Checkliste zur Prüfung der Datenschutzorganisation

DIIR-Arbeitskreis Interne Revision & Datenschutz

Version 2.0

DIIR Deutsches Institut für Interne Revision e.V.

Vorwort 4

1 Datenschutzstrategie 5

1.1 Grundlagen 5

1.2 Implementierung und Kommunikation 6

2 Vorgaben und Anforderungen....7

2.1 Datenschutzvorgaben und Anforderungen, gesetzlich und betrieblich/intern 7

2.2 Berücksichtigung der Anforderungen....8

3 Organisation....10

3.1 Datenschutzorganisation 10

3.2 Operative Einbindung des Datenschutzes....12

3.3 Rahmenbedingungen für den sicheren Einsatz von IT-Systemen....13

3.4 Regelungen zum Umgang mit Datenschutzvorfällen und Betroffenenanfragen .15

4 Ausgewählte Prüffelder im Datenschutz-Audit....17

4.1 Kommunikation der Regelungen zum Datenschutz....17

4.2 Einwilligungsmanagement 17

4.3 Auftragsverarbeitung....18

4.4 Prüfung gemeinschaftlicher Datenverarbeitung....18

4.5 Prüfung von Sperr- und Löschkonzepten 19

4.6 Monitoring und laufende Anpassung des Datenschutzes....20

4.7 Handlungsvorgaben bei Anfragen und Prüfungen der Datenschutzaufsichtsbehörden....20

4.8 Handlungsvorgaben bei Anfragen von Externen 20

5 Reporting 21

5.1 Regelmäßige Berichtslinien gesetzlich und betrieblich/intern (z. B. Tätigkeitsberichte)....21

5.2 Anlassbezogene Berichterstattung (Ad-hoc-Reporting) an Datenschutzbehörde und/oder interne Stelle 23

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. Bestehende Geschäftsmodelle werden um zusätzliche datengetriebene Geschäftsmodelle, vor allem mit Endkundendaten ergänzt.

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

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 durch die Interne Revision.

Der DIIR-Arbeitskreis Interne Revision & Datenschutz bietet im Folgenden eine strukturierte Vorgehensweise (in Form einer Checkliste) zur Überprüfung der Datenschutzorganisation und ihrer Wirksamkeit im Unternehmen an. Unabhängig von Prüfungen kann diese Übersicht einen wichtigen Rahmen für die im Kontext des Datenschutzes zu beachtenden Ansätzen und Regularien darstellen.

Diese Checkliste wurde nach aktuellem Stand sowie bestem Wissen und Gewissen im November 2017 erstellt und im August 2021 aktualisiert. Dabei wurden insbesondere die Kapitel 3 und 4 maßgeblich überarbeitet. Die Checkliste 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 Datenschutzstrategie

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

1.1 Grundlagen

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

- Gibt es eine Datenschutzstrategie und in welcher Form ist diese dokumentiert?
- Hat die Strategie unternehmens-/konzernweite Gültigkeit?
- Wann wurde die Strategie erlassen/aktualisiert?
- Mit wem wurde die Strategie abgestimmt? Sind notwendige interne/externe Stellen einbezogen worden?
- Wer hat die Strategie verabschiedet?
- Welche Quellen zur Erstellung der Strategie (nationales Recht, Best Practices etc.) wurden genutzt?
- Was sind Grundlagen und wesentliche Inhalte der Strategie?
- Ist die Strategie angemessen/plausibel, insbesondere in Bezug auf Unternehmensgröße/Unternehmensstruktur, Geschäftsmodell, regionale Aufteilung und Art der Daten?
- Sind die gültigen gesetzlichen Regelungen (z. B. Art. 25 DS-GVO) ausreichend in der Strategie berücksichtigt?
- Ist die Strategie in das Governance-Modell des Unternehmens eingebettet?

- Ist die Verbindlichkeit der Strategie in allen Konzerngesellschaften/Legaleinheiten nachweisbar?
- Wer verfolgt die Umsetzung der Strategie?
- Gibt es eine im Sinne der DS-GVO (Art. 47) durch die zuständigen Aufsichtsbehörden genehmigte interne Datenschutzvorschrift (z. B. Binding Corporate Rules bei unternehmens-/konzerninternen Datentransfers in Drittstaaten)?

1.2 Implementierung und Kommunikation

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

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

2 Vorgaben und Anforderungen

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

2.1 Datenschutzvorgaben und Anforderungen, gesetzlich und betrieblich/intern

- Gibt es allgemein verbindliche und von der Unternehmensleitung freigegebene Unternehmensrichtlinien?
- Sind die einschlägigen und branchenspezifischen Gesetze, Normen und Standards in den Unternehmensrichtlinien berücksichtigt?
- Gibt es weitere gesetzliche und/oder betriebliche/interne Vorgaben? Wenn ja, sind diese aufeinander abgestimmt?
- Gibt es betriebliche Regelungen (z. B. kollektivrechtliche Vereinbarungen)?
- Ist berücksichtigt, dass die DS-GVO auch für alle außerhalb der EU niedergelassenen Unternehmen gilt, soweit sie mit betroffenen Personen in der EU Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten (Marktortprinzip, Art. 3 DS-GVO)?
- Sind die Vorgaben in Summe aufeinander abgestimmt bzw. ist sichergestellt, dass Mussvorgaben bzw. die strengsten Vorgaben das Regelungsminimum bedeuten?

2.2 Berücksichtigung der Anforderungen

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

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

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

- Erlaubnis zur Erhebung und Verarbeitung personenbezogener Daten. Auch bei der DS-GVO gilt ein Verbot mit Erlaubnisvorbehalt (Art. 6 DS-GVO)
    - Rechtliche Verpflichtung
    - Vertrag/Vorvertrag (Rechtsgeschäft)
    - **Überwiegendes betriebliches Interesse**
    - Vereinbarung mit bestehenden Primärzwecken
    - Einwilligung
    - Schutz lebenswichtiger Interessen
- Datenschutz-Organisation
    - Policies zu Datenschutz und IT-Sicherheit
    - Datenschutzfreundliche Technologien (Art. 25 DS-GVO)
    - IT-Sicherheit nach dem Stand der Technik (Art. 32 DS-GVO)
    - Dokumentationspflichten (Art. 5 DS-GVO)
        - Datenschutzmanagement

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

3 Organisation

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

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

3.1 Datenschutzorganisation

Im nachfolgenden Abschnitt ist Gegenstand der Fragestellungen es, die Angemessenheit der Datenschutzorganisation zu bewerten. Nicht Gegenstand ist die Verarbeitung personenbezogener Daten in einzelnen Fachverfahren. Dieser Analyseteil trifft keine Aussagen zur angemessenen und wirksamen Umsetzung datenschutzrechtlicher Bestimmungen.

3.1.1 Organisationsform

Entspricht die Organisationsform der verabschiedeten Strategie?

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

    - Besteht ein konzerninterner Datenaustausch?
    - Bestehen Datentransfers in Drittländer?
- Bestehen besondere lokale/nationale Anforderungen an den Datenschutz bzw. die Datenschutzorganisation?
- Aufbau der Datenschutzorganisation
    - Besteht eine zentrale/dezentrale Datenschutzorganisation?
    - Besteht es eine Mischform?
    - Besteht ein Organigramm der Datenschutzorganisation?

3.1.2 Leitlinie zu den Aspekten Datenschutz und Datensicherheit

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

3.1.3 Anforderungen an den betrieblichen Datenschutzbeauftragten

- Berücksichtigt die Ausgestaltung der Datenschutzorganisation die Anforderungen an einen betrieblichen Datenschutzbeauftragten hinsichtlich:
    - Zuverlässigkeit
    - Unabhängigkeit
    - Ausstattung
    - Fachkunde
- Sind die Verantwortlichkeiten klar geregelt?
- Wie wurde der Datenschutzbeauftragte vom Datenschutzverantwortlichen (Unternehmensleitung) bestellt?
    - Wurden (in einem Unternehmensverbund) weitere Datenschutzbeauftragte bestellt?

- Sind Datenschutzkoordinatoren in den Organisationseinheiten bzw. Unternehmensteilen benannt?

- Ist der Datenschutzbeauftragte in seiner Funktion der Geschäftsführung unmittelbar unterstellt und unterliegt er in der Ausübung seiner Tätigkeiten keiner fachlichen Weisung durch die Geschäfts- und Bereichsleitung? Besteht eine Tätigkeits-/Aufgabenbeschreibung mit klaren Befugnissen, Rechten und Verpflichtungen?
- Besteht eine risikoorientierte Aufgabenwahrnehmung des Datenschutzbeauftragten?
- Sind die Beratungs- und Überwachungstätigkeiten des Datenschutzbeauftragten beschrieben und kommuniziert?

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

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

3.2 Operative Einbindung des Datenschutzes

Der betriebliche Datenschutzbeauftragte überwacht u. a. die Einhaltung der DS-GVO und anderer Rechtsvorschriften. Er wirkt beratend und unterstützend an der Behebung erkannter Mängel mit. Die Mängelbearbeitung wird schriftlich dokumentiert. Die Bearbeitung einzelner Mängel kann stichprobenartig im Rahmen interner Audits überprüft werden.

- Wird der betriebliche Datenschutzbeauftragte in die Planung und Kontrolle der Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen miteinbezogen?

- Finden die Überwachungstätigkeiten regelmäßig und anlassbezogen statt?
- Pflegt der Datenschutzbeauftragte regelmäßigen Kontakt zur zuständigen Aufsichtsbehörde?

Werden regelmäßige Sensibilisierungs- und Schulungsmaßnahmen durch den betrieblichen Datenschutzbeauftragten durchgeführt (idealerweise als Methodenmix von arbeitsplatzbezogener Schulung bis hin zu E-Learning-Maßnahmen)?

- Bestehen die Unterweisungsnachweise zu den durchgeführten Sensibilisierungsmaßnahmen?

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

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

3.3 Rahmenbedingungen für den sicheren Einsatz von IT-Systemen

Die erforderliche Dokumentation der automatisierten Datenverarbeitung ist von der verantwortlichen Stelle sicherzustellen. Für die Auswahl angemessener technischer und organisatorischer Sicherheitsmaßnahmen und für den Nachweis einer ordnungsgemäßen und

wirksamen Umsetzung bilden die Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) einschließlich der vom BSI in den Standards 200-1 bis 200-4 (Aufbau eines Informationssicherheitsmanagementsystems, Vorgehensweise nach dem IT-Grundschutz, Erstellung einer Risikoanalyse und das Business Continuity Management) definierten Vorgehensweise eine gute Orientierungshilfe für das Unternehmen.

- Wurde ein Informationssicherheitsbeauftragter benannt?
- Sind die Aufgaben des Informationssicherheitsbeauftragten in einer entsprechenden Richtlinie festgelegt?
- Ist der Informationssicherheitsbeauftragte für die Erstellung und Fortschreibung der Sicherheitskonzeption und das Aufrechterhalten des Sicherheitsniveaus verantwortlich?
- Wird vor der Inbetriebnahme neuer Systeme bzw. Prozesse, in denen personenbezogene Daten verarbeitet werden, eine Freigabe der Informationssicherheit und des DSB eingeholt? Wird diese Freigabe angemessen dokumentiert?
- Werden Dienstleister unter Berücksichtigung der definierten Anforderungen der Informationssicherheit und des Datenschutzes ausgewählt?
- Werden Auftragsverarbeitungen ausschließlich auf Basis einer schriftlichen Vereinbarung durchgeführt, auch wenn sie in einzelnen Fachverfahren stattfinden?
- Sind die Vereinbarungen Bestandteil der Dokumentation des IT-Einsatzes?
- Werden Vereinbarungen mit Dienstleistern von der Informationssicherheit und dem DSB geprüft und freigegeben?
- Sind administrative Änderungen an den IT-Systemen nur durch einzelne, explizit berechtigte Mitarbeiter möglich?
- Wurden im Unternehmen konkrete technische und organisatorische Maßnahmen für die Durchführung der administrativen Tätigkeiten an den erfassten Systemen getroffen?
- Erfüllen die vom Unternehmen getroffenen Maßnahmen zur Dokumentation von Änderungen an informationstechnischen Geräten, Programmen und Verfahren die Anforderungen der DS-GVO?
- Werden Änderungen zunächst auf Testsystemen durchgeführt?
  Wird die Durchführung der Tests hierbei schriftlich dokumentiert?
- Erfolgt die Freigabe von wesentlichen Systemänderungen nach Abstimmung mit dem Informationssicherheitsbeauftragten und dem DSB?
- Prüft der Datenschutzbeauftragte regelmäßig die ordnungsgemäße und wirksame Umsetzung der technischen und organisatorischen Maßnahmen der im VvV enthaltenen Systeme bzw. Prozesse?

3.4 Regelungen zum Umgang mit Datenschutzvorfällen und Betroffenenanfragen

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

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

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

- Sind in den Vorgaben die Ansprechpartner, das Vorgehen und evtl. Fristen zur Bearbeitung, Dokumentation und Nachbereitung von Sicherheits- und Datenschutzvorfällen festgelegt?
- Ist sichergestellt, dass alle meldepflichtigen Vorgänge entsprechend den Vorgaben fristgerecht zentral verarbeitet werden können?
- Gibt es einen Reaktionsplan bei einer Verletzung des Schutzes personenbezogener Daten (Art. 33, 34 DS-GVO)?
- Sind die Zuständig- und Verantwortlichkeiten für eine evtl. Meldung an die Aufsichtsbehörde und ggf. für die Information der Betroffenen klar geregelt?
- Werden geeignete Prozesse für die Umsetzung der Informationspflicht bei einer Verletzung des Schutzes personenbezogener Daten genutzt?
  Werden dabei von den Aufsichtsbehörden bereitgestellte Informationskanäle und Formulare genutzt?
- Werden Sicherheits- und Datenschutzvorfälle durch ein eigens hierfür festgelegtes Prozedere mit Krisenmanagement und Datenschutzbeauftragtem sowie ggf. zusätzlichen Mitgliedern bearbeitet?

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

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

4 Ausgewählte Prüffelder im Datenschutz-Audit

4.1 Kommunikation der Regelungen zum Datenschutz

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

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

4.2 Einwilligungsmanagement

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

Es ist zu prüfen, ob Einwilligungserklärungen folgenden Anforderungen entsprechen:

- Klare und verständliche Sprache
- Trennung von anderen Sachverhalten
- Abgabe ohne Zwang

- Leichte Zugänglichkeit
- Kopplungsverbot gem. Art. 7 Abs. 4 DS-GVO
- Widerruflichkeit für die Zukunft
- Führung des Nachweises für das Vorliegen einer Einwilligung (z. B. im CRM-System)

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

4.3 Auftragsverarbeitung

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

4.4 Prüfung gemeinschaftlicher Datenverarbeitung

- Liegen gemeinschaftliche Datenverarbeitungen vor und wurden diese über das Kriterium der gemeinschaftlichen Festlegung der Zwecke und Mittel der Verarbeitung (z.

B. Leiharbeit, Buchungsplattformen, konzernübergreifende Kundendatenbank) als solche klassifiziert?

- Besteht eine Dokumentation der gemeinsamen Festlegung von Verarbeitungszwecken und –mitteln?
- Liegt ein Vertrag oder eine Vereinbarung über die gemeinschaftliche Verantwortung vor (Art. 26 DS-GVO) und sind die notwendigen Bestandteile enthalten?
- Sind die Aufgaben für die Pflichten, Betroffenenrechte, Informationspflichten und Rollenverteilungen nachvollziehbar geregelt?
- Besteht eine Regelung über den Haftungsausgleich unter den Verantwortlichen?
- Werden wesentliche Inhalte den Betroffenen zur Verfügung gestellt (Art. 26 Abs. 2 S. 2)?

4.5 Prüfung von Sperr- und Löschkonzepten

- Sind Löschfristen in den Verzeichnissen von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO bzw. in einem Löschkonzept grundsätzlich definiert?
- Sind die jeweiligen Speicherorte und Datenflüsse der einzelnen Prozesse bekannt?
- Sind sich die Prozessverantwortlichen ihrer Verantwortung für die Löschung bewusst?
- Haben die Prozessverantwortlichen Maßnahmen getroffen, um die manuelle oder automatisierte Löschung umzusetzen?
- Sind Löschungen nachvollziehbar dokumentiert (Vernichtungsnachweis, Datenbankprotokollierungen)?
- Sofern unmittelbar keine Löschung umsetzbar ist, wurden organisatorische und technische Maßnahmen zur Sperrung implementiert?
- Sind Zugriffssperren wirksam umgesetzt?
- Bestehen Vorgaben zur sicheren Löschung bzw. Vernichtung von Daten und Datenträgern?
- Werden berechtigte Löschbegehren wirksam umgesetzt?
- Erstrecken sich die Löschkonzepte ebenso auf Archivsysteme, Testsysteme, Protokolldaten und Backup-Systeme?
- Werden Löschnachweise von Auftragsverarbeitern, insbesondere bei SaaS und externen Hosting Dienstleistern, bei Beendigung des Vertragsverhältnisses eingefordert?

4.6 Monitoring und laufende Anpassung des Datenschutzes

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

4.7 Handlungsvorgaben bei Anfragen und Prüfungen der Datenschutzaufsichtsbehörden

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

4.8 Handlungsvorgaben bei Anfragen von Externen

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

5 Reporting

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

Die Nachweispflicht erstreckt sich insbesondere auf die Punkte:

- Rechtmäßigkeit
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Rechtzeitige Löschung
- Datenintegrität und Vertraulichkeit

Das Berichtswesen sollte sich an den Vorgaben für das Verfahrensverzeichnis gemäß Art. 30 DS-GVO orientieren.

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

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

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

5.1.1 Berichtszyklus und Berichtsumfang

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

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

5.1.2 Berichtsumfang

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

- alle Datenschutzvorfälle in der Berichtsperiode aufzählen und ggf. auf die Falldokumentation verweisen,
- alle wesentlichen Änderungen im Verfahrensverzeichnis in der Berichtsperiode erwähnen,
- statistische Angaben zu Auskunftsersuchen und deren Bearbeitungsdauer (oder Nullmeldung) enthalten,
- ein Statusupdate zu allen datenschutzbezogenen Projekten geben,
- den ihm zu Datenschutzzwecken getriebenen Aufwand im Berichtszeitraum erkennen lassen.

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

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

5.1.3 Dokumentation für die erstellten Berichte

- Entsprechen die letzten Berichte den Vorgaben der o. g. Punkte?
- Erfolgt eine Überprüfung der Korrektheit und Vollständigkeit der Angaben am konkreten Beispiel?
- Werden der Weg der Informationen und die Zuverlässigkeit der Quellen bewertet? Werden z. B. wirklich alle Eingangskanäle für Auskunftsersuchen bei deren Anzahl

berücksichtigt oder vielleicht nur die häufigste Form der Kontaktaufnahme? Und hat der Bericht tatsächlich den geplanten Verteiler erreicht?

- Ist es ohne Inhaltsprüfung belegbar, dass seit Inkrafttreten der Regelung tatsächlich in jeder Berichtsperiode ein Bericht erstellt und zeitnah zum Periodenende verteilt wurde?

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

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

5.2.1 Übersicht über mögliche Anlässe zu meldepflichtigen Vorfällen

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

5.2.2 Lokale Vorgaben

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

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

5.2.3 Dokumentation für die erstellten Berichte

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

Autoren

Erarbeitet vom DIIR-Arbeitskreis Interne Revision & Datenschutz

DIIR – Deutsches Institut für Interne Revision e.V.

Theodor-Heuss-Allee 108

60486 Frankfurt am Main

Kontakt: arbeitskreise@diir.de

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