „reinen Methodenanwendung“ – ggf. mit kleinen Anpassungen – gangbar sein.

[49] Zur DSFA-Erforderlichkeitsprüfung und insbesondere zu den Ausnahmen, eine eigene DSFA durchzuführen, siehe den folgenden Punkt VII.2.

[50] Die Orientierungshilfe ist auf https://www.datenschutz-bayern.de in der Rubrik „DSFA“ abrufbar.

[51] Vgl. Datenschutzkonferenz, Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, Kurzpapier Nr. 5, Internet: https://www.datenschutzkonferenz-online.de/kurzpapiere.html.

[52] Vgl. Fn. 2.

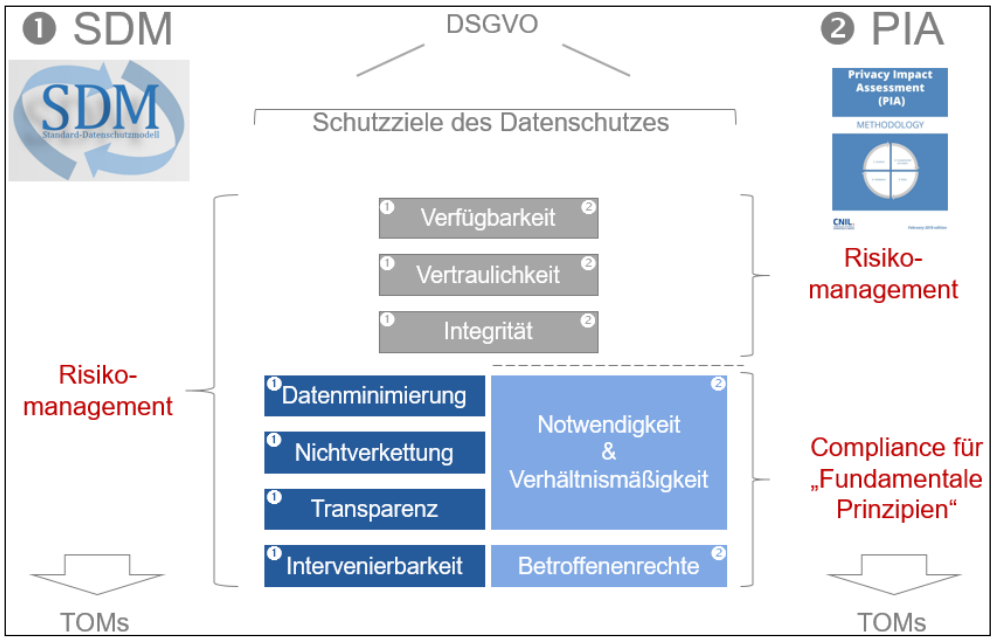


Abb. 22: Übersicht der verwendeten DSFA-Methoden

Auch wenn SDM und PIA insbesondere die Schutzziele des Datenschutzes teilweise etwas anders gruppieren und PIA die Methode des klassischen Risikomanagements für die sogenannten „Fundamentalen Prinzipien“ als eine Teilmenge der Schutzziele ausdrücklich ausschließt,[53] ist die eigentliche Zielrichtung und das angestrebte Ergebnis beider Methoden identisch: **Die betrachtete Datenverarbeitung soll mit Hilfe von identifizierten und wirksam umgesetzten TOMs nachweislich die DSGVO einhalten.**

Die von mir empfohlene Methode, die auf bereits Bestehendes und Anerkanntes Bezug nimmt und dieses kombiniert, erscheint auch in der Praxis als ausreichend verständlich, flexibel und skalierbar. So dienten meine Empfehlungen bereits als Basis für die DSFA von einfacheren und komplexeren folgenabschätzungspflichtigen Verarbeitungsvorgängen sowie als Grundlage für eine gesetzliche DSFA nach Art. 14 Abs. 1 Nr. 2 BayDSG.

Die im Folgenden aufgezeigte DSFA konzentriert sich auf die Mindestanforderungen (siehe Punkt VII.3.a)) und kann in fast beliebigem Maße weiter ausgebaut sowie detailliert werden.

2. Erforderlichkeitsprüfung

Die Prüfung, ob für eine bestimmte Verarbeitungstätigkeit oder ein sonstiger Verarbeitungsvorgang eine DSFA erforderlich ist, ist ein eigenständiger wichtiger Prüfschritt. Falls eine Pflicht zur Durchführung einer eigenen DSFA bestehen und die betroffene Stelle keine entsprechende DSFA vorab durchgeführt haben sollte, kann die zuständige Aufsichtsbehörde wegen Verstoßes gegen Art. 35 Abs. 1 DSGVO von ihren Abhilfebefugnissen gemäß Art. 58

[53] Siehe Fn. 16.

Abs. 2 DSGVO Gebrauch machen, indem sie beispielsweise die wirksame Umsetzung bestimmter unverzichtbarer TOMs gegenüber dem Verantwortlichen anweist.

Die DSFA-Erforderlichkeitsprüfung ist der bisher dargestellten Risikoanalyse vorgelagert und davon zu unterscheiden.

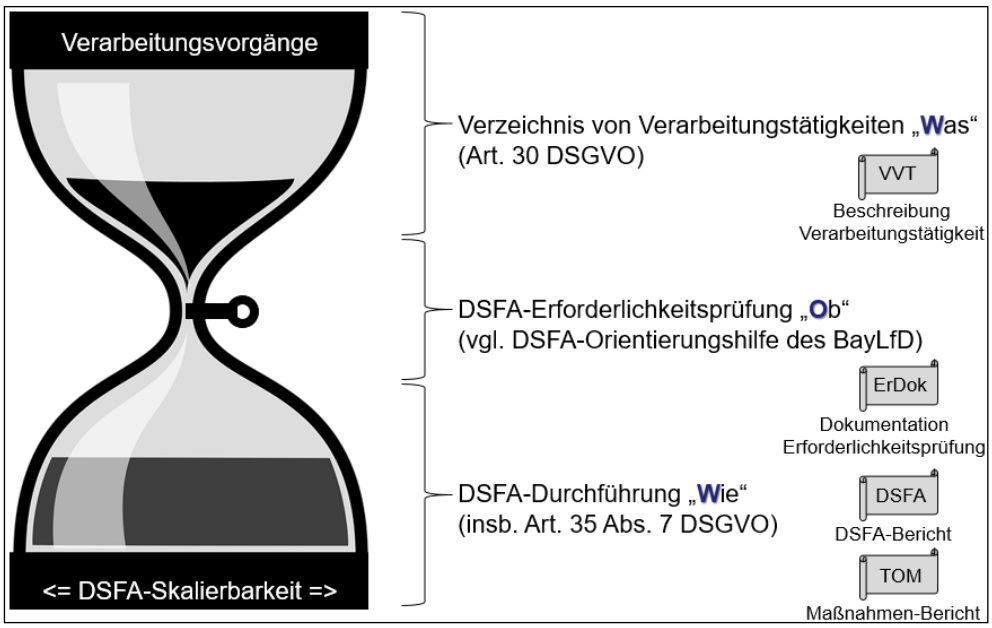


Abb. 23: Kontext der DSFA-Erforderlichkeitsprüfung

Generelle rechtliche Ausführungen zur DSFA, wie etwa die Erforderlichkeit einschließlich einem Prüfschema oder der Umgang mit Bestandsverfahren, sind ausführlich in der Orientierungshilfe „Datenschutz-Folgenabschätzung“ dargelegt.[54]

3. Durchführung

Die DSGVO selbst gibt mit den relativ abstrakt formulierten Anforderungen an die DSFA keine Antworten auf wichtige Methodenfragen und konkrete Vorgehensschritte. Die Entscheidung für eine bestimmte DSFA-Methode, die dann auch praxisgerecht durchführbar ist, ist für den einen oder anderen Verantwortlichen noch mit Schwierigkeiten verbunden.

Da eine veröffentlichte DSFA oder auch nur veröffentlichte Ausschnitte einer DSFA immer noch recht schwer zu finden sind, werden die von mir publizierten Arbeitshilfen, die einzelne DSFA-Arbeitsschritte anhand von konkreten Beispielen veranschaulichen und erleichtern, als Arbeitsgrundlage für bayerische öffentliche Stellen und weitere Einrichtungen gerne bereitgestellt. Dabei hilft die darin enthaltene Fokussierung auf das Wesentliche und die Konkretisierung der Mindestanforderungen an eine DSFA.

[54] Siehe Fn. 25.

a) Mindestanforderungen und Vorgehensschritte

Die Mindestanforderungen an eine DSFA haben Einfluss auf die Strukturierung des DSFA-Berichts. In jedem Fall ist der nach Art. 35 Abs. 7 DSGVO gesetzlich vorgegebene Mindestinhalt einer DSFA abzubilden. Bei der DSFA besteht zusätzlich die Besonderheit, dass im Fall einer sich an die DSFA anschließenden Konsultation nach Art. 36 DSGVO die eigentlichen DSFA-Mindestaspekte durch weitere Informationen ergänzt werden müssen. Zwar sollte eine Konsultation ein eher selten vorkommender Fall sein und sind diese Ergänzungen nicht Teil der eigentlichen DSFA, eine weitest mögliche Berücksichtigung dieser zusätzlichen Angaben im Rahmen der DSFA-Erstellung erscheint jedoch empfehlenswert. Dabei wird der Punkt „Sonstige angeforderte Informationen“ nicht weiter berücksichtigt, da die davon ggf. betroffenen Inhalte einzelfallbezogen und vorab unbestimmt sind.

Damit ergeben sich folgende Mindestpositionen für einen DSFA-Bericht.

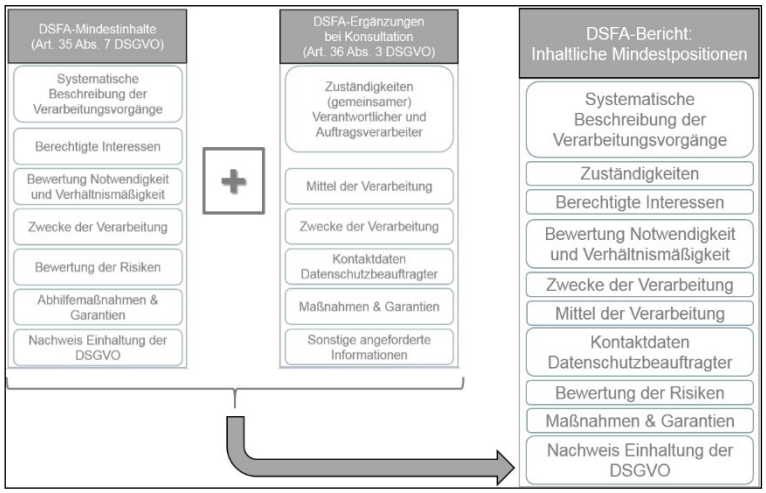


Abb. 24: Mindestpositionen eines DSFA-Berichts

Die Anforderung „Systematische Beschreibung der Verarbeitungsvorgänge“ kann basierend auf der vom PIA-Tool vorgegebenen inhaltlichen Gliederungsstruktur weiter aufgelöst und konkretisiert werden. Dies wird beispielhaft in den veröffentlichten Arbeitshilfen anschaulich gezeigt (siehe Punkt IX.).

Die beiden Positionen „Bewertung der Risiken“ und „Maßnahmen & Garantien“ im DSFA-Bericht weisen auf die Durchführung einer datenschutzrechtlichen Risikoanalyse im Rahmen einer DSFA hin. Folglich sind auch hier die bezüglich der sieben SDM-Gewährleistungsziele bestehenden Risiken und die zur Reduzierung festgelegten TOMs in Form einer datenschutzrechtlichen Risikoanalyse grundsätzlich mittels der schon dargestellten Bausteine (siehe Punkt IV.) zu dokumentieren. Auch die anderen Aspekte, die bereits für eine datenschutzrechtliche Risikoanalyse generell angesprochen wurden (siehe Punkt II. bis Punkt VI.), sind ebenfalls im Rahmen einer DSFA anwendbar. Wichtige Zusatzaspekte, die eine DSFA gegenüber einer allgemeinen Risikoanalyse aufweist, werden in der Abbildung 28 vergleichend gezeigt (siehe Punkt VIII.1).

Im Hinblick auf die Skalierbarkeit der Risikoanalyse einer DSFA wird regelmäßig die Ausbaustufe „Large“ angeraten sein (siehe Punkt VI.4). Nur ausnahmsweise, etwa bei einer geringen Verarbeitungskomplexität, ist auch die Ausbaustufe „Medium“ vorstellbar.

Insgesamt ergibt sich danach folgendes Bild zum DSFA-Bericht und dem dazugehörigen Maßnahmenmanagement. Die darin aufgezeigten Schritte der Risikobewertung und die darauf basierende Maßnahmenauswahl erfolgen so oft iterativ, bis das gewünschte Schutzniveau erreicht wird.

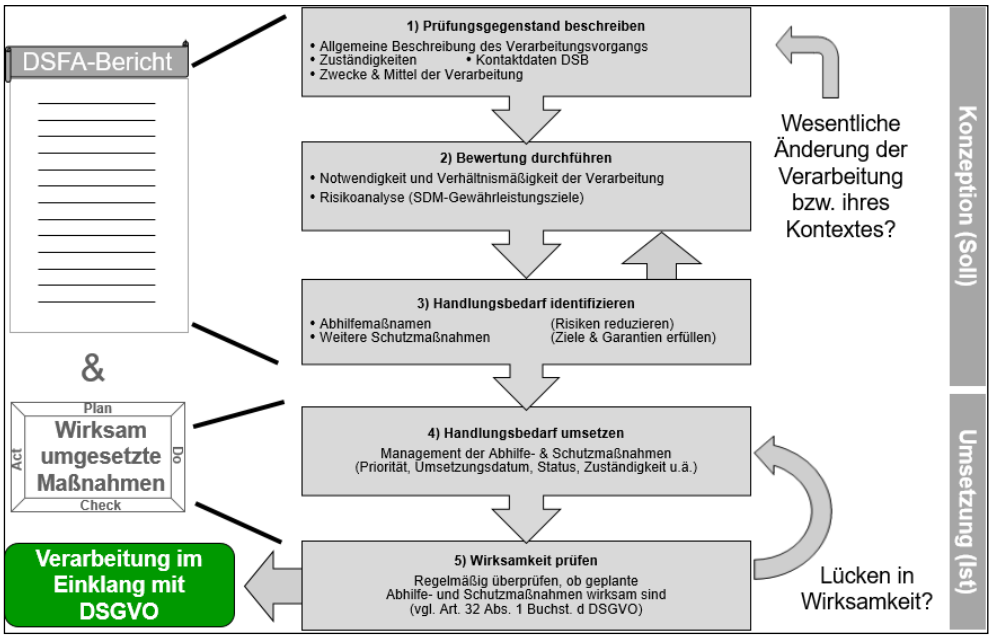


Abb. 25: DSFA, die sich aus dem DSFA-Bericht und dem Maßnahmenmanagement zusammensetzt

b) IT-Unterstützung für den DSFA-Bericht

Die Verwendung von Arbeitshilfen und speziellen IT-Anwendungen sind Möglichkeiten, die Durchführung einer DSFA zu erleichtern. Besonders effizient kann die Unterstützung sein, falls eine IT-Anwendung sowohl die Erstellung und Pflege des DSFA-Berichts als auch das sich daraus ergebende Maßnahmenmanagement unterstützt. Eine IT-Unterstützung kann allerdings mit noch weiteren Nutzenaspekten bedarfsgerecht für die einzelne Institution verbunden sein, indem die IT-Unterstützung beispielsweise auch das Geschäftsprozessmanagement, die IT-Sicherheit sowie weitere Themen mit einem hohen Überschneidungsbereich zum Datenschutz abdeckt.

Nicht selten wird es jedoch sinnvoll sein, vor einer größeren Beschaffung von IT-Systemen die Anforderungen an eine IT-Unterstützung für die betroffene Institution genau zu kennen. Diese Kenntnis kann sich aus einer pilothaft durchgeführten DSFA ergeben. Hierzu kann es hilfreich sein, die „Pilot-DSFA“ mit Hilfe einfacher, sofort zur Verfügung stehender und leicht anpassbarer IT-Werkzeuge durchzuführen.

Auf entsprechende Nachfragen hin habe ich einen „Werkzeugkasten“ für die Durchführung der DSFA und der Risikoanalyse-Allgemein auf meiner Homepage veröffentlicht, den ich bedarfsgerecht auch weiterhin ergänzen werde (vgl. Punkt IX.). Beim Einsatz meiner veröffentlichten Arbeitshilfen ergibt sich folgendes Gesamtbild für die verwendeten allgemein vorhandenen IT-Werkzeuge (Formulare aus Textverarbeitungsprogrammen und Tabellen aus Tabellenkalkulationsprogrammen).

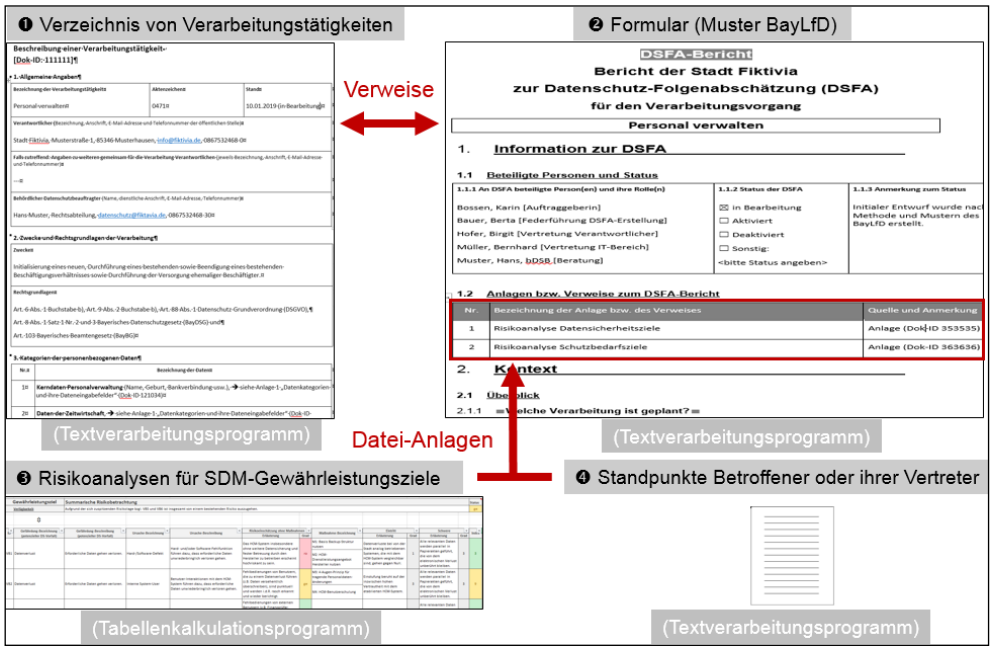


Abb. 26: Bausteine bei der Verwendung der veröffentlichten Arbeitshilfen für den DSFA-Bericht

Neben meinen veröffentlichten Arbeitshilfen zum DSFA-Bericht, deren Nutzung ich grundsätzlich für bayerische öffentliche Stellen empfehle, weise ich auch auf folgende öffentlich und frei zugänglichen IT-Werkzeuge hin:

- **PIA-Tool.** – Die französischen Datenschutz-Aufsichtsbehörde CNIL bietet neben einer umfangreichen Dokumentation zu ihrer DSFA-Methodik „Privacy Impact Assessment“ auch das sog. →PIA-Tool als Software-Unterstützung an, mit dessen Hilfe unter anderem ein DSFA-Bericht für die SDM-Datensicherheitsziele dokumentiert und ausgedruckt werden kann.[55]

[55] Vgl. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

– **ENISA-Tool.** – Die Agentur der Europäischen Union für Cybersicherheit ENISA stellt auf ihrer Homepage ein Online-Tool mit zusätzlichen Unterlagen für die Sicherheit der Verarbeitung personenbezogener Daten zur Verfügung.[56] Schwerpunkt dieser IT-Anwendung ist die Bewertung des Risikoniveaus einer Verarbeitung personenbezogener Daten.

Da diese Tools sowie deren Unterlagen ständig weiterentwickelt werden und teilweise schon Bewertungen hierzu existieren,[57] wird an dieser Stelle auf eine Bewertung verzichtet.

c) IT-Unterstützung für das Maßnahmenmanagement

Im DSFA-Bericht werden angemessene TOMs über Risikobewertungen hergeleitet und so identifiziert, dass diese im anschließenden Maßnahmenmanagement wirksam umgesetzt werden können. Eine DSFA wird daher immer anhand der Dokumentation des DSFA-Berichts und der Dokumentation der wirksam umgesetzten TOMs nachgewiesen (vgl. Abbildung 26). Wie beim allgemeinen Maßnahmenmanagement üblich, müssen die identifizierten TOMs insbesondere in der Form von Vorhaben oder Projekten nach Wichtigkeit und Dringlichkeit implementiert werden. Nach der Umsetzung muss die dauerhafte Wirksamkeit der Maßnahmen kontrolliert und nachgewiesen werden. Für die Unterstützung solcher Abläufe werden nicht wenige IT-Anwendungen angeboten, die das Verwalten und die strukturierte systematische Implementierung von Maßnahmen (TOMs, Aufgaben, Prozesse usw.) vereinfacht ermöglichen.

4. Zusammenspiel DSFA und Verzeichnis von Verarbeitungstätigkeiten

Eine besonders enge Verknüpfung hat die DSFA mit dem „Verzeichnis von Verarbeitungstätigkeiten". Denn die Beschreibung einer Verarbeitungstätigkeit umfasst Informationen, die auch für die DSFA benötigt werden. Um mögliche Inkonsistenzen zu vermeiden, ist bei der nachträglichen Durchführung einer DSFA, etwa im Fall von „Bestandsverfahren", eine gegenseitige Verweisung, wie im folgenden Schema gezeigt, gut denkbar.

[56] Vgl. https://www.enisa.europa.eu/risk-level-tool.

[57] Z. B. Bock/Gonscherowski/Schlehahn, Das PIA-Tool der CNIL im aufsichtsbehördlichen Praxistest, PinG 2019, 138 ff.; Hessischer Beauftragte für Datenschutz und Informationsfreiheit, 47. Tätigkeitsbericht, Nr. 4.10.3.

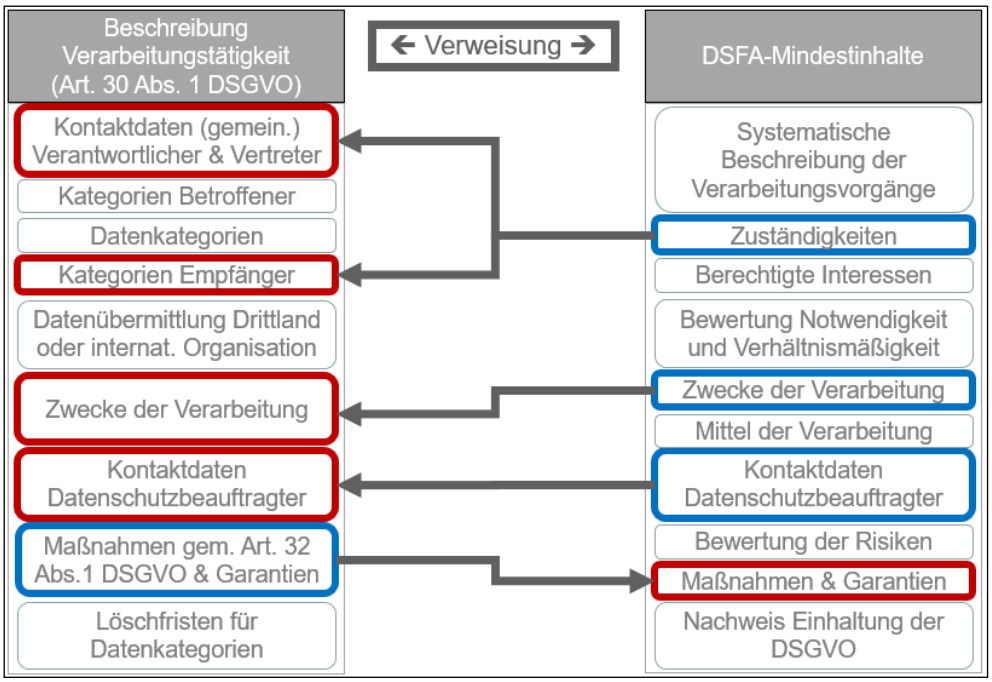


Abb. 27: Verweisungen zwischen der Beschreibung einer Verarbeitungstätigkeit und der DSFA

Grundsätzlich ist die DSFA jedoch vor dem Beginn des betrachteten Verarbeitungsvorgangs zu erstellen, also zu einem Zeitpunkt, zu dem der entsprechende Eintrag im Verzeichnis von Verarbeitungstätigkeiten noch fehlen könnte. In diesem Fall empfiehlt es sich aus Konsistenzgründen ebenfalls, an mehreren Stellen verwendete gleiche Informationen an einer „führenden" Stelle zu pflegen, etwa, indem der (zukünftige) Eintrag in das Verzeichnis von Verarbeitungstätigkeiten bereits im Vorfeld mit erstellt wird.

5. Weitere Aspekte zur DSFA

a) Zusammengesetzte DSFA

Wie schon beschrieben, kann auch eine DSFA grundsätzlich in zwei oder mehrere Teile aufgeteilt werden (siehe Punkt VI. 5.).

b) Gesetzliche DSFA[58]

Der bayerische Gesetzgeber kann unter den Voraussetzungen des Art. 35 Abs. 10 DSGVO eine DSFA durchführen und dadurch die Verantwortlichen entlasten (vgl. hierzu auch Art. 14 Abs. 1 Nr. 2 BayDSG).

[58] Die Ausführungen zur gesetzlichen DSFA entstammen dem im Auftrag des Bayerischen Staatsministeriums des Innern, für Sport und Integration erstellten Papier von Roßnagel u. a., Datenschutz-Folgenabschätzung Notfallregister, Version 1.2, Stand: 3/2021, im Internet abrufbar auf https://www.stmi.bayern.de/med/aktuell/archiv/2021/210506rettungsdienstgesetz/ unter „Downloads".

VII. Anwendungsfall 1: Datenschutz-Folgenabschätzung (DSFA)

Die Ausnahmeregelung des Art. 35 Abs. 10 DSGVO greift für den Verantwortlichen nur dann, wenn die Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 Buchst. c und e DSGVO auf einer Rechtsgrundlage im nationalen oder europäischen Recht beruht, der er unterliegt, und wenn diese Rechtsgrundlage den konkreten Verarbeitungsvorgang regelt.

Die gesetzliche DSFA muss nach Art. 35 Abs. 10 DSGVO ferner „im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage" erfolgen.

Weder der Verordnungswortlaut noch die Erwägungsgründe und die Gesetzgebungshistorie geben Hinweise darauf, ob und wie die vom Gesetzgeber vorzunehmende gesetzliche DSFA von der vom Verantwortlichen durchzuführende eigenen DSFA inhaltlich und formell abweicht. Die konkreten Anforderungen an die Gesetzes-DSFA lässt die DSGVO offen. Auch das BayDSG enthält dazu keine Hinweise.

Für die Ausgestaltung der gesetzlichen DSFA sind grundsätzlich die gleichen Maßstäbe anzulegen wie für eine vom Verantwortlichen selbst durchgeführten DSFA. Nur indem er sich an diesen Vorgaben zur Durchführung einer DSFA orientiert, kann der Durchführende die mit Art. 35 DSGVO verfolgten Schutzziele erreichen.

Allerdings ist der Unterschied zwischen der gesetzlichen Regelung eines Datenverarbeitungsvorgangs und der konkreten Durchführung eines Datenverarbeitungsvorgangs in der Realität zu berücksichtigen. Auch wenn die gesetzlichen Regelungen Anforderungen an die Gestaltung des Datenverarbeitungsvorgangs enthalten und bestimmte Schutzvorkehrungen vorsehen, bleibt eine entscheidende Differenz in der DSFA dieses Gesetzes zur DSFA einer realen Datenverarbeitung. Eine gesetzliche DSFA kann daher nur auf einer abstrakten Ebene die prinzipiellen Risiken erfassen und nur grundsätzlich geeignete Schutzvorkehrungen vorsehen. Sie kann nicht alle Risiken umfassend berücksichtigen, die in den konkreten Verarbeitungsvorgängen im Einzelfall auftreten können.

Da die Regelung des Art. 35 Abs. 10 DSGVO keine Absenkung des Niveaus der DSFA anstrebt, muss sich nachweislich aus dem Gesetzgebungsverfahren ergeben, dass der Gesetzgeber die potentiellen Risiken für die Grundrechte und Freiheiten der betroffenen Personen erkannt und bewertet hat sowie Abhilfemaßnahmen bezogen auf die erkannten Risiken veranlasst hat. Dies ist nur möglich, wenn eine methodisch abgesicherte DSFA auf Basis des Gesetzentwurfs erfolgt ist.

Bei der gesetzlichen DSFA ist zu berücksichtigen, dass gesetzliche Regelungen die Datenverarbeitungsvorgänge regelmäßig nicht umfassend konkret gestalten können, um allein auf der Grundlage dieser Regelungen die Risiken der Datenverarbeitung und ihre Bewältigung exakt beschreiben und bewerten zu können. Daher liegt es nahe, auch im Bereich der SDM-Datensicherheitsziele ausnahmsweise das Zielerfüllungsmanagement als Methode zu verwenden (siehe Punkt III. 4.). Dabei kann der Brückenschlag zum konkret ausgestalteten Risikomanagement der einzelnen verantwortlichen Stelle über eine spezielle TOM erfolgen, die in der gesetzlichen DSFA verankert ist. Eine solche TOM könnte beispielsweise die „Einrichtung eines Risikomanagements, das die technik- und organisationsspezifischen Risiken der jeweiligen verantwortlichen Stelle behandelt" sein.

Die gesetzliche DSFA ist abzugrenzen von dem Fall des Art. 14 Abs. 1 Nr. 1 BayDSG. Bei Art. 14 Abs. 1 Nr. 1 BayDSG führt das Ressort „nur“ die DSFA für den nachgeordneten Bereich durch, um diesen zu entlasten. Die Vorschrift knüpft an das alte Freigabeverfahren an,[59] ist losgelöst von einem etwaigen Gesetzgebungsvorgang und liegt thematisch näher bei den von Art. 14 Abs. 2 BayDSG erfassten Konstellationen.

Durch die Regelungen des Art. 14 BayDSG und Art. 35 Abs. 1 Satz 2 DSGVO entfällt also nicht das Erfordernis einer DSFA als solches. Vielmehr wurde diese bereits im Gesetzgebungsverfahren (Art. 14 Abs. 1 Nr. 2 BayDSG) beziehungsweise durch eine andere Stelle (Art. 14 Abs. 1 Nr. 1, Abs. 2 BayDSG) durchgeführt, oder es kann eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken verwendet werden (Art. 35 Abs. 1 Satz 2 DSGVO). Eine weitere DSFA durch den Verantwortlichen kann somit grundsätzlich unterbleiben, wenn dieser eine bereits entsprechend durchgeführte DSFA „als eigene“ übernimmt. Allerdings werden nicht selten zusätzliche organisationsspezifische Risiken vom Verantwortlichen zu berücksichtigen sein, so dass häufig eine zusammengesetzte DSFA (siehe Punkt VII.5.a)) in der Praxis erforderlich sein wird.

[59] Vgl. Bayerischer Landtag, LT-Drs. 17/19628, S. 38.

VIII. Anwendungsfall 2: „Risikoanalyse-Allgemein“

Die Risikoanalyse außerhalb einer DSFA wird zwar an unterschiedlichen Stellen erwähnt,[60] jedoch noch sehr überschaubar in der Literatur und Datenschutzpraxis behandelt. Diese datenschutzrechtliche Risikoanalyse wird im Folgenden als „Risikoanalyse-Allgemein“ bezeichnet.

1. Vergleich Risikoanalyse-Allgemein und DSFA

Die Risikoanalyse-Allgemein unterscheidet sich von der DSFA in wesentlichen Aspekten wie in der folgenden Abbildung dargestellt.

Aspekt	Risikoanalyse-Allgemein	DSFA (inkl. Risikoanalyse-DSFA)	Anmerkung
Pflicht zur Durchführung	Nachweis „Art & Weise der Verarbeitung ist im DSGVO-Einklang“ kann auch mit anderen Instrumenten geführt werden (z. B. Zertifizierung, Verhaltensregeln)	Bei „Hochrisikoverarbeitungen“ muss grds. DSFA durchgeführt werden, vgl. DSFA-Erforderlichkeitsprüfung	Auf freiwilliger Basis kann natürlich stets eine DSFA durchgeführt werden
Verpflichteter	Verantwortlicher	Verantwortlicher	
Mindestbestandteile	Risikoanalyse in der Ausbaustufe small, medium oder large	Risikoanalyse (i.d.R. large), systematische Beschreibung, ggf. Standpunkte betroffener Personen oder ihrer Vertreter	Wesentlicher Unterschied liegt in der systematischen Beschreibung und der Skalierbarkeit
Gegenstand	Zielverarbeitung	Zielverarbeitung	Siehe Punkt III.1
Empfohlene Methode	Risikomanagement Zielerfüllungsmanagement	Risikomanagement Zielerfüllungsmanagement	
Implementierungskosten TOM	sind ausdrücklich zu berücksichtigen	werden nicht genannt	
Rechtsgrundlage	Art. 24, 25, 32 DSGVO	Art. 35, 36 DSGVO	

Abb. 28: Vergleich Risikoanalyse-Allgemein und DSFA

Die in der Abbildung 28 dargestellte Übersicht zeigt, dass die Risikoanalyse-Allgemein im Vergleich zur DSFA ein vereinfachtes Verfahren darstellt. Aber auch wenn keine Hochrisikoverarbeitungen vorliegt, trifft den Verantwortlichen nach Art. 24, 25 und 32 DSGVO die Pflicht, geeignete technische und organisatorische Maßnahmen wirksam umzusetzen, um sicherzustellen, dass die Art und Weise einer Verarbeitung mit den Vorgaben der DSGVO in

[60] Vgl. z. B. Datenschutzkonferenz, Risiko für die Rechte und Freiheiten natürlicher Personen (Fn. 2), S. 6.

Einklang steht. Die Einhaltung dieser Pflicht muss bei Fehlen eines alternativen Nachweisinstruments (siehe Punkt III) durch den Verantwortlichen angemessen mittels einer Risikoanalyse-Allgemein dokumentiert werden.

2. Durchführung

Es wird empfohlen, eine Risikoanalyse-Allgemein grundsätzlich schrittweise wie folgt durchzuführen.

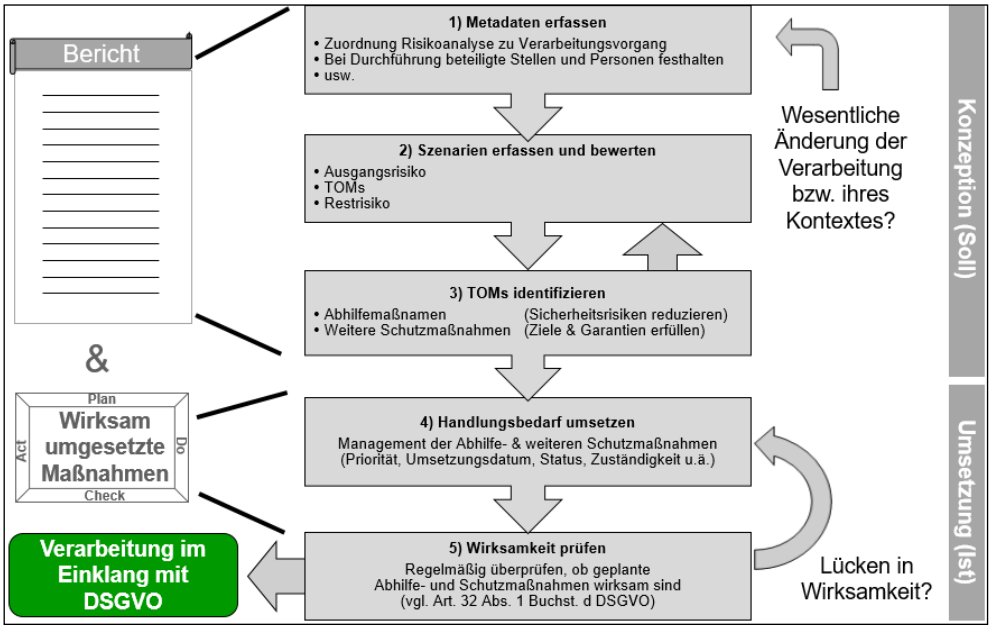


Abb. 29: Durchführung einer Risikoanalyse-Allgemein

Bei der Risikoanalyse-Allgemein sind die beiden aufeinander aufbauenden Bereiche „Konzeption“ und „Umsetzung“ wie folgt zu unterscheiden:

- **Dokumentation zur Risikoanalyse („Risikoanalyse-Bericht“).** – Der Bericht zur Risikoanalyse enthält zum einen eine Beschreibung der Zielverarbeitung sowie weitere Metadaten (z. B. Ersteller, Status, Aktivierungsdatum). Daneben sind die bezüglich der sieben SDM-Gewährleistungsziele bestehenden Risiken und die zur Reduzierung festgelegten TOMs in Form einer datenschutzrechtlichen Risikoanalyse grundsätzlich mittels der dargestellten Bausteine (siehe Punkt IV.) zu dokumentieren.
- **Wirksame Umsetzung der TOMs („Maßnahmenmanagement“).** – Wie beim allgemeinen Maßnahmenmanagement üblich, müssen auch die im Risikoanalyse-Bericht identifizierten TOMs insbesondere in der Form von Vorhaben oder Projekten nach Wichtigkeit und Dringlichkeit implementiert werden. Nach der Umsetzung muss die dauerhafte Wirksamkeit der Maßnahmen kontrolliert und nachgewiesen werden (siehe Punkt V. 1. g)).

VIII. Anwendungsfall 2: „Risikoanalyse-Allgemein“

Bei wesentlichen Änderungen der Zielverarbeitung oder ihres Kontextes muss die Risikoanalyse-Allgemein entsprechend angepasst werden (siehe Punkt VI. 6.). Eine Aufteilung der Risikoanalyse in mehrere Teile ist grundsätzlich möglich (siehe Punkt VI. 5.).

IX. Arbeitshilfen und Beispiele

Zu der Frage, wie ein Bericht zu einer DSFA (DSFA-Bericht) und zu einer Risikoanalyse-Allgemein (Risikoanalyse-Allgemein-Bericht), die eine öffentliche Stelle durchgeführt hat, grundsätzlich aussehen kann, sind aktuell kaum Beispiele veröffentlicht. Daher wurde ein Werkzeugkasten mit Arbeitshilfen bereitgestellt, die einzelne Arbeitsschritte der DSFA und der Risikoanalyse-Allgemein erleichtern sollen.[61] Dieser Werkzeugkasten harmoniert mit dem IT-Grundschutz-Baustein „CON.2 Datenschutz" des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie mit dem SDM.

Es stehen jeweils Leerformulare sowie Ausfüllbeispiele zur Verfügung. Insgesamt können bayerische öffentliche Stellen nun auf detaillierte Anleitungen und Hilfsmittel zurückgreifen, wenn sie DSFAs und Risikoanalysen-Allgemein durchführen.

Dieser Werkzeugkasten wird bedarfsgerecht weiter ausgebaut. Eine Übersicht und erläuternde Hinweise zu den aktuellen Modulen enthält das Dokument „Modulhinweis", das ebenfalls Teil des Werkzeugkastens ist.

[61] Siehe auf https://www.datenschutz-bayern.de die Rubrik „DSFA".

X. Glossar

Begriff /Abkürzung	Erläuterung
Auftragsverarbeiter	Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Nr. 8 DSGVO).
betroffene Person	Die betroffene Person ist das Gegenüber des Verantwortlichen. Ihre personenbezogenen Daten sind Gegenstand der Verarbeitung. Die DSGVO führt diese „Rolle" zusammen mit der Begriffsbestimmung der personenbezogenen Daten ein (Art. 4 Nr. 1 DSGVO).
BSI	Bundesamt für Sicherheit in der Informationstechnik (Internet: https://www.bsi.bund.de).
CNIL	Commission Nationale de l'Informatique et des Libertés (französische Datenschutz-Aufsichtsbehörde, Internet: https://www.cnil.fr).
personenbezogene Daten	Personenbezogene Daten nach Art. 4 Nr. 1 DSGVO.
Datenschutz-Schutzmaßnahmen	Alle Maßnahmen und Garantien, die für die Reduzierung bzw. Beseitigung von Risiken für die Rechte und Freiheiten natürlicher Personen vorgesehen sind, vgl. auch Eintrag „TOM(s) im Glossar.
Dok-ID	Jedes Dokument kann durch seine eindeutige Dokumenten-Identifikationsnummer (Dok-ID) aufgefunden und aufgerufen werden.
DSB	Datenschutzbeauftragter.
DSFA	Datenschutz-Folgenabschätzung nach Art. 35 DSGVO.
DSFA-Bericht	Ein Bericht/Report für eine DSFA.
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder; die DSK besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und

	gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen. Internet: https://www.datenschutzkonferenz-online.de/.
Fachapplikation	IT-System, das die fachliche Sachbearbeitung und damit die fachlichen Geschäftsprozesse unmittelbar unterstützt.
Geschäftsprozessmanagement	Das Geschäftsprozessmanagement ist eine praxiserprobte Methode insbesondere für die Dokumentation, zielgerichtete Steuerung und Überwachung von Prozessen und der gesamten Ablauforganisation einer Institution. Ein einzelner Geschäftsprozess wird dabei über folgende drei Bausteine beschrieben: Dem Auslöser, beliebig nachfolgende Aktivitäten und einem abschließenden Ergebnis. Die einzelne Aktivität in einem Prozess besitzt eine klare Zielsetzung, wird durch Akteure (z. B. Personen, IT-Systeme, Dienste) durchgeführt und benötigt für ihre Durchführung bestimmte Ressourcen.
Hochrisikoverarbeitung	Verarbeitungsvorgang mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten natürlicher Personen.
IT-Planungsrat	Über einen Staatsvertrag wurde der gemeinsame IT-Planungsrat von Bund, Ländern und Kommunen geschaffen mit dem Ziel, die Digitalisierung der öffentlichen Verwaltung voranzutreiben und Organisationsgrenzen zu überwinden, vgl. https://www.it-planungsrat.de.
Maßnahmenmanagement	Das Maßnahmenmanagement stellt sicher, dass beschlossene Maßnahmen insbesondere aus den Bereichen Datenschutz, IT-Sicherheit, Arbeitsschutz und Korruptionsschutz konsequent und organisatorisch etwa in der Form von Vorhaben und Projekten implementiert werden.
Mittel	Der Begriff „Mittel“ der Verarbeitung umfasst nach europäischer Auslegung insbesondere auch den Umfang der Datenverarbeitung, Speicherdauer, die genutzten Betriebsmittel usw.
mittelbares Betriebsmittel	Betriebsmittel können in der Form von technischen und organisatorischen Maßnahmen der Verarbeitungstätigkeit mittelbar dienen, indem sie diese hinsichtlich bestehender Risiken absichern (z. B. Backup-System, Firewall, Anti-Schadsoftware-System).

X. Glossar

PIA	Privacy Impact Assessment Methodik, also DSFA-Methode, die von der französischen Datenschutzaufsicht CNIL "herausgegeben" wird.
PIA-Tool	Software für die Erstellung eines DSFA-Berichts, herausgegeben von der CNIL. Weitere Informationen hierzu siehe Praxishilfe „Software zur Datenschutz-Folgenabschätzung (PIA-Tool)", im Internet auf https://www.datenschutz-bayern.de in der Rubrik „DSFA".
Rechtsgrundlage	Nach Art. 8 Abs. 2 Satz 1 EU-Grundrechte-Charta (GRCh) dürfen personenbezogene Daten „nur mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden." Kann eine Verarbeitung nicht auf eine Rechtsgrundlage gestützt werden, ist sie rechtswidrig. Die möglichen Rechtsgrundlagen nennt Art. 6 Abs. 1 UAbs. 1 DSGVO.
Risikoanalyse	Die Risikoanalyse in der Form der Risikoanalyse-Allgemein und Risikoanalyse-DSFA weist die Erfüllung der SDM-Gewährleistungsziele nach und beantwortet somit die Frage, ob die Art und Weise des jeweils betrachteten Verarbeitungsvorgangs die DSGVO-Anforderungen einhält. Im Hinblick auf einen bestimmten Verarbeitungsvorgang werden alle relevanten Szenarien erhoben, hinsichtlich der Risiken bewertet und ggf. mit Schutzmaßnahmen verknüpft, die ein Risiko bzw. eine Gefährdung bezüglich der DSGVO-Einhaltung darstellen. Mit jedem Szenario wird folglich möglichst differenziert ein Ereignis oder Zustand beschrieben, durch das der betrachtete Verarbeitungsvorgang den normativen DSGVO-Rahmen verlassen würde und das es daher durch die wirksame Umsetzung von Schutzmaßnahmen zu vermeiden gilt. Diese Risikoanalysen sind grundsätzlich. skalierbar (z. B. Ausbaustufen small, medium und large).
Schwachstelle	Schwachstellen sind als Eigenschaften der betrachteten Zielverarbeitung definiert, die geeignet sind, bei hinzutreten einer bestimmten (Risiko-)/(Gefährdungs-)Quelle ein Szenario mit Schadwirkung für die Rechte und Freiheiten natürlicher Personen auszulösen. Ist eine solche Eigenschaft nicht gegeben, so besteht in logischer Konsequenz auch kein Risiko für die Zielverarbeitung, da es keinen Ansatzpunkt für (Risiko-)/(Gefährdungs-)Quellen und somit keine Szenarien mit Schadenswirkung gibt.
SDM	Das Standard-Datenschutzmodell der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

	beschreibt eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele und befindet sich in der hier verwendeten Fassung in der Version 2.0b vom April 2020, Näheres im Internet unter https://www.datenschutz-mv.de/datenschutz/datenschutz-modell/.
SDM-Datensicherheitsziele	Davon umfasst sind die beiden SDM-Gewährleistungsziele Verfügbarkeit und Vertraulichkeit sowie der Teilzielaspekt Datenintegrität des SDM-Gewährleistungsziels Integrität, siehe II. 1.
SDM-Gewährleistungsziel	Die sieben Gewährleistungsziele werden im SDM festgelegt und beschrieben. In dieser Orientierungshilfe werden die SDM-Gewährleistungsziele in SDM-Datensicherheits- und SDM-Schutzbedarfsziele weiter unterteilt.
SDM-Schutzbedarfsziele	Davon umfasst sind die vier SDM-Gewährleistungsziele Datenminimierung, Intervenierbarkeit, Transparenz und Nichtverkettung sowie der Teilzielaspekt Konzeptionseinhaltung und Richtigkeit des SDM-Gewährleistungsziels Integrität, siehe auch II. 1.
Szenario	Ein Szenario beschreibt möglichst differenziert ein Ereignis, durch das die Zielverarbeitung den normativen DSGVO-Rahmen verlassen würde und das es daher zu vermeiden gilt.
TOM(s)	„TOM“ steht als Abkürzung für eine bestimmte technische und organisatorische Maßnahme, während „TOMs“ für eine Mehrzahl von technischen und organisatorischen Maßnahmen steht. TOMs gehören zu den Schutzmaßnahmen im Datenschutz. Unter den Oberbegriff „Schutzmaßnahmen im Datenschutz“ fallen neben den TOMs auch insbesondere Vorgaben, die durch Rechtsetzung und Rechtsprechung als Garantien für den Datenschutz gesetzt werden. Im Kontext der einzelnen Risikoanalysemethode werden TOMs auch als „Abhilfemaßnahmen“ (Risikomanagement) bzw. als „Sicherstellungsmaßnahmen“ (Zielerfüllungsmanagement) bezeichnet.
unmittelbares Betriebsmittel	Betriebsmittel können für die Durchführung einer Verarbeitungstätigkeit unverzichtbar sein und damit unmittelbar die Verarbeitung unterstützen (z. B. IT-gestützter Arbeitsplatz, E-Mail-System).

X. Glossar

Verantwortlicher	Der für die Verarbeitung personenbezogener Daten Verantwortliche ist der zentrale Adressat von datenschutzrechtlichen Pflichten. Art. 4 Nr. 7 DSGVO beschreibt ihn als Stelle, die über die Zwecke und Mittel einer Verarbeitung personenbezogener Daten entscheidet. Die Entscheidung kann allein getroffen werden oder gemeinsam mit anderen Stellen. Für bayerische öffentliche Stellen sieht Art. 3 Abs. 2 BayDSG vor, dass Verantwortlicher regelmäßig die für die Verarbeitung zuständige öffentliche Stelle ist.
Verarbeitungstätigkeit	Der Begriff „Verarbeitungstätigkeit“ umfasst alle Verarbeitungsvorgänge und Vorgangsreihen, die einem gemeinsamen, festgelegten Zweck dienen. Ausgehend von Sinn und Zweck des Verarbeitungsverzeichnisses nach Art. 30 DSGVO sollte dieses alle Verarbeitungstätigkeiten hinreichend konkret, andererseits aber auch nicht zu kleinteilig abbilden, um der Aufsichtsbehörde – aber auch dem Verantwortlichen – eine erste Rechtmäßigkeitskontrolle anhand des Verzeichnisses zu ermöglichen.
Zielverarbeitung	Klar beschriebener und abgegrenzter Verarbeitungsvorgang, der Gegenstand einer bestimmten Risikoanalyse ist.