Checkliste zur Prüfung der Datenschutzorganisation

DIIR-Arbeitskreis Interne Revision & Datenschutz

DIIR Deutsches Institut für Interne Revision e.V.

Vorwort

Der Datenschutz erfährt durch die EU-Datenschutz-Grundverordnung (DS-GVO) sowie die damit korrespondierenden nationalen Gesetze (insbesondere das über das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) neugefasste Bundesdatenschutzgesetz (BDSG)) sowie Landesdatenschutzgesetze für die jeweiligen Landesbehörden und Kommunalverwaltungen) einen neuen Ansatzpunkt. Hieraus ergeben sich höhere Anforderungen zur Einrichtung einer dokumentierten und wirksamen Datenschutzorganisation insbesondere in Hinblick auf die Rechenschaftspflichten und Haftungs-/Sanktionsrisiken (Bußgeld bis zu 20 Mio. € oder bis zu 4% des Jahresumsatzes der Unternehmensgruppe).

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. Diese Checkliste ist bereits zur Überprüfung innerhalb der Umsetzungsfrist (bis Mai 2018) im Sinne eines Readiness-Checks angedacht und kann anschließend für Folgeprüfungen verwendet werden. Unabhängig von Prüfungen kann diese Übersicht einen wichtigen Rahmen für die im Kontext des Datenschutzes zu beachtenden Ansätze und Regularien darstellen.

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

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 aktuellen 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 ist 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 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 neugestaltete Bundesdatenschutzgesetz die unmittelbar geltende DS-GVO. Zudem sind Anpassungen in den Landesdatenschutzgesetzen zu erwarten.

- Fällt das Unternehmen unter den Anwendungsbereich des DSAnpUG-EU?
- Gibt es andere Rechtsvorschriften des Bundes über den Datenschutz, die den Vorschriften des DSAnpUG-EU/BDSG-neu vorgehen?
- Werden deren wesentliche Regelungsinhalte betrachtet?
    - Rechtmäßigkeit der Verarbeitung (§ 47 BDSG, Artikel 6 DS-GVO)
    - Einwilligung (§ 51 BDSG, Artikel 7 DS-GVO)
    - Besondere Kategorien von Daten (§ 51(5) BDSG sowie Artikel 9 DS-GVO)
    - Informationspflichten und Auskunftsrechte (§§ 32,33, 34 BDSG, Artikel 12, 14, 15, 18 DS-GVO)
    - Videoüberwachung (§4 BDSG)

Über die DS-GVO ergeben sich einigen Bereichen Anpassungsbedarfe. . Im Wesentlichen sind das:

- Erlaubnis zur Erhebung und Verarbeitung personenbezogener Daten
    - Im Wesentlichen keine Änderung zum bisherigen BDSG
    - Auch bei der DS-GVO gilt ein Verbot mit Erlaubnisvorbehalt (Art. 6 DS-GVO)
        - Rechtliche Verpflichtung
        - Vertrag/Vorvertrag (Rechtsgeschäft)
        - Überwiegendes Interesse
        - Vereinbarung mit bestehenden Primärzwecken
        - Einwilligung
        - Schutz lebenswichtiger Interessen
- Anpassung der 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, inklusive Informationspflichten
- 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.

3.1 Datenschutzorganisation

Gegenstand dieses Abschnitts ist es, die Sicherheit und Ordnungsmäßigkeit der allgemeinen Verarbeitung von personenbezogenen bzw. -beziehbaren Daten festzustellen. 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?
  - Sitzt die verantwortliche Stelle im Ausland?
- Gibt es besondere lokale/nationale Anforderungen an den Datenschutz bzw. die Datenschutzorganisation?
- Aufbau der Datenschutzorganisation
  - Gibt es eine zentrale/dezentrale Datenschutzorganisation?

- Gibt es eine Mischform?

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 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 er in seiner Funktion der Geschäftsführung unmittelbar unterstellt und unterliegt er in der Ausübung seiner Tätigkeiten keiner fachlichen Weisung durch die Geschäfts- und Bereichsleitung? Gibt es eine Tätigkeits-/Aufgabenbeschreibung mit klaren Befugnissen, Rechten und Verpflichtungen?
- Gibt es 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? Verfügt er über die erforderliche Sachkenntnis?
- Stehen seine anderen dienstlichen Aufgaben innerhalb der betrieblichen Struktur in keinem Konflikt mit seiner Tätigkeit als betrieblicher Datenschutzbeauftragter des Unternehmens?
- Gibt es ein regelmäßiges Reporting? Wie wird dieses nachgehalten (Dokumentation)?
- Gibt es einen Jahres- oder Quartalsbericht an die verantwortliche Stelle (z. B. Geschäftsführung, Vorstand)?

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 er regelmäßigen Kontakt zur zuständigen Aufsichtsbehörde in Fragen des Beschäftigtendatenschutzes und des Schutzes der personenbezogenen Daten der Betroffenen?
- Werden regelmäßige Sensibilisierungs- und Schulungsmaßnahmen durch den betrieblichen Datenschutzbeauftragten durchgeführt (idealerweise als Methodenmix von arbeitsplatzbezogener Schulung bis hin zu E-Learning-Maßnahmen)?

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?
- 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 Einsatz von IT-Systemen

Die verantwortliche Stelle hat die erforderliche Dokumentation der automatisierten Datenverarbeitung sicherzustellen. Das Unternehmen sollte sich bei der Auswahl angemessener technischer und organisatorischer Sicherheitsmaßnahmen und dem Nachweis einer ordnungsgemäßen und wirksamen Umsetzung an den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der vom BSI definierten Vorgehensweise gemäß Standards 100-1 bis 100-3 orientieren.

- Führt der betriebliche Datenschutzbeauftragte die Validierung des Verfahrensverzeichnisses in Übereinstimmung mit den Anforderungen der DS-GVO durch?
- Kann das Verfahrensverzeichnis jederzeit stichprobenartig auf Aktualität und angemessene Dokumentation der aufgeführten Sachverhalte geprüft werden?
- Werden Auftragsverarbeitungen ausschließlich auf Basis einer schriftlichen Vereinbarung durchgeführt, falls diese in einzelnen Fachverfahren stattfinden?
  Sind die Vereinbarungen Bestandteil der Dokumentation des IT-Einsatzes?
- Sind administrative Änderungen an den IT-Systemen nur durch einzelne, explizit berechtigte Mitarbeiterinnen und Mitarbeitern möglich?
- Wurden im Unternehmen konkrete technische und organisatorische Maßnahmen für die Durchführung der administrativen Tätigkeiten an den erfassten Systemen getroffen?
- Erfüllen die durch die Unternehmen getroffenen Maßnahmen zur Dokumentation von Änderungen an informationstechnischen Geräten, Programmen und Verfahren die Anforderungen der DS-GVO?
- Werden Änderungen werden zunächst auf Testsystemen durchgeführt? Wird die Durchführung der Tests hierbei schriftlich dokumentiert?
- Wurde ein IT-Sicherheitsbeauftragter benannt?

- Sind die Aufgaben des IT-Sicherheitsbeauftragten in einer entsprechenden Richtlinie festgelegt?
- Ist der IT-Sicherheitsbeauftragte für die Erstellung und Fortschreibung der Sicherheitskonzeption und das Aufrechterhalten des Sicherheitsniveaus verantwortlich?
- Erfolgt die Freigabe von Systemänderungen nach Abstimmung mit dem IT-Sicherheitsbeauftragten?

3.4 Anpassung der Aufbauorganisation an das One-Stop-Shop-Prinzip

Das One-Stop-Shop-Prinzip ist eine Neuerung aus der DS-GVO. Es 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. Das Unternehmen hat sich bei der Anpassung der Aufbauorganisation an den internen Richtlinien, in denen Aspekte der IT-Sicherheit geregelt sind, zu orientieren.

- Sind in den Vorgaben die Ansprechpartner und das Vorgehen zur Bearbeitung, Dokumentation und Nachbereitung von Sicherheits- und Datenschutzvorfällen festgelegt?
- Werden Sicherheits- und Datenschutzvorfälle durch ein eigens hierfür festgelegtes Prozedere mit Krisenmanagement und Datenschutzbeauftragtem sowie ggf. zusätzlichen Mitgliedern bearbeitet?
- Werden Sicherheits- und Datenschutzvorfälle schriftlich nachbereitet, da die Aufsichtsbehörde deren Dokumentation stichprobenartig vor Ort prüfen kann.
- Nutzt der Datenschutzbeauftragte geeignete Prozesse für die Umsetzung der Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten?

Dem Datenschutzbeauftragten 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 Datenschutzbeauftragten in entsprechende interne Melde- / Informationsprozesse zwingend erforderlich.

- Ist sichergestellt, dass alle meldepflichtigen Vorgänge entsprechend den Vorgaben (siehe Abschnitt 2) fristgerecht zentral verarbeitet werden können?
- Gibt es einen Reaktionsplan bei Verletzung des Schutzes personenbezogener Daten (Art. 33, 34 DS-GVO)?

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

- Prüft der Datenschutzbeauftragte regelmäßig die angemessene Umsetzung der technischen und organisatorischen Maßnahmen zur Berichtigung, Löschung und Sperrung personenbezogener Daten?

4 Kommunikation und Prozesse

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.

4.1 Kommunikation der Regelungen zum Datenschutz

- Werden/wurden regelmäßige Schulungsmaßnahmen zur Sensibilisierung bzw. Unterweisung angeboten/durchgeführt? (Information und Kommunikation, Kenntnisüberprüfung, Nachweis der Belehrung, Teilnahmebescheinigung und -quote, regelmäßige Wiederholung)
- Wie erfolgt die Verpflichtung auf 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 Anpassung der internen Prozesse an die EU-Datenschutz-Grundverordnung

- Sind bestehende Betriebsvereinbarungen im Einklang mit der Datenschutz-Grundverordnung? Es ist zu prüfen, inwieweit bestehende Betriebsvereinbarungen den Anforderungen des Art. 88 DS-GVO entsprechen. Sie dürfen das Schutzniveau der DS-GVO nicht unterschreiten. Regelungsbereich und Inhalt der Betriebsvereinbarungen sind auf die Anforderungen des Art. 88 Abs. 1 und 2 zu beschränken.
- Sind bestehende Einwilligungserklärungen weiterhin wirksam?

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

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.

- Ist die Auftragsverarbeitung vorhanden und kontrolliert?
- Wird sichergestellt, dass die Auftragsverarbeitung den Anforderungen des Art. 28 entspricht?
- Erfolgt die Verarbeitung auf der Grundlage eines gültigen Vertrages zwischen dem Verantwortlichen und dem Auftragsverarbeiter? Die Mindestinhalte dieses Vertrages sind im Art. 28 Abs. 3 DS-GVO definiert.

Vor dem Hintergrund der gemeinsamen Haftung von Verantwortlichem und Auftragsverarbeiter gem. Art. 82 DS-GVO ist ebenfalls zu prüfen, inwieweit das Unternehmen selbst als Auftragsverarbeiter tätig ist.

- Wird sichergestellt, dass das Unternehmen ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DS-GVO führt und funktionierende Meldeprozesse zur Meldung von Datenschutzpannen innerhalb von 72 Stunden hat?
- Sind automatisierte Kontrollmechanismen für die Entdeckung von Datenmissbrauch/Datenverlust vorhanden (Leakage Prevention)?

4.3 Prüfung datenschutzrelevanter externer Prozesse

- Bestehen Auftragsverarbeitungen mit externen Anbietern?
- Sind Einwilligungen (soweit erforderlich) vorhanden?
- Wie wird mit Widersprüchen umgegangen (Werbung/Kommunikation)?
- Sind im Falle der Präsenz in sozialen Medien die Prozesse mit dem Datenschutzbeauftragten/Datenschutzverantwortlichen vor Ort abgestimmt?

4.4 Monitoring und laufende Anpassung des Datenschutzes

- Wie ist die generelle Nachverfolgung von Fehlermeldungen geregelt?
- Werden Feststellungen vorangegangener Prüfungen berücksichtigt?
- Gibt es Datenschutz-KPIs (etwa für Zertifizierungsverfahren) und wie wird damit umgegangen?

4.5 Handlungsvorgaben bei Anfragen und Prüfungen der Datenschutzaufsichtsbehörden

- Gibt es (aktuelle) Handlungsvorgaben?
- Ist die unmittelbare Einbeziehung der Datenschutzorganisation sichergestellt?
- Können geeignete Dokumentationen vorgelegt werden (zu Anfragen bzw. zur Abarbeitung)?

4.6 Handlungsvorgaben bei Anfragen von Externen

- Gibt es eine abgestimmte Vorgehensweise und organisatorische Zuständigkeiten?
- Wie ist die unmittelbare Einbeziehung der Datenschutzorganisation sichergestellt (Verfahrensanweisung, Prozessbeschreibung etc.)?

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 Incidents 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 erreicht. Ebenso muss die Reaktion auf solch ein Ereignis oder ein Auskunftsersuchen an den DSB auch in der geplanten Zeit erfolgen.

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 Incidents 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 Berichtserstattung 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

Veröffentlicht im Oktober 2017 auf www.diir.de

Version 1.0