Das berufliche Leitbild der Datenschutzbeauftragten

3. Ausgabe 2016

Unter Berücksichtigung der
EU-Datenschutzgrundverordnung (EU-DSGVO)

Stand: September 2016

Publikation des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

BvD e.V.
DATENSCHUTZ GESTALTEN

VORWORT

Daten sind der zentrale Faktor in modernen Wertschöpfungsketten. Sie verdienen unsere Professionalität.

Im Rahmen der Digitalisierung rückt die Verarbeitung von Daten – insbesondere von personenbezogenen Daten – immer mehr ins Zentrum der Wertschöpfungskette. Daher steigen die Anforderungen an die Rechtmäßigkeit der Daten und die Sicherheit der Verarbeitungsprozesse stark an. Nicht nur Prozess-Know-how, auch die Datenquantität und insbesondere -qualität entscheiden über den Geschäftserfolg und sind daher als elementarer Erfolgsfaktor und Unternehmenswert zu behandeln.

Unternehmensleitung, wie auch Kunden und Mitarbeiter müssen sich im hochkomplexen und schnell verändernden Umfeld der Digitalisierung darauf verlassen können, dass sie durch qualifizierte Experten mit umfassendem Know-how begleitet und im Kontext der Sicherheit und Compliance unterstützt werden.

Die Datenschutzbeauftragten nehmen sich genau dieser Aufgaben seit Jahrzehnten an. Sie begleiten die Unternehmen auf dem Weg der Digitalisierung und haben dabei einerseits die Betroffenenrechte – insbesondere die Persönlichkeitsrechte von Kunden und Beschäftigten – und andererseits die Bedürfnisse und den Erfolg der Unternehmen im Blick. Datenschutzbeauftragte ermöglichen innovative Lösungen und schützen Unternehmenswerte wie das Unternehmensimage und den Wert der Marke, indem sie Kundenvertrauen aufbauen und erhalten. Sicherer und zulässiger Umgang mit Daten sind zunehmend Gegenstand von Kundenentscheidungen und damit ein wichtiger Wettbewerbsvorteil. In dieser Rolle helfen Datenschutzbeauftragte nicht nur, die geltenden Gesetze einzuhalten, sie tragen mit ihrem Know-how dazu bei, dass der beste Prozess mit einer sicheren Lösung zum Erfolg für alle wird.

Um all diese Herausforderungen stemmen zu können, ist eine hervorragende Qualifikation der Datenschutzbeauftragten unabdingbar. Insbesondere ist Know-how in den folgenden Bereichen erforderlich:

- Prozesse und Organisation
- IT Systeme und Applikationen
- Datenschutzrecht

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hat bereits 2004 damit begonnen, die Anforderungen an die Tätigkeit und das Know-how des Datenschutzbeauftragten zu beschreiben. 2009 entstand daraus das erste „Berufliche Leitbild der Datenschutzbeauftragten" in Europa, auf das sich Mitglieder schriftlich verpflichten müssen, um durch den BvD als entsprechend qualifiziert ausgezeichnet zu werden.

Durch diesen Prozess und die Auszeichnung „Selbstverpflichtung auf das berufliche Leitbild des Datenschutzbeauftragten" können Unternehmen und Institutionen nachweisen, dass qualifizierte Datenschutzbeauftragte benannt wurden.

Die vorliegende dritte Auflage des Leitbilds greift die Änderungen durch die DSGVO auf und stellt die neuen Aufgaben und Anforderungen ins Verhältnis zur erforderlichen Qualifikation der Datenschutzbeauftragten.

Gleichzeitig wurde die vorliegende Ausgabe um eine Detaillierungsebene gekürzt, um die Lesbarkeit zu verbessern.

Berlin, September 2016
Thomas Spaeing
Vorstandsvorsitzender

ÜBERSICHT

VORWORT 3
BEGRIFFE 6
ZUSAMMENFASSUNG 7

1 Die persönlichen und fachlichen Voraussetzungen[1] 9
1.1 Voraussetzung für die Berufsausübung 9
1.2 Fachkenntnisse und Kompetenzen 9
1.3 Weitere persönliche Voraussetzungen 11

2 Aufgaben und Leistungen der Datenschutzbeauftragten 13
2.1 Datenschutzmanagement 13
2.2 Beratungsaufgaben 16
2.3 Prüfaufgaben 17
2.4 Berichten und Informieren 20
2.5 Schulungs- und Sensibilisierungsaufgaben 21

3 Anforderungen an die Berufsausübung 22
3.1 Haltung zur Berufsausübung 22
3.2 Überprüfbarkeit 22
3.3 Verschwiegenheit und Vertraulichkeit 22
3.4 Qualitätssicherung der Aufgabenerfüllung 23
3.5 Benennung zum Datenschutzbeauftragten 24
3.6 Haftung und Versicherungspflicht 26

BEGRIFFE

Aus Gründen der besseren Lesbarkeit werden im nachfolgenden Dokument Begriffe und Abkürzung auf Basis folgender Definition verwenden:

- DSGVO: EU-Datenschutzgrundverordnung im internationalen Kontext: GDPR - General Data Protection Regulation

- Auftragsverarbeiter: Der Begriff des Auftragsverarbeiters wird in Art. 4 Nr. 8 DSGVO definiert: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- Der Verantwortliche: Der Begriff des Verantwortlichen wird in Art. 4 Nr. 7 DSGVO definiert: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

  Im nachfolgenden Dokument wird bei der Verwendung des Begriffs des Verantwortlichen mit der Begrifflichkeit des für die Verarbeitung Verantwortlichen eine erweiterte Auslegung der Definition verwendet, die den Auftragsverarbeiter inkludiert, da dieser aus Sicht der DSGVO Kapitel IV im Bereich des Datenschutz-Managements äquivalente Aufgaben hat und das Dokument so in seiner Lesbarkeit gewinnt.

- Leitung (des für die Verarbeitung Verantwortlichen): Geschäftsleitung, Vorstand, Behördenleitung oder entsprechende Personenkreise.

ZUSAMMENFASSUNG

Ausgangssituation

Die DSGVO stellt insbesondere im Kapitel IV hohe Anforderungen an die Pflichten des Verantwortlichen. Um diese Compliance-Anforderungen insbesondere auch die daraus erwachsenden Nachweispflichten erfüllen zu können und ein betriebliches Organisationsverschulden des Verantwortlichen zu vermeiden, ist der Betrieb eines Managementsystems für den Bereich Datenschutz unabdingbar.

Bewährte Beispiele von Managementsystemen sind bereits im folgenden Kontext gängige Praxis:

- Qualitätsmanagement (DIN EN ISO 9001)
- Umweltmanagement (DIN EN ISO 14001)
- Arbeits- und Gesundheitsschutz (OHSAS 18001 zukünftig DIN EN ISO 45001)
- Informationssicherheit (DIN ISO/IEC 27001)

Der Unterschied besteht allerdings darin, dass die Vorgaben vom europäischen Gesetzgeber kommen und nicht aus einer DIN EN/ISO/IEC Norm.

Umsetzung mit Unterstützung qualifizierter Datenschutzbeauftragter

Die Umsetzung des Datenschutzmanagements obliegt der Leitung des für die Verarbeitung Verantwortlichen – also der Geschäftsleitung, dem Vorstand, der Behördenleitung oder entsprechenden Personenkreisen. Um dieser Pflicht nachzukommen, ist die Unterstützung durch qualifizierte Datenschutzbeauftragte unabdingbar. Die nachfolgenden Kapitel zeigen auf, welche persönlichen und fachlichen Voraussetzungen qualifizierte Datenschutzbeauftragte mitbringen müssen, welche Aufgaben und Leistungen sie erfüllen und welche Anforderungen an die Berufsausübung ge-

stellt werden, um die Herausforderungen des Datenschutzes in einer zunehmend digitalisierten Welt und im Kontext der DSGVO erfüllen zu können:

- Die persönlichen und fachlichen Voraussetzungen (Kapitel 1)
- Aufgaben und Leistungen der Datenschutzbeauftragten (Kapitel 2)
- Anforderungen an die Berufsausübung (Kapitel 3)

Durch den Prozess der „Selbstverpflichtung auf das berufliche Leitbild der Datenschutzbeauftragten“, das in den anschließenden Kapiteln detailliert wird, kann die Leitung des für die Verarbeitung Verantwortlichen nachweisen, dass qualifizierte Datenschutzbeauftragte benannt wurden.

1 DIE PERSÖNLICHEN UND FACHLICHEN VORAUSSETZUNGEN[1]

1.1 Voraussetzung für die Berufsausübung

Die Ausübung des Berufs „Datenschutzbeauftragter" setzt voraus, dass derjenige in der Regel

- über eine angemessene Ausbildung in zumindest einer der Kategorien Organisation und Prozesse, Informations- und Kommunikationstechnologie (IuK) oder Recht besitzt und solide Grundkompetenzen in den beiden anderen Kategorien erworben hat,
- über eine mindestens 2-jährige Berufserfahrung in den genannten Bereichen verfügt und
- eine anerkannte Qualifikation zum Datenschutzbeauftragten erlangt hat.

1.2 Fachkenntnisse und Kompetenzen

Datenschutzbeauftragte verfügen unabhängig von Branche und Größe des Unternehmens bzw. der Behörde über ein Mindestmaß an Fachkenntnissen und deren praktischer Anwendung (Kompetenzen). Darüber hinaus können je nach konkreter Aufgabenstellung in dem Unternehmen bzw. der Behörde weitere individuelle Fachkenntnisse nötig werden.

1.2.1 Datenschutzrechtliche Grundkompetenzen

Datenschutzbeauftragte verfügen über Grundkompetenzen im Datenschutzrecht. Sie kennen die datenschutzrelevanten Vorschriften ihres Fachbereiches / ihrer Branche. Datenschutzbeauftragte sind in der Lage, die für das Aufgabengebiet geltenden Rechtsvorschriften anzuwenden oder sich diese zu erschließen. Grundkompetenzen umfassen die folgenden Bereiche:

- Allgemeines Persönlichkeitsrecht und Grundrechtecharta der EU mit Datenschutzbezug
- Grundlagen des europäischen und des jeweiligen nationalen Datenschutzrechts und dessen Prinzipien
- Rechtsgrundlagen der Verarbeitung personenbezogener Daten
- Datenschutzrechtliche Anforderungen beim Einsatz der IuK

[1] Konkretisierung der Anforderungen aus Art. 37 Abs. 5 DSGVO

1.2.2 IuK-Grundkompetenzen

Datenschutzbeauftragte müssen über technisches Verständnis verfügen und Sachverhalte der Informationstechnologien verstehen:

- Organisation der IuK
- Strukturen von IT-Systemen, IT-Applikationen und IT-Prozessen
- Informationssicherheitsmanagement, basierend auf den Schutzzielen der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
- Erkennen von Risiken für betroffene Personen, die aus IT-Systemen, IT-Applikationen und IT-Prozessen resultieren

Darüber hinaus können Datenschutzbeauftragte grundlegende Risiken für Rechte und Freiheit der betroffenen Personen durch die Verarbeitung personenbezogener Daten erkennen und beurteilen. Datenschutzbeauftragte sind in der Lage, grundlegende Verbesserungen unter Anwendung datenschutzfreundlicher Technologien[2] vorzuschlagen und Normen zur Informationssicherheit zu berücksichtigen.

1.2.3 Betriebswirtschaftliche und organisatorische Grundkompetenz

Datenschutzbeauftragte müssen über folgende betriebswirtschaftliche und organisatorische Grundkenntnisse verfügen, um Sachverhalte im Unternehmens- bzw. Behördenkontext beurteilen zu können:

- Unternehmens- bzw. Behördenprozesse
- Managementsysteme
- Methoden zur Risikoanalyse
- Audit- und Prüfverfahren

Datenschutzbeauftragte können Anforderungen des Datenschutzes abhängig vom jeweiligen Risiko in Prozesse einbinden.

[2] Art. 25 DSGVO

1.2.4 Erweiterte Fachkenntnisse

Zusätzlich zu den Grundkompetenzen sind je nach Branche, spezieller Unternehmens- oder Einsatzbereiche der Datenschutzbeauftragten weitere Spezialisierungen in den Bereichen Recht, Technik und Organisation erforderlich. Dieses können auch Verhaltensregeln[3] der entsprechenden Branche sein.

1.2.5 Aktualität der Fachkunde

Datenschutzbeauftragte aktualisieren und vertiefen ihr Wissen regelmäßig. Dies bezieht insbesondere gesetzliche Änderungen und aktuelle Rechtsprechung zum Datenschutz sowie neue technische Entwicklungen ein.

1.3 Weitere persönliche Voraussetzungen

1.3.1 Persönliche Integrität

Datenschutzbeauftragte, die nicht über eine ausreichende persönliche Integrität verfügen, sind für die Erfüllung der Aufgaben nicht geeignet. Dies gilt auch für Personen, die

- rechtskräftig verurteilt wurden wegen Verletzungen des Geheimnisschutzes des persönlichen Lebensbereiches oder
- infolge strafgerichtlicher Verurteilung die Fähigkeit zur Bekleidung öffentlicher Ämter nicht besitzen.

Die Tätigkeiten sollen außerdem nicht von Personen ausgeübt werden, die innerhalb der letzten zwei Jahre wegen Verletzung von Datenschutzvorschriften, IT- oder Computerstrafrecht rechtskräftig gekündigt wurden[4].

[3] Art. 40 DSGVO, [4] Verstöße gegen Berufsgeheimnisse, siehe Art. 90 Abs. 1 Satz 2 DSGVO

1.3.2 Beratungskompetenzen

Datenschutzbeauftragte verfügen unabhängig von Branche und Größe des Unternehmens bzw. der Behörde über Fertigkeiten und Fähigkeiten, die zur selbständigen Organisation ihres Arbeitsbereiches erforderlich sind.

Datenschutzbeauftragte entwickeln konstruktive Vorschläge für datenschutzkonforme Lösungen unter Berücksichtigung unterschiedlicher Interessen und sind in der Lage, Empfehlungen, Stellungnahmen und Positionen zu vertreten. Hier sind Kompetenzen wie bspw. Kommunikations- und Moderationstechniken und Problemlösungstechniken erforderlich.

1.3.3 Durchsetzungsfähigkeit des eigenen Status

Datenschutzbeauftragte können übertragene Aufgaben selbständig ausführen, den Status einfordern und Einschränkungen abwenden. Zum Status gehören insbesondere die Unabhängigkeit und die Weisungsfreiheit[5].

[5] Art. 38 Abs. 3 mit ErwGr 97 DSGVO

2 AUFGABEN UND LEISTUNGEN DER DATENSCHUTZBEAUFTRAGTEN

2.1 Datenschutzmanagement

2.1.1 Ziele und Aufgaben im Datenschutzmanagement

Um die Anforderungen des Datenschutzes vorausschauend, nachhaltig und effizient in einer Organisation zu implementieren ist ein Datenschutzmanagementsystem zu betreiben. Datenschutzbeauftragte entwickeln bzw. beraten zu betrieblichen Regelungen zum Datenschutz. Die Leitung setzt diese Regelungen in Kraft[6]. Datenschutzbeauftragte überprüfen die Umsetzung und Einhaltung der Vorgaben und informieren die Leitung über Abweichungen.

Das Datenschutzmanagementsystem stellt sicher, dass Geschäftsprozesse, Systeme und Strukturen einer Organisation inklusive interner und externer Schnittstellen regelmäßig überprüft und, wenn notwendig, angepasst werden.

In Anlehnung an bestehende Managementsysteme (DIN EN ISO 9001 Qualitätsmanagement oder DIN ISO/IEC 27001 Informationssicherheitsmanagement) sichert ein iterativer Problemlösungsprozess eine regelmäßige Überprüfung der Einhaltung und eine nachhaltige und effiziente Umsetzung der Datenschutzanforderungen in der Organisation.

2.1.2 Grundsätze und Prozesse

Das Datenschutzmanagementsystem stellt die planmäßige Umsetzung datenschutzrechtlicher Grundsätze[7] bei der Datenverarbeitung personenbezogener Daten sicher. Innerhalb des Datenschutzmanagements sind Prozesse zu definieren und regelmäßig auf ihre Wirksamkeit zu überprüfen, welche die Pflichten der für die Verarbeitung Verantwortlichen als interne Vorgabe der Organisation festschreiben.

[6] Art. 24 mit ErwGr 74 DSGVO, [7] Art. 5 DSGVO

Die Dokumentation der Überprüfung und der daraus abgeleiteten Maßnahmen stellt den Nachweis für die Leitung über die Rechtmäßigkeit der Verarbeitungstätigkeit im Einklang mit der DSGVO und über die Wirksamkeit der Datenschutzorganisation dar.

Zum Datenschutzmanagement gehören insbesondere

- ein Risikomanagement bezogen auf Datenschutzrisiken und die Sicherheit der Verarbeitung, welches die Analyse, Umsetzung, regelmäßige Überprüfung und Anpassung technischer und organisatorischer Maßnahmen umfasst,[8]
- Prozesse zur Umsetzung der Anforderung zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen[9],
- die Dokumentation der Verarbeitungstätigkeiten[10],
- die Zusammenarbeit mit der Aufsichtsbehörde[11],
- das Verfahren von erforderlichen Meldungen an die Aufsichtsbehörde[12],
- die Sicherstellung der Rechte betroffener Personen, insbesondere die Behandlung von Anfragen von betroffenen Personen,
- die Informationspflichten und die Benachrichtigung betroffener Personen bei einer Verletzung des Schutzes personenbezogener Daten,
- das Erkennen der Erforderlichkeit und die Durchführung einer Datenschutz-Folgenabschätzung und
- Umsetzung und Weiterentwicklung des Sensibilisierungs- und Schulungskonzepts[13].

2.1.3 Übersicht der Aufgaben der Datenschutzbeauftragten

Der für die Verarbeitung Verantwortliche hat die Datenschutzbeauftragten ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden, damit diese ihre Aufgaben wahrnehmen können.

[8] Art. 24, Art. 32 DSGVO, [9] Art. 25 DSGVO, [10] Art. 30 DSGVO, [11] Art. 39 Abs. 1 lit. d DSGVO,
[12] Artt. 31, 33 und 36 DSGVO, [13] Art. 39 DSGVO

Aufgabe	Quelle (DSGVO)	Beschreibung
Managementaufgaben	Art. 24 Art. 38 Abs.1 ErwGr 97	• Einbindung der Datenschutzbeauftragten in relevante Managementsysteme • Verfolgen der Ziele und Aufgaben in einem Datenschutzmanagementsystem • Fortschreibung des Datenschutzmanagement-systems
Beratungsaufgaben	Art. 38 Abs. 1, 4 Art. 39 ErwGr 77, 97	• Beratung der Leitung • Beratung der Bereiche, insbesondere der Fachabteilungen • Beratung der betroffenen Personen (Beschäftigte, Kunden, Geschäftspartner) • Beratung der Mitarbeitervertretung • Beratung in Zusammenhang mit der Datenschutz-Folgenabschätzung
Prüfaufgaben	Art. 39 ErwGr 81	• Prüfung datenverarbeitender Geschäftsprozesse und Regelungen • Prüfung von IT-Systemen • Prüfung datenschutzrelevanter Verträge • Prüfung der Dokumentation von Verarbeitungs-vorgängen insb. des Verzeichnisses von Verarbei-tungstätigkeiten • Prüfung der Angemessenheit und Einhaltung der technischen und organisatorischen Maßnahmen • Prüfung von Verfahren, die einer Daten-schutz-Folgenabschätzung unterliegen • Bearbeitung von Beschwerden und sicherheitsrelevanten Vorfällen • Prüfen von Garantien externer Dienstleister (Auftragsverarbeiter) • Veranlassen und Begleiten von Auditierungen
Berichten und Informieren	Art. 39	• Regelmäßige Unterrichtung der Leitung und an ausgewählte Fachbereiche des für die Verarbei-tung Verantwortlichen • Kommunikation mit der Aufsichtsbehörde und Externen • Regelmäßige Tätigkeitsberichte • Dokumentation der Verarbeitungsaktivitäten inkl. deren Risiko
Schulungs- und Sensibilisierungsaufgaben	Art. 39	• Fortentwicklung von Schulungskonzepten und Erstellung von Schulungs- / Sensibilisierungs-unterlagen • Umsetzung des Sensibilisierungs- und Schulungskonzepts

2.2 Beratungsaufgaben

Die Datenschutzbeauftragten beraten die Leitung, alle Fachbereiche der Verantwortlichen, sowie anlassbezogen betroffene Personen bei allen Fragen zum Datenschutz, bei der Ausgestaltung von Maßnahmen zum Datenschutz und bei der Datenschutz-Folgenabschätzung.

2.2.1 Beratungsmaßstab

Die Datenschutzbeauftragten beraten zur Einhaltung des Datenschutzes mit folgenden Zielen:

1. Schutz des Persönlichkeitsrechts der betroffenen Personen
2. Gesetzeskonforme Verarbeitung des für die Verarbeitung Verantwortlichen, also bspw. die Unternehmen und Behörden

Neben diesen Zielen sind die Wirksamkeit, Wirtschaftlichkeit, Praktikabilität, Angemessenheit sowie Akzeptanz der Maßnahmen zu berücksichtigen. Ziel der Beratung ist auch, mit einem hohen Datenschutzniveau zu einem Wettbewerbsvorteil beizutragen.

2.2.2 Beratung der Leitung

Datenschutzbeauftragte beraten die Leitung in allen Angelegenheiten, die den Datenschutz betreffen. Sie geben Hinweise auf die notwendige Festlegung der Verarbeitungszwecke, auf Benachrichtigungspflichten, zu Pflichten zur Datenschutz-Folgenabschätzung, über Meldepflichten, sowie auf die Rechtskonformität geplanter Verfahren personenbezogener Datenverarbeitung. Bei der Festlegung der technischen oder organisatorischen Schutzmaßnahmen wirken sie im Rahmen einer Angemessenheitsabwägung mit der Leitung auf die datenschutzfreundlichste Alternative hin.

2.2.3 Beratung der Bereiche, insbesondere Fachabteilungen

Datenschutzbeauftragte beraten alle relevanten Bereiche der für die Verarbeitung

Verantwortlichen, die personenbezogene Daten verarbeiten. Sie beraten insbesondere hinsichtlich der rechtlichen Voraussetzungen und bei der Planung und Durchführung der technischen und organisatorischen Maßnahmen zum Datenschutz und der Gestaltung von datenverarbeitenden Prozessen und Verfahren unter Berücksichtigung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.

2.2.4 Beratung der betroffenen Person

Wenden sich betroffene Personen an Datenschutzbeauftragte, beraten diese umfassend und vertraulich. Sie unterstützen den für die Verarbeitung Verantwortlichen dabei, den betroffenen Personen über die Verarbeitungen Auskunft zu erteilen. Sie beraten die betroffenen Personen über deren Rechte und die Möglichkeiten diese wahrzunehmen ohne die Identität der betroffenen Person zu offenbaren.

2.2.5 Beratung der Mitarbeitervertretung

Datenschutzbeauftragte beraten die Mitarbeitervertretung bei bestehenden und geplanten Verarbeitungen von personenbezogenen Beschäftigtendaten im Beschäftigungskontext[14] um die schutzwürdigen Interessen der Beschäftigten sicherzustellen.

2.3 Prüfaufgaben

Datenschutzbeauftragte prüfen Geschäftsprozesse, Systeme und Organisationsstrukturen und die damit verbundenen technischen und organisatorischen Maßnahmen auf die Einhaltung datenschutzrechtlicher Vorgaben. Diese ergeben sich bspw. aus gesetzlichen Anforderungen, genehmigten Verhaltensregelungen[15], aus Vorgaben eines (genehmigten) Zertifizierungsverfahrens oder aus unternehmensinternen Datenschutzvorschriften. Die Überprüfungen haben sich am aktuellen Stand der Technik zu orientieren.

Zur Durchführung der Prüfaufgaben erstellen Datenschutzbeauftragte ein Prüfkonzept, welches Umfang, Inhalte, Prüfzyklen und Schwerpunkte definiert. Dieses un-

[14] Art. 88 mit ErwGr 155 DSGVO, [15] Art. 40 DSGVO

terliegt der Weisungsfreiheit der Datenschutzbeauftragten und orientiert sich an möglichen Risiken für betroffene Personen.

Die Prüfungsergebnisse werden strukturiert dokumentiert und der Leitung des für die Verarbeitung Verantwortlichen berichtet. Hierbei ist auf festgestellte Risiken gesondert hinzuweisen.

2.3.1 Prüfmaßstäbe

Als Prüfmaßstäbe sind heranzuziehen:

- die Einhaltung der Rechtskonformität:
  - anzuwendende Gesetze
  - anzuwendende Verordnungen
  - Gerichtsurteile
  - übergreifende Kollektivvereinbarungen (bspw. Tarifvereinbarungen)
- die IT-Sicherheitsgrundsätze und der Informationssicherheitsstandard, die sich am „Stand der Technik“ orientieren:
  - Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit
  - Vorgaben aus Informationssicherheitsstandards wie die ISO/IEC 27000-Reihe und Regelungen des BSI IT-Grundschutz
- Anwendungen der Grundsätze „Datenschutz durch Technikgestaltung“ und „datenschutzfreundliche Voreinstellungen“
- Anerkannte branchenspezifischen Vorgaben – Durch Verbände oder durch andere Vereinigungen erarbeitete Verhaltensregelungen, die der DSGVO entsprechen und von Aufsichtsbehörden anerkannt sind
- individuelle vertragliche Vereinbarungen mit Partnern in Geschäftsbeziehungen, incl. der Formulierung von Einwilligungserklärungen u.a.
- betriebsinterne Regelungen:
  - Unternehmensrichtlinien und Anweisungen (ggf. auch als Grundlage einer Zertifizierung)
  - Betriebs- bzw. Dienstvereinbarungen

2.3.2 Prüfmethoden

Vor der Durchführung einer Prüf-und Kontrollaufgabe definieren Datenschutzbeauftragte das zu prüfende Projekt / den Prüfgegenstand.
Sie bestimmen im Rahmen ihrer Weisungsfreiheit die notwendigen Prüfverfahren, wie bspw.:

- rechtliche Prüfung organisatorischer Vorgaben, Dokumente und Verträge
- Begehung von Örtlichkeiten
- Befragung verantwortlicher und ausführender Personen
- Stichprobenüberprüfung von Dokumenten und Daten
- automatisierte Testverfahren
- Auswertung von Aufzeichnungen wie beispielsweise Log-Dateien, Protokolle, Logbücher

Das Prüfungsergebnis wird in einem Prüfbericht dokumentiert und an den für die Verarbeitung Verantwortlichen kommuniziert.

2.3.3 Überprüfung vor Einführung oder Änderung einer Verarbeitung

Der für die Verarbeitung Verantwortliche bindet Datenschutzbeauftragte vor Einführung und Änderung einer Verarbeitung ordnungsgemäß und frühzeitig ein[16]. Datenschutzbeauftragte beraten im Rahmen der Datenschutz-Folgenabschätzung den für die Verarbeitung Verantwortlichen[17] und prüfen die Einhaltung der DSGVO.

Ist eine Datenschutz-Folgenabschätzung durchzuführen, wird diese maßgeblich durch den Datenschutzbeauftragten begleitet[18].

2.3.4 Veranlassung und Begleitung von Auditierungen

In Abstimmung mit dem für die Verarbeitung Verantwortlichen begleiten Datenschutzbeauftragte die Durchführung von Auditierungen. Datenschutzbeauftragte formulieren Prüfgegenstände und bewerten Ergebnisse. Sie beraten über notwendige Korrekturen bei Abweichungen.

[16] Art. 38 Abs. 1 DSGVO, [17] Art. 39 Abs. 1 lit. c. DSGVO, [18] Art. 35 Abs. 2 DSGVO

2.4 Berichten und Informieren

Datenschutzbeauftragte informieren und berichten[19] gegenüber internen Stellen regelmäßig oder anlassbezogen. Empfänger ist insbesondere die Leitung. Darüber hinaus können anlassbezogen weitere Stellen wie bspw. Aufsichtsbehörden, betroffene Personen oder die Mitarbeitervertretung zu informieren sein.

2.4.1 Regelmäßige Unterrichtung der Leitung

Die Leitung ist als für die Verarbeitung Verantwortlicher erster Empfänger von Berichten und Informationen der Datenschutzbeauftragten. Diese unterrichten die Leitung über

- Datenschutzsituationen an verarbeitenden Stellen im Allgemeinen
- Verstöße gegen gesetzliche, vertragliche und interne Vorschriften
- Umsetzungshindernisse oder Bearbeitungsrisiken
- Optimierungspotenziale
- Statusberichte zur Aktivitäts- und Maßnahmenplanung
- durchgeführte und geplante Tätigkeiten als Datenschutzbeauftragte
- Änderungen rechtlicher oder technischer Rahmenbedingungen

Darüber hinaus können Berichtslinien in der internen Datenschutzorganisation und mögliche Datenschutzkoordinatoren aus den Bereichen IT, HR etc. definiert werden. Unabhängig von beschriebenen Kommunikationspflichten sollten Datenschutzbeauftragte durch einen regelmäßigen Tätigkeitsbericht gegenüber der Unternehmens- und Behördenleitung über den Stand zum Datenschutz berichten. Zu empfehlen ist ein jährlicher Bericht, wenn nicht Anforderungen des Verantwortlichen ein anderes Berichtsintervall angemessen erscheinen lassen.

2.4.2 Kommunikation mit der Datenschutzaufsichtsbehörde

Datenschutzbeauftragte informieren die jeweilige Aufsichtsbehörde

- auf Verlangen der Aufsichtsbehörde
- auf Verlangen der Unternehmens- bzw. Behördenleitung

[19] Art. 38 Abs. 3 Satz 3 DSGVO

Darüber hinaus können Datenschutzbeauftragte nach eigenem Ermessen ihr Recht auf Zusammenarbeit[20] mit der Aufsichtsbehörde in Anspruch nehmen

- bei unlösbaren Konflikten um die Rechtmäßigkeit von Verfahren und Maßnahmen zwischen für die Verarbeitung Veranwortlichen und Datenschutzbeauftragten,
- wenn Zweifelsfälle bestehen
- sowie bei Konflikten um die Unabhängigkeit der Datenschutzbeauftragten.

2.4.3 Umfang und Grenzen

Die Verschwiegenheit und Weisungsfreiheit entbinden Datenschutzbeauftragte nicht von ihren Informations- und Berichtspflichten. Die gesetzliche Vertraulichkeitsverpflichtung (z.B. gegenüber betroffenen Personen) kann diese Berichtspflicht begrenzen. Aus diesem Grund sollten Berichte und Informationen sachbezogen ohne Nennung von betroffenen Personen erfolgen.

2.5 Schulungs- und Sensibilisierungsaufgaben

Die Schulung und Sensibilisierung[21] der Leitung und der Mitarbeiter ist eine grundlegende Voraussetzung für ein funktionierendes Datenschutzmanagement. Datenschutzbeauftragte legen Inhalte und Umfang nach den Datenschutzanforderungen der Leitung fest. Sie können Aufgaben in diesem Bereich delegieren und müssen Qualität und Umsetzung der Maßnahmen überwachen.

Schulungsinhalte und Umfang sind nach Art der Verarbeitung und entsprechend der Datenschutzrisiken zu gestalten. Sie sind zielgruppenspezifisch und handlungsorientiert durchzuführen. Typische Zielgruppen sind neben Personen, die personenbezogene Daten verarbeiten, auch Führungskräfte und die Mitarbeitervertretung. Datenschutzbeauftragte erstellen ein Konzept, welches Schulungs- und Sensibilisierungsmaßnahmen sowie deren Inhalt, Umfang, Zyklen und Mittel definiert und dabei Art, Umfang, Umstände und Zwecke der Verarbeitung berücksichtigt. Dieses Konzept ist Teil des Datenschutzmanagementsystems (vgl. Kap. 2.1).

[20] Art. 39 Abs.1 lit. d DSGVO, [21] Art. 39 Abs. 1 lit. b DSGVO

3 ANFORDERUNGEN AN DIE BERUFSAUSÜBUNG

3.1 Haltung zur Berufsausübung

Datenschutzbeauftragte verstehen sich als Interessensvertreter sowohl der betroffenen Personen als auch der für die Verarbeitung Verantwortlichen. Sie agieren daher in einem Spannungsfeld unterschiedlicher Positionen, in dem sie konstruktive Lösungen entwickeln müssen.

Datenschutzbeauftragte argumentieren auf gängigen Rechtsauffassungen, begründen nachvollziehbar und machen deutlich, wenn sie persönliche Ansichten vertreten. Datenschutzbeauftragte bemühen sich um neutrale und objektive Bewertungen von Sachverhalten.

Soweit Datenschutzbeauftragte einen Interessenskonflikt im Sinne von Kap. 3.5.4 erkennen, sollten diese den Sachverhalt den für die Verarbeitung Verantwortlichen darlegen und sich ggf. auch mit der zuständigen Aufsichtsbehörde darüber abstimmen.

Datenschutzbeauftragte gewährleisten eine hohe Qualität ihrer Tätigkeit. Sie holen sich in Zweifelsfällen fachspezifische Unterstützung. Datenschutzbeauftragte sind in Bereichen tätig, für die sie ausreichendes Fachwissen besitzen. Bei neuen Anforderungen qualifizieren sie sich zeitnah.

3.2 Überprüfbarkeit

Datenschutzbeauftragte dokumentieren ihr Handeln. Dokumentationen sind zutreffend und vollständig. Diese Dokumentationen können auch als Nachweise im Rahmen des Datenschutzmanagements dienen.

3.3 Verschwiegenheit und Vertraulichkeit

Datenschutzbeauftragte sind zu strikter Einhaltung der Verschwiegenheit verpflichtet. Diese Pflichten beziehen sich auf alles, was ihnen in Ausübung ihres Berufes bekannt wird. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Datenschutzbeauftragte behandeln die Einzelheiten von Beschwerden, Datenschutzverletzungen oder die Identität von Informanten vertraulich. Sie halten die Identität der Beschwerdeführer geheim, sofern diese nicht ausdrücklich mit der Offenbarung ihrer Identität einverstanden sind.

Darüber hinaus sind sie zur Verschwiegenheit über alle personenbezogene Informationen sowie Amts-, Betriebs- und Geschäftsgeheimnisse, die sie während ihrer Tätigkeit Kenntnis erlangen, verpflichtet. Dies gilt auch über das Ende ihrer Tätigkeit als Datenschutzbeauftragte hinaus.

Beschäftigen Datenschutzbeauftragte oder die für die Verarbeitung Verantwortlichen Mitarbeiter mit Aufgaben in der Datenschutzorganisation (bspw. Datenschutzkoordinatoren), so sind diese zur gleichen Verschwiegenheit zu verpflichten.

3.4 Qualitätssicherung der Aufgabenerfüllung

Zur Gewährleistung der zuverlässigen Berufsausübung sind geeignete Maßnahmen zur Qualitätskontrolle zu ergreifen.

3.4.1 Eigenkontrolle

Die Qualitätssicherung einer vollständigen und korrekten Aufgabenerfüllung sollen durch Eigenkontrolle und Reflektion gewährleistet werden.

Als weitere Maßnahme sind ein regelmäßiger Austausch und Möglichkeiten zur Nutzung externer Fachkunde und Netzwerke zu sehen. Dazu zählen auch Fort- und Weiterbildungen, die bspw. mit Prüfungen abschließen.

Weitere Möglichkeiten ergeben sich aus Auditierungen sowie Beratungen mit Aufsichtsbehörden, um Ergebnisse und Einschätzungen zu optimieren.

3.4.2 Kontrolle durch den Berufsverband

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. stellt im Rahmen des Selbstverpflichtungsverfahrens geeignete Kontrollmaßnahmen zur Qualitätssicherung bereit. Die auf dieses Berufsbild verpflichteten Datenschutzbeauftragten müssen an diesen Kontrollmaßnahmen teilnehmen. Andernfalls wird das Siegel zur Selbstverpflichtung durch den Berufsverband entzogen.

Das Verfahren ist transparent und in den Dokumenten zur Selbstverpflichtung (www.bvdnet.de) beschrieben. Das Siegel ist personalisiert und beim Berufsverband überprüfbar.

3.5 Benennung zum Datenschutzbeauftragten

3.5.1 Voraussetzung der Benennung

Voraussetzungen zu einer ordnungsgemäßen Benennung zum Datenschutzbeauftragten ergeben sich aus

- persönlichen und fachlichen Voraussetzungen (vgl. Kapitel 1) und
- der Ausübung von Pflichten und Aufgaben in vollständiger Unabhängigkeit und ohne Interessenkonflikt[22].

Zum Beauftragten für den Datenschutz kann auch eine Person auf Grundlage eines Dienstleistungsvertrages benannt werden[23].

3.5.2 Form und Verfahren der Benennung

Datenschutzbeauftragte sind durch den für die Verarbeitung Verantwortlichen, jeweils von der Leitung, schriftlich zu benennen. Datenschutzbeauftragte können ihre Aufgaben für mehrere miteinander verbundene und nicht verbundene Unternehmen oder Behörden wahrnehmen, solange dies nicht ihre Unabhängigkeit gefährdet. Es können ein oder mehrere Stellvertreter benannt werden.

[22] Art. 38 Abs. 6 mit ErwGr 97 DSGVO, [23] Art. 37 Abs. 6 DSGVO,

Die Benennung ist der zuständigen Aufsichtsbehörde mitzuteilen und die Kontaktdaten sind zu veröffentlichen[24].

3.5.3 Dauer, Laufzeiten der Benennung

Die Benennung zum Datenschutzbeauftragten kann zeitlich befristet werden. Langfristige Benennungen werden empfohlen. Die Laufzeit für die Erstbenennung sollte fünf Jahre, die für Wiederbenennung drei Jahre nicht unterschreiten.

3.5.4 Unabhängigkeit der Berufsausübung

Datenschutzbeauftragte müssen ihre Aufgaben in vollständiger Unabhängigkeit und Weisungsfreiheit ausüben können[25]. Unabhängig sind sie, wenn sie frei von fachlichen und zeitlichen Interessenkonflikten sind, ihre Datenschutztätigkeit weisungsfrei und eigenverantwortlich gestalten können und über ausreichende Ressourcen verfügen.

Interessenkonflikte liegen vor, wenn die Tätigkeiten der Datenschutzbeauftragten mit anderen Aufgaben z.B. in einem zeitlichen, fachlichen oder weisungsgebundenen Widerspruch stehen. Dies ist auch dann der Fall, wenn Datenschutzbeauftragte konkurrierende Aufgaben wahrnehmen, bspw. auch bei verbundenen Unternehmen. Für die Verarbeitung Verantwortliche sind verpflichtet, Datenschutzbeauftragten angemessene Ressourcen zur Verfügung zu stellen. Datenschutzbeauftragte schaffen sich räumlich, technisch und organisatorisch die erforderlichen Rahmenbedingungen für Vertraulichkeit und Sicherheit der Arbeitsmaterialien.

[24] Art. 37 Abs. 7 DSGVO, [25] Art. 38 Abs. 6 mit ErwGr 97 DSGVO

3.6 Haftung und Versicherungspflicht

Datenschutzbeauftragte haften nicht für die Datenverarbeitung oder Datenschutzverstöße des für die Verarbeitung Verantwortlichen (des Unternehmens), da sie im Rahmen ihrer Stellung keine Weisungen erteilen können und damit über Datenschutzverstöße nur berichten, aber die Ursachen nicht selbst abstellen können.

Soweit Datenschutzbeauftragte für durch sie schuldhaft verursachte Personen-, Sach- und Vermögensschäden haften, greifen für interne Datenschutzbeauftragte als Angestellte die durch die arbeitsrechtliche Rechtsprechung ausgeprägten Haftungsbeschränkungen für Angestellte.

Externe Datenschutzbeauftragte können in Benennungsverträgen Haftungsbeschränkungen vorsehen.

Externe Datenschutzbeauftragte schließen eine Berufshaftpflichtversicherung zur Deckung der sich aus ihrer Berufstätigkeit ergebenden Haftungsgefahren für Vermögensschäden ab und halten die Versicherung während der Dauer ihrer Benennung aufrecht.

Revision:
V03: 2016 unter Berücksichtigung der DSGVO

Das berufliche Leitbild des Datenschutzbeauftragten ist ein Arbeitsergebnis des Arbeitsausschusses Berufsbild mit den ständigen Mitgliedern
Monika Egle, Barbara Stöferle, Jörg Becker, Jürgen Hartz, Dr. Kai-Uwe Loser,
Klaus Mönikes, Gerfried Riekewolt, Thomas Spaeing

Lektorat: Frank Spaeing

DATENSCHUTZ GESTALTEN

Herausgeber:
Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Budapester Straße 31
10787 Berlin

Tel: +49 30 2636 7760
Fax: +49 30 2636 7763

E-Mail: bvd-gs@bvdnet.de
Internet: www.bvdnet.de