



# DIIR

## Checkliste zur Prüfung der Datenschutzorganisation

DIIR-Arbeitskreis Datenschutz & Data Governance

Version 3.0, April 2026

Vorwort .....	3
1     Datenschutzstrategie .....	5
1.1   Grundlagen .....	5
1.2   Implementierung und Kommunikation .....	6
2     Vorgaben und Anforderungen.....	7
2.1   Datenschutzvorgaben und Anforderungen, gesetzlich und betrieblich/intern .....	7
2.2   Berücksichtigung der Anforderungen.....	8
3     Organisation.....	10
3.1   Datenschutzorganisation .....	10
3.2   Operative Einbindung des Datenschutzes.....	12
3.3   Rahmenbedingungen für den sicheren Einsatz von IT-Systemen.....	14
3.4   Regelungen zum Umgang mit Datenschutzvorfällen und Betroffenenanfragen .	15
4     Ausgewählte Prüffelder im Datenschutz-Audit.....	17
4.1   Kommunikation der Regelungen zum Datenschutz.....	17
4.2   Einwilligungsmanagement .....	17
4.3   Auftragsverarbeitung.....	18
4.4   Prüfung gemeinschaftlicher Datenverarbeitung .....	19
4.5   Prüfung von Sperr- und Löschkonzepten .....	19
4.6   Monitoring und laufende Anpassung des Datenschutzes .....	20
4.7   Handlungsvorgaben bei Anfragen und Prüfungen der Datenschutzaufsichtsbehörden.....	20
4.8   Handlungsvorgaben bei Anfragen von Externen .....	21
5     Reporting .....	22
5.1   Regelmäßige Berichtslinien gesetzlich und betrieblich/intern (z. B. Tätigkeitsberichte).....	22
5.2   Anlassbezogene Berichterstattung (Ad-hoc-Reporting) an Datenschutzbehörde und/oder interne Stelle .....	24

## Vorwort

Spätestens seit Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) im Mai 2018 befindet sich die Datenschutz-Compliance auf der Risikolandkarte der Internen Revision. Die erheblichen Haftungs-/Sanktionsrisiken (Bußgeld bis zu 20 Mio. € oder bis zu 4% des Jahresumsatzes der Unternehmensgruppe)<sup>1</sup> sowie die umfassenden Dokumentations- und Nachweispflichten haben dazu geführt, dass die Einführung entsprechender Datenschutzmanagementsysteme und anderer Standards in den Unternehmen und im öffentlichen Sektor und deren regelmäßige Anpassung/Ergänzung notwendig wurden. Neue Technologien wie künstliche Intelligenz (KI) sind zuletzt rasant gewachsen und sorgen dafür, dass sich die Art und Weise verändert, wie Daten gesammelt, verarbeitet und genutzt werden.

In den ersten Jahren nach Inkrafttreten der DSGVO gab es noch einige Unsicherheit bei allen Beteiligten und gelegentlich auch missbräuchliche Abmahnungen. Mittlerweile haben sich insbesondere Unternehmen gemäß den Anforderungen an den Datenschutz organisiert und erkennen in deren Einhaltung auch Wettbewerbsvorteile. Gleichzeitig sorgen nationale und europäische Gerichte mit einigen Urteilen laufend sowohl für Änderungen in der Datenschutzpraxis als auch für Klarstellungen.

Parallel zur erhöhten Regulierung durch europäische Datengesetze schreitet die Digitalisierung in den Unternehmen und Behörden fort und führt mit den zunehmenden Möglichkeiten des Einsatzes von KI-Systemen dazu, dass fast alle Arbeitsbereiche und Prozesse digital unterstützt werden. Bestehende Geschäftsmodelle werden um zusätzliche datengetriebene Geschäftsmodelle, vor allem mit Endkundendaten, ergänzt.

Eine Vielzahl von Unternehmungen, in deren Geschäftsmodellen früher keine Endkundendaten verarbeitet wurden, stehen im Zuge der Digitalisierung von den Herausforderungen eines wirksamen betrieblichen Datenschutzes. Dabei beschränkt sich die datenschutzrechtliche Thematik keineswegs auf juristische Fragestellungen, sondern umfasst neben den organisatorischen und prozessualen Anforderungen auch die IT-Sicherheit.

Immer hybridere IT-Landschaften und steigende Cyberrisiken erhöhen unmittelbar auch das Datenschutzrisiko einer Organisation. Insbesondere die europäischen Datengesetze

---

<sup>1</sup> Die Gesamtsumme der verhängten Bußgelder steigt seit der DSGVO-Einführung kontinuierlich an. Die Liste der höchsten DSGVO-Bußgelder wird derzeit vom Meta-Konzern (u. a. Facebook, Instagram, WhatsApp) dominiert, sowohl für die meisten Bußgelder als auch für die bislang höchste Summe (1,2 Mrd. Euro im Jahr 2023). Die Strafen wurden von Behörden verschiedener europäischer Mitgliedsstaaten verhängt, überwiegend von der irischen Datenschutzbehörde, wo viele Tech-Unternehmen ihren Sitz haben. Doch auch kleine und mittlere Unternehmen (KMU) sind verstärkt im Fokus der Aufsichtsbehörden.

und Regulatorik zur Informationssicherheit (u. a. NIS-2, Dora etc.) stellen – ähnlich wie die DSGVO – tiefgreifende Anforderungen an Prozesse, Transparenz und Risikomanagement. Der regulatorische Rahmen und die sich stetig ändernden Rahmenbedingungen erfordern eine klare Datenschutz- und Informationssicherheitsstrategie, wirksame Datenschutzprozesse sowie deren Überwachung.

Auch die Global Internal Audit Standards tragen der Relevanz dieser Themen Rechnung, insbesondere in den Standards 5.2 „Schutz von Informationen“ und 10.3 „Technologische Ressourcen“. Standard 5.2 betont die Verantwortung der Internen Revision, Prüfungsinformationen angemessen zu schützen und damit sowohl den Anforderungen des Datenschutzes als auch des Informationsschutzes über den gesamten Prüfungsprozess hinweg Rechnung zu tragen. Standard 10.3 hebt hervor, dass die von der Internen Revision eingesetzten technologischen Ressourcen so auszuwählen und einzusetzen sind, dass sie den Anforderungen an Datenschutz, Informationsschutz sowie an eine ordnungsgemäße, sichere und nachvollziehbare Prüfungsdurchführung entsprechen.

Der DIIR-Arbeitskreis Datenschutz & Data Governance bietet zur Überprüfung der Datenschutzorganisation und ihrer Wirksamkeit im Unternehmen eine strukturierte Vorgehensweise in Form einer Checkliste an. Unabhängig von Prüfungen kann diese Übersicht einen wichtigen Rahmen für die im Kontext des Datenschutzes zu beachtenden Ansätze und Regularien darstellen. Datenschutz, Informationssicherheit und der Umgang mit KI-bezogenen Daten und Technologien müssen zunehmend zusammen bewertet werden. Daher wurden diese Themen neu aufgenommen und in der Checkliste ergänzt.

Diese Checkliste wurde nach aktuellem Stand sowie bestem Wissen und Gewissen im November 2017 erstellt und erstmalig im August 2021 überarbeitet. Die letzte Aktualisierung erfolgte im April 2026. Dabei erfolgte eine allgemeine redaktionelle Überarbeitung aller Kapitel. Die Checkliste erhebt keinen Anspruch auf Verbindlichkeit und Vollständigkeit und ersetzt keinesfalls die Prüfung der individuellen rechtlichen Situation.

Einige Begriffe wie Datenschutzbeauftragter, Verantwortlicher oder Auftragsverarbeiter beruhen auf der nicht gegenderten Sprache der Datenschutz-Grundverordnung.

# 1 Datenschutzstrategie

Eine Strategie bezeichnet nach betriebswirtschaftlichem Verständnis das Rahmenkonzept oder einen Leitfaden für die langfristige Erreichung von unternehmerischen Absichten und Zielen. Eine Strategie gibt zunächst nur eine allgemeine Richtung der (Unternehmens-)Entwicklung vor. Sie muss deshalb durch nachfolgende Maßnahmen konkretisiert werden. Gleichzeitig erfordert eine Strategie die ständige Anpassung an veränderte Rahmenbedingungen. Die Datenschutzstrategie sollte somit ein zentrales Element im Unternehmen sein, um rechtliche Vorgaben und bestehende Bestimmungen in Bezug auf den aktuellen Umgang mit personenbezogenen Daten umzusetzen. Sie sollte sich auch mit sich abzeichnenden neuen Entwicklungen und künftigen Risiken in dem Bereich auseinandersetzen.

## 1.1 Grundlagen

Unter Artikel 25 DSGVO (Erwägungsgrund 78) findet sich die Verpflichtung des Verantwortlichen, für die von ihm geplante Datenverarbeitung eine ausreichende Strategie unter Berücksichtigung der darin genannten Vorgaben vorzuhalten. Diese Strategie ist wiederum Prüfungsgegenstand des betrieblichen Datenschutzbeauftragten gemäß Artikel 39 Abs. 1 lit. b) DSGVO.

- Gibt es eine Datenschutzstrategie und in welcher Form ist diese dokumentiert?
- Wann wurde die Strategie erlassen/aktualisiert?
- Mit wem wurde die Strategie abgestimmt? Sind notwendige interne/externe Stellen einbezogen worden?
- Wer hat die Strategie verabschiedet?
- Hat die Strategie unternehmens-/konzernweite Gültigkeit und ist sie in allen Konzerngesellschaften/Legaleinheiten nachweisbar?
- Welche Quellen zur Erstellung der Strategie (nationales Recht, Best Practices etc.) wurden genutzt?
- Was sind Grundlagen und wesentliche Inhalte der Strategie?
- Ist die Strategie angemessen/plausibel, insbesondere in Bezug auf Unternehmensgröße/Unternehmensstruktur, Geschäftsmodell, regionale Aufteilung und Art der Daten?

- Sind die gültigen gesetzlichen Regelungen (z. B. Art. 25 DSGVO) ausreichend in der Strategie berücksichtigt?
- Berücksichtigt die Datenschutzstrategie wesentliche Elemente des Standard-Datenschutzmodells (SDM)?
- Ist die Strategie in das Governance-Modell des Unternehmens eingebettet?
- Wer verfolgt die Umsetzung der Strategie?
- Gibt es eine im Sinne der DSGVO (Art. 47) durch die zuständigen Aufsichtsbehörden genehmigte interne Datenschutzvorschrift (z. B. Binding Corporate Rules bei unternehmens-/konzerninternen Datentransfers in Drittstaaten)?

## 1.2 Implementierung und Überwachung

Bei der Strategie muss es sich um Vorgaben im Gesamtunternehmen handeln, welche in konkreten Vorgehens- und Handlungsweisen umgesetzt wurden. Der Verantwortliche muss gemäß Artikel 5 Abs. 2 DSGVO die Einhaltung der Vorgaben nachweisen können.

- Wie wurde die Strategie veröffentlicht?
- Wie wurden die Strategie und Vorgaben unternehmensweit kommuniziert sowie Zielgruppen trainiert/sensibilisiert (Kommunikationsplan/-konzept)?
- Gibt es ein Konzept zum Monitoring und Berichtswesen?
- Besteht innerhalb des Unternehmens ein schriftlich dokumentiertes Internes Kontrollsystem (IKS), in das datenschutzrechtliche Sachverhalte integriert sind?
  - Sind im Rahmen des IKS zumindest Prozesse/Kontrollen/Kontrollziele und Verantwortlichkeiten mit Bezug zum Datenschutz dokumentiert?
  - Sind im Rahmen des Sicherheitsmanagements (IT, Gebäudeüberwachung etc.) Prozesse/Kontrollen/Kontrollziele und Verantwortlichkeiten mit Bezug zum Datenschutz (TOMs, Sicherheit der Verarbeitung gem. Art. 32 DSGVO) dokumentiert?

## 2 Vorgaben und Anforderungen

Die Quellen der zu beachtenden Grundlagen ergeben sich aus den anzuwendenden nationalen und internationalen Gesetzen innerhalb und außerhalb der EU, branchenspezifischen Regelungen, betriebsinternen Vorgaben und der aktuellen Rechtsprechung. Prüfungsrelevant ist vor allem die Kenntnis dieser Bestimmungen und deren Implementierung in den betriebsinternen Prozessen. Sofern diese Vorgaben nicht konkret, belastbar und verbindlich in der Datenschutzstrategie festgelegt sind, sollte eine entsprechende Konkretisierung in internen Regelungen erfolgen.

### 2.1 Datenschutzvorgaben und Anforderungen, gesetzlich und betrieblich/intern

- Gibt es allgemein verbindliche und von der Unternehmensleitung freigegebene Unternehmensrichtlinien?
- Existiert eine Data-Governance-Strategie, die den Datenschutz berücksichtigt und was wird darunter konkret verstanden?
  - Ist eine Datenarchitektur definiert, die die Transparenz über die Datenflüsse ermöglicht und deren Integration und Interoperabilität unterstützt?
  - Gibt es Datenmanagement-Prozesse, die die Datenintegration, -harmonisierung und -verteilung ermöglichen?
- Werden ggf. vorhandene branchenspezifische/regulatorische Vorgaben ausreichend berücksichtigt (z. B. in Banken, Versicherungen, Gesundheitsbranche)?
- Wie wurden die Richtlinien kommuniziert und wie sind diese zugänglich?
- Wie ist sichergestellt, dass die einschlägigen und ggf. branchenspezifischen Gesetze, Normen und Standards in den Unternehmensrichtlinien berücksichtigt werden?
- Gibt es weitere gesetzliche und/oder betriebliche/interne Vorgaben? Wenn ja, sind diese aufeinander abgestimmt?
- Gibt es betriebliche Regelungen (z. B. kollektivrechtliche Vereinbarungen)?
- Wie ist sichergestellt, dass die DSGVO auch für alle außerhalb der EU niedergelassenen Unternehmen gilt, soweit sie mit betroffenen Personen in der EU Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten (Marktortprinzip, Art. 3 DSGVO)?

- Sind die Vorgaben in Summe aufeinander abgestimmt bzw. ist sichergestellt, dass Mussvorgaben bzw. die strengsten Vorgaben das Regelungsminimum beachten?

## 2.2 Berücksichtigung der Anforderungen

Die DSGVO enthält Öffnungsklauseln für den nationalen Gesetzgeber sowie konkrete an die Mitgliedstaaten gerichtete Regelungsaufträge. Daraus ergibt sich ein gesetzlicher Anpassungsbedarf im nationalen Datenschutzrecht. In Deutschland ergänzt das Bundesdatenschutzgesetz (BDSG) die unmittelbar geltende DSGVO. Zudem wurden Anpassungen in den Landesdatenschutzgesetzen wie auch korrespondierenden Rechtsvorschriften (etwa Landeskrankenhausgesetze) vorgenommen.

- Fällt das Unternehmen unter den Anwendungsbereich des BDSG?
- Gibt es andere Rechtsvorschriften des Bundes oder der Länder über den Datenschutz, die den Vorschriften des BDSG (etwa auf Grund der Trägerschaft) vorgehen?
- Werden deren wesentliche Regelungsinhalte betrachtet?
  - Rechtmäßigkeit der Verarbeitung (Artikel 6 DSGVO)
  - Einwilligung (Artikel 7 DSGVO)
  - Besondere Kategorien von Daten (§§22ff BDSG sowie Artikel 9 DSGVO)
  - Informationspflichten und Auskunftsrechte (Artikel 12, 13, 14, 15, 18 DSGVO)
  - Videoüberwachung (§4 BDSG)

Die DSGVO regelt die Voraussetzungen für eine datenschutzkonforme Verarbeitung personenbezogener Daten sowie die Anforderungen an wesentliche Teilprozesse im Datenschutz. Im Wesentlichen sind das:

- Erlaubnis zur Erhebung und Verarbeitung personenbezogener Daten. Auch bei der DSGVO gilt ein Verbot mit Erlaubnisvorbehalt (Art. 6 DSGVO)
  - Rechtliche Verpflichtung
  - Vertrag/Vorvertrag (Rechtsgeschäft)
  - Überwiegendes betriebliches Interesse
  - Vereinbarung mit bestehenden Primärzwecken
  - Einwilligung
  - Schutz lebenswichtiger Interessen
- Datenschutz-Organisation
  - Policies zu Datenschutz und IT-Sicherheit

- Datenschutzfreundliche Technologien (Art. 25 DSGVO)
- IT-Sicherheit nach dem Stand der Technik (Art. 32 DSGVO)
- Dokumentationspflichten (Art. 5 DSGVO)
  - Datenschutzmanagement
  - Zuständigkeiten
  - Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)
  - Datenschutz-Folgeabschätzung inklusive Risikobewertung (Art. 35 DSGVO)
  - Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften sowie der Datenschutzstrategien des Verantwortlichen oder des Auftragsverarbeiters (Art. 39 DSGVO)
- Umsetzung der Betroffenenrechte (Art. 15 -21 DSGVO)
- Informationspflichten (Art. 13 f. DSGVO) bei Direkterhebung und mittelbarer Erhebung von personenbezogenen Daten
  - Anpassung von Webseiten und Datenschutzerklärungen (Art. 13 f. DSGVO)
- Datentransfer in Drittländer
  - Feststellung der Angemessenheit des Datenschutzstandards im Zielland (Art. 45 DSGVO)
  - Geeignete Garantien (Art. 46 DSGVO), u. a. Binding Corporate Rules (Art. 46 Abs. 2b, Art. 47), Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde
  - Rechtshilfeabkommen (Art. 48 DSGVO)
  - Sonderfälle und Ausnahmen (Art. 49 DSGVO)

## 3 Organisation

Das Unternehmen hat eine Datenschutzorganisation einzurichten und zu unterhalten, die, gemessen an der Unternehmensgröße und -struktur, in der Lage ist, die für die zu verarbeiteten Daten und die erklärte Strategie erforderlichen Datenschutzmaßnahmen zu unterstützen. Dazu zählen insbesondere die Ausstattung (Budget und Personal) und die fachliche Qualifikation der damit beauftragten Personen.

Bei der Einrichtung der Datenschutzorganisation sollte ebenso berücksichtigt werden, welche Aufsichtsbehörde maßgeblicher Ansprechpartner der verantwortlichen Stelle ist. Im Zuge der DSGVO wurde das One-Stop-Shop-Prinzip eingeführt. Dieses bedeutet, dass bei grenzüberschreitender Verarbeitung (definiert in Art. 4 Nr. 23 DSGVO) die sogenannte federführende Aufsichtsbehörde alleiniger Ansprechpartner des Verantwortlichen bzw. des Auftragsverarbeiters ist.

### 3.1 Datenschutzorganisation

Der nachfolgende Abschnitt bezieht sich auf Fragestellungen in Bezug auf die Bewertung der Angemessenheit der Datenschutzorganisation. Nicht Gegenstand ist die Verarbeitung personenbezogener Daten in einzelnen Fachverfahren bzw. Verarbeitungsverfahren. Dieser Analyseteil trifft keine Aussagen zur angemessenen und wirksamen Umsetzung datenschutzrechtlicher Bestimmungen.

#### 3.1.1 Organisationsform

Entspricht die Organisationsform der verabschiedeten Strategie?

- Nationale und internationale Bezüge im Unternehmen
  - Gibt es Datenverarbeitung im Ausland?
  - Gibt es entsprechendes Vertragsmanagement bei den
    - verbundenen Unternehmen?
    - Dienstleistern?
  - Befindet sich die verantwortliche Stelle im Ausland?

- Besteht ein konzerninterner Datenaustausch?
- Bestehen Datentransfers in Drittländer?
- Bestehen besondere lokale/nationale Anforderungen an den Datenschutz bzw. die Datenschutzorganisation?
- Aufbau der Datenschutzorganisation
  - Besteht eine zentrale/dezentrale Datenschutzorganisation?
  - Besteht eine Mischform?
  - Besteht ein Organigramm der Datenschutzorganisation?
  - Ist die Organisation des Datenschutzes den Verarbeitungstätigkeiten des Verantwortlichen angemessen (im Hinblick auf die Tätigkeiten des Unternehmens, des Risikos der Betroffenen, des Umfangs etc.) aufgebaut?
  - Wie ist sichergestellt, dass die dezentralen Stellen im Unternehmen über ein ausreichendes Know-how verfügen?

### 3.1.2 Leitlinie zu den Aspekten Datenschutz und Datensicherheit

- Wurden die Grundzüge des Datenschutz- und (IT-)Sicherheitsmanagements durch den Verantwortlichen in einer oder mehreren entsprechenden Richtlinien festgelegt?
- Wurde darin der Stellenwert des Datenschutzes und der IT-Sicherheit festgelegt und entsprechende Schutzziele definiert?
- Umfassen die Sicherheitsziele die Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme?
- Beinhalten die Datenschutzziele die Transparenz, Intervenierbarkeit und Nicht-Verkettbarkeit?

### 3.1.3 Anforderungen an den betrieblichen Datenschutzbeauftragten

- Berücksichtigt die Ausgestaltung der Datenschutzorganisation die Anforderungen an einen betrieblichen Datenschutzbeauftragten hinsichtlich:
  - Zuverlässigkeit
  - Unabhängigkeit
  - Ausstattung
  - Fachkunde
- Sind die Verantwortlichkeiten klar geregelt?

- Wie wurde der Datenschutzbeauftragte vom Datenschutzverantwortlichen (Unternehmensleitung) bestellt/ernannt?
  - Wurden (in einem Unternehmensverbund) weitere Datenschutzbeauftragte bestellt/ernannt?
  - Sind Datenschutzkoordinatoren in den Organisationseinheiten bzw. Unternehmensteilen benannt?
- Ist der Datenschutzbeauftragte in seiner Funktion der Geschäftsführung unmittelbar unterstellt und unterliegt er in der Ausübung seiner Tätigkeiten keiner fachlichen Weisung durch die Geschäfts- und Bereichsleitung? Besteht eine Tätigkeits-/Aufgabenbeschreibung mit klaren Befugnissen, Rechten und Verpflichtungen?
- Besteht eine risikoorientierte Aufgabenwahrnehmung des Datenschutzbeauftragten?
- Sind die Beratungs- und Überwachungstätigkeiten des Datenschutzbeauftragten beschrieben und kommuniziert?

Ist die Aufgabenteilung zwischen Datenschutzbeauftragten und (soweit vorhanden) Datenschutz-Koordinatoren entsprechend der gewählten Organisationsform klar definiert? Verfügen diese über die erforderliche Sachkenntnis?

- Wie wird die fachliche Eignung der Datenschutzkoordinatoren oder anderer Mitarbeiter der Datenschutzorganisation sichergestellt?
- Wird der Datenschutzbeauftragte/die Datenschutzorganisation in die Bestellung/Ernennung der Datenschutzkoordinatoren eingebunden?
- Stehen andere dienstliche Aufgaben innerhalb der betrieblichen Struktur in keinem Konflikt mit seiner Tätigkeit als betrieblicher Datenschutzbeauftragter des Unternehmens?
- Besteht ein regelmäßiges Reporting? Wie wird dieses nachgehalten (Dokumentation)?
- Besteht ein Jahres- oder Quartalsbericht an die verantwortliche Stelle (z. B. Geschäftsführung, Vorstand)?
- Ist der Datenschutzbeauftragte behördlich gemeldet?
- Wurde ein Konzerndatenschutzbeauftragter bestellt?

### 3.2 Einbindung und Wirken des Datenschutzbeauftragten

Der betriebliche Datenschutzbeauftragte überwacht u. a. die Einhaltung der DSGVO und anderer Rechtsvorschriften. Er wirkt beratend und unterstützend an der Bearbeitung erfor-

derlicher Maßnahmen zur Risikoreduktion mit. Der Umsetzungsstatus wird schriftlich dokumentiert. Die Bearbeitung einzelner Maßnahmen kann stichprobenartig im Rahmen interner Audits (auch durch die Revision) überprüft werden.

- Wird der betriebliche Datenschutzbeauftragte in die Planung und Kontrolle der Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen miteinbezogen?
- Finden die Überwachungstätigkeiten regelmäßig und anlassbezogen statt?
- Pfllegt der Datenschutzbeauftragte regelmäßigen Kontakt zur zuständigen Aufsichtsbehörde?
- Wird die Umsetzung der regelmäßigen Sensibilisierungs- und Schulungsmaßnahmen des Verantwortlichen durch den betrieblichen Datenschutzbeauftragten überwacht (idealerweise als Methodenmix von arbeitsplatzbezogener Schulung bis hin zu E-Learning-Maßnahmen)? Bestehen die Unterweisungsnachweise zu den durchgeführten Sensibilisierungsmaßnahmen?

Um die operative Einbindung der Datenschutzfunktion gemäß DSGVO nachzuweisen, sind die Maßnahmen über die folgenden vier Phasen zu dokumentieren:

- Planung und Konzeption
  - Erfolgt eine risikoorientierte Konzeption der automatisierten Verfahren hinsichtlich Art, Umfang, Umstände und Zweck?
  - Enthält das vom Unternehmen geführte Verzeichnis von Verarbeitungstätigkeiten (VvV) die in Art. 30 DSGVO genannten Angaben?
  - Führt der betriebliche Datenschutzbeauftragte die Validierung des VvV mit den Anforderungen der DSGVO durch?
  - Kann das VvV jederzeit stichprobenartig auf Aktualität und angemessene Dokumentation der aufgeführten Sachverhalte geprüft werden?
- Umsetzung
  - Wurden geeignete technische und organisatorische Maßnahmen ergriffen und dokumentiert?
  - Wurden die Grundsätze der datenschutzkonformen Verarbeitung (data protection by design (Art. 25 Abs. 1 DSGVO) und data protection by default (Art. 25 Abs. 2 DSGVO) beachtet?
- Erfolgskontrolle und Überwachung
  - Wurden bzw. werden die Maßnahmen regelmäßig überprüft?
- Optimieren und Verbessern
  - Werden die Maßnahmen regelmäßig aktualisiert?

### 3.3 Sicherer Einsatz von IT-Systemen: Zusammenspiel zwischen Informationssicherheits- und Datenschutzbeauftragten

Die erforderliche Dokumentation der automatisierten Datenverarbeitung ist von der verantwortlichen Stelle sicherzustellen. Für die Auswahl angemessener technischer und organisatorischer Sicherheitsmaßnahmen und für den Nachweis einer ordnungsgemäßen und wirksamen Umsetzung bilden die Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) einschließlich der vom BSI in den Standards 200-1 bis 200-4 (Aufbau eines Informationssicherheitsmanagementsystems, Vorgehensweise nach dem IT-Grundschutz, Erstellung einer Risikoanalyse und das Business Continuity Management) oder im internationalen Standard DIN EN ISO 27001 definierten Vorgehensweise eine gute Orientierungshilfe für Unternehmen.

- Wurde ein Informationssicherheitsbeauftragter benannt?
- Sind die Aufgaben des Informationssicherheitsbeauftragten in einer entsprechenden Richtlinie festgelegt?
- Ist der Informationssicherheitsbeauftragte für die Initiierung der Sicherheitskonzeption und die Überprüfung des Sicherheitsniveaus verantwortlich?
- Wird vor der Inbetriebnahme neuer Systeme bzw. Prozesse, in denen personenbezogene Daten verarbeitet werden, eine Freigabe der Informationssicherheit und des Datenschutzbeauftragten eingeholt? Wird diese Freigabe angemessen dokumentiert?
- Werden Dienstleister unter Berücksichtigung der definierten Anforderungen der Informationssicherheit und des Datenschutzes ausgewählt?
- Werden Auftragsverarbeitungen ausschließlich auf Basis einer schriftlichen Vereinbarung durchgeführt, auch wenn sie in einzelnen Fachverfahren stattfinden?
- Sind die Vereinbarungen Bestandteil der Dokumentation des IT-Einsatzes?
- Werden Vereinbarungen mit Dienstleistern von der Informationssicherheit und dem Datenschutzbeauftragten geprüft und freigegeben?
- Sind administrative Änderungen an den IT-Systemen nur durch einzelne, explizit berechnigte Mitarbeiter möglich?
- Wurden orientierte technische und organisatorische Maßnahmen für die Durchführung administrativer Tätigkeiten an den erfassten Systemen getroffen? Haben sich diese Maßnahmen an den konkreten Risiken im Unternehmen orientiert?
- Erfüllen die vom Unternehmen getroffenen Maßnahmen zur Dokumentation von Änderungen an informationstechnischen Geräten, Programmen und Verfahren die Anforderungen der DSGVO?
- Werden Änderungen zunächst auf Testsystemen durchgeführt? Wird die Durchführung der Tests hierbei schriftlich dokumentiert?
- Erfolgt die Freigabe von wesentlichen Systemänderungen nach Abstimmung mit dem Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten?

- Prüft der Datenschutzbeauftragte regelmäßig die ordnungsgemäße und wirksame Umsetzung der technischen und organisatorischen Maßnahmen der im VvV enthaltenen Systeme bzw. Prozesse?

### 3.4 Regelungen zum Umgang mit Datenschutzvorfällen und Betroffenenanfragen

Wird eine Verletzung des Schutzes personenbezogener Daten bekannt, ist unverzüglich zu klären, ob der betreffende Vorfall der Aufsichtsbehörde zu melden ist und ob und wie die Betroffenen hierüber zu informieren sind. Die engen gesetzlichen Fristen, etwa 72 Stunden nach Art. 33 und 34 der DSGVO, sind einzuhalten.

Vergleichbares ist auch bei Anfragen von Betroffenen über die zu ihrer Person gespeicherten Daten, zu deren Korrektur, Sperrung oder Löschung zu gewährleisten. Diese sind gem. Art. 12 der DSGVO unverzüglich, in jedem Fall innerhalb eines Monats, bzw. mit einer entsprechenden Begründung nach weiteren zwei Monaten, zu beantworten. Das Unternehmen hat sich bei der Anpassung der Aufbauorganisation an den internen Richtlinien, in denen Aspekte der Informationssicherheit und des Datenschutzes geregelt sind, zu orientieren.

Dem Datenschutzbeauftragten obliegt eine zentrale Rolle bzgl. der Überwachung der Einhaltung der dezidierten Meldefristen aus der DSGVO. Um die Einhaltung der Pflichten des Verantwortlichen bzw. Auftragsverarbeiters bei der Meldung an die zuständige Aufsichtsbehörde sicherzustellen, ist die Einbindung des Datenschutzbeauftragten in interne Melde-/Informationsprozesse zwingend erforderlich.

- Sind in den Vorgaben, die Ansprechpartner, das Vorgehen und evtl. Fristen zur Bearbeitung, Dokumentation und Nachbereitung von Sicherheits- und Datenschutzvorfällen festgelegt?
- Ist sichergestellt, dass alle meldepflichtigen Vorgänge entsprechend den Vorgaben fristgerecht zentral verarbeitet werden können?
- Gibt es einen Reaktionsplan bei einer Verletzung des Schutzes personenbezogener Daten (Art. 33, 34 DSGVO)?
- Hat der Verantwortliche es organisatorisch ermöglicht, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften gem. § 77 BDSG zugeleitet werden können?
- Sind die Zuständig- und Verantwortlichkeiten für eine evtl. Meldung an die Aufsichtsbehörde und ggf. für die Information der Betroffenen klar geregelt?
- Werden geeignete Prozesse für die Umsetzung der Informationspflicht bei einer Verletzung des Schutzes personenbezogener Daten genutzt?

- Werden dabei von den Aufsichtsbehörden bereitgestellte Informationskanäle und Formulare genutzt?
- Werden Sicherheits- und Datenschutzvorfälle durch ein eigens hierfür festgelegtes Prozedere mit Krisenmanagement und Datenschutzbeauftragtem sowie ggf. zusätzlichen Mitgliedern bearbeitet?

Der Datenschutzbeauftragte steht bei Datenschutzanfragen von Betroffenen beratend zur Verfügung und unterstützt den verantwortlichen Fachbereich bei der Beantwortung.

- Sind in den Vorgaben die Ansprechpartner, evtl. Fristen und das Vorgehen zur Authentifizierung, Bearbeitung, Dokumentation und Nachbereitung von Datenschutzanfragen von Betroffenen, festgelegt?
- Sind die Zuständig- und Verantwortlichkeiten für die Beantwortung von Datenschutzanfragen klar geregelt?
- Ist sichergestellt, dass der Datenschutzbeauftragte bei solchen Anfragen unmittelbar einbezogen wird?
- Werden Anfragen von Betroffenen schriftlich nachbereitet, so dass deren Dokumentation ggf. einer Aufsichtsbehörde vorgelegt werden kann?

## 4 Ausgewählte Prüffelder im Datenschutz-Audit

### 4.1 Kommunikation der Regelungen zum Datenschutz

Grundvoraussetzung für einen wirksamen Datenschutz ist ein angemessenes Datenschutzbewusstsein. Dieses ist insbesondere durch Schulungen (Information) und Beratung zu erreichen. Die Einhaltung der Vorgaben muss in den internen Prozessen abgebildet werden.

- Werden/wurden regelmäßige Schulungsmaßnahmen zur Sensibilisierung bzw. Unterweisung angeboten/durchgeführt (Information und Kommunikation, Kenntnisüberprüfung, Nachweis der Belehrung, Teilnahmebescheinigung und -quote, regelmäßige Wiederholung)?
- Sind die Mitarbeiter über die Organisation und Meldekette informiert? Sind die Informationen über den Datenschutz verfügbar/zugänglich (z. B. online)?
- Wie erfahren die Mitarbeiter über Änderungen der internen Vorgaben und Gesetzesänderungen im Bereich Datenschutz?
- Wie erfolgt die Verpflichtung auf die Vertraulichkeit oder das Datengeheimnis (Definition des Personenkreises, Selbstverpflichtung, Nachweis)? Eine formelle Verpflichtung auf die Einhaltung des Datengeheimnisses (wie dies etwa nach § 5 BDSG a. F. erforderlich war) ist nicht mehr vorgesehen. Allerdings besteht nach Artikel 29 DSGVO die Verpflichtung, dass dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Personen personenbezogene Daten lediglich auf Weisung des Verantwortlichen verarbeiten dürfen. Hieraus ergibt sich die Notwendigkeit einer Vereinbarung bzw. Verpflichtung. Ebenso sind berufsspezifische Verschwiegenheitspflichten (wie etwa aus § 203 StGB) zu beachten.

### 4.2 Einwilligungsmangement

Grundsätzlich müssen Einwilligungserklärungen nach Art. 4 Nr. 11 DSGVO nicht mehr schriftlich erfolgen. Es reicht eine in informierter Weise und unmissverständlich abgegebene Willensbekundung. Der Nachweis der abgegebenen Einverständniserklärung ist jedoch gemäß Art. 7 Abs. 1 DSGVO weiterhin durch das Unternehmen zu führen.

Es ist zu prüfen, ob Einwilligungserklärungen folgenden Anforderungen entsprechen:

- klare und verständliche Sprache,

- sog. „informierte“ Einwilligung,
- Trennung von anderen Sachverhalten,
- Abgabe ohne Zwang,
- leichte Zugänglichkeit,
- Kopplungsverbot gem. Art. 7 Abs. 4 DSGVO,
- Widerruflichkeit für die Zukunft,
- Führung des Nachweises für das Vorliegen einer Einwilligung (z. B. im CRM-System).

Sofern Kinder bis max. 16 Jahren Einwilligungen erteilen sollen, muss zusätzlich zu den o. g. Punkten gem. Art. 8 DSGVO mit angemessenen Anstrengungen sichergestellt werden, dass die Einwilligung durch den Träger der elterlichen Verantwortung oder mit dessen Zustimmung erteilt wird.

### 4.3 Auftragsverarbeitung

- Sind die Auftragsverarbeiter aus dem Verzeichnis der Verarbeitungstätigkeiten zu entnehmen oder liegt ein Register der Auftragsverarbeiter vor, aus dem Aufgabenumfang und Vertragsstatus hervorgeht?
- Besteht ein Konzept, in welchen Rechtsgebieten (EU, USA, Asien) eine Auftragsverarbeitung von der Unternehmung erfolgen darf?
- Unterliegt die Vertragsgestaltung mit den Auftragsverarbeitern den definierten Mindestanforderungen (z. B. EU-Auslandsdatenverarbeitung, EU-Standardvertragsklauseln, Anforderungen an das Sicherheitskonzept etc.)?
- Sind die Verantwortlichkeiten für den Umgang mit Betroffenenrechten und den Umgang mit Datenschutzvorfällen vertraglich geregelt? Werden bei ausgewählten Auftragsverarbeitern (z. B. externes Hosting) Follow-up Prüfungen in Bezug auf den Datenschutz durchgeführt?
- Wie wird sichergestellt, dass die Autorisierung weiterer Subunternehmer im Rahmen der Auftragsverarbeitung ordnungsgemäß erfolgt und vertraglich berücksichtigt wird?
- Wie wird sichergestellt, dass bei EU-Auslandsdatenverarbeitung die erweiterten Anforderungen über so genannte EU-Standardvertragsklauseln und hinreichende Garantien sichergestellt werden?
- Werden die relevanten Auftragsverarbeitungsverträge in einem zentralen System dokumentiert?

#### 4.4 Prüfung gemeinschaftlicher Datenverarbeitung

- Liegen gemeinschaftliche Datenverarbeitungen vor und wurden diese über das Kriterium der gemeinschaftlichen Festlegung der Zwecke und Mittel der Verarbeitung (z. B. Leiharbeit, Buchungsplattformen, konzernübergreifende Kundendatenbank) als solche klassifiziert?
- Besteht eine Dokumentation der gemeinsamen Festlegung von Verarbeitungszwecken und –mitteln?
- Liegt ein Vertrag oder eine Vereinbarung über die gemeinschaftliche Verantwortung vor (Art. 26 DSGVO) und sind die notwendigen Bestandteile enthalten? Wurde der Vertrag an einer zentralen Stelle dokumentiert?
- Sind die Aufgaben für die Pflichten, Betroffenenrechte, Informationspflichten und Rollenverteilungen nachvollziehbar geregelt?
- Besteht eine Regelung über den Haftungsausgleich unter den Verantwortlichen?
- Werden wesentliche Inhalte den Betroffenen zur Verfügung gestellt (Art. 26 Abs. 2, S. 2)?
- Wurde die Zusammenarbeit im Verzeichnis von Verarbeitungstätigkeiten dokumentiert?

#### 4.5 Prüfung von Sperr- und Löschkonzepten

- Sind Löschrufen in den Verzeichnissen von Verarbeitungstätigkeiten grundsätzlich gemäß Art. 30 DSGVO bzw. in einem Löschkonzept definiert?
- Sind die jeweiligen Speicherorte und Datenflüsse der einzelnen Prozesse bekannt?
- Sind sich die Prozessverantwortlichen ihrer Verantwortung für die Löschung bewusst?
- Stehen die vorgesehenen Aufbewahrungszeiten im Einklang mit dem definierten Zweck der Verarbeitung (Löschobliegenheit)?
- Haben die Prozessverantwortlichen Maßnahmen getroffen, um die manuelle oder automatisierte Löschung umzusetzen?
- Sind Löschungen nachvollziehbar dokumentiert (Vernichtungsnachweis, Datenbankprotokollierungen)?
- Sofern unmittelbar keine Löschung umsetzbar ist, wurden organisatorische und technische Maßnahmen zur Sperrung implementiert?
- Sind Zugriffssperren wirksam umgesetzt?

- Bestehen Vorgaben zur sicheren Löschung bzw. Vernichtung von Daten und Datenträgern?
- Werden berechnigte Löschnbegehren wirksam umgesetzt?
- Erstrecken sich die Löschnkonzepte ebenso auf Archivsysteme, Testsysteme, Protokolldaten und Backup-Systeme?
- Werden Löschnnachweise von Auftragsverarbeitern, insbesondere bei SaaS und externen Hosting Dienstleistern, bei Beendigung des Vertragsverhältnisses eingefordert?
- Wie lässt sich die Löschn umsetzen, wenn das verarbeitende KI-System bereits mit den entsprechenden Daten trainiert wurde (vgl. 4.9)?

#### 4.6 Monitoring und laufende Anpassung des Datenschutzes

- Erfolgt eine regelmäßige Risikoanalyse (z. B. vergangene Vorfälle, neue Risiken)?
- Gibt es interne Prüfungskonzepte oder Vorfallsimulationen?
- Werden Feststellungen vorangegangener Prüfungen berücksichtigt?
- Wie ist die generelle Nachverfolgung von Fehlermeldungen geregelt? Erlauben die Meldekette und die Verantwortlichkeiten die Nachverfolgung der Fehler und die Bearbeitung (klare Zuständigkeiten)?
- Gibt es Datenschutz-KPIs (etwa für Zertifizierungsverfahren) und wie wird damit umgegangen?

#### 4.7 Handlungsvorgaben bei Anfragen und Prüfungen der Datenschutzaufsichtsbehörden

- Gibt es (aktuelle) Handlungsvorgaben? Sind die Vorgaben bei international agierenden Unternehmen kommuniziert, umsetzbar und stimmig?
- Ist die unmittelbare Einbeziehung der Datenschutzorganisation sichergestellt? Wie sieht die Einbeziehung der Datenschutzorganisation bei den Tochtergesellschaften aus?
- Können geeignete Dokumentationen vorgelegt werden (zu Anfragen bzw. zur Abarbeitung)?

## 4.8 Handlungsvorgaben bei Anfragen von sonstigen Dritten

- Gibt es eine abgestimmte Vorgehensweise und organisatorische Zuständigkeiten?
- Wie ist die unmittelbare Einbeziehung der Datenschutzorganisation sichergestellt (Verfahrensweisung, Prozessbeschreibung etc.)?
- Wie sieht die Einbeziehung der Datenschutzorganisation bei den Tochtergesellschaften aus?
- Gibt es ein Kommunikations-/Pressekonzept nach außen?

## 4.9 Exkurs: Datenschutz bei der Implementierung von KI

- KI-Systeme verarbeiten oft sensible und personenbezogene Daten. Dies auch im Rahmen der Eingaben durch die Nutzer selbst (etwa bei den Prompts). Es muss sichergestellt werden, dass alle Datenschutzgesetze (z. B. DSGVO) eingehalten und Daten nur für klar definierte, legitime Zwecke genutzt werden. Strenge Richtlinien und Zugriffskontrollen sind unerlässlich.
- Nicht lizenzierte, öffentliche KI-Systeme verarbeiten Daten in der Regel für eigene Zwecke, d. h. zur Weiterentwicklung der KI. Der Einsatz eines KI-Anbieters sollte in der Regel auf einem anforderungsgerechten Auftragsverarbeitungsvertrag beruhen, der auch eine Löschung der KI-Daten ermöglicht.
- Die Anbieter von KI-Systemen haben ihren Rechtssitz nicht selten in Drittländern, vor allem in den USA. Es bedarf der Prüfung, inwiefern ein Angemessenheitsbeschluss der EU-Kommission für das Land bzw. diesen Anbieter vorliegt.
- Sollte eine Verarbeitung von Gesundheitsdaten, die dem besonderen Schutz von Privatgeheimnissen im Sinne des §203 StGB unterliegen, in Frage kommen, ist ebenso zu prüfen, ob diese zulässig außerhalb von Deutschland verarbeitet werden dürfen.
- Sollte die zu prüfende KI im Sinne der KI-Verordnung der EU als Hochrisiko-KI eingestuft sein und personenbezogene Daten verarbeiten, empfiehlt es sich im Rahmen der Datenschutzprüfung Einsicht in die interne Compliance Dokumentation nach KI-Verordnung zu nehmen. Bei Hochrisiko-KI kann eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO erforderlich sein.

## 5 Reporting

Aufgrund der in Art. 5 Abs. 2 DSGVO geforderten Rechenschaftspflicht ergibt sich die Notwendigkeit, dass ein Unternehmen ein geeignetes Berichtswesen aufbauen muss:

Die Nachweispflicht erstreckt sich insbesondere auf die Punkte:

- Rechtmäßigkeit,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- rechtzeitige Löschung,
- Datenintegrität und Vertraulichkeit.

Das Berichtswesen sollte sich an den Vorgaben für das Verfahrensverzeichnis gemäß Art. 30 DSGVO orientieren.

Neben der regelmäßigen Berichterstattung ist auch die ereignisgetriebene Berichterstattung (Ad-hoc-Berichte) zu prüfen, insbesondere als Reaktion auf ein Auskunftersuchen eines Betroffenen (Art. 15 DSGVO) sowie als Reaktion auf eine gemeldete/festgestellte Datenschutzverletzung im Sinne von Art. 32 und 33 DSGVO.

Eine Verletzung der Berichtspflichten aus beiden Bereichen kann Bußgelder der höchsten Klasse (bis zu 20 Mio. € oder 4% des Jahresumsatzes) auslösen.

### 5.1 Regelmäßige Berichtslinien gesetzlich und betrieblich/intern (z. B. Tätigkeitsberichte)

#### 5.1.1 Berichtszyklus und Berichtsumfang

- Existiert eine Arbeitsanweisung/Stellenbeschreibung/Organisationsbeschreibung oder Ähnliches, welche mindestens den Berichtszyklus, die Adressenliste und den Verantwortlichen für die Erstellung und Angaben zum Berichtsumfang enthält?

- Falls diese nicht existieren, gibt es eine Historie über mehrere Perioden, in der nachgewiesen wird, dass die Berichte regelmäßig in einem konsistenten Umfang und Format verteilt werden? In diesem Fall sollte auf die Existenz des gelebten Prozesses aus den vorgelegten historischen Berichten geschlossen werden, wenn nicht offensichtliche Gründe dagegensprechen (z. B. Kündigung des Verantwortlichen, Restrukturierung, die den Informationsfluss unterbricht).

### 5.1.2 Berichtsumfang

Der regelmäßige Bericht muss es dem Adressaten ermöglichen, sich davon zu überzeugen, dass die Datenschutzaktivitäten die gesetzlichen Vorgaben (und eventuelle unternehmens- bzw. branchenspezifische Anforderungen) erfüllen. Dazu sollte der Bericht mindestens

- alle Datenschutzvorfälle in der Berichtsperiode aufzählen und ggf. auf die Falldokumentation verweisen,
- alle wesentlichen Änderungen im Verfahrensverzeichnis in der Berichtsperiode erwähnen,
- statistische Angaben zu Auskunftersuchen und deren Bearbeitungsdauer (oder Nullmeldung) enthalten,
- ein Statusupdate zu allen datenschutzbezogenen Projekten geben,
- den ihm zu Datenschutzzwecken getriebenen Aufwand im Berichtszeitraum erkennen lassen,
- selbst datenschutzrechtliche Vorgaben erfüllen (z. B. Anonymisierung von personenbezogenen Daten).

Werden für unterschiedliche Adressatenkreise unterschiedlich häufige oder unterschiedlich umfangreiche Berichte produziert (intern, extern, Wirtschaftsprüfer, Betriebsrat, IT-Leitung, Muttergesellschaft etc.), so sollten die Unterschiede in Frequenz und Umfang einer nachvollziehbaren Logik folgen, die die unterschiedliche Informationsdichte, aber dennoch einen gleichen Aussagegehalt berücksichtigt.

Auch hier gilt, dass ein durch Zeitreihe nachgewiesener Berichtsumfang die formale Beschreibung des Designs ersetzen kann.

### 5.1.3 Dokumentation für die erstellten Berichte

- Entsprechen die letzten Berichte den Vorgaben der o. g. Punkte?
- Erfolgt eine Überprüfung der Korrektheit und Vollständigkeit der Angaben am konkreten Beispiel?

- Werden der Weg der Informationen und die Zuverlässigkeit der Quellen bewertet? Werden z. B. alle Eingangskanäle für Auskunftersuchen bei deren Anzahl berücksichtigt und nicht nur die häufigste Form der Kontaktaufnahme? Hat der Bericht tatsächlich den geplanten Verteiler erreicht?
- Ist es ohne Inhaltsprüfung belegbar, dass seit Inkrafttreten der Regelung tatsächlich in jeder Berichtsperiode ein Bericht erstellt und zeitnah zum Periodenende verteilt wurde?

## 5.2 Anlassbezogene Berichterstattung (Ad-hoc-Reporting) an Datenschutzbehörde und/oder interne Stelle

Der Prozess zur Erstellung von Ad-hoc-Berichten muss zuverlässig beginnen, wenn Hinweise auf ein Datenleck, den unzulässigen Betrieb einer Anwendung oder die missbräuchliche Verwendung die Organisation auf verschiedenen Wegen erreichen. Ebenso muss die Reaktion auf solch ein Ereignis oder ein Auskunftersuchen an den Datenschutzbeauftragten auch in der geplanten Zeit erfolgen (vgl. 3.4).

### 5.2.1 Übersicht über mögliche Anlässe zu meldepflichtigen Vorfällen

- Hat die Organisation eine Übersicht über alle möglichen Anlässe zu meldepflichtigen Vorfällen?
- Existiert eine Beschreibung für die plausiblen Szenarien, wer welche Informationen zusammenträgt und in welcher Form diese dann weitergeleitet werden?
- Werden neben den Datenschutzvorfällen auch Auskunftersuchen der verschiedenen Gruppen von Betroffenen aufgelistet (Mitarbeiter, Kunden, Interessenten, Bewerber, Angehörige von Kunden/Patienten, Erziehungsberechtigte von Kindern etc.)?

### 5.2.2 Lokale Vorgaben

Eine angemessene Vorbereitung für die Situation einer anlassbezogenen Berichterstattung kann eine allgemein formulierte Anleitung oder auch eine Sammlung von Berichtsmustern für die verschiedenen Situationen sein.

- Gibt es lokale Vorgaben bzgl. der anlassbezogenen Berichterstattung?
- Sind die internen Vorgaben zu Meldeprozessen umgesetzt, z. B. Reaktionsplan?

### 5.2.3 Dokumentation für die erstellten Berichte

- Erfolgte die Berichterstattung für konkret bekannte Anlässe nachvollziehbar?
- Entspricht der anlassbezogene Bericht dem geforderten Umfang?

## Autoren

Erarbeitet vom DIIR-Arbeitskreis Datenschutz & Data Governance

DIIR – Deutsches Institut für Interne Revision e.V.  
Theodor-Heuss-Allee 108  
60486 Frankfurt am Main

Version 1.0 veröffentlicht im Oktober 2017 auf [www.diiir.de](http://www.diiir.de),  
überarbeitet im August 2021 (Version 2.0) und  
aktualisiert im April 2026 (Version 3.0).

Version 3.0