Leitfaden Interne Revision und Datenschutz

DIIR-Arbeitskreis Interne Revision & Datenschutz

Version 2.0, August 2021

DIIR Deutsches Institut für Interne Revision e.V.

Inhalt

Vorwort

Spätestens mit Inkrafttreten der EU-Datenschutz-Grundverordnung (DS-GVO) 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) sowie die gesteigerten Rechenschaftspflichten haben dazu geführt, dass entsprechende Datenschutzmanagementsysteme in den Unternehmen und im öffentlichen Sektor implementiert wurden.

Parallel zur erhöhten Regulierung durch die DS-GVO führen die Digitalisierungsstrategien der Unternehmen und Behörden dazu, dass deutlich mehr Arbeitsbereiche und Prozesse durch IT unterstützt werden, auch in der Internen Revision.

Cloud Sicherheit, Home-Office-Szenarien, die Auswahl von IT-Dienstleistern unter Gesichtspunkten des Datenschutzes (z. B. Datenverarbeitung im EU-Ausland) sind inzwischen Kernfragen im betrieblichen Datenschutz. Immer hybridere IT-Landschaften und steigende Cyberrisiken erhöhen unmittelbar auch das Datenschutzrisiko einer Organisation. Die geänderte Ausganglage erfordert eine klare Datenschutzstrategie, einen wirksamen Datenschutzprozess sowie dessen Überwachung.

Der DIIR-Arbeitskreis Interne Revision & Datenschutz bietet im Folgenden einen Leitfaden zu den Grundfragen des Datenschutzes im Kontext der Internen Revision und zur Gestaltung der entsprechenden Struktur und Prozessabläufe an.

Dieser Leitfaden wurde nach aktuellem Stand sowie bestem Wissen und Gewissen im November 2017 erstellt und im August 2021 aktualisiert. Zusätzlich wurde das Kapitel 2.5 neu aufgenommen. 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, indem Verarbeitungsregeln für personenbezogene Daten und über die Gestaltung und den Einsatz von Informationstechnik (IT) aufgestellt werden. Rechtlich ist der Datenschutz in einem komplexen Zusammenspiel verschiedener Vorschriften geregelt. Für Unternehmen ergeben sich daraus datenschutzrechtliche Pflichten, die seit dem Inkrafttreten der Datenschutzgrundverordnung (DS-GVO) am 25. Mai 2018 verschärft wurden. Die DS-GVO regelt auf europäischer Ebene den Umgang mit personenbezogenen Daten einheitlich und harmonisiert die datenschutzrechtlichen Rahmenbedingungen europaweit. Die in der Verordnung enthaltenen Öffnungsklauseln 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), Vorgaben aus der Landesgesetzgebung[1] und zusätzliche spezialgesetzliche Regelungen,[2] weiterhin von Relevanz.

Zusammenfassend lässt sich festhalten, dass die Rechtmäßigkeit der Verarbeitung personenbezogener Daten wegen ihres Anwendungsvorrangs zuerst nach der DS-GVO 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 abschießend, gilt ergänzend das BDSG. Bereichsspezifische Regelungen finden sich beispielsweise in den Büchern des Sozialgesetzbuchs, im BSI-Gesetz oder in der Abgabenordnung. Diese und viele weitere bereichsspezifischen Regelungen gehen dem BDSG – nicht aber der DS-GVO – vor.

[1] Die Landesdatenschutzgesetze gelten für die jeweiligen Landesbehörden und andere öffentlich-rechtliche Einrichtungen im Landes- und Kommunalbereich, gegebenenfalls ergänzend zu spezialgesetzlichen Regelungen.
[2] Diese Sondervorschriften sind auf die Anforderungen der jeweiligen Bereiche angepasst und gehen grundsätzlich den allgemeineren Regeln vor. Für die Revisionsarbeit in den folgenden Sektoren sind beispielhaft zu nennen und zu beachten: Sozialdatenverarbeiter: § 67 ff. SGB X, Telekommunikationsanbieter: § 91 ff. TKG, Telemedienanbieter: § 11 ff. TMG, Konfessionelle Einrichtungen: Kirchliche Datenschutzordnung (kath.) und Datenschutzgesetz der Evangelischen Kirche Deutschland.

Um eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen, veröffentlicht die Datenschutzkonferenz (DSK)[3] regelmäßig u. a. Orientierungshilfen, Standardisierungen und Stellungnahmen. Diese können Hilfestellung bei der praktischen Umsetzung der Vorgaben geben.[4] Weitere Rechtsquellen sind auch die Stellungnahmen des Europäischen Datenschutzausschusses (EDSA), der gemäß Art. 70 DS-GVO die einheitliche Anwendung der DS-GVO sicherstellen soll.[5]

Der Leitfaden wird sich im Schwerpunkt auf die für die Prüfungstätigkeit der Internen Revision einschlägigen Regelungen der DS-GVO 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.[6]

1.2 Grundprinzipien der DS-GVO

Der Umgang mit personenbezogenen Daten muss gemäß DS-GVO einigen grundsätzlichen Kriterien entsprechen:[7]

- 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«),
- sachliche Richtigkeit und sofern dies im Hinblick auf die Verarbeitungszwecke nicht der Fall ist, angemessene Maßnahmen zur Korrektur oder Löschung (»Richtigkeit«),

---

[3] Die DSK besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder.
[4] https://www.datenschutzkonferenz-online.de/index.html.
[5] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.
[6] 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.
[7] Die Grundsätze sind in Artikel 5 DS-GVO aufgeführt und werden im Erwägungsgrund 39 erläutert.

- 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«).

Der Verantwortliche[8] ist für die Beachtung dieser Grundbedingungen bei jeder Datenverarbeitung verantwortlich und muss deren Einhaltung, in der Regel anhand einer entsprechenden Dokumentation, nachweisen können (sog. Rechenschaftspflicht oder „Accountability“).[9] Das legt nahe, dass im Unternehmen ein Datenschutz-Managementsystem etabliert sein sollte, das die Einhaltung der Schutzziele der DS-GVO gewährleistet.

[8] Begriff „Controller“ (Verantwortlicher) in Art. 4 Nr. 7 DS-GVO.
[9] Art. 5 Abs. 2 DS-GVO.

2 Bedeutung des Datenschutzes für die Interne Revision

2.1 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 werden.[10] Prüfungshandlungen der Internen Revision sind daher regelmäßig mit der Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten und teilweise Dritten (z. B. Geschäftspartnern oder Kunden) verbunden. Es werden Unterlagen und Daten (u. a. Dokumente, Dateien, E-Mails) aus unternehmenseigenen Systemen eingesehen, ausgewertet und zusammengeführt.

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 eine Zweckbestimmung in datenschutzrechtlicher Hinsicht begründen. Die Interne Revision verfügt über ein grundsätzlich uneingeschränktes Informationsrecht.[11] Sie darf die zur Wahrnehmung ihrer Aufgaben notwendigen Informationen einholen und dafür auch Daten einsehen und auswerten, wobei sie sich an die entsprechenden Datenschutzvorgaben zu halten hat.

Ein Grundsatz der DS-GVO ist die rechtmäßige Verarbeitung personenbezogener Daten: Es muss immer eine Rechtsgrundlage zu deren Legitimation vorliegen. Artikel 6 DS-GVO listet die regelmäßig geltenden Erlaubnistatbestände auf. So kann sich - neben der Einwilligung der betroffenen Person - die Zulässigkeit unter anderem ergeben aus:

---

[10] Vgl. weiterführend DIIR: „Datenauswertungen und personenbezogene Datenanalyse“, http://www.diir.de/fileadmin/fachwissen/downloads/09DIIRDatenanalyseWeb.pdf.
[11] DIIR Revisionsstandard Nr. 3, S. 39, Mindeststandard 2 (Stand: April 2017).

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

Die Zulässigkeit der Verarbeitung und Nutzung der Daten im Rahmen der Kontroll- und Überwachungstätigkeit der Internen Revision[12] ergibt sich im Regelfall aus Art. 6 Abs. 1 lit. f DS-GVO (Wahrung berechtigter Interessen).

> *Art. 6 Abs. 1 lit. f DS-GVO 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 (vgl. dazu Kapitel 3).*
>
> *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 DS-GVO aufgeführten Zulässigkeit einer Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung sind vorrangige Rechtsvorschriften gemeint, die zur Verarbeitung der betroffenen Daten verpflichten.[13] Die mittelbare Ableitung einer rechtlichen Verpflichtung der Internen Revision, z. B. über § 91 Abs. 3 AktG, ist hier nicht gemeint.*

Die DS-GVO 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).[14] Bezogen auf die Tätigkeit der Internen Revision findet die DS-GVO immer Anwendung, wenn die Revisionsabteilung in der Europäischen Union niedergelassen ist, unabhängig davon, ob die Verarbeitung der Daten in der Europäischen Union stattfindet.

---

[12] Prüfrecht der Internen Revision abgeleitet aus §§ 93, 116 i. V. m. §§ 91, 107 AktG sowie § 130 i. V. m. § 30 OwiG.
[13] Vgl. Erwägungsgrund 45 DS-GVO.
[14] Art. 3 Abs. 2 DS-GVO.

2.2 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. 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.[15]

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 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 4.3)

2.3 Beschäftigtendaten in der Prüfung

Die DS-GVO enthält keine spezifischen Erlaubnistatbestände für die Verarbeitung von Beschäftigtendaten. Der Beschäftigtendatenschutz gehört zu den Abschnitten der DS-GVO, die eine nationale Regelung bzw. Präzisierung vorsehen. Spezielle Vorschriften für den Datenschutz im Beschäftigungsverhältnis können durch Rechtsvorschriften oder durch Kollektivvereinbarungen ausgestaltet werden (Art. 88 DS-GVO bzw. auch § 26 Abs. 4 BDSG). Damit kann die Datenverarbeitung im Beschäftigungskontext – wie auch schon vor der Einführung der DS-GVO - auf Tarifverträge und Betriebs- oder Dienstvereinbarungen gestützt werden.[16]

---

[15] Art. 4 Ziffer 1 DS-GVO.

[16] Perspektivisch ist ein Gesetz zur Regelung des Beschäftigtendatenschutzes zu erwarten. Gemäß Art. 88 DS-GVO können die Mitgliedsstaaten „spezifischere Vorschriften“ zum Beschäftigtendatenschutz erlassen, d. h. konkretere Regelungen, die spezifisch auf den Datenschutz am Arbeitsplatz zugeschnitten sind. Der interdisziplinäre Beirat Beschäftigtendatenschutz hat am 16. Juni 2020

Im Beschäftigungsverhältnis haben zunächst die allgemeinen Erlaubnistatbestände der DS-GVO Geltung. 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 DS-GVO (Erfüllung eines Vertragsverhältnisses). Die Verarbeitung von Gesundheitsdaten im Beschäftigungsverhältnis richtet sich nach Art. 9 DS-GVO, der die Verarbeitung von besonderen (sensitiven) 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 DS-GVO in Betracht.

Im BDSG ist § 26 für die Datenverarbeitung im Beschäftigungskontext maßgeblich. Die Vorschrift konkretisiert und ergänzt die Vorgaben der DS-GVO, verdrängt die vorrangigen Regelungen der DS-GVO 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 stehenden gleich effektiven Mittel ist (Erforderlichkeit) und schutzwürdige Interessen der Beschäftigten nicht überwiegen. Zur weiteren Ausgestaltung vgl. auch Kapitel 4.

2.4 Unternehmensinterne Ermittlungen

Interne Untersuchungen anlässlich möglicher doloser Handlungen[17] unterscheiden sich von klassischen prozessualen bzw. sachfragenorientierten Prüfungen vor allem dadurch,

---

seine Arbeit unter der Führung des Bundesministeriums für Arbeit und Soziales aufgenommen und soll Perspektiven für einen zukunftsweisenden Beschäftigtendatenschutz erarbeiten. Ein Abschlussbericht mit konkreten Handlungsempfehlungen lag im Juni 2021 noch nicht vor.

[17] 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.

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. Dies zeigt sich insbesondere in der Einbeziehung des Datenschutzbeauftragten, des Betriebsrates sowie ggf. Rechtsabteilung und den besonderen Dokumentationspflichten.

Die datenschutzrechtlichen Anforderungen bei internen Sachverhaltsaufklärungen bzw. internen Ermittlungen ergeben sich vor allem aus der DS-GVO, dem BDSG und der Rechtsprechung des Bundesarbeitsgerichts (BAG).

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
- 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 DS-GVO 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.*
> *In der Fachliteratur wird die Notwendigkeit einer vorherigen Datenschutz-Folgenab-*

schätzungen nach Art. 35 DS-GVO diskutiert. Teilweise wird sie wegen der Einschätzung interner Untersuchungsmaßnahmen als „voraussichtlich hohes Risiko" für die Rechte von Betroffenen empfohlen.[18]

2.5 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 DS-GVO einschlägig sein können, sondern auch gesetzliche Regelungen anderer Länder.

Zum Datentransfer aus Deutschland/der EU in Drittländer:

Die DS-GVO regelt, dass personenbezogene Daten aus EU-Staaten nur unter bestimmten Voraussetzungen in Drittländer gesendet werden dürfen. Darunter fallen vor allem:

- Angemessenheitsbeschluss für das betreffende Drittland
  (also die Festlegung der Europäischen Kommission, dass Länder, wie z. B. Japan, Schweiz, Kanada - und seit 28. Juni 2021 auch Großbritannien für zunächst 4 Jahre - , ein angemessenes Schutzniveau für personenbezogene Daten bieten)[19]
- 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 einer Unternehmensgruppe)[20]

---

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

[19] Ein Angemessenheitsbeschluss ist ein Beschluss, der von der Europäischen Kommission gemäß Art. 45 DS-GVO 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.

[20] 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 DS-GVO. Als eine solche geeignete Garantie

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, scheidet diese Möglichkeit inzwischen aus.

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 Datenschutzbeauftragen 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, Marktsperrungen, Blacklisting) zu vermeiden, ist auch für diese Art des Datentransfers zu empfehlen, bereits vor der Übermittlung mit dem Datenschutzbeauftragen und/oder der Rechtsabteilung Rücksprache zu halten. Die Rechtsabteilung wird sich bei Bedarf ggf. vor Ort über eine lokale Rechtsberatung weitere Unterstützung einholen.

---

sieht Art. 46 Abs. 2 lit. b i. V. m. Art. 47 DS-GVO ausdrücklich verbindliche interne Datenschutzvorschriften (sog. Binding Corporate Rules, kurz: BCR) vor.

3 Rolle des Datenschutzbeauftragten

3.1 Stellung im Unternehmen

Die DS-GVO sieht den betrieblichen Datenschutzbeauftragten (DSB) verpflichtend nur noch bei Behörden oder öffentlichen Stellen vor sowie bei Unternehmen, bei denen besonders risikoreiche Datenverarbeitungen erfolgen (Art. 37 DS-GVO).[21] Seit der Einführung der DS-GVO 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 DS-GVO) oder die umfangreiche Verarbeitung von Daten im Sinne des Art. 37 Abs. 1 lit c DS-GVO.*

In Deutschland hat der Gesetzgeber jedoch weitergehende Pflichten zur Benennung eines Datenschutzbeauftragten im BDSG verankert. Gemäß § 38 Abs. 1 Satz 1 BDSG ist - ergänzend zu den Vorgaben der DS-GVO - 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 Datenschutzbeauftragter immer zu bestellen, soweit u. a. Verarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen (§ 38 Abs. 1 Satz 2 BDSG). Zudem ist die freiwillige Bestellung eines DSB immer möglich.

Der Verantwortliche hat sicherzustellen, dass der DSB ordnungsgemäß und frühzeitig in alle Datenschutzfragen eingebunden wird. Er ist mit den für die Erfüllung seiner Aufgaben

[21] Gemäß den Art. 37 ff DS-GVO 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.

erforderlichen Ressourcen, Zugängen zu personenbezogenen Daten und Verarbeitungsvorgängen auszustatten sowie bei der Erhaltung seines Fachwissens zu unterstützen.[22] 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 DS-GVO vorgeschrieben.[23]

> *Der DSB kann grundsätzlich andere Aufgaben und Pflichten wahrnehmen, sofern diese nicht zu einem Interessenkonflikt führen.[24] 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 DS-GVO und IPPF-Standard Nr. 1112 = Vorkehrungen zur Begrenzung von Beeinträchtigungen der Unabhängigkeit und der Objektivität). Hierfür ist z. B. eine klare Aufgabentrennung zwischen Tätigkeiten mit Revisionsbezug und Datenschutzaufgaben hilfreich.*

Zur Funktion eines zentralen bzw. Konzerndatenschutzbeauftragten nimmt die DS-GVO ebenfalls Stellung: Gemäß Art. 37 Abs. 2 DS-GVO darf eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.

3.2 Aufgaben

Der Datenschutzbeauftragte 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 DS-GVO geregelt und umfassen:

- Unterrichtung und Beratung der Verantwortlichen/Auftragsverarbeiter und der Beschäftigten hinsichtlich ihrer Datenschutzpflichten
- Überwachung („monitor“) der
  - Einhaltung der DS-GVO, des BDSG und anderer Regelungen zum Datenschutz
  - Strategien („policies“) zum Datenschutz, insbesondere im Hinblick auf die Zuweisung von Zuständigkeiten, die Sensibilisierung und Schulung der Mitarbeiter sowie Überprüfungen („audits“) von Verarbeitungsvorgängen

[22] Art. 38 Abs. 1 DS-GVO.
[23] Art. 38 Abs. 3 DS-GVO.
[24] Art. 38 Absatz 6 DS-GVO verpflichtet den Verantwortlichen sicherzustellen, dass es zu keinem Interessenkonflikt mit anderen zu übernehmenden Aufgaben und Pflichten eines DSB kommt.

- Auf Anfrage Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung
- 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 Änderungen eines bestehenden IT-gestützten Revisionstools bzw. Anwendungen zur Unterstützung der Revisionsarbeit (z. B. Analysetools)*
- *Ablage, Archivierung und Löschung von Prüfungsdaten*
- *Grundlegende Prozesse zum Prüfungsvorgehen (z. B. Datenanalysen 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*
- *Erstellung des Verzeichnisses der Verarbeitungstätigkeiten*
- *Datenschutzvorfälle und Betroffenenanfragen*
- *Datenschutzrechtliche Mitarbeitersensibilisierungen /-schulungen*
- *Mitwirkung bei Mitarbeiterkontrollen*

3.3 Der internationale Kontext

Die DS-GVO gibt den EU-Mitgliedstaaten die Möglichkeit, nationale Sonderregelungen hinsichtlich der Bestellung eines Datenschutzbeauftragten zu schaffen. Daher sind bei internationalen Bezügen ergänzend zur DS-GVO 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 DS-GVO, dass eine leichte Erreichbarkeit für Datenschutzbehörden, externe Betroffene und Beschäftigte gewährleistet wird.

4 Umsetzung des Datenschutzes in der Internen Revision

4.1 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 DS-GVO gestiegen. Die DS-GVO formuliert das Prinzip von Privacy by Design/Default[25] erstmals direkt im Gesetzestext aus. Ziel von Artikel 25 DS-GVO 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 DS-GVO mit der Rechenschaftspflicht eine hinreichende Dokumentation, aus der hervorgeht, dass die Anforderungen des Datenschutzes auch tatsächlich identifiziert und wirksam umgesetzt wurden.

Wenn die Interne Revision eigene IT-Systeme für die Planung, Steuerung und Dokumentation von Prüfungen oder Programme (z. B. Analysetools) einsetzt, unterliegen diese, einschließlich der nach Art. 32 Abs. 1 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen, der Überwachung der ordnungsgemäßen Anwendung durch den DSB.[26] Sie sind in das Verarbeitungsverzeichnis (Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO) aufzunehmen und dem DSB zur Kenntnis zu bringen. Bei der Dokumentation für das Verarbeitungsverzeichnis sind Detailkenntnisse über das verwendete IT-

[25] 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 wiederum bezeichnet datenschutzfreundliche Voreinstellungen aus Nutzersicht.
[26] 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).

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.

Nach der DS-GVO sind zur Bestimmung der erforderlichen Sicherheitsmaßnahmen zunächst der Schutzbedarf festzustellen, daraufhin 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.[27] Das Schutzkonzept der DS-GVO setzt damit verstärkt auf das Zusammenwirken von Datenschutz- und IT-Sicherheitsmanagement im Unternehmen.

Nach Maßgabe der DS-GVO müssen nur solche technischen und organisatorischen Maßnahmen umgesetzt werden, die verhältnismäßig sind. Artikel 32 DS-GVO 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 DS-GVO 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.

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

Der detaillierte Katalog des § 64 Abs. 3 BDSG[28] kann ergänzend als Orientierungshilfe für die Einrichtung von technischen und organisatorischen Maßnahmen dienen, da diese Vorgaben konkreter als in Art. 32 DS-GVO 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.

4.2 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 Datenschutzbeauftragten anbieten. Dabei sollte der Fokus nicht auf klassische Personalprüfungen beschränkt sein, sondern die Gesamtheit der Prüfungen einschließen. Der DSB ist der Internen Revision gegenüber nicht 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,*

[28] § 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.

- *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 eingeschränkt hinsichtlich Zeitraum und Personenkreis),*
- *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 Zugriffes bzw. der Einsicht in personenbezogene Daten, sind die Vorgaben zur Auftragsverarbeitung (Art. 28 DS-GVO) 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 DS-GVO erfolgt und den Schutz der Rechte der Betroffenen gewährleistet. Eine wesentliche Änderung durch die DS-GVO bei der Auftragsverarbeitung ist, dass auch die Auftragsverarbeiter verantwortlich für die Einhaltung der technischen und organisatorischen Maßnahmen 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 lokale bzw. länderspezifische Regelungen entgegenstehen.

4.3 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. Kapitel 4.1 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 wiedermöglich. 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. vom Prüfungsteam organisatorisch getrennt im Backoffice.*

Werden im Verlauf der Prüfung potenzielle Verstöße gegen die DS-GVO festgestellt, sind der DSB zu kontaktieren und gegebenenfalls Ad-hoc-Maßnahmen zu ergreifen. Verletzungen des Schutzes personenbezogener Daten führen gemäß Art. 33 DS-GVO 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.

4.4 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, 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.

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 eine Beziehbarkeit zu konkreten Personen hergestellt werden. Deshalb sind durchgängig geeignete Schutzmaßnahmen einzuhalten, z. B. E-Mail-Verschlüsselung bei Berichtsversand, Zugangskontrolle für Berichte.

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

4.5 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, das spezielleren Rechtsvorschriften Vorrang gibt.[29]

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

Bei der Dokumentation und Archivierung von personenbezogenen Daten gilt, dass diese unter Beachtung der Grundprinzipien der DS-GVO 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 4.3). 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, gesperrt und gelöscht werden. 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 reproduzierbar. Insbesondere bei Prüfungen bzw. Dokumenten zu klassischen prozessualen bzw. sachfragenorientierten Inhalten ist zu prüfen, ob die Dokumentation und Archivierung von personenbezogenen Daten erforderlich ist.

(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 Interne Revision & Datenschutz

DIIR – Deutsches Institut für Interne Revision e.V.

Theodor-Heuss-Allee 108

60486 Frankfurt am Main

Version 2.0 veröffentlicht im August 2021 auf www.diir.de.