Leitfaden Interne Revision und Datenschutz

DIIR-Arbeitskreis Interne Revision & Datenschutz

DIIR Deutsches Institut für Interne Revision e.V.

Dieser Leitfaden wurde nach aktuellem Stand sowie bestem Wissen und Gewissen erstellt. Er erhebt keinen Anspruch auf Verbindlichkeit und Vollständigkeit und ersetzt keinesfalls die Prüfung der individuellen rechtlichen Situation.

Anmerkungen und Hinweise können an arbeitskreise@diir.de übermittelt werden.

Inhalt

1 Datenschutz als rechtliche Verpflichtung

1.1 Nationale und europäische Gesetzgebung

Das Recht auf informationelle Selbstbestimmung ist die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es bildet die Grundlage für die bestehenden Datenschutzregelungen in Deutschland. Dies waren bisher im Wesentlichen das Bundesdatenschutzgesetz (BDSG) und Vorgaben aus der Landesgesetzgebung[1] sowie zusätzliche spezialgesetzliche Regelungen[2].

Mit der Europäischen Datenschutz-Grundverordnung (DS-GVO), die im Mai 2016 in Kraft getreten ist, sind weitreichende Auswirkungen auf nahezu alle Unternehmen in Europa verbunden. Über die DS-GVO soll das Datenschutzrecht auf europäischer Ebene weiter vereinheitlicht und angesichts der aktuellen technologischen Entwicklungen modernisiert werden. Ab 25. Mai 2018 ist sie unmittelbar in den Mitgliedsstaaten der EU anwendbar und löst damit die bisherigen nationalen Regelungen ab, wie das bis dahin geltende Bundesdatenschutzgesetz (BDSG).

Die in der Verordnung enthaltenen Öffnungsklauseln ermöglichen es den einzelnen Mitgliedstaaten, bestimmte Aspekte des Datenschutzes auch in der nationalen Gesetzgebung ergänzend zu regeln. In Deutschland wurden durch das Datenschutz-Anpassungs- und Umsetzungsgesetz-EU (DSAnpUG-EU) Regelungen ergänzt und neugefasst. Kernstück des DSAnpUG-EU ist das Bundesdatenschutzgesetz in der Fassung, die ab 25. Mai 2018 in Kraft tritt (sog. BDSG-neu).

In der Übergangszeit bis Mai 2018 und auch nach Inkrafttreten der DS-GVO und der ergänzenden Begleitgesetze sind noch weitere Konkretisierungen für die praktische Umset-

---

[1] Die Landesdatenschutzgesetze gelten - bis zu ihrer Ablösung durch die DS-GVO spätestens im Mai 2018 - für die jeweiligen Landesbehörden und Kommunalverwaltungen und gegebenenfalls ergänzend zu spezialgesetzlichen Regelungen.

[2] Diese Sondervorschriften sind auf die Anforderungen der jeweiligen Bereiche angepasst und gehen grundsätzlich den allgemeineren Regeln des BDSG vor. Für Revisoren aus 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

zung der Neuregelungen zu erwarten, z.B. Interpretations- und Orientierungshilfen der Aufsichtsbehörden. Zusätzlich ist zu erwarten, dass Anpassungen bzgl. der Landesgesetzgebung bzw. bei spezialgesetzlichen Regeln erfolgen.

Der Leitfaden wird sich im Schwerpunkt auf die für die Revisionsarbeit einschlägigen Regelungen der DS-GVO, des BDSG-neu und ihrer praktischen Bedeutung für das revisorische Vorgehen 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.

1.2 Grundprinzipen der DS-GVO

Der Umgang mit personenbezogenen Daten muss gemäß DS-GVO einigen grundsätzlichen Kriterien entsprechen[3]:

- rechtmäßige, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbare 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«),
- Form der Speicherung, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für den Zweck, für die sie verarbeitet werden, erforderlich ist (»Speicherbegrenzung«).
- angemessene Sicherheit zum Schutz vor unrechtmäßiger Verarbeitung, Verlust und Zerstörung durch geeignete technische und organisatorische Maßnahmen (»Integrität und Vertraulichkeit«).

[3] Die Grundsätze sind in Artikel 5 DS-GVO aufgeführt und werden im Erwägungsgrund 39 erläutert.

Der für die Verarbeitung Verantwortliche[4] muss deren Einhaltung, in der Regel anhand einer entsprechenden Dokumentation, nachweisen können („Accountability“[5]).

[4] Begriff des „controller“ (Verantwortlicher) in Art. 4 Nr. 7 DS-GVO

[5] Art. 5 Abs. 2 DS-GVO

2 Bedeutung des Datenschutzes für die Interne Revision

2.1 Grundsätzliches

Datenschutzrechtliche Regelungen sind zu beachten, sobald personenbezogene Daten ins Spiel kommen. 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).

Daten mit Personenbezug liegen oftmals in Zusammenhang mit Geschäftsprozessen vor. Die ständig wachsende Anzahl von Geschäftsvorfällen und Datenbeständen sowie der Einsatz von IT in nahezu allen betrieblichen Bereichen führen dazu, dass diese Daten systematisch und in großen Mengen bei Bedarf betrachtet und ausgewertet werden können[6].

Prüfungshandlungen der Internen Revision sind daher regelmäßig und zunehmend mit der Verarbeitung und Nutzung personenbezogener bzw. -beziehbarer Daten von Beschäftigten und teilweise Dritten (z.B. Geschäftspartner oder Kunden) verbunden. Es werden Unterlagen und Daten (Dokumente, Dateien, E-Mails) aus unternehmenseigenen Systemen eingesehen, ausgewertet und zusammengeführt.

Das reine Vorhandensein in den Systemen rechtfertigt es nicht, dass Unternehmen beliebig über diese Daten verfügen dürfen. So muss jede Verarbeitung personenbezogener Daten auf Grundlage eines legitimen Zwecks erfolgen. Aufgrund der funktionalen Zuständigkeit der Internen Revision lässt sich im Rahmen von Prüfungen eine Zweckbestimmung in datenschutzrechtlicher Hinsicht begründen. Die Interne Revision verfügt über ein grundsätzlich uneingeschränktes Informationsrecht[7]. 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.

Der grundsätzliche Maßstab und die datenschutzrechtlichen Anforderungen an den Umgang mit personenbezogenen Daten sind auch mit der DS-GVO unverändert geblieben.

---

[6] Vgl. weiterführend DIIR: „Datenauswertungen und personenbezogene Datenanalyse“, http://www.diir.de/fileadmin/fachwissen/downloads/09DIIRDatenanalyseWeb.pdf

[7] DIIR Revisionsstandard Nr. 3, Mindeststandard Nr. 2, Stand: Juli 2016

Die DS-GVO hält an dem Prinzip fest, dass jede Verarbeitung personenbezogener Daten einer Erlaubnis bedarf. Art. 6 DS-GVO listet die regelmäßig geltenden Erlaubnistatbestände auf. So kann sich - außer 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
- berechtigtem Interesse nach Interessenabwägung

Die Zulässigkeit der Verarbeitung und Nutzung der Daten im Rahmen der Kontroll- und Überwachungstätigkeit der Internen Revision[8] ergibt sich im Regelfall aus Art. 6 Abs. 1 lit. f DS-GVO (Wahrung berechtigter Interessen), bisher § 28 Abs. 1 Nr. 2 BDSG.

> *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 zu besprechen (vgl. auch 3).*
>
> *Mit der in Art. 6 DS-GVO aufgeführten Zulässigkeit einer Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung sind vorrangige Rechtsvorschriften gemeint, die zur Verarbeitung der betroffenen Daten verpflichten[9]. 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. Bezogen auf die Tätigkeit der Internen Revision findet sie immer Anwendung, wenn die Revisionsabteilung in der Europäischen Union niedergelassen ist, unabhängig davon, ob die Verarbeitung der Daten in der Europäischen Union stattfindet.

---

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

[9] vgl. Erwägungsgrund 45 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[10].

> *Diese Kriterien sind bei revisorischen Tätigkeiten oft 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.*

2.3 Beschäftigtendaten in der Prüfung

Die DS-GVO enthält keine spezifischen Erlaubnistatbestände für die Verarbeitung von Beschäftigtendaten. Der Beschäftigtendatenschutz gehört dabei 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-neu). Damit kann die Datenverarbeitung weiterhin auf Tarifverträge und Betriebs- oder Dienstvereinbarungen gestützt werden.

[10] Art. 4 Ziffer 1 DS-GVO

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-neu ist § 26 maßgeblich für die Datenverarbeitung im Beschäftigungskontext. Die Vorschrift konkretisiert und ergänzt die Vorgaben der DS-GVO, verdrängt die vorrangigen Regelungen der DSGVO aber nicht. § 26 BDSG-neu greift erkennbar auf wesentliche Strukturen und Regelungen des bisherigen § 32 BSDG zurück. Auch 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.*

Datenverarbeitung von Beschäftigten ist damit erlaubt, wenn sie für Zwecke des Beschäftigungsverhältnisses geeignet ist, das mildeste der dem Unternehmen zur Verfügung stehenden gleich effektiven Mittel (Erforderlichkeit) ist und schutzwürdige Interessen des Beschäftigten nicht überwiegen. Zur weiteren Ausgestaltung vgl. Kapitel 4.

2.4 Unternehmensinterne Ermittlungen

Besonders verhält es sich, wenn personenbezogene Daten von Beschäftigten zur Aufdeckung von Straftaten verarbeitet werden sollen. Dies ist nur unter bestimmten Voraussetzungen zulässig. Insbesondere müssen tatsächliche Anhaltspunkte den Verdacht auf eine Straftat im Beschäftigungsverhältnis begründen. Der Begriff Verdacht ist dabei ein Terminus aus der Rechtswissenschaft. Als Abgrenzung zu bloßen Vermutungen wird je nach Verdachtsgrad im deutschen Recht unterschieden zwischen:

Anfangsverdacht

> Möglichkeit der Tatbegehung, die auf Beweisgründen oder Anzeichen (Indizien) beruht, dass jemand eine Straftat begangen hat. Beim Anfangsverdacht besteht eine Pflicht der Strafverfolgungsorgane zur Einleitung eines Ermittlungsverfahrens.

hinreichender Tatverdacht

> Wahrscheinlichkeit, dass der Beschuldigte eine strafbare Handlung begangen hat und verurteilt wird. Hier besteht eine Pflicht der Staatsanwaltschaft zur Anklageerhebung.

dringender Tatverdacht

> Hohe Wahrscheinlichkeit, dass der Beschuldigte eine strafbare Handlung begangen hat. Die belastenden Momente müssen die entlastenden Momente überwiegen. Bestimmte Maßnahmen werden dann zulässig, z.B. Untersuchungshaft (§ 112 StPO).

Untersuchungen anlässlich möglicher doloser Handlungen[11] unterscheiden sich von klassischen prozessualen 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. Dies zeigt sich insbesondere in der Einbeziehung des Datenschutzbeauftragten, des Betriebsrates sowie ggf. Rechtsabteilung und den besonderen Dokumentationsverpflichtungen.

Die Voraussetzungen für die Verarbeitung von Beschäftigtendaten anlässlich der Aufdeckung von Straftaten ergeben sich aus § 26 Abs. 1 Satz 2 BDSG-neu:

- 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 des Betroffenen)

---

[11] 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.

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.

3 Rolle des Datenschutzbeauftragten

3.1 Stellung im Unternehmen

Die DS-GVO sieht den betrieblichen Datenschutzbeauftragten (DSB) verbindlich nur noch vor bei öffentlichen Stellen sowie Unternehmen, bei denen besonders risikoreiche Datenverarbeitungen erfolgen (Art. 37 ff. DSGVO)[12]. Jedoch besteht auf Grund einer Öffnungsklausel eine Regelungsbefugnis für die Mitgliedsstaaten.

Die bislang in Deutschland geltende Bestellpflicht wurde grundsätzlich beibehalten. Gemäß § 38 BDSG-neu müssen Verantwortliche auch dann einen DSB bestellen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. 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.

Der Verantwortliche hat sicherzustellen, dass der DSB ordnungsgemäß und frühzeitig in alle Datenschutzfragen eingebunden wird. Er ist bei der Erfüllung seiner Aufgaben mit den erforderlichen Ressourcen, einem Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen auszustatten sowie zur Erhaltung seines Fachwissens zu unterstützen[13]. 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[14].

> *Der DSB kann grundsätzlich andere Aufgaben und Pflichten wahrnehmen, sofern diese nicht zu einem Interessenkonflikt führen[15]. 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.*

---

[12] 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.

13 Art. 38 Abs. 1 DS-GVO

14 Art. 38 Abs. 3 DS-GVO

[15] 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.

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 klar 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

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 und anderer Regelungen zum Datenschutz
  - Strategien („policies") zum Datenschutz, insbesondere im Hinblick auf Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung der Mitarbeiter, Überprüfungen („audits") von Verarbeitungsvorgängen
- 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. anderer Verfahren zur Verarbeitung personenbezogener Daten*
  - *Ablage, Archivierung und Löschung von Prüfungsdaten*
  - *Grundlegende Prozesse zum Prüfungsvorgehen (z.B. Datenanalysen und temporäre Zugriffe auf Systeme etc.).*
  - *Vorgehensweise bei Ermittlungen bzw. der Klärung von Verdachtsfällen*
  - *Einzelfragen bei Prüfungen*

3.3 Der internationale Kontext

Vergleichbar zu den Regelungen des BDSG-neu in Deutschland sind bei internationalen Bezügen die entsprechenden lokalen Vorschriften zu beachten. Die DS-GVO gibt den EU-Mitgliedstaaten die Möglichkeit, nationale Sonderregelungen hinsichtlich der Bestellung eines Datenschutzbeauftragten zu schaffen.

In Unternehmen mit Sitz sowohl innerhalb als auch außerhalb der EU empfiehlt es sich grundsätzlich, auf lokale Ansprechpartner zurückzugreifen. Wie dabei die von der DS-GVO geforderte leichte Erreichbarkeit für Aufsichtsbehörden, externe Betroffene und Beschäftigte gewährleistet werden kann, sollte die verantwortliche Stelle jedenfalls im Rahmen der Umsetzung der Verordnung bewusst analysieren.

4 Umsetzung datenschutzrechtlicher Vorgaben

4.1 Grundlegende Festlegungen

Die Interne Revision hat als Prozessverantwortlicher klare Regelungen zum Umgang mit personenbezogenen Daten festzulegen. Dabei ist darauf zu achten, sowohl die abteilungsinternen Prozesse als auch das Prüfungsvorgehen datenschutzfreundlich bzw. -konform gestaltet werden Die Beschäftigten der Internen Revision sollten darüber regelmäßig unterwiesen und sensibilisiert werden.

Die Anforderungen an eine datenschutzkonforme Gestaltung der Prozesse sind mit der neuen Gesetzeslage gestiegen. Zwar ist das Prinzip von Privacy by Design/Default[16] nicht neu; es konkretisiert im Grunde das bereits bekannte Gebot der Datensparsamkeit. Die DS-GVO formuliert diesen Grundsatz erstmals direkt im Gesetzestext aus. Ziel von Art. 25 DS-GVO ist es, Systeme und Dienste von Anfang an über den gesamten Lebenszyklus datensparsam und mit möglichst datenschutzfreundlichen Voreinstellungen zu gestalten. Außerdem verlangt die DS-GVO eine hinreichende Dokumentation, aus der hervorgeht, dass die Anforderungen des Datenschutzes auch tatsächlich identifiziert und wirksam umgesetzt wurden.

Wenn die Interne Revision für die Verarbeitung und Nutzung personenbezogener Daten eigene Systeme oder Programme einsetzt, unterliegen diese, einschließlich der nach Art. 32 Abs. 1 DS-GVO bzw. § 64 BDSG-neu erforderlichen technischen und organisatorischen Maßnahmen, der Überwachung der ordnungsgemäßen Anwendung durch den DSB[17]. Sie sind in das Verfahrensverzeichnis (Verzeichnis von Verfahrenstätigkeiten nach Art. 30 DS-GVO) aufzunehmen und dem DSB zur Kenntnis zu bringen.

---

[16] 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.

[17] 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-neu (vgl. 2.3).

Nach Maßgabe der DS-GVO müssen nur solche Maßnahmen umgesetzt werden, die verhältnismäßig sind. Art. 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.

Die DS-GVO schreibt in Art. 32 andere und umfassendere Maßnahmen als der bisherige § 9 BDSG 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.

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[18]. Das Schutzkonzept der DS-GVO setzt damit verstärkt auf das Zusammenwirken von Datenschutz- und IT-Sicherheitsmanagement im Unternehmen.

Auch in § 64 BDSG-neu[19] sind - im Vergleich zur bisherigen Anlage zu § 9 Satz 1 BDSG - neue Datenschutzkontrollen genannt. Dabei sind

- neu: Datenintegrität, Zuverlässigkeit und Wiederherstellbarkeit,
- anders als bisher unterteilt und daher nur scheinbar neu: Transport- und Übertragungskontrolle, Datenträger-, Speicher- und Benutzerkontrolle.

Gemäß § 64 Abs. 1 BDSG-neu hat der Verantwortliche bei der Umsetzung der Maßnahmen die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

---

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

[19] § 64 BDSG-neu („Anforderungen an die Sicherheit der Datenverarbeitung“) enthält eine Übersicht mit der Beschreibung der einzelnen Kontrollen (insgesamt 14).

4.2 Prüfungsauftrag und Prüfungsvorbereitung

Bereits bei der Erstellung des Prüfungsauftrags sollte darauf geachtet werden, datenschutz-relevante 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 keinesfalls auf klassische Personalprüfungen beschränkt sein. Der DSB ist der Internen Revision gegenüber nicht weisungsbefugt, kann aber die datenschutzkonforme Prüfungsumsetzung Einfluss nehmen.

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 personenbezogene Daten enthalten, sollte im Prüfungsauftrag festgehalten werden,*
>
> - für welches Prüfungsziel die Daten verwendet werden,
> - welche Daten einbezogen werden (z.B. besonders sensible Daten wie Gesundheits- oder Gehaltsdaten)
> - ob sich der geplante Zweck nur genau mit den zu verwendenden Daten erfüllen lässt (Geeignetheit und Erforderlichkeit)
> - welche alternativen Vorgehensweisen ggfs. bestehen, durch die die Betroffenen in ihren Persönlichkeitsrechten weniger belastet werden (Angemessenheit)
> - ob besondere, schutzwürdige Interessen eines Betroffenen bestehen, die das Interesse an der Durchführung der Prüfungshandlung überwiegen (Verhältnismäßigkeit).
>
> *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, ist es notwendig, den Datenschutzbeauftragten zu involvieren. Dabei sind in der Regel die Vorgaben zur Auftragsverarbeitung zu berücksichtigen.

Für gesellschaftsübergreifende Zugriffe oder Anforderungen von Daten ist mit den zu prüfenden Gesellschaften die Verwendung personenbezogener Daten schriftlich oder in anders geeigneter Form (z.B. elektronischer Workflow) zu vereinbaren. 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 lokale bzw. länderspezifische Regelungen dem entgegenstehen.

4.3 Prüfungsdurchführung

Die Prüfungsdurchführung hat sich gemäß der im Prüfungsauftrag freigegebenen Umfänge bzw. der im generellen Regelungsgerüst der Abteilung vorgegeben technischen und organisatorischen Maßnahmen zu bewegen.

Nach dem Grundsatz der Datensparsamkeit sind dabei so wenig wie möglich personenbezogene Daten zu verarbeiten. Insbesondere sind diese zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keine 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 (z.B. durch Zahlen- oder Buchstabenkombinationen) pseudonymisierten Daten 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 Organisationseinheiten mit weniger als fünf Beschäftigten unter Umständen ebenfalls Rückschlüsse auf einzelne Personen möglich.*
>
> *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.*

Zur Durchsetzung von Forderungen gegen andere Unternehmen bzw. zur Abwehr von Forderungen gegen das eigene Unternehmen ist es in Einzelfällen ggf. notwendig, personenbezogene Dokumente (z.B. E-Mails) auszuwerten oder zur Verfügung zu stellen.

Insofern die Revision in diesen Prozess involviert wird, sollte auch hier eine entsprechende Abstimmung mit dem zuständigen Datenschutzbeauftragten unter Berücksichtigung der einschlägigen Rechtsvorschriften erfolgen. Es ist zu empfehlen, das Abstimmungsergebnis zu dokumentieren.

4.4 Prüfungsdokumente

Das Ergebnis einer durchgeführten Prüfung wird im Regelfall im Prüfungsbericht dokumentiert. Er enthält Feststellungen aus den Prüfungshandlungen, Risikoeinschätzungen und 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.

Prüfungsberichte können in Einzelfällen personenbezogene oder -beziehbare Daten sowie vertrauliche Geschäftsinformationen enthalten. Grundsätzlich werden Feststellungen und Maßnahmen bzw. Empfehlungen nicht konkreten Personen, sondern Abteilungen oder Bereichen zugewiesen. Allerdings kann z.B. in kleineren Unternehmen oder Einheiten durchaus eine Beziehbarkeit zu konkreten Personen hergestellt werden. Insbesondere in diesen Fällen ist an geeignete Schutzmaßnahmen zu denken. Dies gilt auch, wenn konkrete personenbezogene Daten im Einzelfall selbst Teil des Untersuchungsergebnisses sind.

Die Ergebnisse des Follow-up und die dazugehörigen Dokumente sind wie Prüfungsberichte zu behandeln.

4.5 Archivierung von Prüfungsdaten

Bei der 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[20].

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

Nach Ablauf der gesetzlichen Anforderungen bzw. für Dokumente ohne handelsrechtliche oder steuerliche Relevanz sind in den Fällen, in denen personenbezogene Daten gespeichert wurden, die Datenschutzvorschriften zu beachten. Hierfür sollte ein Löschkonzept vorgehalten werden.

Grundsätzlich gilt bei der Archivierung von personenbezogenen Daten, dass diese sparsam gespeichert werden sollten. Das heißt, dass der Personenbezug – soweit er nicht zwingend erforderlich ist – zu löschen ist bzw. die Daten anonymisiert werden. Darüber hinaus bedeutet das Prinzip der Datenminimierung auch, dass Daten, die nicht mehr gebraucht werden bzw. nicht mehr aufbewahrt werden müssen, gesperrt und gelöscht werden.

(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 Interne Revision & Datenschutz

DIIR – Deutsches Institut für Interne Revision e.V.

Theodor-Heuss-Allee 108

60486 Frankfurt am Main

Veröffentlicht im Oktober 2017 auf www.diir.de

Version 1.0