



DIIR

Leitfaden Interne Revision und Datenschutz

DIIR-Arbeitskreis Datenschutz & Data Governance

Version 3.0, April 2026

Inhalt

Vorwort	3
1 Datenschutz als rechtliche Verpflichtung	5
1.1 Nationale und europäische Gesetzgebung	5
1.2 Grundprinzipien der DSGVO	6
2 Bedeutung des Datenschutzes für die Interne Revision	11
2.1 Grundsätzliches	11
2.2 Personenbezogene Daten	13
2.3 Beschäftigtendaten in der Prüfung	13
2.4 Unternehmensinterne Ermittlungen	15
2.5 Internationale Datenflüsse	16
3 Rolle des Datenschutzbeauftragten	19
3.1 Stellung im Unternehmen	19
3.2 Aufgaben	20
3.3 Der internationale Kontext	22
4 Umsetzung des Datenschutzes in der Internen Revision	23
4.1 Grundlegende Festlegungen	23
4.2 Prüfungsauftrag und Prüfungsvorbereitung	26
4.3 Prüfungsdurchführung	27
4.4 Dokumentation der Prüfungsergebnisse (Berichterstattung)	29
4.5 Dokumentation und Archivierung von Prüfungsdaten	29

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)¹ 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 der 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. Sie 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 vor 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.

¹ 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.

Immer hybridere IT-Landschaften und steigende Cyberrisiken erhöhen unmittelbar auch das Datenschutzrisiko einer Organisation. Insbesondere die europäischen Datengesetze und die 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 im Folgenden einen Leitfaden zu den Grundfragen des Datenschutzes im Kontext der Internen Revision und zur Gestaltung der angemessenen Struktur und Prozessabläufe an. Datenschutz, Informationssicherheit und der Umgang mit KI-bezogenen Daten und Technologien müssen zunehmend zusammen bewertet werden. Daher wurden diese Themen neu aufgenommen und im Leitfaden ergänzt.

Dieser Leitfaden 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. Der Leitfaden erhebt keinen Anspruch auf Verbindlichkeit und Vollständigkeit und ersetzt keinesfalls die Prüfung der individuellen rechtlichen Situation.

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

1 Datenschutz als rechtliche Verpflichtung

1.1 Nationale und europäische Gesetzgebung

Vorrangiges Ziel des Datenschutzes ist es, das Persönlichkeitsrecht des Einzelnen zu schützen und die missbräuchliche Verwendung personenbezogener Daten zu verhindern. Jeder Mensch soll selbst entscheiden können, welche seiner persönlichen Daten verarbeitet, gespeichert oder an Dritte weitergegeben werden dürfen. Indem Verarbeitungsregeln für personenbezogene Daten und über die Gestaltung und den Einsatz von IT aufgestellt werden, soll eine Gefährdung des individuellen Persönlichkeitsrechts verhindert werden. Rechtlich ist der Datenschutz in einem komplexen Zusammenspiel verschiedener Vorschriften geregelt. Für Unternehmen ergeben sich datenschutzrechtliche Pflichten, die mit dem Inkrafttreten der Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018 verschärft wurden. Die DSGVO regelt den Schutz personenbezogener Daten in allen Mitgliedstaaten der EU und soll den Datenschutz europaweit vereinheitlichen sowie die datenschutzrechtlichen Rahmenbedingungen und Standards harmonisieren. Die in der Verordnung enthaltenen Öffnungsklauseln² ermöglichen es den einzelnen Mitgliedstaaten, bestimmte Aspekte des Datenschutzes auch in der nationalen Gesetzgebung ergänzend zu regeln. Daher sind gleichzeitig auch nationale Regelungen, wie bspw. das Bundesdatenschutzgesetz (BDSG),³ Vorgaben aus der Landesgesetzgebung⁴ und zusätzliche spezialgesetzliche Regelungen,⁵ weiterhin relevant.

Zusammenfassend lässt sich festhalten, dass die Rechtmäßigkeit der Verarbeitung personenbezogener Daten wegen ihres Anwendungsvorrangs zuerst nach der DSGVO zu beurteilen ist. Lässt diese einen Regelungsspielraum zu, ist zu prüfen, ob es ein bereichsspezifisches Datenschutzrecht gibt. Ist dies nicht der Fall oder sind die spezialgesetzlichen Vorschriften nicht abschließend, gilt ergänzend das BDSG (§ 1 Abs. 2 Satz 1 BDSG). Bereichsspezifische Regelungen finden sich beispielsweise im Sozialrecht oder Strafrecht,

² Die Mehrzahl dieser Öffnungs- und Spezifizierungsklauseln betrifft die Datenverarbeitung durch öffentliche Stellen.

³ Das BDSG bleibt insbesondere für den Bereich der öffentlichen Verwaltung relevant; es enthält aber auch allgemein anwendbare Normen wie § 26 BDSG, der den Beschäftigtendatenschutz regelt.

⁴ Die Landesdatenschutzgesetze gelten für die jeweiligen Landesbehörden und andere öffentlich-rechtliche Einrichtungen im Landes- und Kommunalbereich, gegebenenfalls ergänzend zu spezialgesetzlichen Regelungen.

⁵ Diese Sondervorschriften sind auf die Anforderungen der jeweiligen Bereiche angepasst und gehen grundsätzlich den allgemeineren nationalen Regeln vor. Sie ergeben sich beispielsweise aus den Büchern des Sozialgesetzbuchs (SGB), der Abgabenordnung (AO), dem Geldwäschegesetz (GwG), dem BSI-Gesetz (BSIG), dem Telekommunikation-Digitale-Dienste-Datenschutzgesetz (TDDDG) oder dem kirchlichen Datenschutzrecht.

und sie gehen den allgemeinen Regelungen des BDSG vor, sofern sie den datenschutzrechtlichen Anforderungen der DSGVO genügen.

Um eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen, veröffentlicht die Datenschutzkonferenz (DSK)⁶ regelmäßig u. a. Orientierungshilfen, Standardisierungen und Stellungnahmen. Diese können Hilfestellung bei der praktischen Umsetzung der Vorgaben geben.⁷ Weitere Rechtsquellen sind auch die Stellungnahmen des Europäischen Datenschutzausschusses (EDSA), der gemäß Art. 70 DSGVO die einheitliche Anwendung der DSGVO sicherstellen soll.⁸

Der Leitfaden wird sich im Schwerpunkt auf die für die Prüfungstätigkeit der Internen Revision einschlägigen Regelungen der DSGVO und des BDSG sowie ihrer praktischen Bedeutung für die Revisionsarbeit mit Schwerpunkt Deutschland beziehen.

Aspekte der Mitbestimmung, im Wesentlichen Fragen zur Verhaltens- und Leistungskontrolle, können oftmals bei Fragestellungen mit Datenschutzbezug aufkommen. Diese werden in diesem Leitfaden jedoch nicht thematisiert.⁹

1.2 Grundprinzipien der DSGVO

Der Umgang mit personenbezogenen Daten muss gemäß DSGVO einigen grundsätzlichen Kriterien entsprechen¹⁰:

- rechtmäßige, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Verarbeitung (»Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz«),
- Erhebung nur für definierte Zwecke (»Zweckbindung«),
- dem Zweck angemessen und für diesen erheblich (»Datenminimierung«),

⁶ Die DSK besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder.

⁷ <https://www.datenschutzkonferenz-online.de/index.html>.

⁸ https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de.

⁹ Vgl. Herold, Ralf: Das Zusammenspiel der Internen Revision mit Datenschutz und Mitbestimmung, <https://zirdigital.de/ce/das-zusammenspiel-der-internen-revision-mit-datenschutz-und-mitbestimmung/detail.html>.

¹⁰ Die Grundsätze sind in Artikel 5 DSGVO aufgeführt und werden im Erwägungsgrund 39 erläutert.

- sachliche Richtigkeit und sofern dies im Hinblick auf die Verarbeitungszwecke nicht der Fall ist, angemessene Maßnahmen zur Korrektur oder Löschung (»Richtigkeit«),
- Form der Speicherung, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für den Zweck, für den die Daten verarbeitet werden, erforderlich ist (»Speicherbegrenzung«).
- angemessene Sicherheit zum Schutz vor unrechtmäßiger Verarbeitung, Verlust und Zerstörung durch geeignete technische und organisatorische Maßnahmen (»Integrität und Vertraulichkeit«).

Die Einhaltung dieser Grundsätze obliegt gemäß Art. 5 Abs. 2 DSGVO dem jeweiligen Verantwortlichen¹¹ und muss anhand einer entsprechenden Dokumentation nachgewiesen werden können (sog. Rechenschaftspflicht oder „Accountability“).¹² Das legt nahe, dass im Unternehmen ein Datenschutzmanagementsystem etabliert sein sollte, das die Einhaltung der Schutzziele der DSGVO gewährleistet.

¹¹ Begriff „Controller“ (Verantwortlicher) in Art. 4 Nr. 7 DSGVO.

¹² Art. 5 Abs. 2 DSGVO.

2 Schnittstellen zwischen Datenschutz, Informationssicherheit und KI-Lösungen

2.1 Datenschutz und Informationssicherheit

Datenschutz und Informationssicherheit sind eng miteinander verbunden, aber dennoch unterschiedliche Konzepte im Umgang mit Daten.

- Datenschutz schützt im Kern die Privatsphäre natürlicher Personen und soll sicherstellen, dass deren Daten nur für legitime und transparente Zwecke verwendet werden und nicht ohne deren Einwilligung erhoben, verarbeitet oder weitergegeben werden.
- Informationssicherheit zielt darauf ab, die Verfügbarkeit, Integrität und Vertraulichkeit aller Informationen zu schützen, unabhängig davon, ob es sich um personenbezogene oder – im Unternehmenskontext – geschäftliche Daten wie beispielsweise Finanzdaten, Geschäftsgeheimnisse, Patente oder urheberrechtlich geschützte Inhalte handelt. Technische und organisatorische Maßnahmen sollen sicherstellen, dass Daten vor unbefugtem Zugriff, Manipulation, Verlust oder Zerstörung geschützt sind, z. B. durch Cyberangriffe, Viren, Trojaner, Diebstahl oder menschliches Fehlverhalten.
- Datenschutz ist stark durch gesetzliche Vorgaben wie die DSGVO oder nationale Datenschutzgesetze geprägt. Unternehmen müssen bestimmte rechtliche Anforderungen erfüllen, wenn sie personenbezogene Daten verarbeiten.
- Informationssicherheit wird zunehmend durch Gesetze mit Vorgaben zu Informationssicherheitsmaßnahmen und -standards geprägt. Diese sind jedoch nicht für alle Branchen einschlägig. Standards und Normen wie ISO 27001 zum Aufbau eines Informationssicherheit-Managementsystems (ISMS) dienen dazu, bewährte Maßnahmen zur Sicherung von Informationen zu etablieren.

Oft überschneiden sich die Anforderungen an den Datenschutz und die Informationssicherheit. Zu den Schnittmengen zwischen DSGVO und ISO 27001 gehören Anforderungen an den technischen Datenschutz: In Art. 32 DSGVO¹³ werden ähnliche Schutzziele als Anforderungen an den Schutz personenbezogener Daten gestellt wie in der ISO 27001 bei den

¹³ Danach hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 5 und Art. 32 DSGVO).

Grundprinzipien der Informationssicherheit. Auch angesichts der ständig wachsenden Cyberbedrohungen empfiehlt es sich, das Risikomanagement und die Konzepte für Datenschutz und Informationssicherheit abzugleichen und sinnvolle Synergien zu nutzen.

Entscheidend für die Arbeit der Internen Revision ist unter anderem die Identifikation, welche jeweilige Regulierung für die im Rahmen des Prüfungsauftrags zu verarbeitenden Daten maßgeblich ist. Sofern keine gesetzliche Anforderung – in den regulierten Branchen z. B. durch das BSI-Gesetz oder den Digital Operational Resilience Act (DORA) – vorliegt, bestehen vielfach interne Vorgaben zur Informationssicherheit (z. B. Klassifizierungsvorgaben für Unternehmensinformationen), deren Einhaltung die Interne Revision sicherstellen soll.

2.2 Schnittstellen beim Einsatz von KI-gestützten Lösungen

Neben datengetriebenen Entscheidungsprozessen und Automatisierung setzen Unternehmen zunehmend KI-gestützte Lösungen ein, um Potenziale zur Effizienzsteigerung und Qualitätsverbesserung bei ihren Abläufen und Geschäftsprozessen zu nutzen. Das ermöglicht es auch Revisionsabteilungen, ihre Prüfprozesse zu optimieren, beispielsweise durch verbesserte Stichproben und Auswertungsmöglichkeiten, Unterstützung bei Recherchen und Dokumentenprüfungen oder das Aufbereiten von Prüfungsergebnissen.¹⁴

Für die Interne Revision bedeutet der Einsatz von KI im Unternehmen unterschiedliche Prüfungsansätze. Das kann die eigene Einbeziehung in die KI-Governance des Unternehmens bedeuten, aber auch die Prüfung von KI-Rahmenwerk und -Governance sowie von KI-Systemen und Produkten und den Einfluss auf Geschäfts- und Unternehmensprozesse betreffen.

Im Hinblick auf die Sicherstellung des Datenschutzes und der Informationssicherheit beim Einsatz künstlicher Intelligenz ist zu unterscheiden zwischen

- externen, eingekauften Lösungen bzw. KI-Systemen,
- intern entwickelten KI-Systemen sowie

¹⁴ Zu den Chancen und Risiken des Einsatzes großer Sprachmodelle (LLMs) bei der Internen Revision und beispielhaften Ansätzen zu deren Einbindung in den Revisionsprozess: Fachbeitrag des DIIR Nr. 4 „Generative KI in der Internen Revision: Chancen und Herausforderungen“, Version 1.0 September 2023.

- Software und Tools, die von einem Anbieter im Rahmen der normalen Leistungserbringung eingesetzt werden und über zusätzliche KI-Funktionen verfügen.

Beim Einsatz interner KI-Systeme müssen in erster Linie die Berechtigungskonzepte und -beschränkungen aus den Systemen, auf die das KI-Modell zugreift, übernommen werden, um zu verhindern, dass Unternehmensinformationen im gesamten Unternehmen miteinander geteilt werden. Auch die Schnittstellen zwischen den einzelnen Systemen müssen sorgfältig aufgesetzt und überprüft werden.

Insbesondere bei externen KI-Systemen sind informationssicherheitsrechtliche Beschränkungen unerlässlich, um vertrauliche Informationen sowie Geschäftsgeheimnisse nicht mit unberechtigten Dritten zu teilen. Dabei ist insbesondere darauf zu achten, dass KI-Systeme nicht mit derartigen Daten trainiert werden und auf diesem Wege Externen gegenüber offenbart werden.

Beim Einsatz KI-gestützter Tools sind sowohl im Unternehmen als auch bei der Internen Revision wichtige Grundprinzipien zu Transparenz, Datenschutz und Informationssicherheit zu beachten und als Leitplanken festzulegen. Dazu gehört, dass keine sensiblen oder vertraulichen Informationen in öffentliche KI-Systeme eingegeben werden, KI-generierte Ergebnisse vor der weiteren Verwendung auf Richtigkeit und Plausibilität geprüft werden und entsprechende Prozesse etabliert sind, wie KI-generierte Inhalte weiterverwendet und verbreitet werden.

3 Bedeutung des Datenschutzes für die Interne Revision

3.1 Grundsätzliches

Bei der Mehrzahl der Geschäftsprozesse fallen personenbezogene Daten an. Die ständig wachsende Anzahl von Geschäftsvorfällen und Datenbeständen sowie der Einsatz von IT in nahezu allen betrieblichen Bereichen führen dazu, dass Geschäftsdaten – und damit auch personenbezogene Daten – systematisch betrachtet und ausgewertet werden¹⁵. Prüfungshandlungen der Internen Revision sind daher regelmäßig mit der Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten und teilweise von Dritten (z. B. Geschäftspartnern oder Kunden) verbunden. Es werden Unterlagen und Daten (u. a. Dokumente, Dateien, E-Mails) aus unternehmenseigenen Systemen eingesehen,¹⁶ ausgewertet und zusammengeführt. Der Einsatz moderner Technologien in der Internen Revision verstärkt diesen Aspekt noch zusätzlich.

Sobald im Rahmen des Revisionsprozesses personenbezogene Daten ins Spiel kommen, sind datenschutzrechtliche Regelungen zu beachten. Grundsätzlich ist das Datenschutzrecht als Abwägungsrecht zu verstehen. Manche Sachverhalte sind nicht eindeutig geregelt. Sie erfordern eine Entscheidung im Einzelfall, bei der die Interessen der datenverarbeitenden Stelle mit den Interessen des Betroffenen abzuwägen sind (Grundsatz der Verhältnismäßigkeit).

Jede Verarbeitung personenbezogener Daten muss auf Grundlage eines legitimen Zwecks erfolgen. Aufgrund der funktionalen Zuständigkeit der Internen Revision lässt sich im Rahmen ihrer Prüftätigkeit meist eine Zweckbestimmung in datenschutzrechtlicher Hinsicht begründen. Die Interne Revision verfügt regelmäßig und im Rahmen ihrer Aufgabenerfüllung über ein grundsätzlich uneingeschränktes Informationsrecht.¹⁷ Sie darf die zur Wahrnehmung ihrer Aufgaben notwendigen Informationen einholen und dafür auch Daten einsehen und auswerten, wobei sie sich an die geltenden Datenschutzvorgaben zu halten hat.

Ein Grundsatz der DSGVO ist die rechtmäßige Verarbeitung personenbezogener Daten: Es muss immer eine Rechtsgrundlage zu deren Legitimation vorliegen. Artikel 6 DSGVO

¹⁵ Vgl. weiterführend DIIR: „Datenanalysen im Anti Fraud-Management“, Fachbeitrag_Nr_5_AFM_Datenanalysen.pdf.

¹⁶ Bereits das Einsehen von personenbezogenen Daten stellt eine Verarbeitung im Sinne der DSGVO dar.

¹⁷ DIIR Revisionsstandard Nr. 3 (Stand: Dezember 2025).

listet die regelmäßig geltenden Erlaubnistatbestände auf. So kann sich – neben der Einwilligung der betroffenen Person – die Zulässigkeit unter anderem ergeben aus:

- Vertrag oder Durchführung vorvertraglicher Maßnahmen,
- Erfüllung einer rechtlichen Verpflichtung,
- öffentlichem Interesse oder in Ausübung hoheitlicher Gewalt oder
- berechtigtem Interesse nach Interessenabwägung.

Die Zulässigkeit der Verarbeitung und Nutzung der Daten im Rahmen der Kontroll- und Überwachungstätigkeit der Internen Revision¹⁸ ergibt sich im Regelfall aus Art. 6 Abs. 1 lit. f DSGVO (Wahrung berechtigter Interessen).

Art. 6 Abs. 1 lit. f DSGVO erfordert eine Abwägung der berechtigten Interessen des Unternehmens gegenüber den schutzwürdigen Belangen der Betroffenen. Hierbei ist eine frühzeitige Einbeziehung des Datenschutzbeauftragten (DSB) empfehlenswert, um das generelle Vorgehen bei der Prüfungstätigkeit der Internen Revision abzustimmen.

Das berechtigte Interesse hinsichtlich der Tätigkeit der Internen Revision kann u .a. darin liegen, sich im Rahmen ihrer Kontroll- und Überwachungstätigkeit davon zu überzeugen, dass rechtliche Vorgaben und unternehmensinterne Regelungen bei den zu prüfenden Geschäftsvorgängen eingehalten werden.

Mit der in Art. 6 Abs. 1 lit. c DSGVO aufgeführten Zulässigkeit einer Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung sind vorrangige Rechtsvorschriften gemeint, die zur Verarbeitung der betroffenen Daten verpflichten.¹⁹ Die mittelbare Ableitung einer rechtlichen Verpflichtung der Internen Revision, z. B. über § 91 Abs. 3 AktG, ist hier nicht gemeint.

Die DSGVO hat einen räumlichen Anwendungsbereich. Sie gilt nicht nur für die in der Europäischen Union niedergelassenen Unternehmen, sondern auch für außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind (Marktortprinzip).²⁰ Bezogen auf die Tätigkeit der Internen Revision findet die DSGVO immer Anwendung, wenn die Revisionsabteilung in der Europäischen Union niedergelassen ist, unabhängig davon, ob die Verarbeitung der Daten in der Europäischen Union stattfindet.

¹⁸ Prüfrecht der Internen Revision abgeleitet aus §§ 93, 116 i. V. m. §§ 91, 107 AktG sowie § 130 i. V. m. § 30 OWiG.

¹⁹ vgl. Erwägungsgrund 45 DSGVO.

²⁰ Art. 3 Abs. 2 DSGVO.

3.2 Personenbezogene Daten

Personenbezogen ist ein Datum immer dann, wenn es sich auf eine bestimmte natürliche Person bezieht oder diese direkt oder indirekt identifiziert werden kann.²¹ Als identifizierbar bzw. bestimmbar „wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung, wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“, bestimmt werden kann.²²

Diese Kriterien sind bei Prüfungstätigkeiten der Internen Revision im Regelfall erfüllt. Einträge von Kundendaten in Systemen, Namen auf Belegen, Kontoauszügen oder Verträgen sowie Benutzerkennungen, Personalnummern, Gehaltsdaten und andere Beschäftigtenangaben machen es erforderlich, dass bei deren Verwendung in einer Revisionsprüfung datenschutzrechtliche Vorgaben zu beachten sind.

Wenn zu Beginn einer Prüfung auf einen Personenbezug verzichtet wird oder mit anonymisierten Daten (d. h. solchen, bei denen der Personenbezug nachhaltig entfernt wurde) gearbeitet wird, müssen die Vorschriften zum Datenschutz nicht herangezogen werden. Ein typisches Beispiel ist eine Beleganalyse, ohne zunächst den buchenden Mitarbeiter oder andere Betroffene in diese Auswertung einzubeziehen. (Zur Anonymisierung und Pseudonymisierung vgl. auch Kapitel 5.5.)

Eine Anonymisierung der zu bewertenden Datensätze könnte ggf. durch den Einsatz von einem KI-System erreicht werden. Dies würde zwar dazu führen, dass für den Einsatz des KI-Systems und den von diesem zu bearbeitenden Datensatz die Datenschutzanforderungen zu berücksichtigen und einzuhalten sind, die Bewertung der dabei generierten Datensätze selbst aber aufgrund der vorherigen Anonymisierung keinen Datenschutzbezug mehr aufweisen würden.

3.3 Beschäftigendaten in der Prüfung

Die DSGVO enthält keine spezifischen Erlaubnistatbestände für die Verarbeitung von Beschäftigendaten, sondern setzt nur den Rahmen im Sinne der einzuhaltenden Leitplanken.

²¹ Bitte beachten, dass hierbei die Rechtsprechung des EUGH vom 4. September 2025 (Rechtssache C-413/23 P) zur Anonymität von Daten auch aufgrund der in der Entscheidung ausdrücklich enthaltenen Hinweise auf eine Einzelfallentscheidung noch nicht berücksichtigt wurden. Aufgrund der als sehr richtungweisend geltenden Entscheidung gilt es, die weitere Diskussion darüber aufmerksam zu beobachten.

²² Art. 4 Ziffer 1 DSGVO.

Der Beschäftigtendatenschutz gehört zu den Abschnitten der DSGVO, die eine nationale Regelung bzw. Präzisierung vorsehen. Spezielle Vorschriften für den Datenschutz im Beschäftigungsverhältnis können durch Rechtsvorschriften oder durch Kollektivvereinbarungen²³ ausgestaltet werden (Art. 88 DSGVO bzw. auch § 26 Abs. 4 BDSG).²⁴

Im Beschäftigungsverhältnis gelten zunächst die allgemeinen Erlaubnistatbestände der DSGVO. Je nach Sachverhalt kommen unterschiedliche Rechtsgrundlagen in Betracht. Die für die Erfüllung des Arbeitsvertrags erforderlichen Verarbeitungsvorgänge erfolgen auf Grundlage von Art. 6 Abs. 1 lit. b DSGVO (Erfüllung eines Vertragsverhältnisses). Eine Besonderheit gilt für die Verarbeitung von Gesundheitsdaten im Beschäftigungsverhältnis. In diesen Fällen sind neben einer erforderlichen Grundlage nach Art. 6 DSGVO zusätzlich die Vorgaben aus Art. 9 DSGVO zu beachten, welcher die Verarbeitung von besonderen (sensitiven) Kategorien personenbezogener Daten regelt. Für Verarbeitungen im Rahmen der Kontroll- und Überwachungstätigkeit der Internen Revision kommt als Rechtsgrundlage auch hier zunächst die Wahrung berechtigter Interessen nach Art. 6 Abs. 1 lit f DSGVO in Betracht.

Im BDSG ist § 26 für die Datenverarbeitung im Beschäftigungskontext maßgeblich. Die Vorschrift konkretisiert und ergänzt die Vorgaben der DSGVO, verdrängt diese als vorrangige Regelungen aber nicht. Hier ist eine Abwägung der berechtigten Interessen des Unternehmens gegenüber denen der Beschäftigten vorzunehmen.

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Die Verarbeitung von Beschäftigtendaten ist damit erlaubt, wenn sie für Zwecke des Beschäftigungsverhältnisses geeignet ist, das mildeste der dem Unternehmen zur Verfügung

²³ Zu beachten ist die Rechtsprechung des EuGH (EuGH, Urteil v. 19. Dezember 2024 – C-65/23) nach welcher eine Abweichung der durch die DSGVO normierten Standards durch innerbetriebliche Vereinbarungen wie etwa innerhalb einer Betriebsvereinbarung für unzulässig erachtet wurde.

²⁴ Schon seit längerer Zeit ist ein Gesetz zur Regelung des Beschäftigtendatenschutzes in Planung. Gemäß Art. 88 DSGVO können die Mitgliedsstaaten "spezifischere Vorschriften" zum Beschäftigtendatenschutz erlassen, d. h. konkretere Regelungen, die spezifisch auf den Datenschutz am Arbeitsplatz zugeschnitten sind. Die aktuelle Bestimmung des § 26 BDSG reicht nach Ansicht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) angesichts aktueller rechtlicher (insbesondere das Urteil des Europäischen Gerichtshofs (EuGH) vom 30. März 2023 in der Rechtsache C-34/21) und technologischer Entwicklungen (z. B. bei der Künstlichen Intelligenz) nicht aus. Im aktuellen Koalitionsvertrag ist der Auftrag verankert, Regelungen zum Beschäftigtendatenschutz zu schaffen.

stehenden gleich effektiven Mittel ist (Erforderlichkeit) und schutzwürdige Interessen der Beschäftigten nicht überwiegen.

3.4 Unternehmensinterne Untersuchungen

Interne Untersuchungen anlässlich möglicher doloser Handlungen²⁵ unterscheiden sich von klassischen prozess- bzw. sachfragenorientierten Prüfungen vor allem dadurch, dass gerade personenbezogene Daten zur Sachverhaltsaufklärung genutzt und als Prüfungsergebnis personenbezogene Aussagen getroffen werden müssen. Hieraus leiten sich besondere Anforderungen an die Sorgfaltspflicht und Vertraulichkeit in der Prüfungsdurchführung ab sowie das Erfordernis, interne Untersuchungen datenschutzkonform zu gestalten, da Betroffenen hinreichende Auskunfts-, Einsichts- und Bereitstellungsansprüche zustehen, um die Rechtmäßigkeit der Verarbeitung sie betreffender Informationen überprüfen zu lassen. Datenschutzverstöße bei internen Ermittlungen bergen nicht nur Bußgeld- und Haftungsrisiken, sondern können auch die gerichtliche Verwertbarkeit der Untersuchungsergebnisse gefährden. Die Einbeziehung des Datenschutzbeauftragten, des Betriebsrates und ggf. der Rechtsabteilung sollten daher bei der Planung und Durchführung berücksichtigt werden.

Die datenschutzrechtlichen Anforderungen bei internen Sachverhaltsaufklärungen bzw. internen Ermittlungen ergeben sich vor allem aus der DSGVO, dem BDSG und der Rechtsprechung des Bundesarbeitsgerichts (BAG) und des Europäischen Gerichtshofs (EuGH). Der Datenschutzbeauftragte sollte in Fragen der Datenbereitstellung und Anonymisierung aktiv eingebunden werden.

Die Voraussetzungen für die Verarbeitung von Beschäftigtendaten zur Aufdeckung von Straftaten sind in § 26 Abs. 1 Satz 2 BDSG genannt:

- tatsächliche Anhaltspunkte und begründeter Verdacht auf eine Straftat,
- Straftat im Beschäftigungsverhältnis,
- Notwendigkeit der Datenerhebung zur Aufdeckung der Straftat,

²⁵ Nach der Definition des IIA umfasst Fraud Unregelmäßigkeiten und unrechtmäßige Handlungen durch vorsätzliche Täuschung oder falsche Darstellung. Der Fraud-Begriff umfasst auch die Korruption. Motiv ist die Erzielung ungerechtfertigter Vorteile für den Täter, die Organisation oder eine andere Person.

- Schutzwürdige Interessen des Beschäftigten und Verhältnismäßigkeit (Ergebnis der Interessenabwägung zwischen Aufklärungsinteresse des Unternehmens gegenüber Wahrung der Persönlichkeitsrechte der betroffenen Person).

Während der Prüfung ist fortlaufend die Zulässigkeit von Auswertungen zu dokumentieren, da in der Anfangsphase der Verlauf der Untersuchung offen ist. Die Beachtung der Verhältnismäßigkeit und Wahrung schutzwürdiger Interessen ist im Verlauf der Prüfung regelmäßig zu bewerten und in den Arbeitsunterlagen mit Nachweisen zu dokumentieren.

Artikel 13 und 14 DSGVO sehen umfassende Transparenzpflichten des Verantwortlichen vor, wenn personenbezogene Daten verarbeitet werden. In der Regel setzen unternehmensinterne Ermittlungen sogar weitreichende Untersuchungsmaßnahmen voraus, die für die betroffenen Personen im Einzelfall besonders eingriffsintensiv sein können. In der Praxis sind Unternehmen gut beraten, ihre Datenschutzinformationen für Beschäftigte gegebenenfalls so zu ergänzen, dass sie die Zwecke, typischen Anlässe, Rechtsgrundlagen und Umstände interner Untersuchungen in transparenter Form beschreiben. Zudem sollten mögliche Ausnahmen von der Informationspflicht (etwa nach § 32 BDSG) genau geprüft und dokumentiert werden. Der Einsatz von KI-Systemen könnte zu einer Erschwerung der Erfüllung der Transparenzpflicht führen, da es in der Regel mit erheblichen Schwierigkeiten verbunden ist, die Verarbeitung personenbezogener Daten durch KI-Systeme verständlich zu erklären – insbesondere im Hinblick auf den Zusammenhang zwischen Eingabe solcher Daten und dem Zusammenspiel des aufgrund eines Algorithmus entstandenen Outputs. In der Fachliteratur wird die Notwendigkeit einer vorherigen Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO diskutiert. Teilweise wird sie wegen der Einschätzung interner Untersuchungsmaßnahmen als "voraussichtlich hohes Risiko" für die Rechte von Betroffenen empfohlen.²⁶ Eine neue Bewertung bestehender Datenschutz-Folgenabschätzungen könnte aufgrund des Einsatzes von KI-Systemen erforderlich werden.

3.5 Internationale Datenflüsse

Sofern personenbezogene Daten von Deutschland aus übermittelt werden oder über Landesgrenzen hinweg Einsicht auf personenbezogene Daten genommen wird, ist zu berücksichtigen, dass nicht nur die Regelungen der DSGVO einschlägig sein können, sondern auch gesetzliche Regelungen anderer Länder.

²⁶ Grundsätzliches zur Datenschutz-Folgenabschätzung im Kurzpapier der Datenschutzkonferenz: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.

Zum Datentransfer aus Deutschland/der EU in Drittländer:

Die DSGVO regelt in Kapitel V (Art. 44 ff.), dass personenbezogene Daten aus EU-Staaten nur unter bestimmten Voraussetzungen in Drittländer gesendet werden dürfen. Darunter fallen vor allem:

- Vorhandensein eines Angemessenheitsbeschlusses für das betreffende (empfangende) Drittland (also die Festlegung der Europäischen Kommission, dass Länder wie z. B. Japan, Schweiz, Kanada – und in Erneuerung der Angemessenheitsbeschlüsse von 2021 seit 19.12.2025 bis zunächst 27.12.2031 – auch Großbritannien, ein angemessenes Schutzniveau für personenbezogene Daten bieten),²⁷
- Standarddatenschutzklauseln (früher: Standardvertragsklauseln) (also standardisierte vertragliche Vereinbarungen, die angemessene Garantien für Datenübermittlungen in Drittländer bereitstellen),
- Binding Corporate Rules (also die verbindlichen internen Datenschutzvorschriften eines Unternehmens oder innerhalb einer Unternehmensgruppe).²⁸

Da der Europäische Gerichtshof (EuGH) im Sommer 2020 das EU-US Privacy Shield Abkommen als Rechtsgrundlage für den Datentransfer in die USA für unwirksam erklärt hat, besteht zum Zeitpunkt der Veröffentlichung dieses Leitfadens nur ein Angemessenheitsbeschluss in Bezug auf US-Unternehmen und Organisationen, die am EU-US Data Privacy Framework (EU-US DPF) teilnehmen.²⁹

Da es auch bei den verbleibenden Möglichkeiten (wie z. B. Standarddatenschutzklauseln) auf die Details ankommt, sollte bereits vor einer Übermittlung geprüft werden, welche Datenübermittlung konkret geplant ist (in welche Länder, welche Daten, welche Datenmengen, an welche Unternehmen etc.), und auf dieser Basis mit dem Datenschutzbeauftragten

²⁷ Ein Angemessenheitsbeschluss ist ein Beschluss, der von der Europäischen Kommission gemäß Art. 45 DSGVO angenommen wird und durch den festgelegt wird, dass ein Drittland oder eine internationale Organisation ein angemessenes Schutzniveau für personenbezogene Daten bietet. Ein solcher Beschluss bedeutet, dass personenbezogene Daten von den EU-Mitgliedstaaten und den Mitgliedstaaten des Europäischen Wirtschaftsraums ohne weitere Anforderungen an dieses Drittland übermittelt werden können. Die Liste der Angemessenheitsbeschlüsse der Europäischen Kommission ist hier veröffentlicht: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

²⁸ Für den Fall, dass kein Angemessenheitsbeschluss für die Übermittlung personenbezogener Daten in ein Drittland vorliegt, dürfen Verantwortliche oder Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern diese hierfür geeignete Garantien vorgesehen haben, Art. 46 Abs. 1 DSGVO. Als eine solche geeignete Garantie sieht Art. 46 Abs. 2 lit. b i. V. m. Art. 47 DSGVO ausdrücklich verbindliche interne Datenschutzvorschriften (sog. Binding Corporate Rules, kurz: BCR) vor.

²⁹ Am 10. Juli 2023 nahm die Europäische Kommission den Angemessenheitsbeschluss zum EU-US Data Privacy Framework an, der unmittelbar in Kraft getreten ist. Datenübermittlungen an Stellen in den USA, die nicht am EU-US DPF teilnehmen, müssen auf ein anderes Übermittlungsinstrument gemäß Kapitel V DSGVO gestützt werden.

und/oder der Rechtsabteilung die geeignete Rechtsgrundlage für die Datenübermittlung diskutiert, dokumentiert und vertraglich vereinbart werden.

Zum Datentransfer von anderen Ländern nach Deutschland/in die EU:

Es empfiehlt sich zu prüfen, ob andere Staaten (Datenschutz-)Regelungen erlassen haben, die den Datentransfer ins Ausland beschränken. Beispielsweise können Einwilligungen der Betroffenen erforderlich sein oder die Anmeldung bei der dortigen Datenschutzbehörde. Des Weiteren gibt es auch Staaten, die den Transfer ins Ausland zwar gestatten, aber die Erstspeicherung im Ursprungsland fordern.

Um negative Konsequenzen (z. B. Bußgelder, Marktsperren, Blacklisting) zu vermeiden, ist auch für diese Art des Datentransfers zu empfehlen, bereits vor der Übermittlung mit dem Datenschutzbeauftragten und/oder der Rechtsabteilung Rücksprache zu halten. Die Rechtsabteilung wird sich bei Bedarf ggf. vor Ort über eine lokale Rechtsberatung weitere Unterstützung einholen.

4 Rolle des Datenschutzbeauftragten

4.1 Stellung im Unternehmen

Die DSGVO sieht den betrieblichen Datenschutzbeauftragten (DSB) verpflichtend nur noch bei Behörden und öffentlichen Stellen (behördlicher DSB)³⁰ vor sowie bei Unternehmen, bei denen besonders risikoreiche Datenverarbeitungen erfolgen (Art. 37 DSGVO).³¹ Seit der Einführung der DSGVO müssen auch Auftragsverarbeiter einen DSB benennen, wenn sie die Voraussetzungen erfüllen.

Für Unternehmen ist dabei zu beachten:

- *Die Datenverarbeitung, die die Benennungspflicht auslöst, muss zur „Kerntätigkeit“ des Verantwortlichen bzw. Auftragsverarbeiters gehören.*
- *Die Tätigkeit muss bestimmte inhaltliche Voraussetzungen erfüllen, nämlich das Erfordernis einer umfangreichen regelmäßigen und systematischen Beobachtung von betroffenen Personen (Art. 37 Abs. 1 lit b DSGVO) oder die umfangreiche Verarbeitung von Daten im Sinne des Art. 37 Abs. 1 lit c DSGVO.*

In Deutschland hat der Gesetzgeber jedoch weitergehende Pflichten zur Benennung eines Datenschutzbeauftragten im BDSG verankert. Gemäß § 38 Abs. 1 Satz 1 BDSG³² ist – ergänzend zu den Vorgaben der DSGVO – ein DSB zu benennen, soweit in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Eine Person gilt als ständig beschäftigt, wenn sie die Aufgabe, die nicht ihre Hauptaufgabe zu sein braucht, regelmäßig wahrnimmt. Ohne Rücksicht auf die Anzahl der Personen ist ein DSB immer zu bestellen, soweit u. a. Verarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen (§ 38 Abs. 1 Satz 2 BDSG). Zudem ist die freiwillige Bestellung eines DSB immer möglich.

³⁰ Zwischen dem behördlichen und dem betrieblichen Datenschutzbeauftragten gibt es nur geringfügige Unterschiede. Die Voraussetzung für die Aufnahme der Tätigkeit als behördlicher DSB ist bei öffentlichen Stellen des Bundes und in allen Bundesländern, dass dieser die erforderliche Fachkunde und Zuverlässigkeit aufweist. Die Aufgaben des behördlichen DSB ergeben sich ebenfalls aus den jeweiligen Landesdatenschutzgesetzen.

³¹ Gemäß den Art. 37 ff DSGVO ist dies etwa in den Fällen vorgesehen, in welchen die Kerntätigkeit in der Verarbeitung personenbezogener Daten zum Zwecke der Überwachung erfolgt oder in der Verarbeitung besonderer Kategorien von Daten (z. B. Gesundheitsdaten) gemäß Art. 9 der Verordnung.

³² Die derzeitige Bundesregierung strebt im Rahmen von Maßnahmen zur Staatsmodernisierung die Aufhebung der Regelungen zur Benennung eines Datenschutzbeauftragten (§ 38 Abs. 1 BDSG) für nichtöffentliche Stellen an.

Der Verantwortliche hat sicherzustellen, dass der DSB ordnungsgemäß und frühzeitig in alle Datenschutzfragen eingebunden wird. Er ist mit den für die Erfüllung seiner Aufgaben erforderlichen Ressourcen, Zugängen zu personenbezogenen Daten und Verarbeitungsvorgängen auszustatten sowie bei der Erhaltung seines Fachwissens zu unterstützen.³³ Der Verantwortliche muss die Weisungsfreiheit des DSB bei der Erfüllung seiner Aufgaben sicherstellen. Der Aspekt der Unabhängigkeit bzw. Weisungsfreiheit des DSB ist auch in der DSGVO vorgeschrieben.³⁴

Der DSB kann grundsätzlich andere Aufgaben und Pflichten wahrnehmen, sofern diese nicht zu einem Interessenkonflikt führen.³⁵ Eine parallele Tätigkeit in der Internen Revision kann zwar grundsätzlich möglich sein, jedoch ist sicherzustellen, dass die jeweiligen Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen (Art. 38 Abs. 6 DSGVO und Standard 2.2 „Wahrung der Objektivität“ in den Global Internal Audit Standards). Hierfür ist z. B. eine klare Aufgabentrennung zwischen Tätigkeiten mit Revisionsbezug und Datenschutzaufgaben hilfreich.

Zur Funktion eines zentralen bzw. Konzerndatenschutzbeauftragten nimmt die DSGVO ebenfalls Stellung: Gemäß Art. 37 Abs. 2 DSGVO darf eine Unternehmensgruppe einen gemeinsamen DSB ernennen, sofern dieser von jeder Niederlassung aus leicht erreicht werden kann.³⁶

4.2 Aufgaben

Der DSB ist im Unternehmen Ansprechpartner für Geschäftsleitung und Beschäftigte für alle Fragen rund um das Thema Datenschutz. Die Aufgaben und Pflichten eines DSB sind in Art. 39 DSGVO geregelt und umfassen:

- Unterrichtung und Beratung der Verantwortlichen/Auftragsverarbeiter und der Beschäftigten hinsichtlich ihrer Datenschutzpflichten,
- Überwachung („monitor“) der Einhaltung der DSGVO, des BDSG und anderer Regelungen zum Datenschutz,

³³ Art. 38 Abs. 1 DSGVO.

³⁴ Art. 38 Abs. 3 DSGVO.

³⁵ Art. 38 Absatz 6 DSGVO verpflichtet den Verantwortlichen sicherzustellen, dass es zu keinem Interessenkonflikt mit anderen zu übernehmenden Aufgaben und Pflichten eines DSB kommt.

³⁶ Bei größeren Unternehmensgruppen bietet es sich an, insoweit nicht nur die Position des Konzerndatenschutzbeauftragten zu besetzen, sondern eine entsprechende Organisationsform vorzusehen und mit entsprechenden Kapazitäten auszustatten.

- Strategien („policies“) zum Datenschutz, insbesondere im Hinblick auf die Zuweisung von Zuständigkeiten, die Sensibilisierung und Schulung der Mitarbeiter sowie Überprüfungen („audits“) von Verarbeitungsvorgängen,
- Auf Anfrage Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung und
- Zusammenarbeit mit der Aufsichtsbehörde.

Grundsätzlich ist bei allen Prozessen der Internen Revision, bei denen personenbezogene Daten verarbeitet werden, an eine Abstimmung mit dem DSB zu denken. Darunter fallen u. a.:

- *Einführung eines neuen oder wesentliche Änderung(en) eines bestehenden IT-gestützten Revisionstools bzw. Anwendungen zur Unterstützung der Revisionsarbeit (Analysetools, Einsatz von KI-Tools etc.),*
- *Ablage, Archivierung und Löschung von Prüfungsdaten,*
- *Grundlegende Prozesse zum Prüfungsvorgehen (Datenanalysen, Einsatz von KI-Tools und temporäre Zugriffe auf Systeme etc.),*
- *Vorgehensweise bei internen Ermittlungen bzw. der Klärung von Verdachtsfällen,*
- *Einzelfragen bei Prüfungen.*

*Darüber hinaus kann der DSB bei der Umsetzung weiterer datenschutzrechtlicher Vorgaben **beraten**, z. B.:*

- *Konzeption rechtlicher Dokumente mit datenschutzrechtlichem Bezug, wie Betriebsvereinbarungen, interne Regelungen (z. B. zur privaten Internet- und E-Mail-Nutzung oder zum Umgang mit Betroffenenanfragen) oder eine allgemeine Datenschutzrichtlinie,*
- *Erstellung von Datenschutzerklärungen zur Erfüllung der Informationspflichten,*
- *Erstellung einer Datenschutz-Dokumentation zur Erfüllung der datenschutzrechtlichen Nachweis- und Rechenschaftspflichten,*
- *Durchführung einer Datenschutz-Folgenabschätzung durch den Verantwortlichen (bzw. den Prozessverantwortlichen),*
- *Erstellung des Verzeichnisses der Verarbeitungstätigkeiten,*
- *Datenschutzvorfälle und Betroffenenanfragen,*
- *datenschutzrechtliche Mitarbeitersensibilisierungen/-schulungen,*
- *Mitwirkung bei Mitarbeiterkontrollen.*

4.3 Der internationale Kontext

Die DSGVO gibt den EU-Mitgliedstaaten die Möglichkeit, nationale Sonderregelungen hinsichtlich der Bestellung eines DSB zu schaffen. Daher sind bei internationalen Bezügen ergänzend zur DSGVO stets die lokalen Vorgaben hinsichtlich der Bestellpflicht eines DSB („Data Protection Officer“) zu beachten.

In Unternehmen mit Sitz oder Niederlassungen sowohl innerhalb als auch außerhalb der EU empfiehlt es sich grundsätzlich, auf lokale Ansprechpartner zurückzugreifen. Dabei fordert die DSGVO, dass eine leichte Erreichbarkeit des DSB für Datenschutzbehörden, externe Betroffene und Beschäftigte gewährleistet wird.

5 Umsetzung des Datenschutzes in der Internen Revision

5.1 Grundlegende Festlegungen

Die Interne Revision hat als Prozessverantwortliche klare Regelungen zum Umgang mit personenbezogenen Daten festzulegen. Dabei ist darauf zu achten, dass sowohl die abteilungsinternen Prozesse als auch das Prüfungsvorgehen datenschutzfreundlich bzw. -konform gestaltet werden. Die Anforderungen an eine datenschutzkonforme Gestaltung der Prozesse sind mit der Einführung der DSGVO gestiegen. Die DSGVO formuliert das Prinzip von Privacy by Design/Default³⁷ erstmals direkt im Gesetzestext. Ziel von Artikel 25 DSGVO ist es, Systeme und Dienste von Anfang an über den gesamten Lebenszyklus datensparsam und mit möglichst datenschutzfreundlichen Voreinstellungen zu gestalten.

Die Beschäftigten der Internen Revision sollten über die Regelungen zum Umgang mit personenbezogenen Daten regelmäßig unterwiesen und sensibilisiert werden. Es empfiehlt sich – je nach Intensität der Befassung bzw. Verarbeitung personenbezogener Daten durch die Interne Revision – eine Anpassung des Schulungszyklus und die regelmäßige Evaluation der Schulungsinhalte.

Außerdem verlangt die DSGVO mit der Rechenschaftspflicht eine hinreichende Dokumentation, aus der hervorgeht, dass die Anforderungen des Datenschutzes auch tatsächlich identifiziert und wirksam umgesetzt wurden.

5.2 Einsatz von IT-Systemen in der Revision

Die von der Internen Revision eingesetzten IT-Systeme für die Planung, Steuerung, Durchführung und Dokumentation von Prüfungen oder Programme (z. B. Analysetools) unterliegen den Datenschutzanforderungen einschließlich der Beachtung der nach Art. 32 Abs. 1 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Ebenso hat sie

³⁷ Der Begriff Privacy by Design beschreibt „Datenschutz durch Technikgestaltung“. Bereits in der Entwicklungs- und Umsetzungsphase der einzusetzenden Techniken soll sichergestellt werden, dass der Datenschutz und die Privatsphäre durch bewusste Gestaltung der Technik gewährleistet werden. Privacy by Default bezeichnet datenschutzfreundliche Voreinstellungen aus Nutzersicht.

sicherzustellen, dass diese datenschutz- und informationssicher gestaltet werden und angemessen kontrolliert eingesetzt werden. Dies steht im Einklang mit den berufsständischen Anforderungen von Standard 10.3 „Technologische Ressourcen“ der Global Internal Audit Standards.

Die Anforderungen sind bereits frühzeitig bei der Auswahl und Anwendung geeigneter IT-Systeme für die Revision zu berücksichtigen, einerseits bei den allgemeinen IT-Systemen (z. B. Kollaborationstools, Revisionssoftware) und andererseits bei den spezifischen IT-Systeme für Datenanalyse (Data Mining, KI-basierte Datenanalyse etc.).

Beim Einsatz KI-unterstützter IT-Systeme gilt es zudem, die internen und externen Anforderungen für den Einsatz und die Nutzung von KI-Systemen zu berücksichtigen. Änderungen an KI-Systemen können weitreichende Anbieterpflichten nach KI-Verordnung nach sich ziehen.

Die IT-Systeme der Revision unterliegen der Überwachung der ordnungsgemäßen Anwendung durch den DSB.³⁸ Sie sind in das Verzeichnis (Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO) aufzunehmen und dem DSB frühzeitig zur Kenntnis zu bringen. Bei der Dokumentation für das Verzeichnis sind Detailkenntnisse über das verwendete IT-System oder die eingesetzten Programme unabdingbar. Deshalb bedarf es einer gut funktionierenden Kommunikation zwischen Interner Revision und DSB, um die Beschreibung der Verarbeitungen von personenbezogenen Daten zu erstellen und aktuell halten zu können.

5.3 Schutzbedarfsermittlung

Nach der DSGVO ist zur Bestimmung der erforderlichen Sicherheitsmaßnahmen zunächst der Schutzbedarf festzustellen. Daraufhin sind die Risiken zu bewerten, verhältnismäßige Maßnahmen zu ergreifen und Nachweise zu erbringen. Damit unterstellt die Verordnung im Grundsatz, dass im Unternehmen ein IT-Sicherheitsmanagement umgesetzt ist.³⁹ Das Schutzkonzept der DSGVO setzt damit verstärkt auf das Zusammenwirken von Datenschutz- und Informationssicherheit im Unternehmen.

³⁸ Werden dabei personenbezogene Daten von Mitarbeitern der Internen Revision (beispielsweise die Zuordnung zu Prüfungen, die Erfassung, Verwaltung und Verrechnung von Aufwänden) verarbeitet, so stützt sich die Zulässigkeit dieser Verarbeitung auf § 26 Abs. 1 BDSG (vgl. 2.3).

³⁹ Vgl. Gola/Jaspers/Müthlein Schwartmann „Datenschutz-Grundverordnung im Überblick“, 1. Aufl. 2017, S. 58.

Nach Maßgabe der DSGVO müssen regelmäßig nur solche technischen und organisatorischen Maßnahmen umgesetzt werden, die verhältnismäßig sind. Artikel 32 DSGVO gibt vor, welche Aspekte bei der Prüfung der Verhältnismäßigkeit – jeweils anhand der konkreten Umstände des Einzelfalls – zu berücksichtigen sind, u. a. Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere von Datenschutzrisiken.

Art. 32 DSGVO schreibt folgende Maßnahmen für die Sicherheit der Verarbeitung vor:

- Pseudonymisierung und Verschlüsselung von personenbezogenen Daten,
- Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste,
- rasche Wiederherstellung der Daten und Zugänge nach einem physischen oder technischen Zwischenfall,
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Welche Maßnahmen konkret erforderlich sind, kann der Verantwortliche in Anlehnung an anerkannte Sicherheitsmaßnahmenkataloge – wie z. B. dem BSI-Grundschutz, der ISO 27001 oder dem Standard-Datenschutzmodell – prüfen.⁴⁰

Ergänzend kann der detaillierte Katalog des § 64 Abs. 3 BDSG⁴¹ als Orientierungshilfe für die Anforderungen an die technischen und organisatorischen Maßnahmen dienen, da diese Vorgaben konkreter als in Art. 32 DSGVO formuliert sind. Zu den darin genannten diversen Datenschutzkontrollen gehören u. a.:

- Kontrollen zur Gewährleistung der Datenintegrität, Zuverlässigkeit und Wiederherstellbarkeit, Verfügbarkeit oder Trennung zu unterschiedlichen Zwecken,
- Zugangs- und Zugriffskontrolle, Transport- und Übertragungskontrolle, Datenträger-, Speicher- und Benutzerkontrolle.

Ein wesentlicher Aspekt von Art. 32 DSGVO ist die Nachweisbarkeit der ergriffenen technischen und organisatorischen Maßnahmen. Der Verantwortliche muss dafür in der Lage sein, schlüssig und mit geeigneter Dokumentation nachzuweisen, dass er die erforderlichen Schutzmaßnahmen gemessen an dem Schutzbedarf der zu verarbeitenden Daten ergriffen hat und diese auch angemessen umgesetzt sind. In der Praxis bestehen häufig

⁴⁰ Mantz, in: Sydow, DSGVO, 2. Aufl. 2018, Art. 32 DSGVO Rn. 36.

⁴¹ § 64 BDSG („Anforderungen an die Sicherheit der Datenverarbeitung“) ist als Bestandteil des Teil 3 des BDSG grundsätzlich nur für die Verarbeitung von personenbezogenen Daten durch öffentliche Stellen gültig. Die enthaltene Übersicht mit der Beschreibung der einzelnen Kontrollen (insgesamt 14) kann aber anderen Verantwortlichen beispielhaft als Anhaltspunkt dienen.

Synergien zu anderen Nachweispflichten. So sind im Kontext des Informationssicherheitsmanagements bereits Umsetzungsnachweise von Schutzmaßnahmen zu erstellen und laufend zu aktualisieren. Darauf kann, soweit möglich, auch für die Nachweisführung gemäß Art. 32 DSGVO zurückgegriffen werden.

Die Interne Revision hat sicherzustellen, dass Prüfungsinformationen angemessen vor unbefugtem Zugriff, Verlust oder unzulässiger Offenlegung geschützt werden. Dies entspricht sowohl den datenschutzrechtlichen Anforderungen (insb. Art. 32 DSGVO) als auch den berufsständischen Anforderungen gemäß GIAS 5.2 (Schutz vor Informationen).

5.4 Prüfungsauftrag und Prüfungsvorbereitung

Bereits bei der Erstellung des Prüfungsauftrags sollte darauf geachtet werden, datenschutzrelevante Inhalte in den Punkten Prüfungsumfang, Risiken und Prüfungsvorgehen zu konkretisieren. Je nach konkretem Prüfungsauftrag kann sich eine Abstimmung mit dem DSB anbieten. Dabei sollte der Fokus nicht auf klassische Personalprüfungen beschränkt sein, sondern die Gesamtheit der Prüfungen einschließen. Der DSB ist der Internen Revision gegenüber weder weisungsabhängig noch weisungsbefugt, kann aber auf die datenschutzkonforme Prüfungsumsetzung Einfluss nehmen und ggf. beratend unterstützen.

Aus dem Prüfungsauftrag sollte sich daher ergeben, ob Schwerpunkt der Prüfung z. B. Geschäftsprozesse sind oder ob personenbezogene Daten im Fokus stehen. Dies ist insbesondere ausschlaggebend für die datenschutzrechtlichen Abwägungen.

Für Prüfungen, die schwerpunktmäßig personenbezogene Daten enthalten, wird empfohlen, im Prüfungsauftrag u.a. die folgenden Aspekte festzuhalten und ggfs. im Prüfungsverlauf zu ergänzen:

- *für welches Prüfungsziel die Daten verwendet werden,*
- *welche aktuellen und prüfungsspezifischen Risiken (inkl. Informationssicherheitsrisiken) im Rahmen der Prüfung für personenbezogene Daten bestehen und welche Risiken geprüft werden sollen,*
- *welche Daten einbezogen werden (z. B. besonders sensible Daten, wie Gesundheits- oder Gehaltsdaten),*
- *in welchen IT-Systemen Daten zu Prüfungszwecken verarbeitet werden und welche Systemzugriffe notwendig sind (bei besonders sensiblen Daten hinsichtlich Zeitraums und Personenkreis eingeschränkt),*

- *ob sich der geplante Zweck, insbesondere die Prüfung der Risiken, nur mit den zu verwendenden Daten erfüllen lässt (Geeignetheit und Erforderlichkeit),*
- *welche alternativen Vorgehensweisen ggf. bestehen, durch die die Betroffenen in ihren Persönlichkeitsrechten weniger belastet werden (Angemessenheit),*
- *ob besondere, schutzwürdige Interessen von Betroffenen bestehen, die das Interesse an der Durchführung der Prüfungshandlung überwiegen (Verhältnismäßigkeit),*
- *ggf. welche gesetzlichen Grundlagen und internen Richtlinien zu beachten sind,*
- *ggf. Dokumentation der Abstimmung mit dem Betriebsrat,*
- *ggf. Abweichungen vom geplanten/freigegebenen Prüfungsumfang.*

Unter Berücksichtigung der Erkenntnisse und eventuell getroffener Modifikationen aus der Prüfung der einzelnen Kriterien findet eine Interessenabwägung statt.

In Einzelfällen kann es notwendig sein, für spezielle Überprüfungen oder Auswertungen externe Dienstleister zu beauftragen. Hat der Dienstleister im Zuge dieses Auftrages die Möglichkeit des Zugriffs auf bzw. der Einsicht in personenbezogene Daten, sind die Vorgaben zur Auftragsverarbeitung (Art. 28 DSGVO) zu berücksichtigen. Die Beauftragung sollte sich nur auf externe Dienstleister beschränken, die hinreichende Garantien bieten, dass geeignete technische und organisatorische Maßnahmen vorhanden sind, so dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der Betroffenen gewährleistet. Eine wesentliche Änderung durch die DSGVO bei der Auftragsverarbeitung ist, dass auch die Auftragsverarbeiter für die Einhaltung der technischen und organisatorischen Maßnahmen verantwortlich sind.

Für gesellschaftsübergreifende Zugriffe oder Anforderungen von Daten sollte mit den zu prüfenden Gesellschaften die Verwendung personenbezogener Daten schriftlich oder in anders geeigneter Form (z. B. elektronischer Workflow) vereinbart werden. In der Praxis kann darauf bereits im Zuge der Prüfungsankündigung mit der jeweiligen Gesellschaft hingewiesen werden. Die zu prüfende Gesellschaft sollte die Möglichkeit bekommen, in einem angemessenen Zeitraum zu prüfen, ob entsprechende Vereinbarungen zu Datenflüssen oder Auftragsverarbeitungen zwischen den Gesellschaften bestehen oder ob dem lokale bzw. länderspezifische Regelungen entgegenstehen.

5.5 Prüfungsdurchführung

Die Prüfungsdurchführung hat sich gemäß der im Prüfungsauftrag festgelegten Umfänge bzw. der in den internen Richtlinien des Unternehmens oder der Abteilung vorgegebenen

technischen und organisatorischen Maßnahmen zu bewegen. Sollte eine Erweiterung des Prüfungsumfanges, ggf. auch erst im Prüfungsverlauf, in Bezug auf personenbezogene Daten notwendig sein, sind entsprechende Maßnahmen einzuleiten (s. Prüfungsvorbereitung).

Nach dem Grundsatz der Datensparsamkeit sind dabei so wenig wie möglich personenbezogene Daten zu verarbeiten oder, falls möglich, außen vor zu lassen. Insbesondere sind diese zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

*Bei der **Anonymisierung** werden personenbezogene Daten so verändert, dass sie nicht mehr einer Person zugeordnet werden können. Hingegen sind bei **pseudonymisierten** Daten (z. B. durch Zahlen- oder Buchstabenkombinationen) weiterhin Rückschlüsse auf die Betroffenen möglich. Die Anonymisierung ist in der betrieblichen Praxis häufig schwer umzusetzen.*

Wenn die Pseudonymisierung von der Internen Revision als datennutzender Stelle selbst durchgeführt wird, ist ein Rückschluss auf die Ursprungsdaten jederzeit möglich. Dadurch kann auch bei großen Datensammlungen trotz erfolgter Pseudonymisierung die Identifikation einer bestimmten Person erfolgen. Um keine Rückschlüsse zuzulassen, müssten die Daten gegebenenfalls getrennt oder verändert werden. Insbesondere sind bei kleineren Organisationseinheiten (in der Regel mit weniger als fünf Beschäftigten) unter Umständen ebenfalls Rückschlüsse auf einzelne Personen möglich. Bei kleineren Gesellschaften oder Organisationseinheiten ist daher im Einzelfall abzuwägen, ob derartige Rückschlüsse möglich sind.

Erhält man trotz entsprechender Anforderung der Internen Revision die Daten von den Fachabteilungen nicht anonymisiert oder pseudonymisiert, so ist zu überlegen, dies innerhalb der Revisionsabteilung nachzuholen, bspw. organisatorisch getrennt vom Prüfungsteam im Backoffice.

Werden im Verlauf der Prüfung potenzielle Verstöße gegen die DSGVO festgestellt, ist der DSB zügig zu kontaktieren und es sind gegebenenfalls Ad-hoc-Maßnahmen zu ergreifen. Verletzungen des Schutzes personenbezogener Daten führen gemäß Art. 33 DSGVO Abs. 1 zu einer Meldepflicht bei der zuständigen Aufsichtsbehörde, wenn diese zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen. Auf Basis der Beurteilung dieser Risiken ist mit dem DSB eine Meldung des Sachverhaltes bei der zuständigen Aufsichtsbehörde abzustimmen. Im Rahmen eines im Unternehmen etablierten Meldeprozesses sind hierbei insbesondere Meldefristen, Meldewege und formale Aspekte zu beachten.

5.6 Dokumentation der Prüfungsergebnisse (Berichterstattung)

Das Ergebnis einer durchgeführten Prüfung wird im Regelfall im Prüfungsbericht dokumentiert. Er enthält Feststellungen aus den Prüfungshandlungen, Risikoeinschätzungen sowie Maßnahmen bzw. Empfehlungen zur Verringerung oder Beseitigung der aufgezeigten Risiken. Die Berichte der Internen Revision unterliegen dem Vertraulichkeitsgebot. Bei Bedarf ist ein besonderer Vertraulichkeitsgrad zu definieren.

Der geeignete Umgang mit vertraulichen Prüfungsergebnissen bzw. Berichten ist innerhalb der Internen Revision zu kommunizieren und ggf. auch an weitere beteiligte Beschäftigte oder Dienstleister, z. B. Wirtschaftsprüfer, Berater oder IT-Dienstleister. Dabei ist an die Unterzeichnung einer Vertraulichkeitserklärung zu denken, insbesondere bei Externen.⁴²

Art und Umfang der Berichtsverteilung sollten durch die Leitung der Internen Revision, ggf. in Abstimmung mit der Unternehmensleitung, festgelegt werden. Ebenso verhält es sich mit einer Weitergabe außerhalb des Berichtsverteilers.

Grundsätzlich werden Feststellungen und Maßnahmen bzw. Empfehlungen nicht konkreten Personen, sondern Abteilungen oder Bereichen zugewiesen. Zusätzlich kann z. B. in kleineren Unternehmen oder Einheiten leichter ein Bezug zu konkreten Personen hergestellt werden. Deshalb sind durchgängig geeignete Schutzmaßnahmen einzuhalten, z. B. E-Mail-Verschlüsselung bei Berichtsversand und Zugangskontrolle für Berichte.

Die Ergebnisse einer Follow-up Prüfung und die dazugehörigen Ergebnisse sind wie Prüfungsberichte zu behandeln.

5.7 Dokumentation und Archivierung von Prüfungsdaten

Bei der Dokumentation und Archivierung von Prüfungsdaten (z. B. Dokumente und E-Mails) sind datenschutzrelevante Vorgaben aus verschiedenen Gesetzen zu beachten. Grundsätzlich gilt bei datenschutzrechtlichen Vorgaben das Subsidiaritätsprinzip, welches spezielleren Rechtsvorschriften Vorrang gibt.⁴³

⁴² Hierbei ist zu beachten, dass eine solche Vertraulichkeitserklärung nicht die Grundlage für eine zulässige Verarbeitung der Daten durch Dritte darstellt, jedoch eine hierfür notwendige organisatorische Maßnahme sein kann.

⁴³ Vorrangige Rechtsvorschriften bezüglich der Archivierung sind beispielsweise (ohne Anspruch auf Vollständigkeit): Handelsrecht: §§ 257, 261 HGB und Grundsätze ordnungsmäßiger Buchführung

Bei der Dokumentation und Archivierung von personenbezogenen Daten gilt, dass diese unter Beachtung der Grundprinzipien der DSGVO gespeichert werden müssen. Hierbei sind besonders die Prinzipien der Zweckbindung und Datenminimierung in die Abwägung einzubeziehen. Das heißt u. a. auch, dass der Personenbezug, soweit er nicht erforderlich ist, gelöscht wird bzw. die Daten anonymisiert oder pseudonymisiert werden (siehe Kapitel 5.5). Hierfür ist ein Löschkonzept erforderlich.

Darüber hinaus bedeutet das Prinzip der Datenminimierung auch, dass Daten, die nicht mehr gebraucht werden bzw. nach Ablauf der gesetzlichen Fristen nicht mehr aufbewahrt werden müssen, zu sperren bzw. zu löschen sind. Ein wichtiger Anhaltspunkt kann dabei die Frage sein, ob die Informationen und Daten mit Personenbezug weiterhin als Nachweis der Prüfungsergebnisse benötigt werden. Gegebenenfalls sind die Unterlagen auch leicht aus den Primärsystemen reproduzierbar. Insbesondere bei Dokumenten zu klassischen Prozess- bzw. sachfragenorientierten Prüfungen ist zu untersuchen, ob innerhalb der Dokumentation und Archivierung tatsächlich personenbezogene Daten erforderlich sind.

(GoB); Grundsatz des Institutes der Deutschen Wirtschaftsprüfer (IDW) RS FAIT 3 (Grundsätze ordnungsgemäßer Buchführung beim Einsatz elektronischer Archivierungsverfahren), Steuerrecht: §§ 146, 147, 200 AO, Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), § 14b Absatz 1 Satz 2 UStG, Abschnitt 14b.1. Umsatzsteuer-Anwendungserlass (UStAE) und diverse BMF-Schreiben, Zivilrecht (insbesondere im Hinblick auf Gerichtsverwertbarkeit): §§ 415 ff. ZPO.

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.diir.de,
überarbeitet im August 2021, (Version 2.0) und
aktualisiert im April 2026 (Version 3.0).

Version 3.0