# GDD-RATGEBER

2. AUFLAGE

© Sergey Nivens - Fotolia.com

# Der betriebliche Datenschutzbeauftragte nach DS-GVO und BDSG

- Benennung
- Aufgaben und Rechtsstellung

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

# Der betriebliche Datenschutzbeauftragte nach DS-GVO und BDSG

**Der betriebliche Datenschutzbeauftragte nach DS-GVO und BDSG**
**- Arbeitshilfe für die betriebliche Praxis -**

**Version: 2.1 (Stand: Juli 2019)**
**Herausgeber: Gesellschaft für Datenschutz und Datensicherheit e.V.**
**Verfasserin: Yvette Reif**

Für eine bessere Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen sollen gleichermaßen für beiderlei Geschlecht gelten.

- Alle Rechte vorbehalten -

© Juli 2019 Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)
Heinrich-Böll-Ring 10 • 53119 Bonn

Telefon: (0228) 96 96 75-00
Telefax: (0228) 96 96 75-25
E-Mail: info@gdd.de
Internet: www.gdd.de

Nachdruck und Vervielfältigung jeder Art sind nur mit ausdrücklicher Genehmigung der GDD gestattet.

# Vorwort

Der Datenschutzbeauftragte hat eine zentrale Rolle im Hinblick auf die Gewährleistung des Datenschutzes im Unternehmen. Er berät die Unternehmensleitung sowie die Fachabteilungen, die mit personenbezogenen Daten umgehen, im Hinblick auf den Datenschutz und überwacht die Einhaltung der bestehenden datenschutzrechtlichen Vorgaben beim Verantwortlichen bzw. Auftragsverarbeiter. Hierdurch leistet er einen wichtigen Beitrag zum Persönlichkeitsrechtsschutz und hilft zugleich Unternehmensrisiken zu reduzieren, welche sich vor dem Hintergrund der immensen Bußgeldandrohungen der DS-GVO in neuem Maße ergeben. Die Aufgabe des Datenschutzbeauftragten erschöpft sich dabei nicht bloß in der Unterrichtung des Verantwortlichen bzw. Auftragsverarbeiters über dessen Verpflichtungen. Er ist vielmehr aktiver Berater in der Weise, dass er an der Legalisierung legitimer Verarbeitungen mitwirkt und Lösungswege aufzeigt. Er unterstützt bei konkreten datenschutzrechtlichen Fragen, Prozesseinführungen sowie -änderungen.

Der vorliegende Ratgeber beleuchtet im Detail, unter welchen Voraussetzungen ein Datenschutzbeauftragter zu benennen ist und welche Aufgaben und welche Rechtsstellung ihm zukommen. Abgerundet werden die Ausführungen durch praxisrelevante Muster und Materialien.

Bonn, im Juli 2019 Vorstand der GDD

**Vorstand:** Prof. Dr. Rolf Schwartmann (Vorsitzender), Dr. Dirk Bornemann, Harald Eul, Prof. Dr. Rainer W. Gerling, Bettina Herman, Gabriela Krader, Prof. Dr. Michael Meier, Thomas Müthlein, Prof. Dr. Gregor Thüsing, Dr. Martin Zilkens

# Inhaltsverzeichnis

**Vorwort** 3

**Inhaltsverzeichnis** 5

**Literatur zum Datenschutzbeauftragten** 9

**Teil A** 13

**Das Recht des betrieblichen Datenschutzbeauftragten** 13

**1. Rechtsgrundlagen** 15

**2. Einführung** 21

**3. Benennung eines Datenschutzbeauftragten** 22

3.1 Kriterien für das Eingreifen der Pflicht zur Benennung 22

3.2 Überblick: Wann ist ein Datenschutzbeauftragter zu benennen? 29

3.3 Anforderungen an die Benennung 30

3.4 Arbeits- und mitbestimmungsrechtliche Aspekte der Benennung 31

3.5 Veröffentlichung/Mitteilung der Kontaktdaten des Datenschutzbeauftragten 32

3.6 Möglichkeit der Benennung eines externen Datenschutzbeauftragten 33

3.7 Exkurs: Rechtsanwälte als Datenschutzbeauftragte 36

3.8 Möglichkeit der Benennung eines gemeinsamen Datenschutzbeauftragten / von Verbandsdatenschutzbeauftragten 37

3.9 Fortgeltung von Altbestellungen 38

**4. Anforderungen an den Datenschutzbeauftragten** 39

4.1 Einführung 39

4.2 Berufliche Qualifikation (insbes. Fachwissen) 40

4.3 Fähigkeit zur Aufgabenerfüllung 43

4.3.1 Allgemeines 43

4.3.2 Keine Interessenkonflikte 44

4.3.3 Zusammenfassung 47

**5. Aufgaben des Datenschutzbeauftragten 48**

5.1 Überblick 48

5.2 Unterrichtung und Beratung 49

5.3 Überwachung der Einhaltung des Datenschutzes 50

5.4 Aufgaben im Zusammenhang mit der Datenschutz-Folgenabschätzung 53

5.5 Zusammenarbeit mit der Aufsichtsbehörde 54

5.6 „Anwalt der betroffenen Personen“ 55

5.7 Verpflichtung zur risikoorientierten Tätigkeit 57

5.8 Bericht an die Leitung und Dokumentation der Tätigkeit als Datenschutzbeauftragter 58

**6. Rechtsstellung des Datenschutzbeauftragten 60**

6.1 Überblick 60

6.2 Unabhängigkeit, insbes. Weisungsfreiheit und organisatorische Stellung des Datenschutzbeauftragten 61

6.3 Anspruch auf Einbindung, Zugang und Ressourcen 63

6.4 Abberufungs- und Kündigungsschutz 68

6.5 Benachteiligungsverbot 73

**7. Haftung und Sanktionen 74**

7.1 Allgemeines 74

7.2 Haftung des Datenschutzbeauftragten 74

7.2.1 Haftung im Verhältnis zur betroffenen Person 74

7.2.2 Haftung im Verhältnis zur benennenden Stelle 78

7.3 Strafbarkeit des Datenschutzbeauftragten 80

7.4 Sanktionen nach Art. 83 DS-GVO 81

**Teil B 85**

**Muster und Materialien 85**

**1. Benennung eines/einer Datenschutzbeauftragten (Muster) 87**

**2. Stellenbeschreibung für eine/n Datenschutzbeauftragte/n (Muster) 89**

**3. DSK Kurzpapier Nr. 12 „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“ (Stand: 17.12.2018) 95**

**4. Art.-29-Datenschutzgruppe: Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), angenommen am 13.12.2016, zuletzt überarbeitet und angenommen am 05.04.2017 (WP 243 rev.01), bestätigt durch den EDSA am 25.05.2018 – Auszug – 102**

**5. Sonstige relevante Muster zum Datenschutzbeauftragten 132**

**Stichwortverzeichnis 133**

# Literatur zum Datenschutzbeauftragten

## Kommentare


- *Ehmann/Selmayr (Hrsg.)*, Datenschutz-Grundverordnung, München 2017
- *Gola (Hrsg.)*, DS-GVO, 2. Aufl., München 2018
- *Kühling/Buchner (Hrsg.)*, DS-GVO/BDSG, 2. Aufl., München 2018
- *Paal/Pauly (Hrsg.)*, DS-GVO/BDSG, 2. Aufl., München 2018
- *Schwartmann/Jaspers/Thüsing/Kugelmann (Hrsg.)*, DS-GVO/ BDSG, Heidelberg 2018
- *Simitis/Hornung/Spiecker gen. Döhmann*, Datenschutzrecht, 1. Auflage 2019
- *Sydow (Hrsg.)*, Europäische Datenschutzgrundverordnung, 2. Aufl., Baden-Baden 2018
- *Wolff/Brink (Hrsg.)*, Beck'scher Online-Kommentar Datenschutzrecht, 24. Edition, München 2018


## Handbücher / Formulare


- *Koreng/Lachenmann,* Formularhandbuch Datenschutzrecht, 2. Aufl., München 2018
- *Laue/Nink/Kremer,* Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016


## Aufsätze


*Bittner*, Der Datenschutzbeauftragte gemäß EU-Datenschutz-Grundverordnungs-Entwurf, RDV 2014, 183; *Eckhardt/Kramer/Mester*, Auswirkungen der geplanten EU-DS-GVO auf den deutschen Datenschutz, DuD 2013, 623; *Eßer/Steffen*, Zivilrechtliche Haftung des Datenschutzbeauftragten, CR 2018,

289; *Franck*, Altverhältnisse unter DS-GVO und neuem BDSG, ZD 2017, 509; *Gierschmann*, Was "bringt" deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD 2016, 51; *Jaspers/Reif*, Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung: Pflicht zur Benennung, Rechtsstellung und Aufgaben, RDV 2016, 61; *Klug*, Der Datenschutzbeauftragte in der EU - Maßgaben der Datenschutzgrundverordnung, ZD 2016, 315; *Lantwin*, Risikoberuf Datenschutzbeauftragter? Die Haftung nach der neuen DS-GVO, ZD 2017, 411; *Marschall/Müller*, Der Datenschutzbeauftragte im Unternehmen zwischen BDSG und DS-GVO, ZD 2016, 415; *Niklas/Faas*, Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung, NZA 2017, 1091; *Steffen*, Zivilrechtliche Haftung von Datenschutzbeauftragten für Bußgelder – Haftung für „durchgereichte“ Bußgelder nach der DS-GVO, DuD 2018, 145 ff.; *Weichert*, Die Zukunft des Datenschutzbeauftragten, CuA 4/2016, 8; *Wybitul/von Gierke*, Checklisten zur DSGVO – Teil 2: Pflichten und Stellung des Datenschutzbeauftragten im Unternehmen, BB 2017, 181

## Aufsichtsbehörden

- *Art.-29-Datenschutzgruppe*, WP 243 rev. 01 „Leitlinien in Bezug auf Datenschutzbeauftragte“, bestätigt durch den Europäischen Datenschutzausschuss (EDSA) am 25.05.2018; http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48137
- *Datenschutzkonferenz*, Kurzpapier Nr. 12 „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“, Stand: 17.12.2018
- *Datenschutzkonferenz*, Entschließung vom 26.04.2018 zur Datenschutzbeauftragten-Bestellpflicht nach Art. 37 Abs. 1 Buchst. c DS-GVO bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs
- *BayLDA*, FAQ Bestellpflicht von DSB wegen ständiger Beschäftigung, Stand: 19.07.2018
- *LfDI Baden-Württemberg*, Der/die betriebliche Beauftragte für den Datenschutz Teil 1 und Teil 2, Stand: 11/2018

- *Der Hessische Datenschutzbeauftragte*, Der behördliche und betriebliche Datenschutzbeauftragte nach neuem Recht, Stand: 06/2017
- *LDI NRW*, Häufig gestellte Fragen zum Datenschutzbeauftragten (FAQ), Stand: 11/2018
- *ULD*, Praxisreihe Datenschutzbestimmungen praktisch umsetzen, Band 2, Datenschutzbeauftragte, Stand: 05/2018
- *LfD Niedersachsen*, Benennung einer oder eines Datenschutzbeauftragten (DSB) nach Art. 37 Abs. 1 Buchst. b) und c) DS-GVO i.V.m. § 38 BDSG 2018: Checkliste für Verantwortliche und Auftragsverarbeiter von Unternehmen und Unternehmensgruppen, Stand: 17.07.2017
- *LfD Niedersachsen*, Benennung einer oder eines Datenschutzbeauftragten (DSB) nach Art. 37 Abs. 1 Buchst. a) DS-GVO: Checkliste für Verantwortliche von Behörden und öffentlichen Stellen, Stand: 05.07.2017
- *LfD Niedersachsen*, Die oder der Datenschutzbeauftragte (DSB) in Behörden und sonstigen öffentlichen Stellen in Niedersachsen; Hinweise für die Erstellung von Arbeitsplatz- oder Dienstpostenbeschreibungen sowie von Arbeitsplatz- oder Dienstpostenbewertungen; Aufgabenwahrnehmung durch eigenes Personal; Stand: 28.06.2018
- *LfD Niedersachsen*, Hilfestellungen für Verantwortliche und den Personalrat bei der Benennung einer oder eines gemeinsamen Datenschutzbeauftragten, Stand: 26.07.2018

# Teil A

# Das Recht des betrieblichen Datenschutzbeauftragten

1. Gesetzliche Grundlagen
2. Einführung
3. Benennung eines Datenschutzbeauftragten
4. Anforderungen an den Datenschutzbeauftragten
5. Aufgaben des Datenschutzbeauftragten
6. Rechtsstellung des Datenschutzbeauftragten
7. Haftung und Sanktionen

# 1. Rechtsgrundlagen

***Artikel 37 DS-GVO***

***Benennung eines Datenschutzbeauftragten***

***(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn***

***a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,***

***b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder***

***c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.***

***(2) Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.***

***(3) Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.***

***(4) In anderen als den in Absatz 1 genannten Fällen können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Daten-***

***schutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, handeln.***

***(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.***

***(6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.***

***(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.***

***Artikel 38 DS-GVO***

***Stellung des Datenschutzbeauftragten***

***(1) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.***

***(2) Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.***

***(3) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte***

***berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.***

***(4) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.***

***(5) Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.***

***(6) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.***

***Artikel 39 DS-GVO***

***Aufgaben des Datenschutzbeauftragten***

***(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:***

***a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;***

***b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;***

***c) Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;***

***d) Zusammenarbeit mit der Aufsichtsbehörde;***

***e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.***

***(2) Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.***

***ErwG 97 DS-GVO***

***In Fällen, in denen die Verarbeitung durch eine Behörde – mit Ausnahmen von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln –, im privaten Sektor durch einen Verantwortlichen erfolgt, dessen Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern, oder wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht, sollte der Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden. Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für***

***die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.***

***§ 38 BDSG***

***Datenschutzbeauftragte nichtöffentlicher Stellen***

***(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen[1] ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.***

***(2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.***

---

[1] Fassung des § 38 Abs. 1 Satz 1 BDSG aufgrund Beschlussfassung des Bundestages vom 27. Juni 2019 zum Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU). Die Neuregelung tritt am Tag nach Verkündung im Bundesgesetzblatt in Kraft. Dies setzt zum Zeitpunkt der Fertigstellung dieses Dokuments noch die Zustimmung des Bundesrats sowie die Unterzeichnung und Freigabe durch den Bundespräsidenten voraus.

***§ 6 BDSG***

***Stellung***

***[…]***

***(4) Die Abberufung der oder des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach dem Ende der Tätigkeit als Datenschutzbeauftragte oder als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.***

***(5) Betroffene Personen können die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der Verordnung (EU) 679/2016, diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffene Person befreit wird.***

***(6) Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.***

# 2. Einführung

Mit der Geltung der Datenschutz-Grundverordnung (DS-GVO) existiert erstmals eine europaweit verbindliche verpflichtende Regelung zur Benennung betrieblicher und behördlicher Datenschutzbeauftragter. Während die Datenschutzrichtlinie (95/46/EG) die Verpflichtung zur Bestellung von Datenschutzbeauftragten lediglich als Regelungsalternative für die Mitgliedstaaten vorsah, um die Meldepflicht gegenüber der Datenschutzaufsichtsbehörde entfallen zu lassen, ergibt sich seit dem 25. Mai 2018 eine Pflicht zur Benennung erstmals unmittelbar aus dem Europarecht. Das deutsche Erfolgsmodell der datenschutzrechtlichen Selbstkontrolle hat sich damit auch auf europäischer Ebene durchgesetzt. Nach dem Europäischen Datenschutzausschuss[2] ist der Datenschutzbeauftragte eine „Schlüsselfigur“, die die Einhaltung der Bestimmungen der DS-GVO erleichtert und als Mittler zwischen den maßgeblichen Interessenträgern, z.B. Aufsichtsbehörden, betroffene Personen und Unternehmensleitung, fungiert.

In Ergänzung zur europarechtlichen (Basis-)Benennungspflicht berechtigt die DS-GVO außerdem über eine Öffnungsklausel die Mitgliedstaaten, eine weitergehende Benennungspflicht auf nationaler Ebene vorzusehen. Die Öffnungsklausel bezieht sich allerdings nur auf die Voraussetzungen, unter denen ein Datenschutzbeauftragter zu benennen ist. Aufgaben und Rechtsstellung des Datenschutzbeauftragten regelt die DS-GVO selbst unmittelbar verbindlich.

[2] *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 4 f. Das WP wurde am 25.05.2018 vom *Europäischen Datenschutzausschuss* übernommen.

# 3. Benennung eines Datenschutzbeauftragten

## 3.1 Kriterien für das Eingreifen der Pflicht zur Benennung

**Nach der DS-GVO** ist ein Datenschutzbeauftragter **in folgenden Fällen verpflichtend zu benennen** (vgl. Art. 37 Abs. 1 DS-GVO):

- Art. 37 Abs. 1 Buchst. a) DS-GVO: Personenbezogene Datenverarbeitung durch **Behörde / öffentliche Stelle** (Ausnahme: justizielle Tätigkeit)
- Art. 37 Abs. 1 Buchst. b) DS-GVO: Die **Kerntätigkeit** des Verantwortlichen oder Auftragsverarbeiters besteht in Verarbeitungsvorgängen, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Beobachtung** von betroffenen Personen erforderlich machen.
- Art. 37 Abs. 1 Buchst. c) DS-GVO: Die **Kerntätigkeit** des Verantwortlichen oder Auftragsverarbeiters besteht in der **umfangreichen Verarbeitung besonderer Kategorien von Daten (Art. 9 DS-GVO) oder von Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO).**

Die für Unternehmen maßgeblichen letzten beiden Fallgruppen haben jeweils zwei Voraussetzungen. **Erstens** muss die die Benennungspflicht auslösende personenbezogene Datenverarbeitung zur **„Kerntätigkeit“** des für die Verarbeitung Verantwortlichen bzw. Auftragsverarbeiters gehören. **Zweitens muss die Tätigkeit bestimmte inhaltliche Voraussetzungen erfüllen**, nämlich das Erfordernis einer umfangreichen regelmäßigen und systematischen Beobachtung von betroffenen Personen oder die umfangreiche Verarbeitung von besonderen Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten.

Art. 37 Abs. 1 Buchst. b) DS-GVO unterfallen z.B. **Auskunfteien, Detekteien und das Bewachungsgewerbe**.[3] Eine Pflicht zur Benennung nach Art. 37 Abs. 1 Buchst. c) DS-GVO kann sich etwa für **größere[4] Gesundheitseinrichtungen**, wie insbesondere Krankenhäuser, mit genetischen oder allgemeinen Gesundheitsuntersuchungen befasste Labors, Beratungsstellen wie Pro Familia, Dienstleister im biometrischen ID-Management oder Anbieter erotischen Zubehörs ergeben.[5]

Die Pflicht zur Benennung eines Datenschutzbeauftragten kann sich aber nicht nur aus der DS-GVO ergeben. Art. 37 Abs. 4 DS-GVO enthält eine **Öffnungsklausel**, die es u.a. den nationalen Gesetzgebern ermöglicht, weitergehende Verpflichtungen zur Benennung von Datenschutzbeauftragten vorzusehen. Auf Art. 37 Abs. 4 DS-GVO beruht **§ 38 Abs. 1 BDSG 2018, der für nichtöffentliche Stellen** in Deutschland **im Kern die Voraussetzungen für die verpflichtende Benennung eines Datenschutzbeauftragten festschreibt, wie sie auch schon unter dem BDSG a.F. galten.** Die Öffnungsklausel bezieht sich nur auf die Voraussetzungen, unter denen ein Beauftragter zu benennen ist. Aufgaben und Stellung können nicht abweichend geregelt werden.

Nach § 38 Abs. 1 Satz 1 BDSG 2018 haben nicht öffentliche Verantwortliche und Auftragsverarbeiter einen Datenschutzbeauftragten verpflichtend zu benennen, **soweit sie in der Regel mindestens 20 Personen[6] ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.** Der Schwellenwert nach § 38 Abs. 1 Satz 1 BDSG 2018 muss also **„in der Regel“** erreicht werden. Maßgeblich ist die Anzahl der normalerweise mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen. Legt man den Maßstab des BDSG a.F. zugrunde, so ist entscheidend, ob der Schwellenwert über einen **Zeitraum von mindestens einem Jahr** erreicht wurde bzw. im Rahmen einer vorausschauenden Betrachtung erreicht

---

3 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 18.

4 Zur Benennungspflicht im Falle von Einzelarztpraxen und kleineren Praxisgemeinschaften vgl. nachfolgend in diesem Abschnitt.

5 *Jaspers/Reif*, RDV 2016, 61, 62.

6 Vgl. Fn. 1.

werden wird.[7] **„Ständig“** beschäftigt ist die Person, wenn sie die Aufgabe, die nicht ihre Hauptaufgabe zu sein braucht, regelmäßig wahrnimmt.[8] **Nicht notwendig ist, dass der Umgang mit personenbezogenen Daten den Kern der Tätigkeit des Beschäftigten bildet**, wie dies z.B. bei Mitarbeitern der Personalabteilung der Fall ist. Ausreichend ist vielmehr, dass im Rahmen der konkreten Tätigkeit auch mit personenbezogenen Daten umgegangen wird. Dies ist bereits bei Anbindung an Kommunikationssysteme wie z.B. Outlook und/oder Zugriff auf unternehmenseigene Adressverzeichnisse der Fall. Solche Mitarbeiter sind im Hinblick auf die Benennungspflicht ebenso mitzuzählen wie Mitarbeiter, die keine weiteren Kompetenzen haben, als sich personenbezogene Daten anzeigen zu lassen.

Ohne Relevanz für die Frage, ob eine Person bei der Prüfung der Benennungspflicht zu berücksichtigen ist, ist ihr arbeitsrechtlicher Status. So sind z.B. auch freie Mitarbeiter und Leiharbeitnehmer zu berücksichtigen, sofern sie für die verantwortliche Stelle ständig (auch) mit personenbezogener Datenverarbeitung befasst sind. Keine Rolle spielt zudem, wo die Datenverarbeitung für die verantwortliche Stelle durchgeführt wird, so dass auch **Telearbeiter** zu berücksichtigen sind. Die Beschäftigten eines Auftragsdatenverarbeiters (§ 11 BDSG) hingegen bleiben außer Betracht.

Ob bei der Prüfung der Benennungspflicht auch **leitende Personen (Vorstände, Geschäftsführer etc.)** zu berücksichtigen sind, ist fraglich. Für eine Berücksichtigung spricht, dass es nach dem Sinn und Zweck der Regelung zur Bestellpflicht, nämlich eine effektive Selbstkontrolle zu erreichen, nicht darauf ankommen kann, welchen Status eine Person innehat, sondern nur darauf, ob sie Aufgaben erfüllt, die mit der personenbezogenen Datenverarbeitung zusammenhängen.

---

7 *Bergmann/Möhrle/Herb*, BDSG, § 4f Rn. 33; *Simitis* in: Simitis, BDSG, § 4f Rn. 19; *Gola/Schomerus*, BDSG, § 4f Rn. 11; andere Ansicht: *Scheja* in: Taeger/Gabel, BDSG, § 4f Rn. 20, der diesen Zeitraum allerdings auf das Tatbestandsmerkmal „ständig“ bezieht.

8 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 27.

Im Zusammenhang mit besonders risikoträchtigen Datenverarbeitungen sieht § 38 Abs. 1 Satz 2 BDSG 2018 zudem eine **Pflicht zur Benennung vor, die unabhängig vom Erreichen des Schwellenwerts gilt**. Sie greift ein, sofern Verarbeitungen durchgeführt werden, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen, oder wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden (§ 38 Abs. 1 Satz 2 BDSG 2018). Bei den mit dieser Regelung angesprochenen Stellen sieht der Gesetzgeber ein besonderes Gefährdungspotenzial für die Persönlichkeitsrechte der betroffenen Person, dem auch durch professionelle betriebliche Selbstkontrolle begegnet werden soll.[9] Eine **Geschäftsmäßigkeit** setzt dabei nicht voraus, dass die Datenübermittlung etc. (Haupt-)Geschäftszweck der Stelle ist. Es genügt, dass das diesbezügliche Tätigwerden auf Wiederholung gerichtet und auf eine gewisse Dauer angelegt ist.[10] Als Zwecke der Markt- oder Meinungsforschung sind Zwecke zu verstehen, die sich auf die Informationsgewinnung über Märkte oder auf die Ermittlung von Meinungen und Stimmungen in der Bevölkerung beziehen.[11]

Sofern eine nationale Stelle den Schwellenwert aus § 38 Abs. 1 Satz 1 BDSG 2018 nicht erreicht, bleibt also jeweils zu prüfen, ob sich ggf. eine schwellenwertunabhängige Benennungspflicht ergibt, wobei Grundlage für eine solche schwellenwertunabhängige Benennungspflicht der zuvor dargestellte § 38 Abs. 1 Satz 2 BDSG 2018 sein kann oder auch Art. 37 Abs. 1 DS-GVO.

Die Verpflichtung zur schwellenwertunabhängigen Benennung nach § 38 Abs. 1 Satz 2 BDSG 2018 wird u.a. dann ausgelöst, wenn der Verantwortliche oder Auftragsverarbeiter **Verarbeitungen** vornimmt, **die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen**. Zwischen der Reichweite der Verpflichtung aus Art. 35 DS-GVO und der Verpflichtung zur Benennung eines Datenschutzbeauftragten besteht also ein unmittelbarer Zusammenhang. Die Anknüpfung der

---

9 *Klug* in: Gola, DS-GVO, 2. Aufl. 2018, Art. 37 Rn. 29.

10 *Kühling/Sackmann* in: Kühling/Buchner, § 38 Rn. 15.

11 *Schulz* in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 91.

Benennungspflicht an das Erfordernis einer Datenschutz-Folgen-abschätzung ist nachvollziehbar, führt sie doch dazu, dass in diesen Fällen besonders risikobehafteter Datenverarbeitung ein spezialisiertes Beratungs- und Überwachungsorgan zur Verfügung steht.

Die von den Aufsichtsbehörden veröffentlichten sog. **Blacklists** (Art. 35 Abs. 4 DS-GVO) haben zu einer ersten Konturierung der Voraussetzungen geführt, unter denen eine Datenschutz-Folgenabschätzung durchzuführen ist. Gleichwohl bleiben Fragen offen. So ist fraglich, inwiefern die Durchführung der **Lohn- und Gehaltsabrechnung** zur Verpflichtung führt, eine Datenschutz-Folgenabschätzung vorzunehmen, und ob allein der Umstand, dass eine Lohn- und Gehaltsabrechnung durchgeführt wird, eine Benennungspflicht herbeiführen kann. Dies ist insofern praxisrelevant, als Lohn- und Gehaltsabrechnungen von den allermeisten datenverarbeitenden Stellen durchgeführt werden und es je nach Antwort zu einer massiven Ausweitung der Benennungspflicht käme.

Gegen die Annahme einer Verpflichtung zur Benennung eines Datenschutzbeauftragten allein aufgrund des Umstands, dass Lohn- und Gehaltsabrechnungen durchgeführt werden, spricht, dass damit das gesetzliche Regel-/Ausnahmeverhältnis verkehrt und die schwellenwertunabhängige Benennungspflicht zur Regel würde (teleologische Auslegung von § 38 Abs. 1 BDSG 2018). § 38 Abs. 1 Satz 1 BDSG 2018 würde nahezu bedeutungslos. Auch knüpft der Wortlaut von § 38 Abs. 1 Satz 2 BDSG 2018 die Benennungspflicht an „Verarbeitungen“ (Plural), die einer Datenschutz-Folgenabschätzung unterliegen. Insofern lässt sich die Auffassung vertreten, dass eine einzelne Art. 35 DS-GVO unterfallende Verarbeitung die Benennungspflicht noch nicht auslöst.[12]

Ansatzpunkt für eine mögliche Verpflichtung zur Datenschutz-Folgenabschätzung in den Fällen der Lohn- und Gehaltsabrechnung ist, dass aus steuerrechtlichen Gründen bei der Abrechnung u.a. die Verarbeitung der Konfession der beschäftigten Person erforderlich ist. Auch Krankheitszeiten und damit Gesundheitsdaten spielen bei der Lohn- und Gehaltsabrechnung eine Rolle, entfällt doch ab einer bestimmten Dauer der Erkrankung der Anspruch auf Entgeltfortzahlung. Nach

[12] Anderer Ansicht *Moos* in: BeckOK § 38 Rn. 13; wohl auch *Pauly* in: Paal/Pauly, § 38 Rn. 12.

Art. 35 Abs. 3 Buchst. b) DS-GVO ist eine Datenschutz-Folgenabschätzung u.a. insbesondere dann erforderlich, wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO erfolgt. Fraglich ist allerdings, wann eine solche „umfangreiche" Verarbeitung besonderer Kategorien von personenbezogenen Daten i.S.v. Art. 35 Abs. 3 Buchst. b) DS-GVO vorliegt. Klare Schwellenwerte bzw. Zahlen existieren hierzu nicht. Der Gesetzgeber hat sich gegen eine schematische Herangehensweise entschieden, so dass bei der Beurteilung, ob eine umfangreiche Verarbeitung vorliegt, stets auch der konkrete Verarbeitungszusammenhang zu beachten ist.[13]

Die Datenverarbeitung zu Zwecken der Lohn- und Gehaltsabrechnung wurde bereits von zwei Aufsichtsbehörden[14] in Europa als Verarbeitungsvorgang anerkannt, der von Art. 35 DS-GVO ausgenommen ist, sog. **White List** (Art. 35 Abs. 5 DS-GVO). Zwar können sich deutsche Verantwortliche auf die Entscheidungen der ausländischen Behörden nicht unmittelbar berufen, eine richtungsweisende Tendenz dürften sie gleichwohl haben. Für die Einordnung auf der White List spricht insbesondere, dass die Datenverarbeitung zu Zwecken der Lohn- und Gehaltsabrechnung im Kern nicht zur Disposition des Verantwortlichen steht, sondern im Wesentlichen nur rechtlichen Verpflichtungen nach-

[13] Der Ansicht, dass „Gehaltsabrechnungen großer und mittelständischer Unternehmen" eine Verpflichtung zur Datenschutz-Folgenabschätzung auslösen können, ist *Kiesche*, CuA 2/2017, 31, 34. Für ein Eingreifen der Verpflichtung bei „Einführung neuer Gehaltsabrechnungssysteme in großen und mittelständischen Unternehmen" *Laue/Nink/Kremer*, S. 236 f.

[14] Verordnung der *österreichischen Datenschutzbehörde* über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV) sowie *Commission de la protection de la vie privée (CPVP), Belgien,* Recommandation 01/2018 concernant l'analyse d'impact relative à la protection des données et la consultation préalable (CO-AR-2018-001). Mit dem 25.05.2018 ist die L'Autorité de protection des données (APD) anstelle der CPVP getreten. Die APD führt das genannte CPVP-Dokument auf ihrer Homepage und scheint insofern an der Liste festzuhalten.

gekommen wird bzw. rechtliche Rahmenbedingungen umgesetzt werden.[15]

Praxisrelevant ist auch die Frage nach der **Benennungspflicht bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs**, sofern diese weniger als 20 Personen mit der Verarbeitung personenbezogener Daten beschäftigen. Maßgeblich ist insofern, ob eine umfangreiche Verarbeitung von Gesundheitsdaten i.S.v. Art. 37 Abs. 1 Buchst. c) DS-GVO stattfindet. Sofern es sich um einen einzelnen Arzt oder sonstigen Angehörigen eines Gesundheitsberufs handelt, spricht ErwG 91 Satz 4 DS-GVO gegen die Annahme einer solchen umfangreichen Verarbeitung.[16] Nach Ansicht der Datenschutzkonferenz soll zudem regelmäßig selbst dann nicht von einer umfangreichen Verarbeitung auszugehen sein, wenn Angehörige eines Gesundheitsberufs in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder weitere Angehörige eines Gesundheitsberufs beschäftigen und weniger als 10 Personen mit der Verarbeitung personenbezogener Daten befasst sind.[17] Eine Benennungspflicht auch in diesen Fällen könne sich aber ergeben, wenn z.B. wegen des Einsatzes von neuen Technologien eine Datenschutz-Folgenabschätzung vorgeschrieben sei (§ 38 Abs. 1 Satz 2 BDSG), so die Konferenz. Insbesondere angesichts der Sensitivität der

---

15 Art. 35 Abs. 10 DS-GVO, wonach sich bei Datenverarbeitungen aufgrund einer rechtlichen Verpflichtung Ausnahmen vom Erfordernis einer Datenschutz-Folgenabschätzung ergeben können, greift insofern nicht ein. Diese Möglichkeit des Absehens von der Durchführung einer Datenschutz-Folgenabschätzung gilt nur für Verarbeitungen aufgrund von Gesetzen, die nach dem Inkrafttreten der DS-GVO erlassen wurden, denn nur für derartige Gesetze kann entsprechend den Maßgaben der DS-GVO eine Datenschutz-Folgenabschätzung durchgeführt werden, vgl. *Nolte/Werkmeister* in: Gola, Art. 35 Rn. 72. Überdies verlangt Art. 35 Abs. 10 DS-GVO, dass die in Frage stehenden Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln.

16 Die Regelung hat folgenden Wortlaut: *„Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt.“*

17 Beschluss der *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder* – Düsseldorf, 26. April 2018, Datenschutzbeauftragten-Bestellpflicht nach Art. 37 Abs. 1 Buchst. c) DS-GVO bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs.

verarbeiteten Daten kann sich im Übrigen bei Arztpraxen usw. eine freiwillige Benennung empfehlen.[18]

Den Umstand, dass die **freiwillige Benennung von Datenschutzbeauftragten** unbenommen ist, stellt Art. 37 Abs. 4 DS-GVO klar. Maßgebliches Argument für eine Benennung auch ohne Pflicht ist, dass Datenschutzbeauftragte einen zentralen Beitrag zur Gewährleistung von Datenschutzkonformität und damit zur Vermeidung von Unternehmensrisiken darstellen. Auch für einen freiwillig benannten Datenschutzbeauftragten bestimmen sich Stellung und Aufgaben nach der DS-GVO.[19] Sollen Aufgaben und Rechtsstellung von der DS-GVO abweichen, bedarf es einer anderen Bezeichnung, z.B. als Datenschutzkoordinator oder Referent für Datenschutz, sowie einer entsprechenden Stellenbeschreibung.[20] Da die entsprechende Regelung im BDSG 2018 wie bisher an das Bestehen einer Pflicht zur Benennung anknüpft, genießen freiwillig benannte Datenschutzbeauftragte jedoch keinen Kündigungsschutz.

## 3.2 Überblick: Wann ist ein Datenschutzbeauftragter zu benennen?

- Öffentliche Stelle: immer
- Nichtöffentliche Stellen:
  - **Schwellenwertabhängig:**
    in der Regel **mindestens 20 Personen**[21] ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt

---

18 Vgl. auch *Datenschutzkonferenz*, Kurzpapier Nr. 12 (Stand: 16.01.2018), S. 2, wonach die Benennung unabhängig von Erwägungsgrund 91 S. 4 „generell zu empfehlen“ ist.

19 *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 24 (bestätigt durch EDSA am 25.05.2018); *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 38; *Heberlein* in: Ehmann/Selmayr, Art. 37 Rn. 37; *Bergt* in: Kühling/Buchner, Art. 37 Rn. 26.

20 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 38.

21 Vgl. Fn. 1.

- Unabhängig vom Erreichen des Schwellenwerts in folgenden Fällen:
    - **Datenschutz-Folgenabschätzung**
    - **Geschäftsmäßige Verarbeitung** personenbezogener Daten **zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung**
    - **Kerntätigkeit**, die **umfangreiche regelmäßige und systematische Beobachtung** von betroffenen Personen erforderlich macht
    - **Kerntätigkeit, die in der umfangreichen Verarbeitung besonderer Kategorien von Daten** (Art. 9 DS-GVO) **oder von Daten über strafrechtliche Verurteilungen und Straftaten** (Art. 10 DS-GVO) **besteht**

## 3.3 Anforderungen an die Benennung

Die **Form der Benennung** wird durch die DS-GVO nicht geregelt. Zur Gewährleistung von Rechtssicherheit und aus Dokumentationsgründen ist eine Benennung zumindest in Textform gleichwohl ratsam.

Im Sinne eines effektiven und kontinuierlichen Datenschutzes ist **für interne Datenschutzbeauftragte regelmäßig von einer unbefristeten Benennung auszugehen**.[22] Befristete Benennungen hindern den Datenschutzbeauftragten unliebsame Positionen gegenüber Unternehmensleitung und Fachabteilung einzunehmen und gefährden insofern die Unabhängigkeit (ErwG 97) des Datenschutzbeauftragten. Auch um

[22] *LfDI Baden-Württemberg*, Praxisratgeber Die/der Beauftragte für den Datenschutz Teil 2, S. 14 f. Jedenfalls „unzulässig kurze“ Befristungen ablehnend *Bergt* in: Kühling/Buchner, Art. 37 Rn. 42; ähnlich *Heberlein* in: Ehmann/Selmayr, Art. 37 Rn. 18; *Drewes* in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 37 Rn. 55.

eine Aushöhlung des gesetzlichen Abberufungsschutzes (Art. 38 Abs. 3 Satz 2 DS-GVO) zu vermeiden, dürfen Befristungen daher nur erfolgen, wenn ein sachlicher Grund vorliegt, z.B., weil das Amt im Rahmen einer Elternzeitvertretung wahrgenommen wird. **Verträge mit externen Datenschutzbeauftragten** bedürfen zur Gewährleistung der notwendigen Unabhängigkeit einer **Mindestlaufzeit**.[23] Empfohlen wird eine regelmäßige Mindestvertragslaufzeit von vier Jahren. Bei Erstverträgen ist wegen der Notwendigkeit der Überprüfung der Eignung eine kürzere Frist von ein bis zwei Jahren zulässig.

Die Benennung sollte auf Basis einer **Stellenbeschreibung** erfolgen, die Aufgaben und Stellung des jeweiligen Datenschutzbeauftragten im Einzelnen und bezogen auf die individuellen Besonderheiten beim Verantwortlichen bzw. Auftragsverarbeiter beschreibt.[24]

Eine **Benennung mehrerer Personen** zum Datenschutzbeauftragten kommt nur in Betracht, sofern eine klare Aufgabentrennung besteht.[25]

**Weigert sich der Mitarbeiter, das Amt des Datenschutzbeauftragten zu übernehmen,** und ist für die benennende Stelle offenkundig, dass er den gesetzlichen Aufgaben nicht nachkommen wird, ist eine dennoch erfolgende Benennung unwirksam.

## 3.4 Arbeits- und mitbestimmungsrechtliche Aspekte der Benennung

Die Benennung zum Datenschutzbeauftragten ist regelmäßig nicht über das **Direktionsrecht** des Arbeitgebers gedeckt, sondern setzt eine Änderung des Inhalts des Arbeitsvertrags voraus.[26] Eine einvernehmliche Benennung beinhaltet dabei zugleich den notwendigen arbeitsrechtlichen Änderungsvertrag, sofern der Änderungsvertrag im Einzel-

---

23 *LfDI Baden-Württemberg*, Praxisratgeber Die/der Beauftragte für den Datenschutz Teil 2, S. 15.

24 Ein entsprechendes Muster findet sich im Teil B dieses Ratgebers.

25 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 23.

26 *BAG*, Urteil vom 13.03.2007 - 9 AZR 612/05, NJW 2007, 2507, 2508; DB 2007, 1199; RDV 2007, 123; vgl. auch *BAG*, Urteil vom 29.09.2010 - 10 AZR 588/09, NJW 2011, 476; BB 2011, 637; NZA 2011, 151; RDV 2011, 88.

fall nicht an Formvorgaben gebunden ist. Ein spezielles auf die Benennung des Datenschutzbeauftragten bezogenes **Mitbestimmungsrecht der Mitarbeitervertretung** existiert nicht. Mitbestimmungsrechte können im Einzelfall dennoch eingreifen, sofern mit der Benennung eine Einstellung, Eingruppierung, Umgruppierung oder Versetzung verbunden ist (§ 99 BetrVG und § 75 Abs. 1 Nr. 1, 2 und 3 BPersVG).

## 3.5 Veröffentlichung/Mitteilung der Kontaktdaten des Datenschutzbeauftragten

Nach Art. 37 Abs. 7 DS-GVO **veröffentlicht** der Verantwortliche bzw. Auftragsverarbeiter die **Kontaktdaten des Datenschutzbeauftragten und teilt diese der Aufsichtsbehörde mit**. Die Veröffentlichung bzw. Mitteilung der Kontaktdaten soll gewährleisten, dass betroffene Personen von ihrem Recht zur Anrufung des Datenschutzbeauftragten (Art. 38 Abs. 4 DS-GVO) Gebrauch machen können und die Aufsichtsbehörde mit diesem in Kontakt treten kann (Art. 39 Abs. 1 Buchst. d) und e) DS-GVO).[27] Wie ein Vergleich z.B. mit Art. 13 Abs. 1 Buchst. a) DS-GVO zeigt, wo von „Name und Kontaktdaten“ die Rede ist, setzt die Angabe der bloßen Kontaktdaten, z.B. auf der Homepage, nicht zwingend voraus, dass auch der Name des Datenschutzbeauftragten genannt wird. Im Verhältnis zur Aufsichtsbehörde ist die namentliche Nennung des Beauftragten gleichwohl sinnvoll und diese kann den Namen ohnehin auch über Art. 30 Abs. 1 Satz 2 Buchst. a) i.V.m. Abs. 4 DS-GVO erlangen. Anzugeben sind **mindestens die Adresse, die Telefonnummer und die E-Mail-Adresse** des Datenschutzbeauftragten.[28] Die Verpflichtung zur Veröffentlichung/Mitteilung der Kontaktdaten gilt unabhängig davon, ob sich die Pflicht zur Benennung des Datenschutzbeauftragten aus der DS-GVO selbst oder aus nationalem Recht ergibt.

---

[27] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 47.

[28] *LDI*, Häufig gestellte Fragen zum Datenschutzbeauftragten (FAQ), Stand: 11/2018, S. 14 f.

Informationen zum jeweiligen **Meldeprozedere** finden sich auf den Internetseiten der Aufsichtsbehörden. Teilweise bieten die Aufsichtsbehörden die Möglichkeit, den Datenschutzbeauftragten über entsprechende Online-Formulare zu melden, oder stellen zumindest PDF-Formulare für den Versand per Post, Mail oder Fax zur Verfügung. Eine Verpflichtung zur Verwendung eines bestimmten Formulars besteht allerdings nicht.

Die Verpflichtung zur Veröffentlichung / Mitteilung der Kontaktdaten ist eine Verpflichtung des Verantwortlichen bzw. Auftragsverarbeiters. In Fällen, in denen ein **Konzerndatenschutzbeauftragter** benannt ist, bleiben also die einzelnen Konzernunternehmen verpflichtet.

## 3.6 Möglichkeit der Benennung eines externen Datenschutzbeauftragten

Nach Art. 37 Abs. 6 DS-GVO kann der Datenschutzbeauftragte Beschäftigter des Verantwortlichen oder Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen. Dem Verantwortlichen bzw. Auftragsverarbeiter wird somit explizit die **Möglichkeit** eingeräumt, **einen sog. externen Datenschutzbeauftragten zu benennen.** Aus Sicht der benennenden Stelle kann dies eine Reihe von Vorteilen bieten. Insbesondere kann die Stelle, statt einen eigenen Mitarbeiter erst ausbilden zu müssen, ggf. direkt auf einen Datenschutzbeauftragten mit vielfältigen Erfahrungen zurückgreifen. Zudem genießt der interne Beauftragte nicht nur den Abberufungsschutz aus Art. 38 Abs. 3 Satz 2 DS-GVO, welcher sich gleichermaßen auf externe Beauftragte bezieht, sondern nach § 38 Abs. 2 i.V.m. § 6 Abs. 4 BDSG 2018 auch Kündigungsschutz. Sich von einem externen Beauftragten wieder zu trennen, ist daher im Ergebnis um einiges leichter. Ein besonderer Vorteil des internen gegenüber dem externen Beauftragten ist dagegen die regelmäßig bessere Kenntnis der betrieblichen Abläufe. Gerade bei größeren Unternehmen kann von einem eigenen Mitarbeiter eher erwartet werden, dass er die unternehmensspezifischen Risiken und Besonderheiten kennt und die Ressourcen so nutzt, dass er die Vorgaben des Datenschutzrechts sinnvoll in die Un-

ternehmensorganisation einbindet.[29] Zweckmäßig kann der Einsatz eines externen Datenschutzbeauftragten vor allem bei kleinen und mittleren Unternehmen sein. Auch **öffentliche Stellen** dürfen nach der DS-GVO einen externen Datenschutzbeauftragten benennen.

Wird ein **„Konzerndatenschutzbeauftragter“** benannt, so ist auch dieser im Hinblick auf diejenigen Gesellschaften, die nicht sein Arbeitgeber sind, externer Datenschutzbeauftragter.[30]

**Juristische Personen als Datenschutzbeauftragte?**

Fraglich ist, ob zum externen Datenschutzbeauftragten nur eine natürliche Person oder auch eine **juristische Person wie z.B. eine Unternehmensberatungsgesellschaft** benannt werden kann. Die Benennung einer juristischen Person wird teilweise abgelehnt[31].

Die Auslegung, welche nur eine Benennung von natürlichen Personen zulässt, führt in der Praxis zu nicht unerheblichen Schwierigkeiten, die daraus resultieren, dass bei einer entsprechenden Umsetzung die benannte Person (Angehöriger der Beratungsgesellschaft) und der Vertragspartner der verantwortlichen Stelle (Beratungsgesellschaft) auseinanderfallen. Dies wirft insbesondere dann Probleme auf, wenn die benannte natürliche Person ihren bisherigen Arbeitgeber verlässt, denn die Kündigung des Arbeitsverhältnisses lässt die Benennung prinzipiell unberührt.

Eine solche Auslegung ist auch nicht zwingend geboten, insbesondere sieht die DS-GVO keine Beschränkung auf die Benennung natürlicher Personen vor. Fachkenntnisse der Gesellschafter bzw. Mitarbeiter können der juristischen Person zugerechnet werden, das Vorliegen von Interessenkonflikten kann anhand der Personen beurteilt werden, welche

29 *Koch*, Der betriebliche Datenschutzbeauftragte, 6. Aufl., S. 35.

30 Zum Konzerndatenschutzbeauftragten vgl. ausführlich unter 3.8.

31 *LDI*, Häufig gestellte Fragen zum Datenschutzbeauftragten (FAQ), Stand: 11/2018, S. 11 f.; *Heberlein* in: Ehmann/Selmayr, Art. 37 Rn. 43; *Laue/Nink/Kremer*, S. 197.

die Aufgaben des Datenschutzbeauftragten konkret wahrnehmen.[32] Auch der **Europäische Datenschutzausschuss** vertritt die Auffassung[33], dass juristische Personen zum Datenschutzbeauftragten benannt werden können und die praktische Aufgabenwahrnehmung durch deren Angehörige erfolgt. Im Interesse der Rechtssicherheit und einer ordnungsgemäßen Organisation sowie um Interessenkonflikte der Teammitglieder zu vermeiden empfiehlt er allerdings, eine klare Aufgabenverteilung innerhalb des Datenschutzbeauftragten-Teams vorzusehen sowie eine einzelne Person als primären Ansprechpartner festzulegen, der zugleich für den jeweiligen Kunden zuständig ist.

Nach einer Entscheidung des Bundesfinanzhofs[34] aus dem Jahr 2003 übt ein selbstständiger externer Datenschutzbeauftragter eine gewerbliche Tätigkeit und keine Tätigkeit als Freiberufler aus und unterliegt daher der **Gewerbesteuer**. Aktuell ist die Frage nach der Einordnung selbstständiger externer Datenschutzbeauftragter erneut beim BFH zur Entscheidung anhängig.[35]

Auch der externe Datenschutzbeauftragte darf keinen Interessenkollisionen unterliegen. Besonderer Prüfung bedarf es insofern, wenn ein **IT-Dienstleister** bzw. einer seiner Mitarbeiter zugleich das Amt als Datenschutzbeauftragter übernehmen soll. Hier besteht die gleiche Gefahr, dass eine effektive Datenschutzüberwachung nicht stattfindet, wie wenn der IT-Leiter zum Datenschutzbeauftragten benannt würde. Ausgeschlossen ist die Übernahme der Funktion durch den IT-Dienstleister indes nicht. Es ist allerdings darauf zu achten, dass die Person, die die Aufgaben des Datenschutzbeauftragten konkret übernimmt, mit dem IT-Auftrag nicht befasst ist. Auch bedarf es getrennter Verträge für die IT- bzw. Datenschutzdienstleistung.

---

32 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 45; *Klug* in: Gola, DS-GVO, 2. Aufl., Art. 37 Rn. 15.

33 *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 14 f. (bestätigt durch EDSA am 25.05.2018); die Ansicht im Grundsatz befürwortend auch *HessDSB*, 46. TB (2017), 2.3.7.

34 NJW 2003, 3368; DB 2003, 2316; BB 2003, 2108; RDV 2003, 240; kritisch hierzu *Klug*, Anmerkung zum BFH-Urteil, RDV 2003, 241 f.

35 BFH - VIII R 27/17.

## 3.7 Exkurs: Rechtsanwälte als Datenschutzbeauftragte

Unter anderem die zunehmende Komplexität des Datenschutzrechts hat dazu geführt, dass immer häufiger auch **Rechtsanwälte als externe Datenschutzbeauftragte** benannt werden. Insoweit ist § 45 Abs. 1 Nr. 4 BRAO zu beachten. Danach darf ein Rechtsanwalt nicht tätig werden, „wenn er in derselben Angelegenheit außerhalb seiner Anwaltstätigkeit … bereits beruflich tätig war“. Hat ein Unternehmen also einen Anwalt zum Datenschutzbeauftragten benannt, führt dies für diesen zu einem berufsrechtlichen Verbot, in datenschutzrechtlichen Angelegenheiten für das Unternehmen anwaltlich tätig zu werden.[36] Dieses Verbot endet erst, wenn das Amt als Datenschutzbeauftragter endet. Auch datenschutzrechtlich wäre es problematisch, wenn das Amt als Beauftragter und das Datenschutzmandat zusammenfielen, denn der Anwalt vertritt nur die Interessen seines Mandanten, während der Datenschutzbeauftragte die Interessen der betroffenen Personen zu wahren und mit der Aufsichtsbehörde zusammenzuarbeiten hat (Art. 39 DS-GVO).[37]

Wer als angestellter Rechtsanwalt für Kunden seines Arbeitgebers als externer Datenschutzbeauftragter tätig ist, genießt nach Auffassung des BGH nicht die Möglichkeit der Zulassung als **Syndikusrechtsanwalt**.[38] Ein solcher Anwalt werde nicht in Rechtsangelegenheiten des Arbeitgebers tätig, denn er berate die Kunden seines Arbeitgebers und sei nicht der anwaltliche Berater des Arbeitgebers. Die Wahrnehmung von Rechtsangelegenheiten des Arbeitgebers sei aber tatbestandliche Voraussetzung für die Zulassung als Syndikusrechtsanwalt, so der BGH. Auch nach dem BGH ist es allerdings möglich, dass eine Tätigkeit im Bereich des Datenschutzes eine "Rechtsangelegenheit des Arbeitgebers" sein kann, nämlich dann, wenn sie intern von (juristischen) Mitarbeitern des Arbeitgebers wahrgenommen wird.

---

36 *Siegmund*, NJW-aktuell 32/2018, S. 15.

37 *Siegmund*, a.a.O.

38 BGH, Urteil vom 02.07.2018 - AnwZ (Brfg) 49/17.

## 3.8 Möglichkeit der Benennung eines gemeinsamen Datenschutzbeauftragten / von Verbandsdatenschutzbeauftragten

Für Unternehmensgruppen[39] besteht nach Art. 37 Abs. 2 DS-GVO die Möglichkeit der **Benennung eines gemeinsamen Datenschutzbeauftragten**. Die Regelung vermindert den administrativen Aufwand im Zusammenhang mit der Benennung sog. **Konzerndatenschutzbeauftragter**, indem sie der Konzernleitung ermöglicht, alle verpflichtenden oder freiwilligen Benennungen in einem Akt vornehmen.[40] Vorteil eines Konzerndatenschutzbeauftragten ist insbesondere, dass eine solche zentrale Lösung die einheitliche Behandlung von Fragestellungen und Problemen gewährleistet, die mehrere Konzernunternehmen betreffen.

Die Benennung eines gemeinsamen Beauftragten durch Unternehmensgruppen wird von der DS-GVO allerdings nicht uneingeschränkt gestattet, sondern ist an die Voraussetzung geknüpft, dass dieser **von jeder Niederlassung aus leicht erreichbar** ist. Der Europäische Datenschutzausschuss[41] und die nationale Datenschutzkonferenz[42] empfehlen insofern für den Regelfall die Benennung eines Datenschutzbeauftragten mit Sitz in der Europäischen Union.

Leichte Erreichbarkeit bedeutet auch, dass der Kommunikation mit dem Datenschutzbeauftragten **keine Sprachbarrieren** entgegenstehen dürfen. Die fließende Beherrschung der Arbeitssprache des Konzerns

---

39 Nach Art. 4 Nr. 19 DS-GVO ist eine „Unternehmensgruppe" eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

40 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 31; ebenso *Bergt* in: Kühling/Buchner, Art. 37 Rn. 27; *Klug* in: Gola, Art. 37 Rn. 17; *Paal* in: Paal/Pauly, Art. 37 Rn. 10; *Maier/Ossoinig* in: Roßnagel, Europäische DS-GVO, S. 210; *Gierschmann*, ZD 2016, 51, 52; *Marschall/Müller*, ZD 2016, 415, 416; wohl auch *Heberlein* in: Ehmann/Selmayr, Art. 37 Rn. 29; anderer Ansicht *Laue/Nink/Kremer*, S. 195.

41 *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 13 (bestätigt durch EDSA am 25.05.2018).

42 Kurzpapier Nr. 12 (Stand: 16.01.2018), S. 2.

allein ist insofern nicht entscheidend, denn der Datenschutzbeauftragte hat nicht nur interne Aufgaben, sondern ist auch Ansprechpartner im Verhältnis zu den betroffenen Personen und zur Aufsichtsbehörde. Maßgeblich ist die **Sprache des Landes der Niederlassung**,[43] wobei Sprachbarrieren auch mit Hilfe von vor Ort ansässigem Hilfspersonal des Datenschutzbeauftragten überwunden werden können.[44]

Wird ein gemeinsamer Datenschutzbeauftragter benannt, ist diesem in angemessenem Umfang **Hilfs- und Korrespondenzpersonal** in den einzelnen Stellen zur Verfügung zu stellen (Art. 38 Abs. 2 DS-GVO).

Auch im öffentlichen Bereich können nach Art. 37 Abs. 3 DS-GVO mehrere Stellen einen gemeinsamen Datenschutzbeauftragten benennen, wobei Organisationsstruktur sowie Größe der Stellen zu berücksichtigen sind. Art. 37 Abs. 4 DS-GVO beinhaltet spezielle Regelungen für **Verbandsdatenschutzbeauftragte**.

## 3.9 Fortgeltung von Altbestellungen

Der aufgrund von früheren BDSG-Fassungen benannte Datenschutzbeauftragte wird automatisch zum Datenschutzbeauftragten nach DS-GVO bzw. BDSG 2018. **Altbestellungen gelten also fort.**[45] Die Urkunde und etwaige darin enthaltene Zusatzvereinbarungen und Aufgabenzuweisungen sollten aber auf ihre Vereinbarkeit mit den neuen Regelungen überprüft und ggf. angepasst werden.[46]

---

43 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 32; *Bergt* in: Kühling/Buchner, Art. 37 Rn. 29; *Paal* in: Paal/Pauly, Art. 37 Rn. 10; *Bittner*, RDV 2014, 183, 184.

44 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 32; *Laue/Nink/Kremer*, S. 196.

45 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 29; *Laue/Nink/Kremer*, S. 199; *Franck*, ZD 2017, 509, 512; ebenso Datenschutzkonferenz, Kurzpapier Nr. 12 (Stand: 16.01.2018), S. 3.

46 *Datenschutzkonferenz*, Kurzpapier Nr. 12 (Stand: 16.01.2018), S. 3.

Im **Fall der externen Bestellung** ist der zugrundeliegende Geschäftsbesorgungsvertrag an die geänderten rechtlichen Rahmenbedingungen anzupassen (§ 313 BGB). Im Rahmen der Anpassung ist auch der erhöhte zeitliche Aufwand zu berücksichtigen, der sich durch die Beratung im Hinblick auf die Umsetzung der DS-GVO ergibt.

# 4. Anforderungen an den Datenschutzbeauftragten

## 4.1 Einführung

Nach Art. 37 Abs. 5 DS-GVO wird der Datenschutzbeauftragte auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 genannten Aufgaben. Welche Anforderungen sich hieraus konkret ergeben, ist in der DS-GVO nicht geregelt und muss daher im Wege der Auslegung ermittelt werden. Angesichts der Abstraktheit der DS-GVO-Anforderungen zur Fachkunde und bereits in der Vergangenheit festzustellender großer qualitativer Unterschiede im Hinblick auf die Ausbildung von Datenschutzbeauftragten bedarf es der Entwicklung einheitlicher europaweiter Standards im Hinblick auf die Qualifikation von Datenschutzbeauftragten.[47]

Im Interesse einer qualitativen Absicherung der Fachkunde und einer Verbesserung der Markttransparenz bietet die GDD die Möglichkeit, nach entsprechender Ausbildung eine **Zertifizierung der Datenschutzqualifikation** zu erlangen. Eine entsprechende Zertifizierung ist nicht zwingend vorgeschrieben. Vor allem externe Dienstleister auf dem Gebiet des Datenschutzes können sich durch eine solche Qualifizierung positiv von ihren Mitbewerbern abgrenzen, aber auch Unternehmen, die einen internen Datenschutzbeauftragten benannt haben, müssen dessen Fachkunde gegenüber der Aufsichtsbehörde belegen

[47] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 41; *Heberlein* in: Ehmann/Selmayr, Art. 37 Rn. 39.

können[48]. In diesem Zusammenhang kommt dem Erwerb einer Zertifizierung im Vergleich zu einem reinen Seminarbesuch besonderes Gewicht zu.

## 4.2 Berufliche Qualifikation (insbes. Fachwissen)

Bezüglich der notwendigen beruflichen Qualifikation ergeben sich keine grundlegenden Unterschiede im Vergleich zu den Anforderungen, die sich diesbezüglich aus dem BDSG a.F. (§ 4f Abs. 2 Satz 1) ergaben. Erforderlich ist weiterhin eine **Trias rechtlicher, technischer und praktisch-organisatorischer Kenntnisse**.

Das **Rechtswissen** muss die nationalen und europäischen Datenschutzgesetze umfassen einschließlich vertiefter Kenntnisse der DS-GVO und der nationalen Anpassungs- und Umsetzungsgesetzgebung, also in Deutschland des BDSG 2018. Mit einer oberflächlichen Kenntnis der zentralen Datenschutzregelungen ist es insofern nicht getan. Der Datenschutzbeauftragte muss, nötigenfalls nach weiterer Fortbildung, die Fähigkeit besitzen, trotz des hohen Abstraktionsgrades von DS-GVO und BDSG und der vielfach verwendeten unbestimmten Rechtsbegriffe zu einer eigenständigen datenschutzrechtlichen Bewertung bezüglich der im Unternehmensalltag auftretenden Sachverhalte zu kommen. Hierzu muss der Datenschutzbeauftragte auch über die datenschutzrelevante Rechtsprechung und Literatur informiert sein und sich regelmäßig mit den aufsichtsbehördlichen Stellungnahmen befassen.

Im Bereich der Informations- und Kommunikationstechnik benötigt der Datenschutzbeauftragte die **Fähigkeit, die potenziellen Risiken für den Datenschutz sowie die Angemessenheit von Datensicherheitsmaßnahmen (Art. 32 DS-GVO) zu beurteilen**. Erforderlich sind insoweit Kenntnisse der Informations- und Kommunikationstechnologie sowie der Datensicherheit, insbesondere der Aspekte physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen.[49]

---

48 Datenschutz-Prüfungsaktion des *BayLDA* 2013, Frage 2.1 (RDV 2013, 265, 266).

49 *Düsseldorfer Kreis*, Beschluss vom 24./25.11.2010.

Nach Art. 37 Abs. 5 DS-GVO soll sich das Fachwissen der zu benennenden Person explizit auch auf die **Datenschutzpraxis** beziehen, d.h. darauf, wie datenschutzrechtliche Vorgaben konkret umgesetzt werden können. Notwendig sind insbesondere Kenntnisse bezüglich der praktischen Durchführung von Überwachungsmaßnahmen, der Risikoanalyse, der Beratung und Strategieentwicklung, der Prüfung von Sicherheitskonzepten, der Dokumentation und der Zusammenarbeit mit der Mitarbeitervertretung.[50] Überdies bedarf es eines Verständnisses für betriebswirtschaftliche Zusammenhänge. Eine effektive Datenschutzberatung und -überwachung setzt schließlich eine gute Kenntnis der Strukturen der zu betreuenden Stelle bzw. des einschlägigen Wirtschaftszweigs sowie der dort stattfindenden Datenverarbeitungsprozesse voraus.[51] Gerade in größeren Organisationen wird es dem Datenschutzbeauftragten allerdings naturgemäß schwer fallen, einen detaillierten Überblick über alle datenschutzrelevanten Prozesse zu erlangen bzw. diesen zu behalten. Insofern gehört es zu den Pflichten des Verantwortlichen bzw. Auftragsverarbeiters, dem Datenschutzbeauftragten fachkundige Ansprechpartner zur Unterstützung zur Verfügung zu stellen. Diese Verpflichtung besteht insbesondere im Verhältnis zu einem externen Datenschutzbeauftragten.

Das erforderliche **Niveau des Fachwissens** des Datenschutzbeauftragten ist nicht für jede Organisation identisch. Nach ErwG 97 soll es sich vielmehr nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz der vom Verantwortlichen oder Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Erhöhte Anforderungen an das Fachwissen können sich etwa ergeben, wenn besonders komplexe Datenverarbeitungen durchgeführt, große Mengen von sensitiven Daten verarbeitet oder systematisch Datentransfers in Länder außerhalb der EU vorgenommen werden.[52] Die Anforderungen an den Beauftragten sind also an den konkreten Erfordernissen der jeweiligen Stelle auszurichten. So kann bei der einen Stelle, z.B. wegen des Bestehens spezieller Berufsgeheimnisse, das

---

50 *Düsseldorfer Kreis*, Beschluss vom 24./25.11.2010.

51 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 40.

52 *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 13 (bestätigt durch EDSA am 25.05.2018).

Erfordernis juristischer Kenntnisse im Vordergrund stehen, während es bei anderen Stellen vor allem auf technisch-organisatorische Kenntnisse ankommt. Insofern lässt sich auch nicht die Aussage treffen, dass bei der Benennung Personen mit bestimmter Vorbildung, also z.B. Juristen, Informatiker oder Betriebswirte, vorzugswürdig sind.

**Exkurs: Datenschutzberatung nur durch Rechtsanwälte?**

Der Pflicht zur Hinwirkung auf die Einhaltung des Datenschutzrechts ist immanent, dass sich der Datenschutzbeauftragte auch mit Rechtsfragen auseinandersetzen muss. Daher stellt sich die nicht abschließend geklärte Frage, inwiefern die Wahrnehmung des Amtes des Datenschutzbeauftragten durch andere Personen als Rechtsanwälte mit den **Bestimmungen des Rechtsdienstleistungsgesetzes (RDG)** vereinbar ist. Hierzu ist zunächst festzustellen, dass das RDG ausschließlich selbstständig erbrachte (außergerichtliche) Rechtsdienstleistungen regelt (§ 3 RDG). Die Erbringung von Rechtsdienstleistungen in abhängiger Beschäftigung wird dagegen vom RDG nicht erfasst, so dass sich ein Konflikt im Hinblick auf interne Beauftragte bereits deshalb ausschließt. Im Hinblick auf die Tätigkeit eines externen Datenschutzbeauftragten ist zu differenzieren. Nach § 2 Abs. 1 RDG ist eine Rechtsdienstleistung eine Tätigkeit, die in einer konkreten fremden Angelegenheit erbracht wird und eine rechtliche Prüfung des Einzelfalls erfordert. Schulungen, Publikationen sowie allgemeine Rechtsauskünfte des Beauftragten, die einen großen Teil seiner Tätigkeit ausmachen, unterfallen mangels Bezug auf einen konkreten Einzelfall nicht § 2 Abs. 1 RDG. Das Gleiche gilt für das reine Auffinden von Lektüre oder Fundstellen oder die Wiedergabe bzw. allein schematische Anwendung von Rechtsvorschriften. Selbst wenn „echte“ rechtliche Prüfungen im Sinne von einzelfallbezogenen juristischen Subsumtionsvorgängen durchgeführt werden, so ergibt sich daraus nicht zwingend, dass das Amt des Datenschutzbeauftragten nur von einem Rechtsanwalt bekleidet werden darf. Erlaubt sind nach § 5 Abs. 1 RDG nämlich auch Rechtsdienstleistungen im Zusammenhang mit einer anderen Tätigkeit, wenn sie als „Nebenleistung“ zum Berufs- oder Tätigkeitsbild gehören. Bei der Tätig-

keit des Datenschutzbeauftragten steht aber die rechtliche Beratung nicht im Mittelpunkt, vielmehr handelt es sich im Schwerpunkt um eine Management- und Organisationsaufgabe.

Das erforderliche Fachwissen muss grundsätzlich **bereits im Zeitpunkt der Benennung des Beauftragten** gegeben sein. Im Einzelfall können allerdings zu Beginn der Benennung noch bestehende Informationsdefizite durch den Besuch entsprechender Fortbildungsveranstaltungen ausgeglichen werden. Ohnedies gilt, dass einmal erworbenes Fachwissen nicht ausreichend ist. Es besteht vielmehr die Verpflichtung zur laufenden Weiterbildung. Nach Art. 38 Abs. 2 DS-GVO sind dem Datenschutzbeauftragten die erforderlichen Ressourcen zur Erhaltung des Fachwissens zur Verfügung zu stellen.[53]

## 4.3 Fähigkeit zur Aufgabenerfüllung

### 4.3.1 Allgemeines

Die in Art. 37 Abs. 5 DS-GVO angesprochene Fähigkeit zur Aufgabenerfüllung setzt neben persönlicher **Integrität** und einem entsprechenden **Berufsethos** der zu benennenden Person **soziale Kompetenz, Kommunikationsfähigkeit und die Fähigkeit zu einem Risiko-Management** i.S.v. Art. 39 Abs. 2 DS-GVO voraus.[54] Zur notwendigen persönlichen Integrität gehört auch, dass der Datenschutzbeauftragte u.U. in der Lage ist, gegen die Interessen der Leitung des Verantwortlichen bzw. Auftragsverarbeiters zu handeln. Nicht jede Vorstrafe oder begangene Ordnungswidrigkeit schließt eine Benennung aus, in jedem Fall aber einschlägige Verhaltensweisen, wie z.B. der Verstoß gegen Vertraulichkeitsverpflichtungen. Der Umstand, dass der Datenschutzbeauftragte keine Aufgaben und Pflichten wahrnehmen darf, die zu einem **Interessenkonflikt** mit seiner Tätigkeit führen, ist in Art. 38 Abs. 6 DS-GVO gesondert geregelt.[55]

---

53 Zu Art. 38 Abs. 2 DS-GVO vgl. im Einzelnen 6.3.

54 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 37 Rn. 42.

55 Vgl. dazu im Einzelnen den nachfolgenden Abschnitt.

### 4.3.2 Keine Interessenkonflikte

Ein Interessenkonflikt ergibt sich regelmäßig dann, wenn der Datenschutzbeauftragte im Rahmen seiner sonstigen Tätigkeit für die gleiche Organisation Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt[56] und sich insofern selbst überwachen müsste. Ob ein „echter" Interessenkonflikt i.S.v. Art. 38 Abs. 6 Satz 2 DS-GVO vorliegt, der die Amtsübernahme ausschließt, kann regelmäßig nur im konkreten Einzelfall entschieden werden.[57]

Die nachfolgende Übersicht stellt entscheidende Leitlinien für die Beurteilung auf:

| **Position** | **Konflikt ja / nein** |
|---|---|
| **Inhaber** des Verantwortlichen bzw. Auftragsverarbeiters **oder Personen, die mit der Leitung betraut sind, wie Geschäftsführer oder Vorstände** | Ausgeschlossen von der Amtswahrnehmung |
| **Leiter und andere Schlüsselfiguren aus den Abteilungen IT[58], Personal, Vertrieb oder Marketing** | Regelmäßig ausgeschlossen |
| **Geldwäschebeauftragter** | Ausgeschlossen, da Tätigkeit personenbezogene Auswertungen erforderlich machen kann[59] |

[56] *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 19 (bestätigt durch EDSA am 25.05.2018).

[57] Ebenso *Art.-29-Datenschutzgruppe,* a.a.O.; *Bergt* in: Kühling/Buchner, Art. 38 Rn. 40.

[58] Zur Unvereinbarkeit der Position als „IT-Manager" vgl. BayLDA, 7. Tätigkeitsbericht (2015/2016), 4.1. Zur Frage, ob der IT-Dienstleister einer Stelle externer Datenschutzbeauftragter sein bzw. einen solchen stellen kann, siehe vorstehend 3.6.

[59] *LfDI Baden-Württemberg*, Praxisratgeber Die/der Beauftragte für den Datenschutz Teil 2, S. 11; *BayLDA*, 5. TB (2011/2012), S. 16; ähnlich *Bergt* in: Kühling/Buchner, Art. 38 Rn. 42 und *Laue/Nink/Kremer*, S. 201.

| | |
|---|---|
| **Leiter oder Mitarbeiter Revision** | Für diese Ämterkombination spricht, dass der Revisionsleiter bzw. Mitarbeiter die organisatorischen Abläufe bei dem Verantwortlichen bzw. Auftragsverarbeiter gut kennt sowie Prüf- und Audittechniken beherrscht, die auch im Rahmen der Datenschutzüberwachung zur Anwendung kommen.[60] Ein Konflikt entsteht, sofern der Datenschutzbeauftragte im Rahmen seiner Revisionstätigkeit selbst Datenauswertungen durchführt bzw. verantwortet.[61] |
| **Compliancebeauftragter/ Mitarbeiter aus dem Bereich Compliance** | Vgl. die vorstehenden Ausführungen zum Leiter/Mitarbeiter der Revision |
| **IT-Sicherheitsbeauftragter oder Mitarbeiter der IT-Sicherheit** | Empfehlenswerte Ämterkombination[62] |
| **Leiter oder Mitarbeiter der Rechtsabteilung** | Kombination nicht ausgeschlossen[63] |

60 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 28; für Revisionsmitarbeiter als Datenschutzbeauftragte BayLDA, 5. TB (2011/2012), S. 16 f.

61 *Jaspers/Reif*, a.a.O.; *Bergt* in: Kühling/Buchner, Art. 38 Rn. 42; *Heberlein* in: Ehmann/Selmayr, Art. 38 Rn. 23.

62 Vgl. auch *LAG Hamm*, Beschluss vom 8. April 2011 - 13 TaBV 92/10.

63 Für Beschäftigte der Rechtsabteilung als Datenschutzbeauftragte auch BayLDA, 5. TB (2011/2012), S. 16 f.; differenzierend *Bergt* in: Kühling/Buchner, Art. 38 Rn. 42; auch eine Benennung des Leiters der Rechtsabteilung ist denkbar nach Auffassung von *Heberlein* in: Ehmann/Selmayr, Art. 38 Rn. 23; ähnlich *Laue/Nink/ Kremer*, S. 201, nach denen der konkrete Aufgabenzuschnitt des Leiters entscheidend ist.

| | |
|---|---|
| **Betriebs-/Personalrat** | Nach einer BAG Entscheidung aus 2011[64] ist allein die Mitgliedschaft im Betriebsrat kein ausreichender Grund, die Zuverlässigkeit eines Datenschutzbeauftragten in Frage zu stellen.<br><br>Ein Konflikt kann sich aber ergeben, wenn die betreffende Person als Betriebsratsmitglied für die EDV des Betriebsrats zuständig ist.[65] |

Strittig ist, ob ein Teilzeit-Datenschutzbeauftragter aus einer EU-Niederlassung zugleich **Vertreter in der Union gemäß Art. 27 DS-GVO** sein kann. Der Europäische Datenschutzausschuss lehnt eine solche Personalunion ab und führt zur Begründung aus, dass der Datenschutzbeauftragte weisungsfrei und unabhängig zu sein habe, während der Vertreter nach Art. 27 DS-GVO vom Verantwortlichen bzw. Auftragsverarbeiter bevollmächtigt sei und in dessen Interesse sowie unter dessen direkter Weisung handele.[66] In der rechtswissenschaftlichen Literatur wird demgegenüber zum Teil eine vermittelnde Auffassung vertreten: Ein Interessenkonflikt i.S.v. Art. 38 Abs. 6 Satz 2 DS-GVO bestehe bei bloßer Aufgabenerfüllung als Anlaufstelle nicht. Nur wenn die Vertreterposition vertraglich mit weiteren Aufgaben i.S.v. Art. 4 Nr. 17 DS-GVO aufgeladen werde, ergebe sich ein Konflikt.[67]

64 Urteil vom 23.03.2011 - 10 AZR 562/09 -, RDV 2011, 237; NZA 2011, 1036.

65 *Bergt* in: Kühling/Buchner, Art. 38 Rn. 45. Zur Überwachung des Betriebsrats durch den Datenschutzbeauftragten vgl. Abschnitt 5.3.

66 Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), Version for public consultation, adopted on 16.11.2018, S. 20 f.; ablehnend auch *Piltz* in: Gola, DS-GVO, Art. 27 Rn. 6; *Kremer* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 27 Rn. 16.

67 *Franck*, RDV 2018, 303, 307.

### 4.3.3 Zusammenfassung

| Anforderungen an den Datenschutzbeauftragten (Überblick) | |
|---|---|
| **Berufliche Qualifikation, insbes. Fachwissen** | **Fähigkeit zur Aufgabenerfüllung** |
| **Aspekte**<br>• Rechtliche Kenntnisse, insbes. DS-GVO und BDSG 2018<br>• Technische Kenntnisse:<br>Beratung im Hinblick auf und Überwachung von Datensicherheitsmaßnahmen<br>• Praktische/organisatorische Kenntnisse<br>- Kenntnisse im praktischen DS-Management<br>- Betriebswirtschaftliches Verständnis<br>- Kenntnis der Strukturen der zu betreuenden Stelle bzw. des einschlägigen Wirtschaftszweigs<br>**Maßstab**<br>• Art der durchgeführten Datenverarbeitungsvorgänge<br>• Schutzbedarf der verarbeiteten personenbezogenen Daten | **Aspekte**<br>• Persönliche Integrität<br>• Berufsethos, soziale Kompetenz, Kommunikationsfähigkeit, risikoorientiertes Arbeiten<br>• Bei Teilzeit-DSB:<br>keine Interessenkollisionen, die sachgemäße Aufgabenerledigung verhindern |

# 5. Aufgaben des Datenschutzbeauftragten

## 5.1 Überblick

Nach Art. 39 Abs. 1 DS-GVO kommen dem Datenschutzbeauftragten folgende Aufgaben zu:

- Unterrichtung und Beratung (Art. 39 Abs. 1 Buchst. a) DS-GVO)
- Überwachung der Einhaltung des Datenschutzes (Art. 39 Abs. 1 Buchst. b) DS-GVO)
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) und Überwachung ihrer Durchführung (Art. 39 Abs. 1 Buchst. c) DS-GVO)
- Zusammenarbeit mit der Aufsichtsbehörde (Art. 39 Abs. 1 Buchst. d) und e) DS-GVO)

Die Aufgabenwahrnehmung durch den Datenschutzbeauftragten hat dabei nach Art. 39 Abs. 2 DS-GVO risikoorientiert zu erfolgen.[68]

Weitere Aufgaben des Datenschutzbeauftragten sind in Art. 38 DS-GVO enthalten. So berichtet der Datenschutzbeauftragte nach Art. 38 Abs. 3 Satz 3 DS-GVO unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters. Gemäß Art. 38 Abs. 4 DS-GVO unterstützt der Datenschutzbeauftragte außerdem die betroffenen Personen, sofern diese Fragen zur Verarbeitung ihrer Daten oder zur Wahrnehmung ihrer Rechte haben.

Dem Datenschutzbeauftragten dürfen **weitere Aufgaben** übertragen werden, die über die in der DS-GVO ausdrücklich vorgesehenen Aufgaben hinausgehen bzw. diese präzisieren,[69] sofern hierdurch keine Interessenkonflikte[70] entstehen und genügend Zeit für die Pflichtaufgaben verbleibt.[71] Insbesondere kann dem Datenschutzbeauftragten die Auf-

---

68 Zu Art. 39 Abs. 2 DS-GVO vgl. im Einzelnen Abschnitt 5.7.

69 Vgl. auch *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 20, Fn. 35 (bestätigt durch EDSA am 25.05.2018).

70 *Datenschutzkonferenz*, Kurzpapier Nr. 12 „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“ (Stand: 16.01.2018), S. 3.

71 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 8.

gabe übertragen werden, die Mitarbeiter zum Datenschutz zu schulen, wie es auch nach dem BDSG a.F. seine Aufgabe war. Auch die Führung des Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DS-GVO) kann dem Datenschutzbeauftragten übertragen werden.[72] Die notwendigen Informationen für das Verzeichnis beizubringen bleibt Aufgabe der Fachabteilung, die die Verantwortung für die Verarbeitung und das Vorhandensein und die Vollständigkeit der Dokumentation trägt.[73] Die Durchführung der Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) kann dem Datenschutzbeauftragten nicht überantwortet werden.[74]

## 5.2 Unterrichtung und Beratung

Der Datenschutzbeauftragte hat den Verantwortlichen bzw. Auftragsverarbeiter sowie die konkret mit der Datenverarbeitung Beschäftigten hinsichtlich ihrer Pflichten nach der DS-GVO sowie nach den sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten zu unterrichten und beraten (Art. 39 Abs. 1 Buchst. a) DS-GVO). **Unterrichtung** meint insofern die allgemeine Information über die bestehenden datenschutzrechtlichen Pflichten, **Beratung** die Unterstützung bei der Lösung von konkreten datenschutzrechtlichen Fragestellungen.[75] Richtig verstanden ist der Datenschutzbeauftragte dabei Berater in der Weise, dass er an der Legalisierung legitimer Verarbeitungen mitwirkt, also nicht nur „Nein“ sagt, sondern auch datenschutzkonforme Lösungswege aufzeigt.

Die **Schulung der Mitarbeiter**, d.h. die zielgerichtete pädagogische Aufbereitung der für die konkret ausgeübte Tätigkeit relevanten datenschutzrechtlichen Informationen ist hingegen – anders als nach BDSG a.F. – nicht Aufgabe des Datenschutzbeauftragten, sondern des

---

72 *Art.-29-Datenschutzgruppe*, WP 243 rev. 01, S. 22 (bestätigt durch EDSA am 25.05.2018).

73 *Jaspers/Reif*, a.a.O.

74 *Jaspers/Reif*, a.a.O.

75 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 9 ff.

für die Verarbeitung Verantwortlichen.[76] Nach der DS-GVO kommt dem Datenschutzbeauftragten bezüglich der Schulung lediglich eine beratende bzw. überwachende[77] Funktion zu. Der für die Verarbeitung Verantwortliche ist jedoch frei, dem Datenschutzbeauftragten auch die Durchführung der Schulungsaufgabe zu übertragen.

## 5.3 Überwachung der Einhaltung des Datenschutzes

Weitere Kernaufgabe des Datenschutzbeauftragten neben der Unterrichtung und Beratung ist die **Überwachung der Einhaltung des Datenschutzes** (Art. 39 Abs. 1 Buchst. b) DS-GVO). Zu überwachen ist im Einzelnen die Einhaltung

- der **DS-GVO**,
- **anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten** sowie
- der **Strategien des Verantwortlichen oder Auftragsverarbeiters für den Schutz personenbezogener Daten** (einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen).

Die Verpflichtung zur Überwachung der Datenschutzkonformität des Unternehmenshandelns war auch schon Bestandteil der „Hinwirkungspflicht“ des Datenschutzbeauftragten nach BDSG a.F. Die Funktion des Datenschutzbeauftragten als Überwachungsorgan erfährt durch die DS-GVO aber eine erhebliche Ausprägung, indem dem Datenschutzbeauftragten einerseits operative Aufgaben wie die Mitarbeiterschulung, die Vorabkontrolle und die Bereitstellung des Verfahrensverzeichnisses für jedermann nicht mehr zufallen, ihm aber andererseits zudem die

---

[76] Anderer Ansicht *Paal* in: Paal/Pauly, Art. 39 Rn. 5 f.; wie hier *Bergt* in: Kühling/Buchner, Art. 39 Rn. 12; *Klug* in: Gola, DS-GVO, Art. 39 Rn. 4; *Marschall/Müller*, ZD 2016, 415, 418.

[77] Fraglich ist, ob es sich bei der Datenschutzschulung um eine betriebliche Bildungsmaßnahme nach § 98 BetrVG handelt mit der Folge, dass diese mitbestimmungspflichtig ist. Jedenfalls rein arbeitsplatzbezogene Unterweisungen ohne weiterbildenden Charakter dürften wohl nicht unter § 98 BetrVG fallen.

Überwachung der Einhaltung der Datenschutzstrategien des Verantwortlichen bzw. Auftragsverarbeiters übertragen wird.

Trotz der Ausweitung der Überwachungsaufgabe durch die DS-GVO ist eine **Einordnung** des Datenschutzbeauftragten **als sog. Überwachergarant abzulehnen**.[78] Jedenfalls allein auf Basis der gesetzlichen Aufgabenbeschreibung besitzt nämlich der Datenschutzbeauftragte nach wie vor keine eigenen Entscheidungs- oder Weisungsbefugnisse, um Datenschutzverletzungen zu unterbinden.[79] Letztere sind aber notwendig für die Stellung als Überwachergarant.

**Tätigkeitsschwerpunkte im Rahmen der Überwachungsfunktion** sind das Sammeln von Informationen, um Verarbeitungsaktivitäten zu identifizieren, die Analyse und Überprüfung der Verarbeitungsaktivitäten auf Einhaltung der rechtlichen Vorgaben, die Information und Beratung des Verantwortlichen oder Auftragsverarbeiters sowie die Abgabe von Empfehlungen an diesen.[80]

Nach einer Entscheidung des BAG[81] aus dem Jahr 1997 sollte der Datenschutzbeauftragte nach BDSG a.F. nicht berechtigt sein, eine **Datenschutzkontrolle beim Betriebsrat** durchzuführen, was faktisch zu einem kontrollfreien Raum bei der verantwortlichen Stelle führte. Heute dürften aufgrund der unmittelbaren Geltung der höherrangigen DS-GVO die Argumente für ein Überwachungsrecht des Datenschutzbe-

---

78 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 14; *Helfrich* in: Sydow, Europäische Datenschutzgrundverordnung, 2018, Art. 39 Rn. 72; *Lantwin*, ZD 2017, 411, 414; anderer Ansicht *Bergt* in: Kühling/Buchner, Art. 37 Rn. 55; *Wybitul*, ZD 2016, 203, 205; *Wybitul/von Gierke*, BB 2017, 181, 182; *Laue/Nink/Kremer*, S. 211; tendenziell dafür, im Ergebnis aber offen *Golla*, RDV 2017, 123, 127; für „klärungsbedürftig“ hält die Garantenstellung *Paal* in: Paal/Pauly, Art. 39 Rn. 12; unentschieden letztlich auch *Nolde*, PinG 2017, 114, 119. Bereits unter dem BDSG a.F. sprach sich *Marschall*, ZD 2014, 66, 68 für eine Garantenstellung aus.

79 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 14.

80 *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 20 (bestätigt durch EDSA am 25.05.2018); *LDI*, Häufig gestellte Fragen zum Datenschutzbeauftragten (FAQ), Stand: 11/2018, S. 21.

81 Beschluss vom 11.11.1997 - 1 ABR 21/97 -, RDV 1998, 64; NJW 1998, 2466; NZA 1998, 385.

auftragten auch gegenüber dem Betriebsrat überwiegen.[82] Insofern ist es Aufgabe des Betriebsrats, nicht personenbezogene allgemeine Informationen zur Betriebsratstätigkeit durch entsprechende organisatorische Vorkehrungen vor unerwünschter Kenntnisnahme zu schützen. Bewusst Aspekte auszuforschen, die nicht zur Aufgabenstellung gehören, bzw. entsprechende Zufallserkenntnisse weiterzugeben, die anlässlich der Überprüfung des Betriebsrats gewonnen wurden, wird dem Datenschutzbeauftragten im Übrigen aus persönlichkeitsrechtlichen Gründen untersagt sein.[83]

Die BAG-Entscheidung aus 1997 bezog sich allein auf die Einsichts- und Nachschaurechte des Datenschutzbeauftragten beim Betriebsrat. Schon nach altem Recht war dem Datenschutzbeauftragten insofern nicht verboten, der Unternehmensleitung Zweifel im Hinblick auf die Datenschutzkonformität von solchen Verfahrensweisen des Betriebsrats mitzuteilen, die unternehmensintern bzw. ihm auf Grund von Beschwerden bekannt sind.

Auch wenn DS-GVO/BDSG bzw. das BetrVG/BPersVG keine ausdrücklichen Aussagen über das **Miteinander von Datenschutzbeauftragtem und Mitarbeitervertretung** machen, sollte im Übrigen die von der Sache her gebotene Zusammenarbeit selbstverständlich sein. Schließlich verfolgen der Datenschutzbeauftragte und der Betriebs-/Personalrat im Hinblick auf die Personaldatenverarbeitung die gleiche Zielsetzung, nämlich die Wahrung der Persönlichkeitsrechte der betroffenen Mitarbeiter zu gewährleisten. Ausgangspunkt der Datenschutzpflichten des Betriebsrats ist dabei § 75 Abs. 2 BetrVG, welcher die Mitarbeitervertretung verpflichtet, sich für die Förderung der freien Entfaltung der Persönlichkeit der Arbeitnehmer und damit insbesondere für den Persönlichkeitsrechtsschutz bei den durch automatisierte Datenverarbei-

---

82 *Gola/Pötters*, RDV 2017, 279, 283; *Kort*, ZD 2017, 3, 6; *Taeger/Rose*, BB 2016, 819, 828; *Bergt* in: Kühling/Buchner, Art. 38 Rn. 18; *Paal* in: Paal/Pauly, Art. 39 Rn. 6b; für ein Überwachungsrecht, sofern man den Betriebsrat als Teil des Verantwortlichen wertet, auch *Wybitul/v. Gierke* BB 2017, 181, 184; anderer Ansicht *Dotting*, AiB 2018, 42 f.

83 Für eine Berechtigung und Verpflichtung des Datenschutzbeauftragten, Informationen vertraulich zu behandeln, die ihm im Rahmen einer Beratung oder Überwachung des Betriebsrates bekannt geworden sind, auch *Gola/Pötters*, ebd.

tung eröffneten Möglichkeiten der Mitarbeiterkontrolle einzusetzen, sowie § 80 Abs. 1 Nr. 1 BetrVG, wonach es zu den Aufgaben des Betriebsrats gehört, die Einhaltung der zu Gunsten der Mitarbeiter geltenden Normen zu überwachen. Arbeitnehmerschutzvorschriften im letztgenannten Sinne sind auch die Regelungen des § 26 BDSG. Datenschutzbeauftragter und Mitarbeitervertretung verfolgen ihren Kontrollauftrag allerdings unabhängig voneinander, so dass es in der Praxis durchaus zu unterschiedlichen datenschutzrechtlichen Bewertungen kommen kann. Bei datenschutzrechtlichen Fragen des Betriebsrats ist der Datenschutzbeauftragte der **„geborene Sachverständige“**[84], der vom Betriebsrat zunächst zu befragen ist, bevor auf den externen Sachverstand von Rechtsanwälten etc. zurückgegriffen werden darf (§ 80 Abs. 2 Satz 4, Abs. 3 BetrVG).

## 5.4 Aufgaben im Zusammenhang mit der Datenschutz-Folgenabschätzung

Anders als die Vorabkontrolle nach dem BDSG a.F. ist die Durchführung der **Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)** dem Datenschutzbeauftragten nicht übertragen. Zuständig ist vielmehr der für die Verarbeitung Verantwortliche und damit in abgeleiteter Verantwortung die jeweilige Fachabteilung. Die Aufgaben des Datenschutzbeauftragten im Zusammenhang mit der Datenschutz-Folgenabschätzung liegen zum einen in der **Überwachung, ob diese ordnungsgemäß durchgeführt wird**, und zum anderen in der Verpflichtung, **auf Anfrage** im Hinblick auf deren Durchführung **zu beraten** (Art. 39 Abs. 1 Buchst. c) DS-GVO). Korrespondierend zur Beratungspflicht des Datenschutzbeauftragten besteht eine Verpflichtung der Fachabteilung, dessen Rat auch einzuholen (Art. 35 Abs. 2 DS-GVO). Falls den Empfehlungen des Datenschutzbeauftragten im Zusammenhang mit der Datenschutz-Folgenabschätzung nicht gefolgt wird, ist in der Dokumentation

[84] *Gola/Schomerus*, BDSG a.F., § 4f Rn. 36.

ausdrücklich schriftlich zu begründen, warum (Nachweispflicht aus Art. 24 Abs. 1 DS-GVO).[85]

Die **Durchführung der Datenschutz-Folgenabschätzung kann** dem Datenschutzbeauftragten **nicht übertragen werden**, denn dann entfiele die von der DS-GVO insoweit vorgesehene Überwachungsinstanz und der Datenschutzbeauftragte müsste sich selbst überwachen.[86]

## 5.5 Zusammenarbeit mit der Aufsichtsbehörde

Nach der DS-GVO arbeitet der Datenschutzbeauftragte mit der Aufsichtsbehörde zusammen und fungiert als deren „Anlaufstelle"; zudem berät sich der Datenschutzbeauftragte mit der Behörde „zu allen sonstigen Fragen" (Art. 39 Abs. 1 Buchst. d) und e) DS-GVO).

Die **Tätigkeit als Anlaufstelle für die Behörde** bezieht sich auf die Fälle der vorherigen Konsultation (Art. 36 DS-GVO) durch den Verantwortlichen sowie alle anderen mit der Verarbeitung personenbezogener Daten zusammenhängenden Fragen. Der Datenschutzbeauftragte ist erster Ansprechpartner für die Behörde und koordiniert den Kontakt mit der datenschutzrechtlich verantwortlichen Unternehmensleitung und der zuständigen Fachabteilung. Durch die Pflicht des Verantwortlichen bzw. Auftragsverarbeiters, der Aufsichtsbehörde die Kontaktdaten des Datenschutzbeauftragten zur Verfügung zu stellen (Art. 37 Abs. 7 DS-GVO), ist sichergestellt, dass eine direkte Kontaktaufnahme seitens der Behörde problemlos möglich ist.[87] Wichtig im Verhältnis zwischen Aufsichtsbehörde und Datenschutzbeauftragtem ist, dass es sich um voneinander unabhängige Überwachungsorgane handelt. Der Datenschutzbeauftragte ist nicht etwa Gehilfe der Behörde, sondern zur eigenständigen Meinungsbildung berechtigt und verpflichtet.

---

85 *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 20 f. (bestätigt durch EDSA am 25.05.2018).

86 *Heberlein* in: Ehmann/Selmayr, Art. 39 Rn. 21; *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 8.

87 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 19.

Ein Anlass zur **Konsultation der Behörde** durch den Datenschutzbeauftragten wird sich insbesondere dann ergeben, wenn sich dieser über die Auslegung einschlägiger gesetzlicher Regelungen oder die Angemessenheit einzelner Datenschutzmaßnahmen im Unklaren ist. Nach Art. 57 Abs. 3 DS-GVO erfolgt die Beratung durch die Behörde für den Datenschutzbeauftragten unentgeltlich.

Eine **Verpflichtung des Datenschutzbeauftragten, eigeninitiativ Datenschutzverstöße an die Behörde zu melden, ist** aufgrund fehlender konkreter Anhaltspunkte hierfür in der DS-GVO und wegen der damit verbundenen weitreichenden Konsequenzen für den Datenschutzbeauftragten **abzulehnen**.[88] Bevor der Datenschutzbeauftragte einen Verstoß an die Behörde meldet, hat er im Übrigen zunächst alle internen Möglichkeiten auszuschöpfen, um diesen abzustellen.[89] Dies ergibt sich aus der Treuepflicht gegenüber dem Arbeit- bzw. Auftraggeber.

## 5.6 „Anwalt der betroffenen Personen“

Nach Art. 38 Abs. 4 DS-GVO können betroffene Personen den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer Daten und mit der Wahrnehmung ihrer Rechte aus der Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen. **Der Datenschutzbeauftragte ist** demnach **verpflichtet, Datenschutzbeschwerden zu prüfen und die betroffenen Personen über das Ergebnis seiner Prüfung zu informieren.** Stellt er Datenschutzverletzungen, z.B. die Missachtung von Betroffenenrechten, fest, hat er darauf hinzuwirken, dass diese abgestellt werden.

Die Anrufung des Datenschutzbeauftragten ist **nicht formgebunden**, kann also auch mündlich erfolgen. Von der Anrufung des Datenschutz-

---

88 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 20. Für eine Informationspflicht bei besonders schweren Verstößen ist *Heberlein* in: Ehmann/Selmayr, Art. 39 Rn. 19. Etwas zurückhaltender *Bergt* in: Kühling/Buchner, Art. 39 Rn. 19 („[…] auch wenn der Datenschutzbeauftragte – allenfalls mit Ausnahme besonders schwerer Verstöße wie Straftaten – nicht verpflichtet ist, von sich aus Verstöße gegen Datenschutzrecht der Aufsichtsbehörde zu melden.“).

89 So auch *Paal* in: Paal/Pauly, Art. 39 Rn. 8.

beauftragten zu unterscheiden sind **allgemeine Datenschutzanfragen** sowie Eingaben, mit denen die betroffene Person ihre Rechte nach Art. 12 ff. DS-GVO geltend macht, wie z.B. Berichtigungs- oder Löschungsansprüche oder Widersprüche. Für solche Anfragen ist die Unternehmensleitung zuständig bzw. in abgeleiteter Verantwortung die jeweilige Fachabteilung.

Insbesondere Beschäftigte des Verantwortlichen, die sich an den Datenschutzbeauftragten wenden, haben regelmäßig ein Bedürfnis, dass der Datenschutzbeauftragte ihre Angelegenheiten vertraulich behandelt. Die Wahrung der Vertraulichkeit ist essenziell für eine effektive Ausübung der Tätigkeit als Datenschutzbeauftragter. Art. 38 Abs. 5 DS-GVO verpflichtet den Datenschutzbeauftragten insofern zur **Wahrung der Geheimhaltung bzw. Vertraulichkeit** bei der Erfüllung seiner Aufgaben, überlässt allerdings die nähere Ausgestaltung dieser Verpflichtung dem Unionsrecht bzw. Recht der Mitgliedstaaten.[90]

Auf Art. 38 Abs. 5 DS-GVO beruht **§ 6 Abs. 5 Satz 2 i.V.m. § 38 Abs. 2 BDSG 2018**, wonach der Datenschutzbeauftragte zur **Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf diese zulassen**, verpflichtet ist, soweit er nicht von dieser befreit wird. Datenschutzbeauftragte, die für einen Berufsgeheimnisträger tätig sind, können sich bei Verletzung der Vertraulichkeit strafbar machen (§ 203 Abs. 4 Satz 1 StGB). Solchen Datenschutzbeauftragten steht zur Absicherung der Verschwiegenheit ein Zeugnisverweigerungsrecht zu (§ 6 Abs. 6 i.V.m. § 38 Abs. 2 BDSG 2018).

Die Verschwiegenheitspflicht führt insbesondere dazu, dass die betroffene Person in Äußerungen und Berichten des Datenschutzbeauftragten **nicht namentlich genannt werden darf**. Ebenso wenig darf diese auf Grund der Umstände oder der Sachverhaltsdarstellung bestimmbar sein. Kann ein Datenschutzverstoß nicht aufgeklärt oder wird abgestellt werden, ohne dass die Identität nachvollziehbar wird, muss der Datenschutzbeauftragte Rücksprache nehmen. Die betroffene Person muss dann entscheiden, ob sie den Beauftragten von der Ver-

[90] *Heberlein* in: Ehmann/Selmayr, Art. 38 Rn. 19; *Bergt* in: Kühling/Buchner, Art. 38 Rn. 38; *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 25.

pflichtung zur Verschwiegenheit entbindet oder aber auf dessen weiteres Tätigwerden verzichtet.

Für den Verantwortlichen bzw. Auftragsverarbeiter ergeben sich in organisatorischer Sicht folgende Pflichten:[91]

- **Zurverfügungstellung eines E-Mail-Postfachs speziell für die Tätigkeit als Datenschutzbeauftragter** (dsb@firma.de) **sowie einer von Dritten nicht abhörbaren Mailbox**,
- **Ausnahme** des Telefonanschlusses des Datenschutzbeauftragten **von einer ggf. stattfindenden Telefondatenerfassung** und
- **ungeöffnete Weiterleitung von** an den Datenschutzbeauftragten adressierter **Post.**

Dem Datenschutzbeauftragten sollte ein **eigenes Büro** zur Verfügung stehen. Jedenfalls muss er die Möglichkeit haben, Telefonate und Gespräche vertraulich zu führen.

## 5.7 Verpflichtung zur risikoorientierten Tätigkeit

Nach Art. 39 Abs. 2 DS-GVO hat der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung zu tragen, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt, sog. **Pflicht zur risikoorientierten Tätigkeit**. Mit Verarbeitungen, die aufgrund des hohen Risikos für die Rechte und Freiheiten der betroffenen Personen einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) bedürfen, wird der Datenschutzbeauftragte sich danach regelmäßig zeitnah befassen müssen.[92] Dasselbe gilt für an ihn gerichtete Beschwerden betroffener Personen. Zur Gewährleistung der garantierten **Unabhängigkeit** (ErwG 97 DS-GVO) muss im Übrigen die Bewertung, welche Verarbeitungsvorgänge wegen des mit ihnen verbundenen Risikos einer vorrangigen Prüfung bedürfen, dem Datenschutzbeauftragten selbst obliegen. So dürfen etwa Prüfaufträge gegenüber

---

91 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, a.a.O.

92 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 23; *Heberlein* in: Ehmann/Selmayr, Art. 39 Rn. 22f.

dem Datenschutzbeauftragten diesen nicht daran hindern, aus seiner Sicht vordringlichen datenschutzrechtlichen Angelegenheiten nachzugehen.

Bemerkenswert im Zusammenhang mit Art. 39 Abs. 2 DS-GVO ist, dass die DS-GVO hier im Gegensatz zu allen anderen Stellen nur von Risiko spricht und nicht von Risiko für die Rechte und Freiheiten betroffener Personen. Dies spricht dafür, dass der Datenschutzbeauftragte insofern **– auch – das Risiko für das Unternehmen zu berücksichtigen** hat. Schließlich soll der Datenschutzbeauftragte das Unternehmen unterstützen.

## 5.8 Bericht an die Leitung und Dokumentation der Tätigkeit als Datenschutzbeauftragter

Nach Art. 38 Abs. 3 Satz 3 DS-GVO **berichtet der Datenschutzbeauftragte unmittelbar der höchsten Managementebene** des Verantwortlichen oder Auftragsverarbeiters.[93] Eine Verpflichtung zur Dokumentation seiner Tätigkeit ist in der DS-GVO nicht enthalten. Die **Dokumentation der Tätigkeit** ist gleichwohl **im Eigeninteresse ratsam**, insbesondere damit der Datenschutzbeauftragte sich entlasten kann, falls er haftbar gemacht werden soll.[94] Eine Dokumentation ist vor allem dann von Bedeutung, wenn Empfehlungen und Einwänden des Datenschutzbeauftragten nicht oder nicht ausreichend Rechnung getragen werden.[95]

Ein Mittel zur Entlastung des Datenschutzbeauftragten können auch regelmäßige an die Leitung gerichtete **Tätigkeitsberichte** sein.[96] Insbesondere bei Berichtswegen, die entgegen den gesetzlichen Vorgaben nicht unmittelbar zur Unternehmensleitung führen, hilft ein solcher an die Geschäftsleitung gerichteter Bericht, eine entsprechende Bösgläu-

---

93 Zu den organisatorischen Konsequenzen der Regelung vgl. Abschnitt 6.2.

94 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 28; *Heberlein* in: Ehmann/Selmayr, Art. 39 Rn. 8; ebenso *Datenschutzkonferenz*, Kurzpapier Nr. 12 (Stand: 16.01.2018), S. 4.

95 *Heberlein* in: Ehmann/Selmayr, Art. 39 Rn. 8.

96 *Laue/Nink/Kremer*, S. 211.

bigkeit der Unternehmensleitung herbeizuführen. Zugleich ermöglicht ein Tätigkeitsbericht, die Aufmerksamkeit rechtzeitig auf sich anbahnende Veränderungen im Verarbeitungsbereich bzw. im Bereich der Informationstechnologie zu lenken.

Der **Aufbau eines Tätigkeitsberichts**[97] kann etwa wie folgt aussehen:

1. Bericht über Aktivitäten im abgelaufenen Berichtsjahr
   - Prüfung von (Neu-)Konzeptionen / geplanten Verfahren im Hinblick auf Datenschutzbelange
   - Weitere durchgeführte Prüfungen und Beanstandungen (z.B. Entsorgung, vertrauliche Behandlung von Unterlagen)
   - Stellungnahmen zu sonstigen datenschutzrelevanten Sachverhalten bzw. zu Mitarbeiteranfragen an den DSB
   - Angefallene Datenschutzbeschwerden (Kunden bzw. Mitarbeiter)
   - Informations- und Beratungsaktivitäten; ggf. Schulungstätigkeit, soweit diese Aufgabe übertragen wurde
2. Für das Folgejahr geplante Aktivitäten bzw. anstehende Entwicklungen (z.B. Gesetzesänderungen, Trends im Datenschutz)

Selbstverständlich hat der Datenschutzbeauftragte beim Verfassen des Berichts seine **Verschwiegenheitsverpflichtung** (§ 6 Abs. 5 Satz 2 i.V.m. § 38 Abs. 2 BDSG 2018) zu beachten.

Bei einem **Wechsel des Datenschutzbeauftragten** ist auf eine **Übergabe der relevanten Unterlagen des bisherigen Datenschutzbeauftragten** an den neuen Datenschutzbeauftragten zu achten, um im Interesse des Unternehmens und der betroffenen Personen (Kunden, Mitarbeiter, Lieferanten etc.) eine möglichst reibungslose und effektive Weiterarbeit des neuen Datenschutzbeauftragten sicherzustellen sowie die Persönlichkeitsrechte der betroffenen Personen zu wahren.[98]

---

[97] Die nachfolgende Darstellung orientiert sich an *Schaffland/Wiltfang*, BDSG a.F., § 4g Rn. 42.

[98] *BayLDA*, 7. Tätigkeitsbericht (2015/2016), S. 36.

Zu übergeben sind insbesondere Dokumentationen über durchgeführte Beratungen und Überwachungsmaßnahmen im Hinblick auf noch aktuelle Unternehmensprozesse, beim Datenschutzbeauftragten noch laufende Beschwerdefälle von betroffenen Personen sowie für die Zukunft noch relevante abgeschlossene Fälle und für das Unternehmen erstellte Tätigkeitsberichte. Vertraulich an die konkrete Person des Datenschutzbeauftragten gerichtete Anfragen und Beschwerden von betroffenen Personen sind zu löschen bzw. zu vernichten; bei noch laufenden Fällen vertraulicher Art ist durch Rückfrage bei der betroffenen Person zu klären, wie diese ihr Anliegen weiterbehandelt haben möchte.[99]

# 6. Rechtsstellung des Datenschutzbeauftragten

## 6.1 Überblick

Entscheidend für die Rechtsstellung des Datenschutzbeauftragten sind die nachfolgend aufgezählten rechtlichen Gewährleistungen:

- Unabhängigkeit, insbesondere Weisungsfreiheit
- Anspruch auf Einbindung, Zugang und Ressourcen
- Abberufungs- und Kündigungsschutz
- Benachteiligungsverbot

[99] Zum gesamten Absatz vgl. *BayLDA*, a.a.O. Zu Konfliktsituationen bei Amtsübergabe und insbes. der Frage, ob auf das E-Mail-Postfach des bisherigen Datenschutzbeauftragten zugegriffen werden darf, vgl. Piltz BvD-NEWS Ausgabe 3/2018, S. 40 ff. (https://www.bvdnet.de/wp-content/uploads/2018/11/News18-3_web.pdf).

## 6.2 Unabhängigkeit, insbes. Weisungsfreiheit und organisatorische Stellung des Datenschutzbeauftragten

Die Unabhängigkeit ist Kern der Rechtsstellung des Datenschutzbeauftragten. Als übergeordnete Gewährleistung wird sie in ErwG 97 DS-GVO angesprochen. Die unmittelbaren Ausprägungen der Unabhängigkeit, nämlich insbesondere die Weisungsfreiheit und der unmittelbare Berichtsweg zur höchsten Managementebene, sind im normativen Teil der DS-GVO geregelt (Art. 38 Abs. 3 Sätze 1 und 3).

Zentrales Element der Weisungsfreiheit ist, dass der Datenschutzbeauftragte **unabhängig bezüglich der datenschutzrechtlichen Beurteilung der stattfindenden Datenverarbeitungsvorgänge** ist. Der Datenschutzbeauftragte ist insofern nicht Anwalt des Verantwortlichen, der dessen Rechtsauffassung vertritt und verteidigt, sondern er ist zur Meinungsbildung nach seinen eigenen Kenntnissen und Erfahrungen verpflichtet.

Der Datenschutzbeauftragte darf selbst entscheiden, wie er seine Aufgaben priorisiert und welche Systeme und Prozesse einer Prüfung unterzogen werden sollen. Zwar trifft ihn hierbei die Pflicht zur risikoorientierten Tätigkeit (Art. 39 Abs. 2 DS-GVO). Zur Gewährleistung der garantierten Unabhängigkeit obliegt aber auch die Bewertung, welche Verarbeitungsvorgänge wegen des mit ihnen verbundenen Risikos einer vorrangigen Betrachtung bedürfen, grundsätzlich dem Datenschutzbeauftragten selbst.[100] Gleichwohl nicht ausgeschlossen ist, dass der Verantwortliche bzw. Auftragsverarbeiter **den Datenschutzbeauftragten um die Prüfung datenschutzrelevanter Sachverhalte ersucht**. Denn die Beratung der benennenden Stelle gehört zu seinen zentralen Aufgaben, wobei die diesbezügliche Initiative auch vom Verantwortlichen bzw. Auftragsverarbeiter selbst ausgehen kann. Solange er nicht gehindert wird, aus seiner Sicht vordringlichen datenschutzrechtlichen Angelegenheiten nachzugehen, muss sich der Datenschutzbeauftragte entsprechenden Anfragen daher annehmen.

---

[100] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 23; *Bergt* in: Kühling/Buchner, Art. 39 Rn. 23.

**Überwachungs- bzw. Prüfaufgaben** werden dem Datenschutzbeauftragten in der Praxis zum Teil auch **durch Betriebs- bzw. Dienstvereinbarung** übertragen. Hierbei ist allerdings Vorsicht geboten. Die Übertragung darf keine sachfremden oder operativen Tätigkeiten erfassen (z.B. die Pflege des Berechtigungskonzepts) und nicht mit einem Eingriff in die Unabhängigkeit/Weisungsfreiheit des Datenschutzbeauftragten verbunden sein. Die Mitarbeitervertretung allein ist zur Erteilung von Prüfaufträgen gegenüber dem Datenschutzbeauftragten nicht berechtigt.[101] Im Rahmen einer sachgemäßen Aufgabenwahrnehmung wird dieser datenschutzrelevanten Hinweisen des Betriebsrats aber regelmäßig nachgehen müssen.

Die Weisungsfreiheit ist beschränkt auf die Wahrnehmung der Aufgaben als Datenschutzbeauftragter. Daraus ergibt sich zunächst, dass ein nebenamtlicher Beauftragter bezüglich seiner sonstigen Aufgaben weiterhin Weisungen erhalten darf. Überdies ist der Datenschutzbeauftragte Weisungen regelmäßig insofern unterworfen, als **allgemeine organisatorische Vorgaben**, wie z.B. Vorgaben zur Arbeitszeit, Reisekosten- oder IT-Richtlinien, betroffen sind.[102]

Aus der Weisungsfreiheit folgt schließlich nicht, dass dem Datenschutzbeauftragten eigene Entscheidungsbefugnisse zur Gewährleistung des Datenschutzes zustünden. Die Einhaltung der datenschutzrechtlichen Vorgaben ist nach der DS-GVO ausschließlich Angelegenheit des Verantwortlichen (Art. 24 DS-GVO), während dem Datenschutzbeauftragten **lediglich ein Beratungs- und Überwachungsauftrag** zukommt.

Nach Art. 38 Abs. 3 Satz 3 DS-GVO **berichtet** der Datenschutzbeauftragte **unmittelbar der höchsten Managementebene.** Der Datenschutzbeauftragte soll in datenschutzrelevanten Fragen die Entscheidung der Leitung ohne Umwege herbeiführen können. Art. 38 Abs. 3 Satz 3 DS-GVO ist insoweit nicht ausschließlich als Vorgabe eines Berichtswegs zu verstehen, sondern zugleich als organisatorische Anforderung, die es verbietet, den Datenschutzbeauftragten einer anderen

---

101 A. A.: *Simitis* in: Simitis, BDSG, § 4f Rn. 124.

102 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 17; *Bergt* in: Kühling/Buchner, Art. 38 Rn. 26; *Heberlein* in: Ehmann/Selmayr, Art. 38 Rn. 14.

Stelle als unmittelbar der Leitung zu unterstellen.[103] Die Sonderstellung verschafft dem Amtsinhaber bei denjenigen, die personenbezogene Daten verarbeiten, die notwendige Autorität und ist Ausdruck der Unabhängigkeit des Datenschutzbeauftragten (ErwG 97 S. 4 DS-GVO). Die Unterstellung ist allerdings rein funktionsbezogen. Handelt es sich um einen nebenamtlichen Beauftragten, also eine Person, die neben dem Datenschutz noch weitere Aufgaben im Unternehmen wahrnimmt, bleibt es bezüglich dieser weiteren Aufgaben bei der bisherigen organisatorischen Einordnung.

In der Praxis relevant ist die Frage, auf welche **Kostenstelle** die Funktion des Datenschutzbeauftragten gebucht wird und wer seine Ausgaben freizeichnet. So darf es z.B. nicht sein, dass durch die Zuordnung der Kosten zu einer Fachabteilung, wie z.B. der Revision, der entsprechende Abteilungsleiter die Möglichkeit erhält, Einfluss auf die Erlangung bzw. Aufrechterhaltung der Fachkunde sowie die Arbeit des Datenschutzbeauftragten zu nehmen, indem er sich weigert, Kosten für Weiterbildungsmaßnahmen oder Vorortprüfungen zu übernehmen.

## 6.3 Anspruch auf Einbindung, Zugang und Ressourcen

Eine erfolgreiche Tätigkeit als Datenschutzbeauftragter hängt wesentlich auch von der Unterstützung durch den Verantwortlichen bzw. Auftragsverarbeiter ab. Dem trägt die DS-GVO Rechnung, indem sie einen Anspruch des Datenschutzbeauftragten auf Einbindung und Unterstützung vorsieht (Art. 38 Abs. 1 und 2 DS-GVO), der im Einzelnen Folgendes umfasst:

- Ordnungsgemäße und frühzeitige Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen

[103] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 21; ähnlich *Heberlein* in: Ehmann/Selmayr, Art. 38 Rn. 16 und *v.d. Bussche* in: Plath, Art. 38 Rn. 2; anderer Auffassung, allerdings die unmittelbare Unterstellung empfehlend *Bergt* in: Kühling/Buchner, Art. 38 Rn. 25.

- Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen
- Ressourcen zur Aufgabenerfüllung / Erhaltung des Fachwissens

Die **ordnungsgemäße und frühzeitige Einbindung** ist essenziell für die erfolgreiche Aufgabenwahrnehmung durch den Datenschutzbeauftragten und damit für einen effektiven Datenschutz, kann doch der Datenschutzbeauftragte seinem Beratungs- (Art. 39 Abs. 1 Buchst. a) und c) DS-GVO) und Überwachungsauftrag (Art. 39 Abs. 1 Buchst. b) DS-GVO) nicht sachgemäß nachkommen, sofern über datenschutzrelevante Sachverhalte nicht oder nur verspätet informiert wird.[104] **Ordnungsgemäße Einbindung** bedeutet, dass dem Datenschutzbeauftragten **ungefragt** alle für seine Beurteilung potenziell relevanten Informationen zur Verfügung zu stellen sind.[105] Es ist also nicht Aufgabe des Datenschutzbeauftragten, den datenschutzrelevanten Sachverhalt zu ermitteln. Es obliegt ihm jedoch, zu konkretisieren, welche Informationen er für seine Bewertung benötigt. **Frühzeitig** ist die Einbindung, sofern sie erfolgt, sobald ein Verfahren personenbezogener Datenverarbeitung bzw. dessen Änderung konkret in Erwägung gezogen wird.[106] Jedenfalls für größere Stellen ist empfehlenswert, dass der Datenschutzbeauftragte – unabhängig von einem konkreten Anlass – in einem regelmäßigen Informationsaustausch mit der Leitungsebene und dem mittleren Management steht.[107] In jedem Fall muss der Datenschutzbeauftragte ein Vorspracherecht bei den die Verarbeitung betreffenden Leitungsbesprechungen erhalten.[108] Er ist zudem über die mit den Verarbeitungen betrauten Personen zu informieren.[109]

Eng mit der Einbindungspflicht zusammen hängt die Pflicht, dem Datenschutzbeauftragten **Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen** zu gewähren (Art. 38 Abs. 2 DS-GVO). Zugang

---

[104] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 7.

[105] *Heberlein* in: Ehmann/Selmayr, Art. 38 Rn. 7.

[106] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 7.

[107] Vgl. auch *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 16. Das WP wurde am 25.05.2018 vom Europäischen Datenschutzausschuss übernommen.

[108] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 7; *Paal* in: Paal/Pauly, Art. 38 Rn. 4.

[109] *Paal* in: Paal/Pauly, Art. 38 Rn. 4.

zu personenbezogenen Daten und Verarbeitungsvorgängen meint einerseits den physikalischen Zutritt zu Bereichen, in denen personenbezogene Daten verarbeitet werden, z.B. Serverräumen, andererseits einen lesenden Zugriff auf die relevanten EDV-Systeme.[110]

Die relevanten Ressourcen, die dem Datenschutzbeauftragten zur Verfügung zu stellen sind, entsprechen im Wesentlichen den in § 4f Abs. 5 Satz 1 BDSG a.F. Genannten, also **Hilfspersonal, Räume, Einrichtungen, Geräte sowie finanzielle und sonstige Mittel**.[111] Unter anderem sind dem Datenschutzbeauftragten alle gängigen Kommunikationsmittel zur Verfügung zu stellen, wobei jegliche Kontrolle der Kommunikation im Hinblick auf deren Vertraulichkeit (Art. 38 Abs. 5 DS-GVO i.V.m. § 6 Abs. 5 Satz 2 BDSG 2018) zu unterbleiben hat[112].

In der Praxis ist für den Datenschutzbeauftragten vor allem auch relevant, dass ihm das für die Wahrnehmung der Tätigkeit notwendige Zeitbudget zur Verfügung gestellt wird. Soweit dem Datenschutzbeauftragten seine Position neben den bisherigen Aufgaben übertragen wird, es sich also um einen nebenamtlichen Beauftragten handelt, hat die benennende Stelle dafür zu sorgen, dass er **im Hinblick auf seine sonstigen Aufgaben angemessen entlastet** wird. Mit der Unterstützungspflicht unvereinbar ist es, einem bereits ausgelasteten Mitarbeiter die Aufgabe ohne weitere Vorkehrungen einfach zusätzlich zu übertragen.

Das konkrete Maß der erforderlichen Unterstützung ist im **Einzelfall** zu bestimmen. **Kriterien für eine ausreichende finanzielle und materielle Ausstattung** sowie ein **angemessenes Zeitbudget** für die Wahrnehmung der gesetzlichen Aufgaben sind beispielsweise:

- Größe des Unternehmens
  - Anzahl der Mitarbeiter
  - Anzahl der Standorte/Betriebsstätten

[110] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 13.
[111] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 10.
[112] Vgl. hierzu auch Abschnitt 5.6.

- Organisation des Unternehmens
  - Einbindung in eine Konzernstruktur
  - national oder international
  - Matrixorganisation
  - Komplexität der Geschäftsprozesse
  - Home-Office/Telearbeit
  - Außendienst-/Vertriebsorganisation
  - Delegationsmöglichkeiten (Rechtsabteilung/Revisionsabteilung/ IT-Sicherheitsbeauftragter/externe Berater)
  - Inanspruchnahme externer Dienstleister (Outsourcing)
- Branche
- Art und Anzahl der zu verwaltenden Personengruppen (Mitarbeiter, Kunden, Lieferanten, Dritte, Kontaktpersonen etc.)
- Sensibilität der verarbeiteten personenbezogenen Daten bzw. der verwendeten Verfahren

In größeren Organisationen sollte der Datenschutzbeauftragte zur Gewährleistung seiner Unabhängigkeit ein **eigenes Budget** erhalten, mittels dessen er die regelmäßigen Ausgaben für Fortbildung, Fachliteratur etc. bestreiten kann.[113]

Bestandteil der Ressourcen zur Aufgabenerfüllung ist darüber hinaus, dass der Datenschutzbeauftragte **Zugang zu fachkundiger Beratung** bekommt, sofern notwendig. Entsprechende Beratung kann insbesondere dann erforderlich werden, wenn besonders komplexe Verfahren zu beurteilen oder besonders sensible Datenverarbeitungsprozesse betroffen sind. Die Unterstützung kann durch **Bereitstellung interner Ressourcen[114] (z.B. Rechtsabteilung, IT-Sicherheitsbeauftragter, Revision)** wie auch durch **Zurverfügungstellung externer Beratungsleis-**

[113] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 11.

[114] *Art.-29-Datenschutzgruppe* WP 243 rev. 01, S. 17. Das WP wurde am 25.05.2018 vom Europäischen Datenschutzausschuss übernommen.

**tungen**[115], z.B. eines IT-Experten oder einschlägig spezialisierten Rechtsanwalts, geschehen. Einen Anspruch auf Unterstützung durch einen externen Berater hat der Datenschutzbeauftragte erst, nachdem alle ihm zur Verfügung gestellten internen Beratungsmöglichkeiten ausgeschöpft wurden.

Der Datenschutzbeauftragte hat schließlich Anspruch auf die erforderlichen zeitlichen und finanziellen Mittel für die **Erhaltung seines Fachwissens** (Art. 38 Abs. 2 DS-GVO). Er ist berechtigt und verpflichtet, sich durch den regelmäßigen Besuch von Seminaren, Fachforen etc. über die relevanten technischen und rechtlichen Entwicklungen auf dem Laufenden zu halten.[116] Er kann verlangen, dass ihm die **Reisekosten zum Besuch eines GDD-Erfa-Kreises** erstattet werden. Zu den notwendigen Ressourcen gehört außerdem, dass der Datenschutzbeauftragte angemessen mit **Fachliteratur**, also Gesetzeskommentierungen, Fachbüchern und -zeitschriften, ausgestattet ist.

Die **Verpflichtung, einen neu zu benennenden Datenschutzbeauftragten angemessen auszubilden**, ergibt sich aus Art. 37 Abs. 5 DS-GVO. Hiernach darf nur eine entsprechend beruflich qualifizierte Person benannt werden, die über das benötigte Fachwissen verfügt.

**Schulungskonzept der GDD-Datenschutzakademie:**

Auf Basis jahrzehntelanger Ausbildungserfahrung bietet dieGDD-Datenschutz-Akademie ein gestuftes Schulungskonzept zur Aus- und Weiterbildung von Datenschutz- und Sicherheitsbeauftragten. Grundlage des Konzepts bilden die Basis-Schulungen, welche die erforderlichen Inhalte des Datenschutzrechts (Basis-Schulung Teil 1), des technisch-organisatorischen Datenschutzes (Basis-Schulung Teil 2) sowie des Datenschutz-Managements (Basis-Schulung Teil 3) vermitteln. Aufgabenspezifische Seminare, wie z.B. zum Datenschutz bei SAP oder zum grenzüberschreitenden Datenverkehr, vertiefen aktuelle Datenschutz- und Datensicherheitsfragen. Informationen sowie Termine finden sich unter https://www.gdd.de/seminare.

[115] *Bergt* in: Kühling/Buchner, Art. 38 Rn. 21.

[116] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 14.

Bei **Benennung eines externen Datenschutzbeauftragten** wird die Fortbildung zumeist Bestandteil der vereinbarten Vergütung sein und muss dann nicht zusätzlich erbracht werden.

## 6.4 Abberufungs- und Kündigungsschutz

Der Datenschutzbeauftragte genießt gemäß Art. 38 Abs. 3 Satz 2 DS-GVO **Abberufungsschutz**. Es handelt sich hierbei allerdings nicht um einen umfassenden Schutz. **Verboten ist** ausweislich des gesetzlichen Wortlauts lediglich die **Abberufung aus solchen Gründen, die mit der Erfüllung der Aufgaben als Datenschutzbeauftragter zusammenhängen** („Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen […] werden."). **Betriebliche bzw. organisatorische Gründe können eine Abberufung** des Datenschutzbeauftragten hiernach also **rechtfertigen**.[117] Diese Regelung ist insofern bedenklich, als Gefahr besteht, dass solche Gründe lediglich vorgeschoben werden, um sich eines unliebsamen Datenschutzbeauftragten zu entledigen. Die Beweislast für das Vorliegen eines nicht mit der Amtsführung zusammenhängenden Grundes liegt jedenfalls bei der benennenden Stelle.[118]

Ein weitergehender Abberufungsschutz als derjenige der DS-GVO ist in § 6 Abs. 4 Satz 1 BDSG 2018 enthalten, der nach § 38 Abs. 2 DS-GVO auch für Datenschutzbeauftragte nichtöffentlicher Stellen gelten soll. Hierbei soll es sich ausweislich der Gesetzesbegründung – ebenso wie beim Kündigungsschutz[119] des Datenschutzbeauftragten nach BDSG – um eine arbeitsrechtliche Regelung handeln, die ergänzend zu den DS-GVO-Vorgaben beibehalten werden kann. Diese Argumentation wird allerdings nur bezogen auf den internen Datenschutzbeauftragten gelten können.

---

[117] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 18; *Bergt* in: Kühling/Buchner, Art. 38 Rn. 30; *Paal* in: Paal/Pauly, Art. 38 Rn. 10.

[118] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 18; *Bergt* in: Kühling/Buchner, Art. 38 Rn. 30.

[119] Zum Kündigungsschutz vgl. nachfolgend in diesem Abschnitt.

Anders als das BDSG a.F. enthält die DS-GVO keine Regelung zur **Abberufung auf Verlangen der Aufsichtsbehörde**. Dies ist problematisch. Die Regelung in § 4f Abs. 3 Satz 4 BDSG a.F. verhinderte, dass die verantwortliche Stelle in Konflikt mit den gesetzlichen Abberufungsvorgaben geriet, wenn die Behörde den Datenschutzbeauftragten für ungeeignet hielt. Nach der DS-GVO kann aber genau dieses Problem entstehen, da nach Art. 38 Abs. 3 Satz 2 die Abberufung nicht auf die Aufgabenerfüllung des Datenschutzbeauftragten gestützt werden darf. Der nationale Gesetzgeber hat das Problem gesehen und in § 40 Abs. 6 Satz 2 BDSG 2018[120] geregelt. Hiernach kann die Aufsichtsbehörde die Abberufung des Datenschutzbeauftragten verlangen, wenn dieser die zur Erfüllung der Aufgaben erforderliche Fachkunde nicht besitzt oder im Fall des Art. 38 Abs. 6 DS-GVO ein schwerwiegender Interessenkonflikt vorliegt. Das Verlangen der Aufsichtsbehörde führt nicht automatisch zum Wegfall der Bestellung. Der benennenden Stelle steht allerdings **kein Ermessen** zu, ob sie dem behördlichen Verlangen nachkommen will, sie ist hierzu verpflichtet.[121] Hält sie die Anordnung für unbegründet, muss sie den hierin liegenden Verwaltungsakt anfechten. In jedem Fall hat die Aufsichtsbehörde zu berücksichtigen, dass ein Abberufungsverlangen einen schwerwiegenden Eingriff darstellt. Bei fehlender Fachkunde wird eine Verhältnismäßigkeit regelmäßig nur gegeben sein, wenn die Fachkunde nicht in angemessener Zeit durch geeignete Maßnahmen erworben werden kann.[122] Eine Befugnis der Aufsichtsbehörde, die Benennung eines fehlenden Datenschutzbeauftragten zu verlangen, ist nicht vorgesehen.[123] Soweit die Pflicht zur Benennung

---

[120] § 40 BDSG gilt ausweislich der amtlichen Überschrift nur für die "Aufsichtsbehörden der Länder". Eine entsprechende Regelung für den/die BfDI findet sich nicht, obgleich nicht nachvollziehbar ist, warum diesem/dieser nicht die gleichen Befugnisse zustehen sollten.

[121] So bereits zur Regelung in § 38 Abs. 5 Satz 3 BDSG a.F., an der sich die Neuregelung orientiert, *Simitis* in: Simitis, BDSG, § 38 Rn. 74 sowie *Gola/Klug/Körffer* in: Gola/Schomerus, BDSG, § 38 Rn. 28.

[122] *Brink/Wilhelm* in: BeckOK Datenschutzrecht, Wolff/Brink, § 40 Rn. 43; ähnlich *Pauly* in: Paal/Pauly, § 40 Rn. 40; *Dix* in: Kühling/Buchner, § 40 Rn. 17.

[123] Für eine solche Befugnis nach BDSG a.F. *Thieser*, DuD 2014, 738. Diese Auffassung war aber bereits damals zweifelhaft.

nach Art. 37 DS-GVO verletzt wird, kann die Behörde an die fehlende Benennung jedoch ein Bußgeld knüpfen (Art. 83 Abs. 4 Buchst. a) DS-GVO).[124]

Ebenso wenig enthält die DS-GVO eine Regelung zum arbeitsrechtlichen **Kündigungsschutz des Datenschutzbeauftragten**. Ein solcher ist aber in § 6 Abs. 4 Satz 2 BDSG 2018 (für nichtöffentliche Stellen i.V.m. § 38 Abs. 2 BDSG 2018) vorgesehen. Nach § 6 Abs. 4 Satz 2 BDSG 2018 ist die Kündigung des Arbeitsverhältnisses des Datenschutzbeauftragten unzulässig, es sei denn, dass Tatsachen vorliegen, welche zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen, also zu einer außerordentlichen Kündigung. Wichtige Gründe in diesem Sinne sind etwa ein beharrliches Untätigsein des Datenschutzbeauftragten, ein schwerwiegender Verstoß gegen Verschwiegenheitspflichten oder die Verletzung persönlichkeitsschützender Normen. Allein die Organisationsentscheidung, nunmehr konzernweit einen externen Datenschutzbeauftragten mit dem Datenschutz betrauen zu wollen, stellt nach dem BAG keinen wichtigen Grund in diesem Sinne dar.[125] Die Abschaffung einer dezentralen zugunsten einer neuen zentralen Datenschutzorganisation („Konzerndatenschutzbeauftragter“), um eine verbesserte Steuerbarkeit und Einheitlichkeit des Datenschutzes zu gewährleisten, ist folglich regelmäßig nur im Einvernehmen mit den bislang benannten Datenschutzbeauftragten möglich.

Der Kündigungsschutz wirkt noch ein Jahr über das Ende der Tätigkeit als Datenschutzbeauftragter hinaus (sog. **nachwirkender Kündigungsschutz**, § 6 Abs. 4 Satz 3 BDSG 2018). Für diesen Zeitraum bleibt die Kündigung an die gleichen Voraussetzungen geknüpft wie während der Tätigkeit des Datenschutzbeauftragten. Der Kündigungsschutz gilt auch für **stellvertretende Datenschutzbeauftragte**, sofern diese tatsächlich aktiv geworden sind.[126] Nach Auffassung des ArbG Dortmund[127] sollte

[124] Die Pflicht zur Benennung aus § 38 Abs. 1 BDSG ist wohl nicht bußgeldbewehrt. Vgl. hierzu im Detail Abschnitt 7.4.

[125] BAG, Urteil vom 23.03.2011 - 10 AZR 562/09 -, RDV 2011, 237; NZA 2011, 1036.

[126] BAG, Urteil vom 27.7.2017 - 2 AZR 812/16; zum Stellvertreter des Datenschutzbeauftragten und zu seinem Hilfspersonal umfassend *Franck/Reif*, ZD 2015, 405.

überdies der Abberufungs- und Kündigungsschutz nach § 4f BDSG a.F. nicht erst nach Ablauf der **Probezeit**, sondern bereits mit Tätigkeitsaufnahme greifen. Die Argumentation des Gerichts, andernfalls wäre während der Probezeit die Unabhängigkeit des Datenschutzbeauftragten nicht gewährleistet, hat an Sinnhaftigkeit nichts eingebüßt, allerdings liegt die Letztentscheidung über die Interpretation des DS-GVO-Abberufungsschutzes beim EuGH.

Der in § 6 Abs. 4 Satz 2 i.V.m. § 38 Abs. 2 BDSG 2018 geregelte Kündigungsschutz bezieht sich lediglich auf solche **Beauftragte, zu deren Benennung der Verantwortliche bzw. Auftragsverarbeiter verpflichtet ist**. Diese Einschränkung ist insofern sinnvoll, als eine Ausdehnung auf nicht zur Benennung verpflichtete Stellen diese davon abhalten könnte, freiwillig einen Datenschutzbeauftragten zu benennen.

Der Widerruf der Benennung lässt das zugrunde liegende Schuldverhältnis mit dem Datenschutzbeauftragten grundsätzlich unberührt, also im Falle des internen Beauftragten den regelmäßig bestehenden Arbeitsvertrag. Gleichwohl ist es so, dass der Umstand, der den Anlass für den Benennungswiderruf bildet, gleichzeitig auch die Basis entsprechender arbeitsrechtlicher Maßnahmen sein kann. Ist Grund für den Widerruf etwa eine gravierende Verletzung der Verschwiegenheitspflicht, so wird diese Pflichtverletzung gleichzeitig in der Regel auch eine außerordentliche Kündigung des Arbeitsverhältnisses rechtfertigen. **Die DS-GVO- und die arbeitsrechtliche Ebene sind also jeweils getrennt voneinander zu beurteilen.** Es gelten insoweit auch jeweils unterschiedliche Formerfordernisse. Während die DS-GVO den Benennungswiderruf – ebenso wie die Benennung – an keine bestimmte Form knüpft und daher insofern von Formfreiheit auszugehen ist, setzt eine Beendigungs- bzw. Änderungskündigung nach § 623 BGB Schriftform (§ 126 BGB) voraus. Kündigt der Verantwortliche bzw. Auftragsverarbeiter das Arbeitsverhältnis mit dem Datenschutzbeauftragten, so wird hiermit regelmäßig der konkludente Widerruf der Benennung verbunden sein.

[127] Urteil vom 20.02.2013 - 10 Ca 4800/12 -, AuA 2015, 675 = RDV 2013, 319 = ZD 2015, 452.

Mögliche weitere Gründe für ein Ende der Benennung als Datenschutzbeauftragter sind die **einvernehmliche Beendigung der Benennung**, welche aus Beweisgründen schriftlich dokumentiert sein sollte, sowie die **Niederlegung des Amts** durch den Datenschutzbeauftragten. Datenschutzrechtlich kann der Beauftragte nicht gezwungen werden, das Amt gegen seinen Willen weiter auszuüben. Erfolgt die Niederlegung des Amts ohne entsprechenden Anlass, wie z.B. eine dauerhafte Verweigerung der notwendigen Unterstützung (Art. 38 Abs. 2 DS-GVO), stellt sich diese aber als Verletzung des Arbeitsvertrages dar bzw. im Falle eines externen Beauftragten, sofern dieser nicht von bestehenden Kündigungsrechten Gebrauch macht, als Verletzung des bestehenden Dienstleistungsvertrages. Legt ein Datenschutzbeauftragter sein Amt einseitig nieder, sollte er zudem zuvor prüfen bzw. prüfen lassen, inwiefern arbeitsrechtlich ein Anspruch darauf besteht, wieder im ursprünglichen Umfang auf die alte Stelle zurückzukehren. Denn mit der Annahme der Benennung ist ein arbeitsrechtlicher Änderungsvertrag verbunden, der dazu führt, dass sich die Stundenzahl reduziert, mit welcher die bisherige Tätigkeit wahrgenommen wird. Beim Vollzeitdatenschutzbeauftragten reduziert sich diese Stundenzahl auf null.

Praktisch bedeutsam ist die Frage, welche Folge eine **Unternehmensfusion** für die Datenschutzbeauftragten derjenigen Unternehmen hat, die von der Fusion betroffen sind. Da der Beauftragte dem Verantwortlichen bzw. Auftragsverarbeiter zugeordnet ist, endet seine Benennung, wenn dieser nicht mehr existiert, also auch in dem Fall, in dem dieser in einem anderen Unternehmen aufgeht (§ 20 UmwG).[128] Die arbeitsrechtlichen Bestimmungen zum Betriebsübergang in § 613a BGB regeln lediglich den Eintritt des übernehmenden Rechtsträgers in die Rechte und Pflichten aus einem ggf. bestehenden Arbeitsverhältnis, sichern also den Anspruch auf eine adäquate Beschäftigung, führen jedoch nicht zu einem Fortbestand der Benennung.[129]

[128] So auch das BAG für die Fusion gesetzlicher Krankenkassen: Urteil vom 29.09.2010 - 10 AZR 588/09 -, NJW 2011, 476; BB 2011, 637; NZA 2011, 151; RDV 2011, 88.

[129] ArbG Cottbus, Urteil vom 14.02.2019 – 3 Ca 1043/12 -, RDV 2013, 207.

## 6.5 Benachteiligungsverbot

Der Datenschutzbeauftragte **darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden** (Art. 38 Abs. 3 Satz 2 DS-GVO). Ebenso wie der Abberufungs- und besondere Kündigungsschutz beruht auch diese Regelung auf der Anerkennung des Umstandes, dass der Tätigkeit des Datenschutzbeauftragten ein nicht unerhebliches Konfliktpotenzial innewohnt. Nimmt der Datenschutzbeauftragte seine Aufgabe ernst, so kann seine Tätigkeit dazu führen, dass Prozesse, an welchen Unternehmensleitung und Fachabteilung ein großes Interesse haben, verzögert oder gar nicht bzw. nur nach vorherigen Anpassungen durchgeführt werden.

Nach dem Sinn und Zweck der Vorschrift ist der **Begriff der Benachteiligung weit zu interpretieren**. Ein Verstoß gegen das Benachteiligungsverbot wäre es etwa, wenn dem Datenschutzbeauftragten soziale Leistungen vorenthalten werden oder dieser karrieretechnisch „kaltgestellt“ wird, er also z.B. anders als seine Kollegen bei Beförderungen nicht mehr berücksichtigt wird oder keine Gehaltserhöhungen mehr erhält. Eine Benachteiligung kann auch in der räumlichen Auslagerung des Datenschutzbeauftragten verbunden mit einer Isolierung von unternehmensinternen Informationsabläufen liegen, der fehlenden Bereitstellung adäquater Büroausstattung, dem Entzug gewünschter Aufgaben oder der nachteiligen Zuteilung neuer Aufgaben. Das Benachteiligungsverbot richtet sich an die Leitung des Verantwortlichen bzw. Auftragsverarbeiters wie auch an die dort jeweils Beschäftigten. Die **Beweislast liegt bei der benennenden Stelle**, d.h., diese muss beweisen, dass eine objektive Benachteiligung des Datenschutzbeauftragten nicht mit dessen Amtstätigkeit zusammenhängt.[130]

[130] *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 38 Rn. 20; *Bergt* in: Kühling/Buchner, Art. 38 Rn. 31.

# 7. Haftung und Sanktionen

## 7.1 Allgemeines

Eine Haftung bzw. Sanktionierung des Datenschutzbeauftragten erscheint aus verschiedenen Blickwinkeln denkbar: So könnte er unmittelbar von der betroffenen Person auf Schadensersatz in Anspruch genommen werden. Möglich ist auch, dass der Verantwortliche bzw. Auftragsverarbeiter den Datenschutzbeauftragten in Anspruch nimmt, um sich die Kosten zurückzuholen für anzupassende Datenverarbeitungsprozesse, von der Aufsichtsbehörde verhängte Bußgelder und/ oder für Schadensersatzansprüche, die die betroffene Person gegen den Verantwortlichen bzw. Auftragsverarbeiter geltend macht. Schließlich stellt sich die Frage, inwiefern der Datenschutzbeauftragte selbst Adressat von Bußgeldern sein bzw. sich einer Datenschutzstraftat strafbar machen kann. All diese Konstellationen sollen im Folgenden näher beleuchtet werden.

## 7.2 Haftung des Datenschutzbeauftragten

### 7.2.1 Haftung im Verhältnis zur betroffenen Person

Zwischen dem Datenschutzbeauftragten und den betroffenen Personen besteht **kein Vertragsverhältnis.** Vertragliche Ansprüche der betroffenen Personen könnten sich daher allenfalls über die Annahme eines Vertrags zu Gunsten Dritter (§ 328 Bürgerliches Gesetzbuch - BGB) bzw. eines Vertrags mit Schutzwirkung zu Gunsten Dritter ergeben.

In einem Vertrag kann vereinbart werden, dass die Leistung nicht an den Gläubiger selbst, sondern an einen Dritten erbracht werden soll, § 328 BGB, sog. **Vertrag zu Gunsten Dritter**.

Im Gegensatz dazu steht beim **Vertrag mit Schutzwirkung zu Gunsten Dritter** der Anspruch auf die geschuldete Leistung alleine dem Gläubiger zu, der Dritte wird jedoch in die vertraglichen Schutz- und

Obhutspflichten einbezogen, so dass ihm bei Verletzung dieser Pflichten ein vertraglicher Schadensersatzanspruch zusteht.

Die Annahme eines Vertrags zu Gunsten Dritter scheitert daran, dass mit der Benennung des Datenschutzbeauftragten nicht das Ziel verfolgt wird, den betroffenen Personen eigene Ansprüche einzuräumen. Die Benennung erfolgt nicht im Interesse konkreter einzelner Personen, sondern zum Schutz des Persönlichkeitsrechts der Gesamtheit der möglichen betroffenen Personen.[131]

Ein **Vertrag mit Schutzwirkung zu Gunsten Dritter** wird zum Teil mit der Begründung abgelehnt, dass es für den Datenschutzbeauftragten nicht erkennbar sei, wem gegenüber die Haftung im Einzelnen begründet werden soll.[132] Auch der BGH verlangt allerdings nicht, dass dem Schuldner Name und Zahl der zu schützenden Dritten bekannt sind. Es fehlt aber ganz allgemein, d.h. sowohl bezüglich der Arbeitnehmer als auch hinsichtlich der sonstigen betroffenen Personen, an der notwendigen „Leistungsnähe".[133] Das Institut des Vertrags mit Schutzwirkung zu Gunsten Dritter kann nur eine Einbeziehung in im Verhältnis zwischen Gläubiger und Schuldner bestehende Schutzpflichten ermöglichen. Der Datenschutzbeauftragte schuldet der benennenden Stelle aber nicht den Schutz ihrer Persönlichkeitsrechte, sondern Überwachung des Datenschutzes und Beratung.

Eine Haftung des Datenschutzbeauftragten gegenüber den betroffenen Personen kann sich nach alledem regelmäßig nur aus **deliktischen Anspruchsnormen** ergeben.

Das **Deliktsrecht**, das auch als Recht der unerlaubten Handlungen bezeichnet wird, ist in den §§ 823 ff. BGB geregelt. Während im Vertragsrecht die Sonderverbindung zwischen den Vertragsparteien Grund der Haftung ist, knüpft die deliktische Haftung an jedermann verbotene Handlungen an. Schutzgut im Bereich des Deliktsrechts ist auch das allgemeine Persönlichkeitsrecht.

---

131 *Schlemann*, Recht des betrieblichen Datenschutzbeauftragten, Frechen 1997, S. 283.

132 *Wind*, RDV 1991, 16, 21; *Gola/Schomerus*, BDSG a.F., § 4g Rn. 32.

133 A.A. *Schlemann*, a.a.O., S. 284, sofern Arbeitnehmer betroffen sind.

In Betracht kommt insbesondere eine Haftung gemäß § 823 Abs. 1 BGB wegen Verletzung des allgemeinen Persönlichkeitsrechts in der Gestalt des informationellen Selbstbestimmungsrechts („sonstiges Recht") sowie eine Haftung gemäß § 823 Abs. 2 BGB i.V.m. den verletzten Regelungen der DS-GVO. Art. 39 Abs. 1 Buchst. a) und b) DS-GVO, welche die Beratungs- und Überwachungspflicht des Datenschutzbeauftragten regeln, sind als Schutzgesetze im Sinne des § 823 Abs. 2 BGB anzusehen.[134] Insbesondere ist es für die Annahme eines Schutzgesetzes nicht entscheidend, ob die Regelung der betroffenen Person eigene Rechte einräumt. Maßgeblich ist, ob die Norm zumindest auch dazu dienen soll, den Einzelnen oder einzelne Personenkreise gegen die Verletzung eines bestimmten Rechtsguts zu schützen.[135] Die Rechtsfigur des Datenschutzbeauftragten ist aber gerade eine besondere organisatorische Vorkehrung, die der Gefahr von Verletzungen des Persönlichkeitsrechts der betroffenen Personen entgegenwirken soll.

Relativ unproblematisch sind insofern Fälle, in denen die Datenschutzverletzung auf ein **aktives Handeln** des Datenschutzbeauftragten zurückzuführen ist. Dies ist z.B. dann der Fall, wenn die benennende Stelle aufgrund falscher Beratung durch den Datenschutzbeauftragten eine datenschutzwidrige Maßnahme durchführt mit der Konsequenz, dass die Rechte der betroffenen Person beeinträchtigt werden.

In der Praxis wird der Vorwurf gegenüber dem Datenschutzbeauftragten allerdings häufig darin liegen, dass er eine gegen Datenschutzrecht verstoßende Maßnahme der benennenden Stelle nicht unterbunden hat, also in einem **Unterlassen**. Ein Unterlassen kann jedoch nur dann zu einer Haftung führen, wenn es pflichtwidrig ist, also eine Rechtspflicht zum Handeln besteht. Als Anknüpfungspunkt kommt in diesem Zusammenhang insbesondere der Überwachungsauftrag aus Art. 39 Abs. 1 Buchst. b) DS-GVO in Betracht. So wird aus dieser Überwachungsaufgabe **teilweise** auch **eine Stellung als sog. Überwacherga-**

---

134 So auch *Bergt* in: Kühling/Buchner, Art. 37 Rn. 54. Dafür, dass auf Basis ihres Schutzzwecks (Art. 1 Abs. 1 DS-GVO) die Normen der DS-GVO regelmäßig als deliktsrechtliche Schutzgesetze einzuordnen sind, sind *Gola/Piltz* in: Gola, DS-GVO, Art. 82 Rn. 26 sowie *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 25.

135 *Sprau* in: Palandt, BGB, § 823 Rn. 57.

**rant abgeleitet**.[136] Dem ist entgegenzuhalten, dass der Datenschutzbeauftragte – jedenfalls allein auf Basis der gesetzlichen Aufgabenbeschreibung – nach wie vor keine eigenen Entscheidungs- oder Weisungsbefugnisse besitzt, um Datenschutzverletzungen zu unterbinden.[137]

Auch eine **Aufklärungspflicht des Datenschutzbeauftragten aufgrund „Informationsvorsprungs“** ist regelmäßig abzulehnen. Ein solcher Informationsvorsprung ist zwar ausnahmsweise denkbar, wenn der Datenschutzbeauftragte Informationen erhält, die der Unternehmensleitung nicht zur Verfügung stehen, z.B. über das Bestehen eines Datenlecks. Bezogen auf bestehende oder geplante unternehmensinterne Prozesse wird ein Informationsvorsprung jedoch im Regelfall abzulehnen sein, denn diese sind jedenfalls den zuständigen Unternehmenseinheiten gleichermaßen bekannt und die Geschäftsleitung muss sich deren Kenntnis regelmäßig zurechnen lassen. Ein Informationsvorsprung im vorgenannten Sinne ergibt sich auch nicht schon allein aus dem Umstand, dass der Datenschutzbeauftragte über bessere Kenntnisse des Datenschutzrechts verfügt.[138]

Schwierigkeiten bereitet in Unterlassenskonstellationen auch die Begründung, dass das Nichteinschreiten des Datenschutzbeauftragten tatsächlich ursächlich für die Rechtsverletzung gegenüber der betroffenen Person geworden ist (**sog. haftungsbegründende Kausalität**).[139] Insofern stellt sich zunächst die Frage, ob dieser über die betreffende Datenverarbeitung rechtzeitig informiert war, er also überhaupt die Möglichkeit gehabt hätte, das Verfahren zu monieren. Selbst wenn der Datenschutzbeauftragte auf bestehende Datenschutzverstöße hinweist, bedeutet dies im Übrigen nicht zwingend, dass die Unter-

---

136 *Bergt* in: Kühling/Buchner, Art. 37 Rn. 55; *Wybitul*, ZD 2016, 203, 205*; Wybitul/von Gierke*, BB 2017, 181, 182; *Laue/Nink/Kremer*, S. 211; tendenziell dafür, im Ergebnis aber offen *Golla*, RDV 2017, 123, 127; für „klärungsbedürftig“ halten die Garantenstellung *Paal/Pauly*, Art. 39 Rn. 12; unentschieden letztlich auch *Nolde*, PinG 2017, 114, 119. Bereits unter dem BDSG a.F. sprach sich *Marschall*, ZD 2014, 66, 68 für eine Garantenstellung aus.

137 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 14.

138 A. A. wohl Marschall, ZD 2014, S. 66, 68.

139 Ähnlich *Eßer/Steffen*, CR 2018, 289, 292.

nehmens- bzw. Behördenleitung den Hinweis auch umsetzt und damit die Rechtsverletzung unterbleibt.[140]

Für interne Datenschutzbeauftragte gelten schließlich die von der Rechtsprechung aufgestellten Grundsätze zur **Haftungserleichterung von Arbeitnehmern (sog. innerbetrieblicher Schadensausgleich)**. Danach hat der Arbeitgeber bei einem nur durch leichte Fahrlässigkeit verursachten Schaden den Datenschutzbeauftragten im Innenverhältnis von einer Haftung gegenüber der betroffenen Person freizustellen. Bei mittlerer Fahrlässigkeit ist die Haftung zwischen Arbeitgeber und Datenschutzbeauftragtem zu quoteln (§ 254 BGB analog).

Externe Datenschutzbeauftragte sind über die Grundsätze des innerbetrieblichen Schadensausgleichs nicht geschützt, da sie nicht aufgrund eines Arbeitsvertrages tätig sind. Daher kann sich insbesondere für sie der Abschluss einer **Berufshaftpflichtversicherung** empfehlen.

### 7.2.2 Haftung im Verhältnis zur benennenden Stelle

Anders als im Verhältnis zur betroffenen Person kommt im Verhältnis zur benennenden Stelle auch eine **Haftung des Datenschutzbeauftragten aus vertraglichen Ansprüchen** in Betracht, besteht doch mit dem internen Beauftragten ein Arbeitsverhältnis und mit dem externen Beauftragten ein Geschäftsbesorgungsvertrag (§ 675 BGB). Potenzielle Rechtsgrundlage für die Haftung ist insofern § 280 BGB.

**§ 280 Abs. 1 BGB: Schadensersatz wegen Pflichtverletzung**

Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat.

Ein Schaden der benennenden Stelle könnte sich z.B. dann ergeben, wenn sich diese aufgrund einer falschen Beratung des Datenschutzbeauftragten nunmehr einem von der betroffenen Person geltend gemachten Schadensersatzanspruch gegenübersieht. Eine Falschbera-

[140] So auch *Eßer/Steffen*, CR 2018, 289, 292

tung kann auch dazu führen, dass bereits aufgenommene Datenverarbeitungsverfahren im Nachhinein kostenintensiven Änderungen unterzogen werden müssen.

Voraussetzung ist das Vorliegen einer Pflichtverletzung im Verhältnis zur benennenden Stelle. Als verletzte Pflicht kommt die **Beratungspflicht des Datenschutzbeauftragten nach Art. 39 Abs. 1 Buchst. a) DS-GVO** in Betracht. Diese originär gesetzliche Verpflichtung wird durch die Bezugnahme im Arbeits- bzw. Geschäftsbesorgungsvertrag auch zu einer vertraglichen Verpflichtung. Eine inhaltlich falsche Beratung verletzt diese Beratungspflicht. **Zu beachten ist allerdings, dass die gesetzliche Beratungspflicht und damit auch die – regelmäßig identische – vertragliche Verpflichtung nicht existiert, um die benennende Stelle vor Schäden zu bewahren.** Der Datenschutzbeauftragte ist eine organisatorische Vorkehrung des Gesetzgebers zum Schutz der Persönlichkeitsrechte natürlicher Personen. Dem Schutz der betroffenen Personen dient auch dessen Beratungsauftrag. Zwar schützt die Tätigkeit des Datenschutzbeauftragten faktisch auch die benennende Stelle vor einer Inanspruchnahme wegen Datenschutzverletzungen. Dies ist jedoch nicht Intention der gesetzlichen Regelung, sondern lediglich Reflexwirkung. Vieles spricht also dafür, eine Haftung des Datenschutzbeauftragten im Verhältnis zur benennenden Stelle entgegen verbreiteter Auffassung[141] regelmäßig schon dem Grunde nach abzulehnen. Selbstverständlich kann der Datenschutzbeauftragte im Einzelfall vertraglich eine weitergehende, auch auf den Schutz der benennenden Stelle bezogene Beratungspflicht übernehmen.

**Vorgesagtes gilt entsprechend im Hinblick auf eine Haftung wegen einer möglichen Verletzung des Überwachungsauftrags (Art. 39 Abs. 1 Buchst. b) DS-GVO)** durch den Datenschutzbeauftragten. Auch diese Pflicht besteht im Interesse der betroffenen Personen und nicht zum Schutz der benennenden Stelle.

[141] Vgl. etwa *Bergt* in: Kühling/Buchner, Art. 37 Rn. 53; *Paal* in: Paal/Pauly, Art. 39 Rn. 12; auch *Eßer/Steffen,* CR 2018, 289, 291 ff. halten eine Haftung gegenüber der benennenden Stelle für möglich.

## 7.3 Strafbarkeit des Datenschutzbeauftragten

Da dem Datenschutzbeauftragten keine eigenen Datenverarbeitungskompetenzen zustehen, ist zentrale Frage im Hinblick auf eine mögliche strafrechtliche Verantwortung, inwiefern dieser sich seinerseits strafbar machen kann, weil er eine Datenschutzstraftat trotz Kenntnis nicht unterbunden hat, z.B. einen illegalen Verkauf von Kundendaten (§ 42 Abs. 1 bzw. 2 BDSG 2018).

Voraussetzung für eine solche Strafbarkeit wegen Unterlassens ist das Bestehen einer sog. **Garantenstellung** seitens des Datenschutzbeauftragten, d.h., dieser müsste rechtlich dafür einzustehen haben, dass der strafrechtlich missbilligte Erfolg ausbleibt (§ 13 Abs. 1 StGB).

**§ 13 StGB:**

(1) Wer es unterlässt, einen Erfolg abzuwenden, der zum Tatbestand eines Strafgesetzes gehört, ist nach diesem Gesetz nur dann strafbar, wenn er rechtlich dafür einzustehen hat, dass der Erfolg nicht eintritt, und wenn das Unterlassen der Verwirklichung des gesetzlichen Tatbestandes durch ein Tun entspricht.

(2) Die Strafe kann nach § 49 Abs. 1 gemildert werden.

Im Jahr 2009 entschied der BGH[142], dass **Beauftragte, denen die Corporate Compliance anvertraut ist**, regelmäßig strafrechtlich eine Garantenpflicht im Sinne des § 13 Abs. 1 StGB trifft, im Zusammenhang mit der Tätigkeit des Unternehmens stehende Straftaten von Unternehmensangehörigen zu verhindern. Dies sei die notwendige Kehrseite ihrer gegenüber der Unternehmensleitung übernommenen Pflicht, Rechtsverstöße und insbesondere Straftaten zu unterbinden. Zugleich stellte der BGH fest, dass sich eine entsprechende Garantenstellung auch aus der Übernahme einer gesetzlich vorgesehenen Funktion als Beauftragter ergeben könne, wie z.B. der Funktion als Beauftragter für Gewässer-, Immissions- oder Strahlenschutz.

Zum Datenschutzbeauftragten hat sich der BGH nicht explizit geäußert und es ist umstritten, inwiefern die vorgenannte Äußerung des Ge-

[142] BGH, NJW 2009, 3173; BB 2009, 2059.

richts auf diesen übertragen werden kann.[143] Zu den Argumenten gegen eine Garantenstellung des Datenschutzbeauftragten vgl. bereits vorstehend unter 7.2.1.

Unabhängig von der Garantenstellung müsste zudem das Unterlassen des Datenschutzbeauftragten kausal für die eingetretene Rechtsverletzung geworden sein. Daran kann es etwa fehlen, wenn der Verantwortliche bzw. Auftragsverarbeiter sich bereits in der Vergangenheit geweigert hat, bestimmte Prozesse anzupassen bzw. abzusichern, oder wenn im Falle eines Datenlecks die Ursache für den Informationsabfluss unbekannt ist.

## 7.4 Sanktionen nach Art. 83 DS-GVO

Nach Art. 83 Abs. 4 Buchst. a) DS-GVO können bei Verstößen gegen die Art. 37 bis 39 DS-GVO **Geldbußen von bis zu 10 Millionen EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist**. Sanktioniert werden können nach dem expliziten Wortlaut der Regelung allerdings nur Pflichtverletzungen des Verantwortlichen bzw. Auftragsverarbeiters. Die **Aufgaben des Datenschutzbeauftragten aus Art. 39 DS-GVO** gehören nicht zum Pflichtenkreis des Verantwortlichen bzw. Auftragsverarbeiters. Es handelt sich um **Pflichten des Datenschutzbeauftragten selbst, gegen den mangels Einbeziehung in den Bußgeldtatbestand kein Bußgeld verhängt werden kann**.[144]

Mit einem Bußgeld belegt werden können sollen über Art. 83 Abs. 4 Buchst. a) DS-GVO **sämtliche Verstöße des Verantwortlichen bzw. Auftragsverarbeiters gegen Pflichten aus Art. 37 bis 39 DS-GVO**. Auch europarechtlich dürfen allerdings Sanktionen nur verhängt werden,

---

143 Für die Annahme einer Garantenstellung *Barton*, RDV 2010, 247 ff.; *Wybitul*, Handbuch Datenschutz im Unternehmen, Rn. 351.

144 *Jaspers/Reif* in: Schwartmann/Jaspers/Thüsing/Kugelmann, Art. 39 Rn. 34; *Bergt*, DuD 2017, 555, 561; *Eßer/Steffen*, CR 2018, 289, 292; *Piltz*, K&R 2017, 85, 91. Zur umstrittenen Frage, ob der Datenschutzbeauftragte als Überwachergarant einzustufen ist, vgl. Abschnitt 7.2.1.

wenn sie auf einer klaren und unzweideutigen Rechtsgrundlage beruhen und die abzuleitenden Rechtsfolgen vorhersehbar festgelegt sind **(Bestimmtheitsgebot)**.[145] Den Verpflichtungen des Verantwortlichen bzw. Auftragsverarbeiters nach Art. 37 f. DS-GVO fehlt jedoch mit wenigen Ausnahmen, wie z.B. der Verpflichtung zur Veröffentlichung / Meldung der Kontaktdaten des Datenschutzbeauftragten (Art. 37 Abs. 7 DS-GVO), eine klare Konturierung, so dass für die Verantwortlichen bzw. Auftragsverarbeiter nicht ohne Weiteres zu erkennen ist, welches Verhalten verboten und mit Geldbuße bedroht ist. So knüpft die Benennungspflicht für nichtöffentliche Stellen (Art. 37 Abs. 1 Buchst. b) und c) DS-GVO) an die unbestimmten Rechtsbegriffe „Kerntätigkeit“ sowie „umfangreiche“ Überwachung bzw. Verarbeitung an. Auch das Maß der „erforderlichen“ Ressourcen im Hinblick auf die Unterstützung des Datenschutzbeauftragten (Art. 38 Abs. 2 DS-GVO) und die Anforderungen an die Qualifikation des Datenschutzbeauftragten (Art. 37 Abs. 5 DS-GVO) werden nicht näher konkretisiert. Verstöße von öffentlichen Stellen können allgemein nicht mit Bußgeld geahndet werden, es sei denn, diese nehmen am Wettbewerb teil (§ 43 Abs. 3 BDSG 2018).

**Unklar ist, ob allein ein Verstoß gegen die nationale Benennungspflicht aus § 38 Abs. 1 BDSG 2018 ein Bußgeld rechtfertigen kann.** Dagegen spricht, dass das nationale Recht eine entsprechende Bußgeldbewehrung nicht vorsieht und Art. 83 Abs. 4 Buchst. a) DS-GVO an einen Verstoß gegen Art. 37 DS-GVO anknüpft, die Benennungspflicht sich in den maßgeblichen Fällen jedoch aus nationalem Recht ergibt. Berücksichtigt man zudem Art. 37 Abs. 4 Satz 1 Hs. 2 DS-GVO, lässt sich der Verstoß gegen die nationale Benennungsverpflichtung gleichwohl zumindest dem Wortlaut nach unter Art. 83 Abs. 4 Buchst. a) DS-GVO subsumieren.

Nach Art. 37 Abs. 4 Satz 1 DS-GVO können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, in anderen als den in Art. 37 Abs. 1 DS-GVO genannten Fällen einen Datenschutzbeauftragten benennen (freiwillige Benennung); falls dies

[145] *Holländer*, BeckOK Datenschutzrecht, Wolff/Brink, Art. 83 Rn. 5.

nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, „müssen sie einen solchen benennen“. Der zweite Halbsatz lässt sich dahingehend interpretieren, dass im Falle des Verstoßes gegen die nationale Benennungspflicht zugleich ein Verstoß gegen die DS-GVO vorliegen soll.

Trotz des vermeintlich eindeutigen Wortlauts kann man sich allerdings fragen, ob der europäische Gesetzgeber mit dieser Passage tatsächlich darauf abgezielt hat, Verstöße gegen die im Verhältnis zur DS-GVO erweiterten nationalen Benennungsvorgaben zu sanktionieren. Es erscheint wenig plausibel, dass es der europäische Gesetzgeber dem nationalen Gesetzgeber zwar überlassen hat, erweiterte Benennungsvoraussetzungen vorzusehen, er aber gleichzeitig zwingend die Hoheit über die Frage der Sanktionierung möglicher Verstöße gegen entsprechendes nationales Recht behalten wollte. Naheliegender erscheint, dass die Formulierung „müssen sie einen solchen benennen“ vor allem gewählt wurde, um in Abgrenzung zur freiwilligen Benennung nach Art. 37 Abs. 4 Satz 1 Hs. 1 DS-GVO zu treten („können … benennen“).

# Teil B

# Muster und Materialien

1. Benennung eines/einer Datenschutzbeauftragten (Muster)
2. Stellenbeschreibung (Muster)
3. DSK Kurzpapier Nr. 12 „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“
4. Art.-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), WP 243 rev.01 (bestätigt durch EDSA am 25.05.2018) (Auszug)
5. Sonstige relevante Muster zum Datenschutzbeauftragten

# 1. Benennung eines/einer Datenschutzbeauftragten (Muster)

**Benennung zum/zur Datenschutzbeauftragten**

Herrn/Frau _____

Hiermit werden Sie mit sofortiger Wirkung [*alternativ: zum ….*] zum/zur Datenschutzbeauftragten gem. Art. 37 ff. Datenschutz-Grundverordnung (DS-GVO), § 38 Bundesdatenschutzgesetz (BDSG) der/des/von … [*Name der benennenden Stelle*] benannt.

Ihre Aufgaben als Datenschutzbeauftragte/r und Ihre Stellung ergeben sich aus Art. 38 f. DS-GVO, § 38 Abs. 2 BDSG. [*Optional zusätzlich:*] *Diese werden durch Stellenbeschreibung vom …. näher konkretisiert.* [*Anm.: Eine detaillierte Stellenbeschreibung wird empfohlen, vgl. nachfolgendes Muster.*]

Im Hinblick auf die Erfüllung Ihrer Aufgaben als Datenschutzbeauftragte/r sind Sie weisungsfrei.

In Ihrer Funktion als Datenschutzbeauftragte/r sind Sie der Unternehmensleitung unmittelbar unterstellt. Zuständiges Leitungsmitglied ist …. . Über Ihre Tätigkeit werden Sie der Unternehmensleitung regelmäßig Bericht erstatten.

Mit der Benennung bin ich einverstanden.

| | |
|---|---|
| _____ | _____ |
| Ort Datum | Ort Datum |
| _____ | _____ |
| Unterschrift (Leitung) | Unterschrift (DSB) |

## Hinweise zum Benennungsformular:

- Besondere **Formanforderungen** an die Benennung bestehen nicht, allerdings ist der Verantwortliche bzw. Auftragsverarbeiter nachweispflichtig im Hinblick auf die Benennung. Die Benennung sollte daher regelmäßig zumindest in Textform (z.B. per E-Mail) erfolgen. Textform setzt keine eigenhändige Unterschrift voraus. Es genügt, dass die Nachricht den Namen des Erklärenden enthält.
- Sinnvollerweise sollte der/die Datenschutzbeauftragte **bestätigen**, z.B. durch Unterschrift im Fall der Schriftform oder durch eindeutige Antwort bei Benennung per E-Mail, **dass er/sie mit der Benennung einverstanden ist**.
- Nach Auffassung der GDD resultiert aus Art. 38 Abs. 3 Satz 3 DS-GVO nicht nur eine Vorgabe zum Berichtsweg des Datenschutzbeauftragten, sondern zugleich die Verpflichtung, den/die Datenschutzbeauftragte/n **unmittelbar der Leitung zu unterstellen**.
- Das Formular kann, z.B. im Konzern, auch eingesetzt werden, um den/die Datenschutzbeauftragte/n **für mehrere Stellen zu benennen**. In diesem Fall müssen alle Stellen aufgeführt werden, für die der/die Datenschutzbeauftragte benannt werden soll. Zudem muss für jede Stelle eine jeweils berechtigte Person unterschreiben bzw. eine entsprechende Vertretungsbefugnis vorliegen. Alternativ kann im Wege der Textform vorgegangen werden, siehe oben.

# 2. Stellenbeschreibung für eine/n Datenschutzbeauftragte/n (Muster)

Es empfiehlt sich, der Benennung zum/zur Datenschutzbeauftragten auch eine klare Stellenbeschreibung beizufügen. Diese Stellenbeschreibung soll sich auf die konkreten Aufgaben und Anforderungen im einzelnen Unternehmen beziehen. Sie ist daher den unternehmensindividuellen Gegebenheiten anzupassen.

**1. Stellenbezeichnung** Datenschutzbeauftragte/r

**2. Organisatorische Eingliederung**

Zur organisatorischen Eingliederung des Stelleninhabers / der Stelleninhaberin vgl. Benennungsschreiben vom …. .

**3. Stellvertretung**

Der/die Stelleninhaber/in wird vertreten durch … [*Hier kann eine konkrete Person genannt werden oder abstrakt der/die Inhaber/in einer bestimmten Position, z.B. „den/die Leiter/in der Abteilung Recht“.*].

Ein Vertretungsfall liegt vor, wenn der/die Stelleninhaber/in seine/ihre Aufgaben längerfristig nicht wahrnehmen kann (z.B. wegen Elternzeit) oder sofern im Fall kürzerer Abwesenheitszeiten ein Tätigwerden des/der Datenschutzbeauftragten unaufschiebbar ist.

**4. Aufgabe (allgemein)**

Der/die Stelleninhaber/in nimmt bei …. [*Verantwortliche Stelle / Auftragsverarbeiter*] die Aufgaben eines/einer Datenschutzbeauftragten nach Art. 37 ff. Datenschutz-Grundverordnung (DS-GVO) iVm § 38 Bundesdatenschutzgesetz (BDSG) wahr. In dieser Funktion hat der/die Stelleninhaber/in insbesondere die Einhaltung datenschutzrechtlicher Vorgaben zu überwachen und Unternehmensleitung wie Fachabteilungen entsprechend zu beraten. Mit der Feststellung von Mängeln sollen Vorschläge zu deren Beseitigung einhergehen.

Der/die Stelleninhaber/in gibt Anregungen zur ständigen Verbesserung des Datenschutzes, insbesondere zur Fortentwicklung der betrieblichen Datenschutzorganisation. Hierzu stimmt er/sie sich, sofern vorhanden, mit den Bereichen Revision, Organisation und IT/IT-Sicherheit(s-Management) ab.

## 5. Aufgabenbereich im Einzelnen

### 5.1 Allgemeines

Die Aufgaben des/der Stelleninhabers/in ergeben sich aus Art. 39 Abs. 1 DS-GVO. Die Aufgabenwahrnehmung hat nach Art. 39 Abs. 2 DS-GVO risikoorientiert zu erfolgen. Die Bewertung, welche Vorgänge wegen des mit ihnen verbundenen Risikos einer vorrangigen Bewertung bedürfen, obliegt grundsätzlich dem/der Stelleninhaber/in selbst.

### 5.2 Unterrichtung und Beratung

Der/die Stelleninhaber/in unterrichtet und berät die Unternehmensleitung sowie die Mitarbeiter der Fachabteilungen hinsichtlich ihrer datenschutzrechtlichen Pflichten. Unterrichtung meint die allgemeine Information über die bestehenden Verpflichtungen, Beratung die Unterstützung bei der Lösung von konkreten datenschutzrechtlichen Fragestellungen.

Datenschutzrechtliche Fragen der Unternehmensleitung bzw. Fachabteilungen beantwortet der/die Stelleninhaber/in, soweit dies ihn/sie nicht daran hindert, aus seiner/ihrer Sicht vordringlichen Angelegenheiten nachzugehen.

Der/die Stelleninhaber/in unterstützt die (Fort-)Entwicklung unternehmensinterner Strategien und Richtlinien zum Datenschutz.

Sicherzustellen und nachzuweisen, dass durchgeführte Datenverarbeitungen im Einklang mit den datenschutzrechtlichen Anforderungen stehen, ist Aufgabe der Fachabteilung. Sofern Letztere von Empfehlungen des Datenschutzbeauftragten abweichen will, sind die Gründe, aus denen dem Rat des Datenschutzbeauftragten nicht gefolgt wird, zu dokumentieren.

## 5.3 Überwachung der Einhaltung des Datenschutzes

Der/die Stelleninhaber/in überwacht die Einhaltung der geltenden Datenschutzvorschriften sowie der unternehmensinternen Vorgaben zum Datenschutz und informiert, sofern aus seiner/ihrer Sicht Anpassungen notwendig sind.

## 5.4 Aufgaben im Zusammenhang mit der Datenschutz-Folgenabschätzung

Für Verarbeitungen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, sieht Art. 35 DS-GVO vor, dass eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen ist. Die Durchführung ist Aufgabe der jeweiligen Fachabteilung, die insoweit den Rat des Stelleninhabers / der Stelleninhaberin zwingend einzuholen hat. Der/die Stelleninhaber/in hat zu überwachen, dass die DSFA gemäß Art. 35 DS-GVO durchgeführt wird.

## 5.5 Zusammenarbeit mit der Aufsichtsbehörde

Der/die Stelleninhaber/in arbeitet mit der Aufsichtsbehörde zusammen und fungiert als deren „Anlaufstelle“, d.h., er/sie ist erster Ansprechpartner für die Behörde und koordiniert den Kontakt mit der datenschutzrechtlich verantwortlichen Unternehmensleitung und der zuständigen Fachabteilung. Der/die Stelleninhaber/in wird insofern weder als verlängerter Arm der Behörde tätig, noch fungiert er/sie als Anwalt des Unternehmens und verteidigt dessen Vorgehensweise.

## 5.6 Ansprechpartner für die betroffenen Personen

Betroffene Personen können den/die Stelleninhaber/in zu allen mit der Verarbeitung ihrer Daten und mit der Wahrnehmung ihrer Rechte aus der DS-GVO im Zusammenhang stehenden Fragen zu Rate ziehen. Er/sie ist verpflichtet, sich solchen unmittelbar an ihn/sie gerichteten Anfragen anzunehmen und die betroffenen Personen in angemessener Zeit zu informieren.

Für allgemeine Datenschutzanfragen sowie die Bearbeitung von Eingaben, mit denen die betroffene Person ihre Rechte nach Art. 12 ff.

DS-GVO geltend macht, wie z.B. Berichtigungs- oder Löschungsansprüche oder Widersprüche, ist die jeweilige Fachabteilung zuständig. Auskunftsbegehren werden zentral durch …. [*z.B. den Kundenservice*] bearbeitet.

### 5.7 Hinzuziehung bei potenziellen Datenschutzverletzungen

Im Zusammenhang mit potenziellen Datenschutzverletzungen (Art. 33, 34 DS-GVO) wird der/die Stelleninhaber/in beratend einbezogen.

## 5.8 Zusätzliche Aufgaben [*Optional*]

*Anm.: Dem Datenschutzbeauftragten dürfen weitere Aufgaben übertragen werden, die über die in der DS-GVO ausdrücklich vorgesehenen Aufgaben hinausgehen, sofern hierdurch keine Interessenkonflikte entstehen und genügend Zeit für die Pflichtaufgaben verbleibt, z.B.:*

*Der/die Stelleninhaber/in macht die Mitarbeiter mit den für sie relevanten datenschutzrechtlichen Bestimmungen vertraut.*

***oder*** *Der/die Stelleninhaber/in unterstützt bei der (Fort-)Entwicklung eines Schulungskonzepts zum Datenschutz, mittels dessen die Mitarbeiter mit den für sie relevanten datenschutzrechtlichen Bestimmungen vertraut gemacht werden.*

*Der/die Stelleninhaber/in führt das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO). Die Erstellung und Aktualisierung des Verzeichnisses obliegt der jeweiligen Fachabteilung als Bringschuld.*

### 5.9 Berichterstattung / *Tätigkeitsbericht [Optional]*

Der/die Stelleninhaber/in informiert die Unternehmensleitung [*alternativ: das gemäß Benennungsschreiben vom … zuständige Mitglied der Unternehmensleitung*] in regelmäßigen Abständen über seine/ihre Tätigkeit.

***oder*** *Zum Ende eines jeden Geschäftsjahres legt der/die Stelleninhaber/in der Unternehmensleitung [alternativ: dem gemäß Benennungsschreiben vom … zuständigen Mitglied der Unternehmensleitung] einen Tätigkeitsbericht vor.*

## 6. Rechte und Kompetenzen

Im Hinblick auf die Erfüllung seiner/ihrer Aufgaben als Datenschutzbeauftragte/r unterliegt der/die Stelleninhaber/in keinen Weisungen. Er/sie ist zur eigenständigen Meinungsbildung berechtigt und verpflichtet.

Die Unternehmensleitung unterstützt ihn/sie bei der Erfüllung der Aufgaben und stellt die hierzu notwendigen Ressourcen zur Verfügung. Dies sind neben Räumen, Einrichtungen, Geräten, finanziellen/sonstigen Mitteln und ggf. Hilfspersonal insbesondere die zur Aufgabenwahrnehmung notwendigen zeitlichen Kapazitäten. Aktuell nimmt der/die Stelleninhaber/in die Tätigkeit als Datenschutzbeauftragte/r mit einer wöchentlichen Arbeitszeit von …. [*vereinbarte Stundenzahl*] Stunden wahr. Von anderen Tätigkeiten wird er/sie hierzu entsprechend freigestellt. Soweit erforderlich ist das Zeitbudget in Abstimmung mit dem/der Stelleninhaber/in angemessen anzupassen.

Zwecks Erhalt der Fachkunde hat der/die Stelleninhaber/in ein Recht auf Fortbildung in angemessenem Umfang. *[Optional zusätzlich] Hierzu kann er/sie bis zu …. Arbeitstage p.a. beanspruchen. [Optional zusätzlich] Ihm/ihr steht ein Fortbildungsbudget i.H.v. … Euro p.a. zur Verfügung.*

Der/die Stelleninhaber/in ist von der jeweiligen Fachabteilung über geplante Verarbeitungen personenbezogener Daten bzw. deren Änderung zu unterrichten. Hierzu sind ihm/ihr ungefragt alle für seine/ihre Beurteilung potenziell relevanten Informationen, mindestens die Informationen nach Art. 30 Abs. 1 bzw. Abs. 2 DS-GVO (Verzeichnis von Verarbeitungstätigkeiten) frühzeitig zur Verfügung zu stellen. Zu informieren ist auch über die jeweiligen Verfahrensverantwortlichen (process owner).

Zur Aufgabenerfüllung hat der/die Stelleninhaber/in ein ungehindertes Überwachungs-, Zutritts- und Auskunftsrecht im gesamten Unternehmen. Er/sie erhält Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen und ist befugt, alle potenziell relevanten Unterlagen einzusehen. Ihm/ihr steht ein Vorspracherecht bei den die Verarbeitung betreffenden Leitungsbesprechungen zu.

Bzgl. potenzieller Datenschutzverstöße setzt der/die Stelleninhaber/in sich zunächst mit der zuständigen Fachabteilung und, sofern dies nicht zum Ziel führt, mit der Unternehmensleitung ins Benehmen. Gegenüber Letzterer besteht ein direktes Vortragsrecht.

## 7. Verschwiegenheitspflicht

Der/die Stelleninhaber/in unterliegt einer Verschwiegenheitspflicht über die Identität der betroffenen Personen sowie über Umstände, die Rückschlüsse auf diese zulassen, soweit er/sie nicht durch diese hiervon befreit wird. Die Verschwiegenheitspflicht besteht nach Beendigung des Amtes fort.

*Anm.: Sofern dies im konkreten Fall zutrifft, sind in diesem Abschnitt zusätzlich zu erwähnen:*

- *mögliche Strafbarkeit des Datenschutzbeauftragten gemäß § 203 Abs. 4 StGB bei Vertraulichkeitsverstößen*
- *Zeugnisverweigerungsrecht des Datenschutzbeauftragten gemäß § 38 Abs. 2 i.V.m. § 6 Abs. 6 BDSG*

# 3. DSK Kurzpapier Nr. 12 „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“ (Stand: 17.12.2018)

*Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.*

Die nachfolgenden Erläuterungen zum Datenschutzbeauftragten (DSB) gelten sowohl für Verantwortliche als auch für Auftragsverarbeiter.

**Benennung des DSB**

Eine Pflicht zur Benennung eines DSB kann sich sowohl aus der DS-GVO als auch aus dem nationalen Recht ergeben. Eine Benennungspflicht kann für den Verantwortlichen, für den Auftragsverarbeiter oder für beide bestehen, je nachdem wer durch seine Tätigkeit selbst die Voraussetzungen für diese Pflicht erfüllt. Wer bisher einen DSB bestellen musste, muss in der Regel auch weiterhin einen DSB benennen.

**Benennung des DSB nach Art. 37 DS-GVO**

Nach Art. 37 Abs. 1 lit. a - c DS-GVO ist auf jeden Fall ein DSB zu benennen, wenn eine der folgenden Voraussetzungen gegeben ist:

- Behörde oder öffentliche Stelle (mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln),
- Kerntätigkeit mit umfangreicher oder systematischer Überwachung von Personen oder
- Kerntätigkeit mit umfangreicher Verarbeitung besonders sensibler Daten (Artikel 9, 10 DSGVO).

„Kerntätigkeit" ist die Haupttätigkeit eines Unternehmens, die es untrennbar prägt, und nicht die Verarbeitung personenbezogener Daten als Nebentätigkeit (ErwGr. 97 der DS-GVO). Zu den Kerntätigkeiten

gehören danach auch alle Vorgänge, die einen festen Bestandteil der Haupttätigkeit des Verantwortlichen darstellen. Hierzu gehören nicht die das Kerngeschäft unterstützenden Tätigkeiten wie z.B. die Verarbeitung der Beschäftigtendaten der eigenen Mitarbeiter.

Für die Definition des Begriffs "umfangreich" können aus ErwGr. 91 der DS-GVO folgende Faktoren herangezogen werden:

- Menge der verarbeiteten personenbezogenen Daten (Volumen),
- Verarbeitung auf regionaler, nationaler oder supranationaler Ebene (geografischer Aspekt),
- Anzahl der betroffenen Personen (absolute Zahl oder in Prozent zur relevanten Bezugsgröße) und
- Dauer der Verarbeitung (zeitlicher Aspekt).

Sind mehrere Faktoren hoch, so kann dies für eine "umfangreiche" Überwachung bzw. Verarbeitung sprechen.

Erfolgt eine Verarbeitung von Patienten- oder Mandantendaten durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalt, handelt es sich regelmäßig nicht um eine die Benennungspflicht auslösende umfangreiche Datenverarbeitung (siehe ErwGr. 91). Unter Berücksichtigung der Umstände des Einzelfalls und der konkreten Elemente einer umfangreichen Verarbeitung im Sinne des
ErwGr. 91 – beispielsweise bei einer Anzahl von Betroffenen, die erheblich über den Betroffenenkreis eines durchschnittlichen, durch ErwGr. 91 Satz 4 privilegierten Einzelarztes hinaus geht – kann eine umfangreiche Verarbeitung gegeben sein, sodass ein DSB zu benennen ist. Ungeachtet dessen ist die Benennung generell zu empfehlen, um die Einhaltung der datenschutzrechtlichen Bestimmungen zu erleichtern und damit gegebenenfalls aufsichtsbehördliche Maßnahmen zu vermeiden.

Die Regelung des Art. 37 Abs. 4 Satz 1 DS-GVO sieht vor, dass DSBe auch auf freiwilliger Basis benannt werden können. Soweit keine Pflicht zur Benennung eines DSB vorliegt, kann eine freiwillige Benennung eines DSB empfehlenswert sein.

## Benennung des DSB bei weiteren Verantwortlichen und Auftragsverarbeitern nach § 38 BDSG-neu

Die EU-Mitgliedsstaaten haben die Möglichkeit, die Pflicht zur Benennung eines DSB in ihren nationalen Ausführungsgesetzen auf weitere Stellen auszudehnen (Art. 37 Abs. 4 Satz 1 DS-GVO). Der Bundesgesetzgeber hat diesen Regelungsspielraum genutzt, um die Pflicht zur Benennung von betrieblichen DSBen dem in Deutschland bestehenden „Status quo“ anzupassen (vgl. § 4f BDSG-alt sowie § 38 BDSG-neu).

Demnach ist eine Benennung eines DSB auch in folgenden Fällen erforderlich:

- es werden in der Regel mindestens zehn[1] Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt oder
- es werden Verarbeitungen vorgenommen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen oder es werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet;

dann muss unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen ein DSB benannt werden.

## Gemeinsamer DSB

Eine Unternehmensgruppe darf einen gemeinsamen DSB benennen (vgl. Art. 37 Abs. 2 DS-GVO). Voraussetzung hierfür ist, dass der DSB von jeder Niederlassung aus leicht erreicht werden kann. Hiervon ist auch der Fall erfasst, dass nach deutschem Recht eine Pflicht zur Benennung eines DSB besteht und dieser DSB außerhalb Deutschlands für deutsche Niederlassungen benannt wird. In diesem Zusammenhang wird jedoch empfohlen, den DSB in der Europäischen Union anzusiedeln, um die Aufgabenerfüllung in Bezug auf die DS-GVO zu erleichtern.

---

[1] Der Wert soll nach Bundestagsbeschluss vom 27. Juni 2019 auf 20 angehoben werden. Vgl. Fn. 1 im Teil A.

Behörden oder öffentliche Stellen haben die Möglichkeit, für mehrere Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe einen gemeinsamen DSB zu benennen (Art. 37 Abs. 3 DS-GVO). Der Bezug auf Organisationsstruktur und Größe bedeutet auch, dass der Verantwortliche sicherstellen muss, dass der gemeinsame DSB in der Lage ist, die Aufgaben zu erfüllen, welche ihm in Bezug auf sämtliche Behörden oder öffentliche Stellen übertragen wurden.

**Leichte Erreichbarkeit des DSB**

Es sind Vorkehrungen zu treffen, die es den betroffenen Personen oder anderen Stellen ermöglichen, den DSB leicht zu erreichen (z.B. Einrichtung einer Hotline oder eines Kontaktformulars auf der Homepage). Dem DSB muss eine Kommunikation in der Sprache möglich sein, welche für die Korrespondenz mit Aufsichtsbehörden und betroffenen Personen notwendig ist.

**Berufliche Qualifikation und Fachwissen**

Der DSB wird aufgrund seiner beruflichen Qualifikation und insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie seiner Fähigkeit, die Aufgaben gemäß Artikel 39 DS-GVO zu erfüllen, benannt.

**Interner und externer DSB**

Der DSB kann Beschäftigter des Unternehmens oder der Behörde sein (interner DSB) oder seine Aufgaben aufgrund eines Dienstleistungsvertrages erfüllen (externer DSB, Art. 37 Abs. 6 DS-GVO).

**Form der Benennung**

Da die DS-GVO lediglich von einer Benennung des DSB spricht, ist eine Schriftform – im Gegensatz zum § 4f Abs. 1 Satz 1 BDSG-alt – nicht mehr vorgeschrieben. Aus Beweisgründen im Hinblick auf die Nachweispflichten gemäß Art. 24 Abs. 1 DS-GVO und Art. 5 Abs. 2 DS-GVO und zur Rechtssicherheit ist es jedoch empfehlenswert, die Benennung eines DSB in geeigneter Form zu dokumentieren. Die bereits vor Geltung der DS-GVO und dem BDSG-neu unterzeichneten Bestellungsur-

kunden gelten vor diesem Hintergrund fort. Die Urkunde und etwaige darin enthaltenen Zusatzvereinbarungen und Aufgabenzuweisungen sollten auf ihre Vereinbarkeit mit den neuen Regelungen der DS-GVO überprüft und ggf. angepasst werden.

### Stellung des DSB und Pflichten des Verantwortlichen oder des Auftragsverarbeiters

Der Verantwortliche oder der Auftragsverarbeiter muss die Weisungsfreiheit des DSB bei der Erfüllung seiner Aufgaben sicherstellen. Der DSB darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der besondere Abberufungs- und Kündigungsschutz für DSB gemäß § 4f Abs. 3 Satz 4 – 6 BDSG-alt ist im BDSG-neu beibehalten worden (§ 6 Abs. 4 i. V. m. § 38 Abs. 2 BDSG-neu). Der DSB berichtet unmittelbar der höchsten Leitungsebene (Art. 38 Abs. 3 Satz 3 DS-GVO).

Es muss nach Art. 38 DS-GVO sichergestellt werden, dass der DSB ordnungsgemäß und frühzeitig in alle Datenschutzfragen eingebunden wird. Der DSB muss bei der Erfüllung seiner Aufgaben unterstützt werden, indem ihm Folgendes zur Verfügung gestellt wird:

- die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen (einschließlich Personals),
- der Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie
- die zur Erhaltung seines Fachwissens erforderlichen Ressourcen.

Der DSB ist bei der Erfüllung seiner Aufgaben zur Wahrung der Geheimhaltung oder Vertraulichkeit verpflichtet. Das BDSG-neu regelt für DSB ergänzend die Pflicht zur Verschwiegenheit über die Identität der betroffenen Person, die den DSB zu Rate zieht, sowie über die Umstände, die Rückschlüsse auf die betroffene Person zulassen. Darüber hinaus erstreckt § 6 Abs. 6 i. V. m. § 38 Abs. 2 BDSG-neu die Pflicht zur Wahrung der Geheimhaltung und Vertraulichkeit auf das Zeugnisverweigerungsrecht.

Der Verantwortliche kann dem DSB noch weitere Aufgaben übertragen, wobei er sicherstellen muss, dass keine Interessenkonflikte auftreten. Dies ist insbesondere anzunehmen, wenn gleichzeitig Positionen des leitenden Managements wahrgenommen werden oder die Tätigkeitsfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen.

## Aufgaben des DSB

Der DSB hat nach Art. 39 DS-GVO folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Datenschutzpflichten (lit. a);
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen (lit. b);
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und Überwachung ihrer Durchführung (lit. c);
- Zusammenarbeit mit der Aufsichtsbehörde (lit. d) und Tätigkeit als Anlaufstelle für die Aufsichtsbehörde (lit. e).

Hinzu kommt die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der DS-GVO im Zusammenhang stehenden Fragen (Art. 38 Abs. 4 DS-GVO).

## Risikoorientierte Aufgabenerfüllung durch den DSB

Der DSB nimmt seine Aufgaben nach Art. 39 Abs. 2 DS-GVO risikoorientiert wahr. Er trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

## Verantwortung für die Einhaltung der DS-GVO

Die DS-GVO stellt in Art. 24 Abs. 1 DS-GVO ausdrücklich klar, dass es die Pflicht des Verantwortlichen bzw. des Auftragsverarbeiters – und nicht die des DSB – bleibt, sicherzustellen und nachzuweisen, dass die Datenverarbeitungen im Einklang mit den Regelungen der DS-GVO stehen. Gleichwohl sollte der DSB seine Tätigkeiten in angemessener Weise dokumentieren, um ggf. nachweisen zu können, dass er seinen Aufgaben (insbesondere Unterrichtung und Beratung) ordnungsgemäß nachgekommen ist.

## Veröffentlichungs- und Mitteilungspflichten der Kontaktdaten des DSB

Die Kontaktdaten des DSB sind nach Art. 37 Abs. 7 DS-GVO zu veröffentlichen und der Aufsichtsbehörde mitzuteilen. Die Aufsichtsbehörden werden den mitteilungspflichtigen Stellen ein Formular zur Mitteilung der Kontaktdaten des DSB zur Verfügung stellen.

## Rechtsfolgen bei Verstoß

Verletzungen der Vorschriften zum DSB aus Art. 37 bis 39 DS-GVO (z.B. Nicht-Benennung oder unzureichende Unterstützung des DSB) sind nach Art. 83 Abs. 4 lit. a DS-GVO mit Geldbuße bedroht.

## Hinweis

Die Artikel-29-Datenschutzgruppe hat zur näheren Erläuterung der Art. 37 bis 39 DS-GVO inzwischen „Leitlinien in Bezug auf Datenschutzbeauftragte“ (Working Paper 243) erstellt.

***Quellenvermerk:***
***Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)***
***Datenlizenz Deutschland – Namensnennung – Version 2.0***
***(www.govdata.de/dl-de/by-2-0)***
***Volltext unter:***
***https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_12.pdf***

# 4. Art.-29-Datenschutzgruppe: Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), angenommen am 13.12.2016, zuletzt überarbeitet und angenommen am 05.04.2017 (WP 243 rev.01), bestätigt durch den EDSA am 25.05.2018 – Auszug –

## Inhaltsverzeichnis

1 Einführung

2 Benennung eines DSB
- 2.1. Obligatorische Benennung
  - *2.1.1 „Behörden oder öffentliche Stellen“*
  - *2.1.2 „Kerntätigkeit“*
  - *2.1.3 „Umfangreiche Verarbeitung“*
  - *2.1.4 „Regelmäßige und systematische Überwachung“*
  - *2.1.5 Besondere Kategorien von Daten und Daten über strafrechtliche Verurteilungen und Straftaten*
- 2.2. DSB des Auftragsverarbeiters
- 2.3. Benennung eines gemeinsamen DSB für mehrere Organisationen
- 2.4. Erreichbarkeit und Standort des DSB
- 2.5. Fähigkeiten und Fachkenntnisse des DSB
- 2.6. Veröffentlichung und Mitteilung der Kontaktdaten des DSB

3 Stellung des DSB
- 3.1. Einbindung des DSB in alle mit dem Schutz personenbezogener Daten in Zusammenhang stehende Angelegenheiten
- 3.2. Erforderliche Ressourcen
- 3.3. Anweisungen und „Ausübung der Pflichten und Aufgaben in vollständiger Unabhängigkeit“
- 3.4. Abberufung oder Benachteiligung des DSB wegen der Erfüllung seiner Aufgaben

3.5. Interessenkonflikte

4 Aufgaben des DSB
4.1. Überwachung der Einhaltung der DS-GVO
4.2. Die Funktion des DSB bei einer Datenschutz-Folgenabschätzung
4.3. Zusammenarbeit mit der Aufsichtsbehörde und Tätigkeit als Anlaufstelle
4.4. Risikobasierter Ansatz
4.5. Die Funktion des DSB bei der Führung von Verzeichnissen

5 Anhang zu den DSB-Leitlinien: Was Sie wissen müssen
[…]
[*Hier nicht abgedruckt*]

## 1 Einführung

Die Datenschutz-Grundverordnung (DS-GVO)[1], die am 25. Mai 2018 in Kraft treten soll, wird einen modernisierten, auf dem Prinzip der Rechenschaftspflicht beruhenden Handlungsrahmen für die Überprüfung der Einhaltung der Datenschutzvorschriften in Europa bieten. Den Kern dieser neuen Rechtsgrundlage werden für viele Einrichtungen Datenschutzbeauftragte (DSB) bilden, die die Einhaltung der Bestimmungen der DS-GVO erleichtern.

Nach der DS-GVO sind Verantwortliche und Auftragsverarbeiter unter bestimmten Voraussetzungen verpflichtet, einen DSB[2] zu ernennen.

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 04.05.2016).
Die DS-GVO ist mit Bedeutung für den EWR und wird nach ihrer Aufnahme in das EWR-Abkommen angewendet.

[2] Auch bei den zuständigen Behörden ist die Ernennung eines DSB zwingend vorgeschrieben nach Artikel 32 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des

Diese Pflicht besteht für alle Behörden und öffentlichen Stellen (unabhängig von der Art der verarbeiteten Daten) wie auch für sonstige Einrichtungen, die – als Kerntätigkeit – systematisch und in großem Umfang Einzelpersonen überwachen oder in großem Umfang besondere Kategorien von personenbezogenen Daten verarbeiten.

In Fällen, in denen die DS-GVO die Bestellung eines DSB nicht ausdrücklich vorschreibt, können Einrichtungen es mitunter für zweckmäßig erachten, einen solchen auf freiwilliger Basis zu ernennen. Die Artikel-29-Datenschutzgruppe („WP29“) fördert derartige freiwillige Anstrengungen.

Das dem DSB zugrundeliegende Konzept ist nicht neu. Wenngleich nach der Richtlinie 95/46/EG[3] keine Einrichtung zur Ernennung eines DSB verpflichtet ist, hat sich die Praxis der Ernennung eines DSB in zahlreichen Mitgliedstaaten im Laufe der Jahre immer mehr verbreitet.

Vor dem Erlass der DS-GVO argumentierte die WP29, dass der DSB ein wichtiger Akteur im Bereich der Rechenschaftspflicht sei und dass die Ernennung eines DSB die Einhaltung der Vorschriften erleichtere und überdies Unternehmen als Wettbewerbsinstrument diene.[4] DSB erleichtern nicht nur die Einhaltung der Bestimmungen, indem sie etwa Instrumente zur Anwendung bringen, die der Einhaltung der Rechenschaftspflicht dienen (wie etwa die Erleichterung oder Durchführung von Datenschutz-Folgenabschätzungen und -Überprüfungen), sondern fungieren darüber hinaus auch als Mittler zwischen den maßgeblichen Interessenträgern (z. B. Aufsichtsbehörden, betroffene Personen und für die Geschäftsführung zuständige Stellen einer Einrichtung).

---

Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) und nach den nationalen Durchführungsbestimmungen. Diese Leitlinien stellen zwar vorrangig auf DSB im Rahmen der DS-GVO ab, sind jedoch auch für DSB im Rahmen der Richtlinie 2016/680 im Hinblick auf die darin enthaltenen ähnlichen Bestimmungen relevant.

3 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

4 Vgl. http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2015/20150617_appendix_core_issues_plenary_de.pdf

DSB sind im Falle der Nichteinhaltung der DS-GVO nicht persönlich verantwortlich. Aus der DS-GVO geht klar hervor, dass es Aufgabe des Verantwortlichen oder des Auftragsverarbeiters ist, sicherzustellen und nachweisen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt (Artikel 24 Absatz 1). Für die Einhaltung der datenschutzrechtlichen Bestimmungen ist der Verantwortliche oder der Auftragsverarbeiter verantwortlich.

Dem Verantwortlichen oder dem Auftragsverarbeiter kommt zugleich eine wichtige Rolle dabei zu, die Voraussetzung dafür zu schaffen, dass der DSB seinen Aufgaben wirksam nachgehen kann. Die Ernennung eines DSB stellt hierbei nur einen ersten Schritt dar: Um ihren Aufgaben wirksam nachgehen zu können, müssen DSB auch über hinreichende Eigenständigkeit und genügend Ressourcen verfügen.

In der DS-GVO werden die Bedeutung des DSB als Schlüsselfigur im neuen Data-Governance-System anerkannt und die Bedingungen für seine Ernennung, Stellung und Aufgaben dargelegt. Ziel dieser Leitlinien ist es, die einschlägigen Bestimmungen der DS-GVO klarzustellen, um die Verantwortlichen und Auftragsverarbeiter bei der Erfüllung der gesetzlichen Vorgaben zu unterstützen und den DSB bei ihrer Tätigkeit Hilfestellung zu leisten. Die Leitlinien enthalten zugleich Empfehlungen für bewährte Verfahren, denen die in verschiedenen EU-Mitgliedstaaten gesammelten Erfahrungen zugrunde liegen. Die WP29 wird die Umsetzung dieser Leitlinien beaufsichtigen und erforderlichenfalls im Detail ergänzen.

## 2 Benennung eines DSB

### 2.1. Obligatorische Benennung

Nach Artikel 37 Absatz 1 der DS-GVO ist die Benennung eines DSB in drei bestimmten Fällen[5] vorgeschrieben:

a) falls die Datenverarbeitung durch Behörden oder öffentliche Stellen erfolgt[6],

[5] Hierbei ist zu beachten, dass nach Artikel 37 Absatz 4 Gemeinschafts- oder einzelstaatliche Rechtsvorschriften die Benennung eines DSB auch in anderen Fällen zwingend erforderlich machen können.

b) falls die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in Datenverarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang erfordern, oder

c) falls die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten[7] oder[8] von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten[9] besteht.

In den nachfolgenden Unterabschnitten stellt die WP29 Anleitungen in Bezug auf die in Artikel 37 Absatz 1 zugrunde gelegten Kriterien und die darin enthaltene Terminologie bereit.

Sofern eine Einrichtung offenkundig nicht verpflichtet ist, einen DSB zu benennen, empfiehlt die WP29, dass die Verantwortlichen und Auftragsverarbeiter die durchgeführte interne Analyse zur Klärung der Frage, ob ein DSB benannt werden muss, dokumentieren, um nachweisen zu können, dass die maßgeblichen Faktoren ordnungsgemäß berücksichtigt wurden.[10] Diese Analyse ist Teil der Dokumentation nach dem Prinzip der Rechenschaftspflicht. Sie kann von der Aufsichtsbehörde angefordert werden und ist gegebenenfalls zu aktualisieren, z. B. wenn die Verantwortlichen oder die Auftragsverarbeiter neue Tätigkeiten durchführen oder neue Leistungen erbringen, die unter Artikel 37 Absatz 1 fallen können.

---

6 Mit Ausnahme von Gerichten, die in ihrer justiziellen Eigenschaft agieren. Siehe Artikel 32 der Richtlinie (EU) 2016/680.

7 Nach Artikel 9 zählen hierzu personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

8 In Artikel 37 Absatz 1 Buchstabe c wird das Wort „und“ verwendet. Erläuterungen zur Verwendung von „oder“ anstelle von „und“ finden sich nachfolgend in Abschnitt 2.1.5.

9 Artikel 10.

10 Vgl. Artikel 24 Absatz 1.

Wenn eine Einrichtung einen DSB auf freiwilliger Basis ernennt, so unterliegen dessen Benennung Artikel 37 bis 39, Stellung und Aufgabenbereich den Anforderungen wie bei einer obligatorischen Benennung.

Einer Einrichtung, die zur Benennung eines DSB nicht gesetzlich verpflichtet ist und die nicht gewillt ist, einen solchen auf freiwilliger Basis zu benennen, steht es frei, Mitarbeiter oder externe Berater/Beraterinnen mit Aufgaben zu betrauen, die mit dem Schutz personenbezogener Daten in Zusammenhang stehen. In einem solchen Fall gilt es jegliche Unklarheit hinsichtlich ihrer Funktionsbezeichnung, ihres Status, ihrer Stellung und ihres Aufgabenfelds zu vermeiden. Daher sollte aus allen Mitteilungen innerhalb des Unternehmens und gegenüber Datenschutzbehörden, betroffenen Personen und der breiten Öffentlichkeit klar hervorgehen, dass die Funktionsbezeichnung der natürlichen Person bzw. des Beraters/der Beraterin nicht die eines Datenschutzbeauftragten (DSB) ist.[11]

Der DSB wird für alle vom Verantwortlichen oder Auftragsverarbeiter durchgeführten Verarbeitungsvorgänge ernannt, unabhängig davon, ob die Ernennung obligatorisch ist oder auf freiwilliger Basis erfolgt.

### *2.1.1 „BEHÖRDEN ODER ÖFFENTLICHE STELLEN“*

Die DS-GVO enthält keine Definition von *„Behörden oder öffentliche Stellen“*. Die WP29 ist der Ansicht, dass dieser Begriff nach Maßgabe des einzelstaatlichen Rechts zu bestimmen ist. Der Begriff „Behörden und öffentliche Stellen“ schließt landesweite, regionale und lokale Behörden ein, beinhaltet jedoch nach geltendem einzelstaatlichem Recht außerdem üblicherweise noch eine Reihe weiterer dem öffentlichen Recht unterliegender Stellen.[12] In solchen Fällen ist die Benennung eines DSB obligatorisch.

---

[11] Dies betrifft auch leitende Datenschutzbeauftragte (engl. Chief Privacy Officers, CPO) und sonstige in bestimmten Firmen im Datenschutzbereich tätige Personen, die möglicherweise nicht immer die Kriterien der DS-GVO (beispielsweise in Bezug auf die verfügbaren Ressourcen oder ihre garantierte Unabhängigkeit) erfüllen und in einem solchen Fall nicht als DSB betrachtet oder bezeichnet werden dürfen.

[12] Vgl. hierzu z.B. die Definition von „öffentliche Stelle“ und „Einrichtung des öffentlichen Rechts“ in Artikel 2 Absatz 1 und Absatz 2 der Richtlinie 2003/98/EG des Eu-

Eine öffentliche Aufgabe und öffentliche Gewalt kann nicht nur von öffentlichen Einrichtungen und Stellen wahrgenommen bzw. ausgeübt werden[13], sondern auch von jeglicher natürlichen oder juristischen Person, die – je nach den einzelstaatlichen Bestimmungen des betreffenden Mitgliedstaates – in Bereichen wie etwa dem öffentlichem Transportwesen, der Wasser- und Energieversorgung, der Verkehrsinfrastruktur, dem öffentlich-rechtlichen Rundfunk, dem sozialen Wohnungsbau oder den Disziplinarkommissionen für reglementierte Berufe öffentlichem oder privatem Recht unterliegt.

In diesen Fällen können sich Betroffene in einer sehr ähnlichen Situation befinden, wie wenn ihre Daten von einer Behörde oder öffentlichen Stelle verarbeitet würden. Insbesondere können Daten zu ähnlichen Zwecken verarbeitet werden, wobei natürliche Personen oftmals nur wenig bis gar keine Einflussmöglichkeit darauf haben, wie ihre Daten verarbeitet werden, und von daher möglicherweise jenes zusätzlichen Schutzes bedürfen, den die Benennung eines DSB ermöglichen kann.

Wenn auch in solchen Fällen keine Verpflichtung besteht, empfiehlt die WP29 gleichwohl als bewährtes Verfahren, dass private Einrichtungen, die öffentliche Aufgaben wahrnehmen oder Staatsgewalt ausüben, einen DSB benennen. Die Tätigkeit eines solchen DSB erfasst zugleich sämtliche durchgeführten Datenverarbeitungsvorgänge, einschließlich solcher, die nicht mit der Wahrnehmung einer öffentlichen Aufgabe oder Ausübung einer öffentlichen Pflicht im Zusammenhang stehen (z. B. das Führen einer Personaldatenbank).

ropäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 345 vom 31.12.2003, S. 90).

[13] Artikel 6 Absatz 1 Buchstabe e.

### *2.1.2 „KERNTÄTIGKEIT“*

Artikel 37 Absatz 1 Buchstabe b und Buchstabe c der DS-GVO bezieht sich auf die *„Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters“*. In ErwG 97 ist dargelegt, dass sich die Kerntätigkeit eines Verantwortlichen auf *„seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit“* bezieht. Als „Kerntätigkeit“ lassen sich die wichtigsten Arbeitsabläufe betrachten, die zur Erreichung der Ziele des Verantwortlichen oder des Auftragsverarbeiters erforderlich sind.

Gleichwohl sollte der Begriff „Kerntätigkeit“ nicht dahingehend interpretiert werden, dass sich dieser nicht auch auf Tätigkeiten erstreckte, bei denen die Verarbeitung von Daten einen untrennbaren Bestandteil der Tätigkeit des Verantwortlichen oder Auftragsverarbeiters darstellt. So besteht beispielsweise die Kerntätigkeit eines Krankenhauses darin, medizinische Versorgung zu leisten. Ohne dabei gesundheitsbezogenen Daten wie etwa Krankenakten von Patienten zu verarbeiten, wäre ein Krankenhaus nicht in der Lage, dies in sicherer und wirksamer Form zu tun. Daher ist die Verarbeitung solcher Daten als Kerntätigkeit eines jeden Krankenhauses anzusehen, weshalb selbige zur Benennung eines DSB verpflichtet sind.

Als weiteres Beispiel sei ein privates Sicherheitsunternehmen angeführt, das private Einkaufszentren und öffentliche Plätze überwacht. Überwachung stellt die Kerntätigkeit des Unternehmens dar, die wiederum untrennbar mit der Verarbeitung personenbezogener Daten einhergeht. Daher ist auch ein solches Unternehmen verpflichtet, einen DSB zu benennen.

Hingegen führen alle Einrichtungen gewisse Tätigkeiten wie etwa die Entlohnung ihrer Mitarbeiter oder die Leistung von Standard-IT-Support aus. Hierbei handelt es sich um Beispiele von für die Kerntätigkeit oder das Kerngeschäft der Einrichtung notwendigen Unterstützungsfunktionen. Trotz ihrer Notwendigkeit oder Unverzichtbarkeit werden solche Tätigkeiten gemeinhin eher als Nebenfunktionen denn als Kerntätigkeit angesehen.

### *2.1.3 „UMFANGREICHE VERARBEITUNG“*

Artikel 37 Absatz 1 Buchstabe b und Buchstabe c sieht vor, dass das Erfordernis der Benennung eines DSB nur dann besteht, wenn eine umfangreiche Verarbeitung personenbezogener Daten erfolgt. In der DS-GVO ist nicht näher quantifiziert, was unter „umfangreich“ zu verstehen ist. Gleichwohl liefert ErwG 91 diesbezüglich einen gewissen Anhaltspunkt.[14]

Es ist nicht möglich, eine genaue, auf jeden Einzelfall anwendbare Zahlenangabe bezüglich der Menge an verarbeiteten Daten oder der Zahl an betroffenen natürlichen Personen zu machen. Dies schließt indes nicht aus, dass sich im Laufe der Zeit eine Standard-Praxis dafür entwickeln wird, wie sich der Begriff „umfangreiche Verarbeitung“ in Bezug auf bestimmte Formen gängiger Datenverarbeitungsvorgänge spezifischer und quantitativer definieren lässt. Die WP29 plant, durch Weitergabe und Veröffentlichung von Beispielen für maßgebliche Schwellenwerte für die Bestimmung eines DSB zu dieser Entwicklung beizutragen.

Auf alle Fälle empfiehlt die WP29, bei der Klärung der Frage, ob sich von einer umfangreichen Verarbeitung sprechen lässt, die folgenden Faktoren zu berücksichtigen:

---

[14] Diesem Erwägungsgrund zufolge bezieht sich dieser Begriff besonders *auf „umfangreiche Verarbeitungsvorgänge […], die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und - beispielsweise aufgrund ihrer Sensibilität - wahrscheinlich ein hohes Risiko mit sich bringen“*. Andererseits ist im Erwägungsgrund ausdrücklich vorgesehen: *„Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt.“* In diesem Zusammenhang gilt es zu berücksichtigen, dass in diesem Erwägungsgrund Extrembeispiele (die Verarbeitung durch einen einzelnen Arzt gegenüber der Verarbeitung von landes- oder gar europaweiten Daten) angeführt werden und zwischen diesen Extremen eine große Grauzone besteht. Auch ist zu beachten, dass sich dieser Erwägungsgrund auf Datenschutz-Folgeabschätzungen bezieht. Dies bringt es mit sich, dass manche dieser Elemente möglicherweise kontextspezifisch sind und nicht unbedingt in der genau gleichen Weise für die Bestimmung eines DSB gelten.

- die Zahl der betroffenen Personen – entweder als bestimmte Zahl oder als Anteil an der maßgeblichen Bevölkerung
- das Datenvolumen und/oder das Spektrum an in Bearbeitung befindlichen Daten
- die Dauer oder Permanenz der Datenverarbeitungstätigkeit
- die geografische Ausdehnung der Verarbeitungstätigkeit

Beispiele für eine umfangreiche Verarbeitung stellen dar:

- die Verarbeitung von Patientendaten im gewöhnlichen Geschäftsbetrieb eines Krankenhauses
- die Verarbeitung von Reisedaten natürlicher Personen, die ein Verkehrsmittel des kommunalen ÖPNV nutzen (z. B. Nachverfolgung über Netzkarten)
- die Verarbeitung von Geolokalisierungsdaten von Kunden einer internationalen Fast-food-Kette in Echtzeit zu statistischen Zwecken durch einen auf Dienstleistungen dieser Art spezialisierten Auftragsverarbeiter
- die Verarbeitung von Kundendaten im gewöhnlichen Geschäftsbetrieb eines Versicherungsunternehmens oder einer Bank
- die Verarbeitung personenbezogener Daten durch eine Suchmaschine zu Zwecken der verhaltensbasierten Werbung
- die Verarbeitung von Daten (Inhalte, Datenverkehrsaufkommen, Standort) durch Telefon- oder Internetdienstleister

Keine umfangreiche Verarbeitung stellen die folgenden Beispiele dar:

- die Verarbeitung von Patientendaten durch einen einzelnen Arzt
- die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten durch einen einzelnen Rechtsanwalt

### *2.1.4 „REGELMÄßIGE UND SYSTEMATISCHE ÜBERWACHUNG“*

Der Begriff der regelmäßigen und systematischen Überwachung ist in der DS-GVO zwar nicht definiert, doch das Konzept einer *„Beobachtung des Verhaltens von betroffenen Personen“* wird in ErwG 24[15] erwähnt und erstreckt sich demnach eindeutig auf jede Form der Verfolgung und Profilerstellung im Internet, darunter auch zu Zwecken der verhaltensbasierten Werbung.

Gleichwohl beschränkt sich der Begriff der Überwachung nicht auf die Online-Umgebung, weshalb die Online-Verfolgung nur als ein Beispiel für die Überwachung des Verhaltens von betroffenen Personen angesehen werden sollte.[16]

Die WP29 interpretiert den Begriff „regelmäßig“ als mindestens eine der folgenden Eigenschaften:

- fortlaufend oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommend
- immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretend
- ständig oder regelmäßig stattfindend

Die WP29 interpretiert den Begriff „systematisch“ als mindestens eine der folgenden Eigenschaften:

- systematisch vorkommend
- vereinbart, organisiert oder methodisch

---

15 *„Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von betroffenen Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, einschließlich der möglichen nachfolgenden Verwendung von Techniken zur Verarbeitung personenbezogener Daten, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.“*

16 Zu beachten ist, dass Erwägungsgrund 24 sich auf die extraterritoriale Anwendung der DS-GVO konzentriert. Überdies besteht ein Unterschied zwischen den Formulierungen *„das Verhalten betroffener Personen zu beobachten“* (Artikel 3 Absatz 2 Buchstabe b) *und „regelmäßige und systematische Überwachung von betroffenen Personen“* (Artikel 37 Absatz 1 Buchstabe b), so dass diese als unterschiedliche Begrifflichkeiten interpretiert werden können.

- im Rahmen eines allgemeinen Datenerfassungsplans erfolgend
- im Rahmen einer Strategie erfolgend

Folgende Tätigkeiten können eine regelmäßige und systematische Überwachung von betroffenen Personen darstellen: Betrieb eines Telekommunikationsnetzes, Anbieten von Telekommunikationsdienstleistungen, verfolgende E-Mail-Werbung, datengesteuerte Marketingaktivitäten, Typisierung und Scoring zu Zwecken der Risikobewertung (zum Beispiel zu Zwecken der Kreditvergabe, der Festlegung von Versicherungsprämien, Maßnahmen zur Verhinderung von betrügerischen Handlungen, Ermittlung von Geldwäsche), Standortverfolgung (beispielsweise durch Mobilfunkanwendungen), Treueprogramme, verhaltensbasierte Werbung, Überwachung von Wellness-, Fitness- und gesundheitsbezogenen Daten über in Kleidung integrierte Geräte (Wearables), Überwachungskameras oder vernetzte Geräte (zum Beispiel intelligente Stromzähler, intelligente Autos, Haustechnik usw.)

### *2.1.5 BESONDERE KATEGORIEN VON DATEN UND DATEN ÜBER STRAFRECHTLICHE VERURTEILUNGEN UND STRAFTATEN*

Artikel 37 Absatz 1 Buchstabe c behandelt die Verarbeitung besonderer Kategorien von Daten nach Artikel 9 sowie personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten nach Artikel 10. Wenn auch in der Bestimmung das Wort „und“ verwendet wird, besteht kein politischer Grund dafür, dass die beiden Kriterien gleichzeitig angewandt werden müssten. Der Wortlaut sollte daher im Sinne eines „oder“ verstanden werden.

## 2.2. DSB des Auftragsverarbeiters

Artikel 37 gilt im Hinblick auf die Benennung eines DSB gleichermaßen für Verantwortliche[17] und Auftragsverarbeiter[18]. Je nachdem, wer die Kriterien für eine zwingend vorgeschriebene Benennung erfüllt, sind in manchen Fällen lediglich der Verantwortliche oder der Auftragsverarbeiter, in anderen wiederum beide zur Benennung eines DSB verpflichtet (und sollten in solchen Fällen zusammenarbeiten).

Dabei gilt es hervorzuheben, dass selbst dann, wenn der Verantwortliche die Kriterien für eine obligatorische Benennung eines DSB erfüllt, dies nicht zwangsläufig auch für dessen Auftragsverarbeiter gilt. Dies kann indes ein bewährtes Verfahren darstellen.

Beispiele:

- Ein im Vertrieb von Haushaltswaren in einer einzelnen Stadt tätiges kleines Familienunternehmen nimmt die Dienste eines Auftragsverarbeiters in Anspruch, dessen Kerntätigkeit in der Bereitstellung von Website-Analysediensten und der Unterstützung bei zielgruppenorientierten Werbe- und Marketingmaßnahmen besteht. Bei den Tätigkeiten des Familienunternehmens und seiner Kunden fällt in Anbetracht der geringen Kundenzahl und der vergleichsweise beschränkten Tätigkeiten keine „umfangreiche Verarbeitung“ von Daten an. Die Tätigkeiten des Auftragsverarbeiters hingegen, der über eine große Zahl an Kunden wie diesem Kleinunternehmen verfügt, ergeben zusammen eine durchaus als umfangreich einzustufende Verarbeitung. Der Auftragsverarbeiter ist daher zur Benennung eines DSB nach Artikel 37 Absatz 1 Buchstabe b verpflichtet. Für das Familienunternehmen hingegen besteht eine solche Pflicht nicht.

---

17 Der Verantwortliche ist nach Artikel 4 Absatz 7 als natürliche oder juristische Person definiert, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

18 Der Auftragsverarbeiter ist nach Artikel 4 Absatz 8 als natürliche oder juristische Person definiert, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- Ein mittelgroßer Fliesenhersteller beauftragt einen externen Auftragsverarbeiter, der über eine Vielzahl ähnlicher Kunden verfügt, mit der Erbringung seiner arbeitsmedizinischen Dienste. Sofern dabei eine Verarbeitung von Daten in großem Umfang erfolgt, ist der Auftragsverarbeiter nach Artikel 37 Absatz 1 Buchstabe c zur Benennung eines DSB verpflichtet. Gleiches gilt nicht zwangsläufig auch für den Fliesenhersteller.

Der von einem Auftragsverarbeiter benannte DSB beaufsichtigt auch die von der Einrichtung des Auftragsverarbeiters durchgeführten Tätigkeiten, wenn diese als für die Verarbeitung eigenständiger Verantwortlicher auftritt (z. B. Personal-, IT- oder Logistikabteilungen).

## 2.3. Benennung eines gemeinsamen DSB für mehrere Organisationen

Artikel 37 Absatz 2 gestattet einer Unternehmensgruppe die Benennung eines gemeinsamen DSB, sofern dieser *„von jeder Niederlassung aus […] leicht erreicht werden kann“*. Der Begriff der Erreichbarkeit bezieht sich auf die Aufgaben des DSB als Ansprechpartner für Betroffene[19] und für die Aufsichtsbehörde[20], gilt jedoch auch für dessen Aufgaben als einrichtungsinterner Ansprechpartner, denn eine der Aufgaben des DSB ist ja die *„Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung“*.[21]

Um die Erreichbarkeit des DSB sowohl intern als auch extern zu gewährleisten, ist dafür Sorge zu tragen, dass die Kontaktdaten im Einklang mit den Vorgaben der DS-GVO zur Verfügung stehen[22].

---

[19] Artikel 38 Absatz 4: *„Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.“*

[20] Artikel 39 Absatz 1 Buchstabe e: *„Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.“*

[21] Artikel 39 Absatz 1 Buchstabe a.

[22] Vgl. auch Abschnitt 2.6.

Der DSB muss – gegebenenfalls mithilfe eines Teams – in der Lage sein, mit Betroffenen wirksam zu kommunizieren[23] und mit den zuständigen Aufsichtsbehörden effektiv zusammenzuarbeiten[24]. Dies bedeutet, dass die Kommunikation in der bzw. den von den Aufsichtsbehörden und dem Betroffenen verwendeten Sprache(n) erfolgen muss. Damit die Betroffenen den DSB kontaktieren können, ist es unverzichtbar, dass dieser (entweder physisch auf dem gleichen Gelände wie die Beschäftigten oder über eine Hotline oder andere sichere Kommunikationskanäle) persönlich erreichbar ist.

Nach Artikel 37 Absatz 3 kann von mehreren öffentlichen Einrichtungen und Stellen in Anbetracht ihrer Organisationsstruktur und Größe ein gemeinsamer DSB benannt werden. Gleiches gilt für die erforderlichen Ressourcen und die Kommunikation: Da der DSB eine Vielzahl von Aufgaben wahrzunehmen hat, ist es Sache des Verantwortlichen oder des Auftragsverarbeiters, dafür Sorge zu tragen, dass einzelne DSB trotz der Zuständigkeit für mehrere öffentliche Einrichtungen und Stellen in der Lage sind, diesen – gegebenenfalls mithilfe eines Teams – wirksam nachzugehen.

### 2.4. Erreichbarkeit und Standort des DSB

Nach Abschnitt 4 der DS-GVO bedarf es der effektiven Erreichbarkeit des DSB.

Die WP29 empfiehlt, die effektive Erreichbarkeit des DSB durch die Ernennung eines DSB mit Sitz in der Europäischen Union zu gewährleisten, unabhängig davon, ob der Verantwortliche oder der Auftragsverarbeiter in der Union niedergelassen ist.

---

[23] Artikel 12 Absatz 1 besagt diesbezüglich: *„Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten“.*

[24] Artikel 39 Absatz 1 Buchstabe d sieht eine *„Zusammenarbeit mit der Aufsichtsbehörde“* vor.

Jedoch ist nicht ausgeschlossen, dass in Situationen, in denen der Verantwortliche oder der Auftragsverarbeiter nicht in der Europäischen Union niedergelassen ist[25], ein außerhalb der EU niedergelassener DSB seine Aufgaben effektiver ausüben kann.

## 2.5. Fähigkeiten und Fachkenntnisse des DSB

Nach Artikel 37 Absatz 5 wird der Datenschutzbeauftragte *„auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben“*. Nach ErwG 97 sollte sich das erforderliche Niveau des Fachwissens nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz der vom Verantwortlichen oder vom Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten.

- **Fachwissen**

Das verlangte Fachwissen ist nicht genau umrissen, muss jedoch mit der Sensibilität, der Komplexität und der Menge der Daten, die eine Einrichtung verarbeitet, im Einklang stehen. Wenn etwa eine Datenverarbeitungstätigkeit besonders komplex ist oder in großem Umfang sensible Informationen betrifft, bedarf der DSB unter Umständen eines höheren Maßes an Fachkompetenz und Unterstützung. Ebenso macht es einen Unterschied aus, ob die Einrichtung personenbezogene Daten systematisch an Orte außerhalb der Europäischen Union übermittelt oder dies nur gelegentlich geschieht. Die Wahl des DSB sollte daher mit Bedacht erfolgen; sich innerhalb der Einrichtung stellenden Datenschutzfragen ist dabei in angemessener Weise Rechnung zu tragen.

- **Berufliche Qualifikation**

Auch wenn Artikel 37 Absatz 5 keine Angaben bezüglich der beruflichen Qualifikation enthält, die es bei der Bestimmung eines DSB zu berücksichtigen gilt, gilt diesbezüglich die maßgebliche Überlegung, dass ein DSB über Erfahrung sowohl im einzelstaatlichen als auch im europä-

[25] Siehe Artikel 3 DS-GVO zum räumlichen Anwendungsbereich.

ischen Datenschutzrecht und in der diesbezüglichen Praxis sowie über ein umfassendes Verständnis der DS-GVO verfügen muss. Von Vorteil ist es auch, wenn die Aufsichtsbehörden angemessene und regelmäßige Schulungen für DSB fördern.

Branchenkenntnis und Vertrautheit mit der Organisationsstruktur des Auftragsverarbeiters sind von ebenfalls Nutzen. Auch sollte der DSB über ein gutes Verständnis der durchgeführten Datenverarbeitungsvorgänge, der betreffenden Informationssysteme sowie der Datensicherheits- und Datenschutzerfordernisse des Auftragsverarbeiters verfügen.

Im Fall von Behörden oder öffentlichen Stellen sollte der DSB zudem über fundierte Kenntnis ihrer Verwaltungsvorschriften und -verfahren verfügen.

- **Fähigkeit zur Erfüllung seiner Aufgaben**

Der Begriff der Fähigkeit zur Erfüllung der dem DSB obliegenden Aufgaben ist im Sinne sowohl seiner persönlichen Eigenschaften und Kenntnisse als auch seiner Position innerhalb der Einrichtung zu verstehen. Zu den persönlichen Eigenschaften sollten beispielsweise Integrität und ein ausgeprägtes Berufsethos zählen; vorrangiges Anliegen des DSB sollte die Schaffung der Voraussetzungen für die Einhaltung der Vorgaben der DS-GVO sein. Dem DSB kommt eine zentrale Rolle dabei zu, die Verbreitung einer Datenschutzkultur innerhalb der Einrichtung zu fördern und zur Umsetzung wesentlicher Bestandteile der DS-GVO beizutragen, darunter die Grundsätze der Datenverarbeitung[26], die Rechte der betroffenen Personen[27], Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[28], die Aufzeichnung von Verarbeitungstätigkeiten[29], die Sicherheit der Verarbei-

[26] Kapitel II.
[27] Kapitel III.
[28] Artikel 25.
[29] Artikel 30.

tung[30] sowie die Meldung und Mitteilung von Verstößen gegen den Schutz personenbezogener Daten[31].

- **Im Rahmen eines Dienstleistungsvertrags beschäftigte DSB**

Die Funktion eines DSB kann auch auf Grundlage eines Dienstleistungsvertrags ausgeübt werden, der mit einer natürlichen oder juristischen Person geschlossen wird, die nicht der Einrichtung des Verantwortlichen oder Auftragsverarbeiters angehört. In letzterem Falle ist es unverzichtbar, dass jedes Mitglied der Einrichtung, das die Funktionen eines DSB wahrnimmt, sämtliche in Abschnitt 4 der DS-GVO genannten Anforderungen erfüllt (sodass Interessenkonflikte ausgeschlossen werden können). Ebenso wichtig ist es, dass jedes Mitglied durch die Bestimmungen der DS-GVO geschützt ist (keine ungerechtfertigte Kündigung von Dienstleistungsverträgen in Bezug auf Tätigkeiten als DSB und keine ungerechtfertigte Entlassung einer der Einrichtung angehörigen natürlichen Person, welche die Aufgaben eines DSB wahrnimmt). Zugleich lassen sich individuelle Qualifikationen und Stärken so miteinander kombinieren, dass Einzelpersonen durch die Zusammenarbeit im Team ihren Mandanten noch wirksamere Dienste leisten können.

Im Interesse der Rechtssicherheit und einer ordnungsgemäßen Organisation, aber auch, um Interessenkonflikte der Teammitglieder zu vermeiden, wird empfohlen, eine klare Aufgabenverteilung innerhalb des DSB-Teams vorzusehen und eine einzelne Person als primären Ansprechpartner festzulegen, der zugleich für den jeweiligen Kunden „zuständig“ ist. Es ist generell von Nutzen, diese Punkte im Dienstleistungsvertrag festzuhalten.

### 2.6. Veröffentlichung und Mitteilung der Kontaktdaten des DSB

Artikel 37 Absatz 7 der DS-GVO sieht vor, dass der Verantwortliche bzw. Auftragsverarbeiter

- die Kontaktdaten des DSB veröffentlicht und
- diese Daten den zuständigen Aufsichtsbehörden mitteilt.

[30] Artikel 32.
[31] Artikel 33 und 34.

Durch diese Anforderung soll sichergestellt werden, dass sich Betroffene (sowohl innerhalb als auch außerhalb der Einrichtung) und die Aufsichtsbehörden ohne Weiteres auf direktem Wege an den DSB wenden können, ohne mit einem anderen Teil der Einrichtung in Kontakt treten zu müssen. Ein weiterer wichtiger Gesichtspunkt ist Vertraulichkeit: So könnten z. B. Arbeitnehmer zögern, eine Beschwerde an den DSB zu richten, wenn die Vertraulichkeit ihrer Kommunikation nicht gewährleistet ist. Der DSB ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden (Artikel 38 Absatz 5).

Die Kontaktdaten des DSB sollten Angaben enthalten, die Betroffene ebenso wie die Aufsichtsbehörde in die Lage versetzen, den DSB auf einfachem Wege (postalisch, über eine persönliche Telefonnummer und/oder über eine persönliche E-Mail-Adresse) zu erreichen. Wo dies angezeigt ist, können zum Zwecke der Kommunikation mit der Öffentlichkeit weitere Kommunikationsmöglichkeiten (z.B. eine persönliche Hotline oder ein an den DSB persönlich adressiertes Kontaktformular auf der Website der Einrichtung) angeboten werden.

Artikel 37 Absatz 1 schreibt nicht vor, dass in den veröffentlichten Kontaktdaten auch der Name des DSB aufzuführen ist. Auch wenn es sich hierbei um ein bewährtes Verfahren handeln mag, liegt die Entscheidung, ob dies unter den gegebenen Umständen erforderlich oder hilfreich ist, im Ermessen des Verantwortlichen oder Auftragsverarbeiters und des DSB[32].

Die Mitteilung des Namens des DSB an die Aufsichtsbehörde ist jedenfalls erforderlich angesichts der Tätigkeit des DSB als Anlaufstelle der Einrichtung für die Aufsichtsbehörde (Artikel 39 Absatz 1 Buchstabe e).

Darüber hinaus empfiehlt die WP29 als bewährtes Verfahren, dass jede Einrichtung ihren Mitarbeitern den Namen und die Kontaktdaten des DSB zur Kenntnis bringen sollte. Beispielsweise könnten der Name und

[32] Artikel 33 Absatz 3 Buchstabe b, in dem die Angaben aufgeführt sind, die der Aufsichtsbehörde und den Betroffenen im Falle einer Verletzung datenschutzrechtlicher Bestimmungen übermittelt werden müssen, sieht im Unterschied zu Artikel 37 Absatz 7 ausdrücklich vor, dass auch der Name (und nicht nur die Kontaktdaten) des DSB mitzuteilen sind.

die Kontaktdaten des DSB im Intranet der betreffenden Einrichtung sowie in ihrem internen Telefonverzeichnis und in ihren Organigrammen veröffentlicht werden.

## 3 Stellung des DSB

### 3.1. Einbindung des DSB in alle mit dem Schutz personenbezogener Daten in Zusammenhang stehende Angelegenheiten

Nach Artikel 38 der DS-GVO haben der Verantwortliche und der Auftragsverarbeiter dafür Sorge zu tragen, dass der Datenschutzbeauftragte *„ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden“* wird.

Es ist von größter Bedeutung, dass der DSB oder sein Team vom frühestmöglichen Zeitpunkt an in alle im Zusammenhang mit dem Datenschutz stehenden Angelegenheiten eingebunden wird. In Bezug auf Datenschutz-Folgenabschätzungen sieht die DS-GVO ausdrücklich die frühzeitige Einbindung des DSB vor und besagt, dass der Verantwortliche bei der Durchführung solcher Folgenabschätzungen den DSB zu Rate zu ziehen hat.[33] Die systematische Unterrichtung und Konsultation des DSB von Anfang an vereinfacht die Einhaltung der DS-GVO und dient der Praxis eines „eingebauten Datenschutzes“ und sollte daher ein Standardverfahren der Führung von Einrichtungen darstellen. Überdies ist wichtig, dass der DSB innerhalb der Einrichtung als Gesprächspartner angesehen wird und dass er den maßgeblichen Arbeitsgruppen angehört, die mit Datenverarbeitungstätigkeiten innerhalb der Einrichtung befasst sind.

Dementsprechend sollte die Einrichtung beispielsweise dafür Sorge tragen, dass

- der DSB zur regelmäßigen Teilnahme an Treffen des leitenden und des mittleren Managements eingeladen wird.
- Seine Anwesenheit empfiehlt sich bei der Fällung von Entscheidungen, welche Fragen des Datenschutzes tangieren. Jegliche maßgeblichen Informationen sind dem DSB zeitnah zu übermit-

[33] Artikel 35 Absatz 2.

teln, damit dieser in adäquater Weise als Ratgeber fungieren kann.

- Der Meinung des DSB ist stets die gebührende Beachtung zu schenken. Im Falle einer abweichenden Meinung empfiehlt die WP29 als bewährtes Verfahren, die Gründe, aus denen dem Rat des DSB nicht gefolgt wird, zu dokumentieren.
- Bei einer Verletzung datenschutzrechtlicher Bestimmungen oder einem sonstigen Vorfall ist der DSB unverzüglich hinzuzuziehen.

Gegebenenfalls sollte der Verantwortliche oder der Auftragsverarbeiter Datenschutzrichtlinien oder -programme ausarbeiten, in denen festgelegt ist, wann der DSB zu Rate zu ziehen ist.

### 3.2. Erforderliche Ressourcen

Artikel 38 Absatz 2 der DS-GVO sieht vor, dass alle Einrichtungen ihrem DSB Unterstützung leisten, *„indem sie die für die Erfüllung [seiner] Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen“*.

Dies beinhaltet insbesondere

- eine aktive Unterstützung der Funktion des DSB durch das leitende Management (beispielsweise auf Vorstandsebene)
- die Gewährung von genügend Zeit für die Erfüllung seiner Pflichten. Besonders wichtig ist dies in Fällen, in denen ein interner DSB seiner Arbeit in Teilzeit nachgeht oder ein externer DSB seine Datenschutztätigkeit neben anderen Pflichten wahrnimmt. Andernfalls besteht die Gefahr einer Vernachlässigung der DSB-eigenen Pflichten infolge einander zuwiderlaufender Prioritäten. Über genügend Zeit für die Erledigung der dem DSB obliegenden Aufgaben zu verfügen, ist von größter Wichtigkeit. In Fällen, in denen die DSB-Funktion nicht in Vollzeit geleistet wird, empfiehlt es sich, hierfür einen festen Prozentsatz der Arbeitszeit vorzusehen. Ebenso empfiehlt es sich, die zur Wahrnehmung der Funktion benötigte Zeit sowie die Priorität,

die DSB-eigenen Pflichten beizumessen ist, zu ermitteln und von Seiten des DSB (oder der Einrichtung) ein Arbeitsprogramm zu erstellen;

- angemessene Unterstützung durch Finanzmittel, Infrastrukturen (Räumlichkeiten, Einrichtungen, Ausrüstung) sowie gegebenenfalls Personal;
- die offizielle Unterrichtung aller Beschäftigten über die Benennung eines DSB, damit dessen Existenz und Funktion einrichtungsweit bekannt sind;
- den nötigen Zugang zu anderen Dienststellen wie Personal-, Rechts-, IT- Sicherheitsabteilung usw., damit DSB unverzichtbare Unterstützung, Anregungen und Informationen von diesen erhalten können;
- kontinuierliche Fortbildung: Dem DSB sollte Gelegenheit gegeben werden, sich in Bezug auf Entwicklungen im Bereich des Datenschutzes auf dem aktuellen Stand zu halten. Ziel sollte dabei sein, die Fachkompetenz der DSB kontinuierlich zu erhöhen, und DSB sollten ermuntert werden, an Fortbildungsveranstaltungen über Datenschutz und an sonstigen Formen der beruflichen Weiterbildung (Datenschutzforen, Workshops usw.) teilzunehmen;
- Je nach Größe und Aufbau der Einrichtung kann es erforderlich sein, ein DSB-Team (bestehend aus einem DSB und dessen Mitarbeitern) einzurichten. In solchen Fällen sollten die Zusammensetzung des Teams sowie die Aufteilung der Aufgaben und Zuständigkeiten unter den Mitgliedern klar festgelegt werden. Falls die Funktion des DSB von einem externen Dienstleister wahrgenommen wird, kann ein Team aus für diese Stelle tätigen Personen die Aufgaben eines DSB unter der Verantwortung eines ernannten primären Ansprechpartners für den Kunden in effizienter und entsprechender Weise ausführen. Allgemein gilt:

Je komplexer und/oder sensibler die Datenverarbeitungsvorgänge sind, desto mehr Ressourcen müssen dem DSB zur Verfügung gestellt werden. Der Unternehmensbereich Datenschutz muss effektiv arbeiten

können und über eine ausreichende Mittelausstattung für die durchgeführte Datenverarbeitung verfügen.

### 3.3. Anweisungen und *„Ausübung der Pflichten und Aufgaben in vollständiger Unabhängigkeit“*

In Artikel 38 Absatz 3 sind grundlegende Garantien festgelegt, die dazu beitragen sollen, dass DSB ihren Aufgaben mit hinreichender Eigenständigkeit innerhalb ihrer Einrichtung nachgehen können. Insbesondere sind Verantwortliche/Auftragsverarbeiter verpflichtet, dafür Sorge zu tragen, dass der DSB *„keine Anweisungen bezüglich der Ausübung [seiner] Aufgaben erhält“*. ErwG 97 fügt hinzu: *„Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.“*

Dies bedeutet, dass DSB bei der Erfüllung ihrer Aufgaben nach Artikel 39 keine Anweisungen erteilt werden dürfen, wie sie bei einem gegebenen Sachverhalt zu verfahren haben, also beispielsweise, welches Ergebnis erzielt werden soll, wie einer Beschwerde nachzugehen ist oder ob die Aufsichtsbehörde zurate gezogen werden soll oder nicht. Des Weiteren dürfen sie nicht angewiesen werden, in einer datenschutzrechtlichen Frage einen bestimmten Standpunkt (beispielsweise in Bezug auf die Auslegung eines Gesetzes) zu vertreten.

Die Eigenständigkeit der DSB schließt jedoch keine über ihr Aufgabenfeld nach Artikel 39 hinausgehende Entscheidungsbefugnis ein.

Der Verantwortliche bzw. der Auftragsverarbeiter trägt stets die Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen und muss diese Einhaltung nachweisen können.[34] Trifft der Verantwortliche bzw. der Auftragsverarbeiter Entscheidungen, die der DSGVO und den Empfehlungen des DSB zuwiderlaufen, sollte der DSB die Möglichkeit haben, seine abweichende Meinung der höchsten Managementebene und den Entscheidungsträgern deutlich zur Kenntnis zu bringen. Nach Artikel 38 Absatz 3 berichtet der DSB „unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auf-

[34] Artikel 5 Absatz 2.

tragsverarbeiters“. Dadurch soll sichergestellt werden, dass das leitende Management (beispielsweise auf Vorstandsebene) von den Anregungen und Empfehlungen des DSB im Rahmen seiner Aufgabe, den Verantwortlichen oder den Auftragsverarbeiter zu unterrichten und zu beraten, Kenntnis erlangt. Ein weiteres Beispiel für unmittelbare Berichterstattung ist die Erstellung eines Jahresberichts über die Tätigkeit des DSB, der der höchsten Managementebene vorgelegt wird.

### 3.4. Abberufung oder Benachteiligung des DSB wegen der Erfüllung seiner Aufgaben

Gemäß Artikel 38 Absatz 3 dürfen DSB *„von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden“*.

Diese Anforderung stärkt die Eigenständigkeit der DSB und trägt dazu bei, dass diese unabhängig agieren können und bei der Ausführung ihrer datenschutzbezogenen Aufgaben hinreichenden Schutz genießen.

Strafen sind nach der DS-GVO nur dann unzulässig, wenn sie gegen den DSB allein deshalb verhängt werden, weil dieser seinen Pflichten als DSB nachgekommen ist. Beispielsweise kann es vorkommen, dass ein DSB zu der Einschätzung gelangt, dass eine bestimmte Form der Datenverarbeitung ein hohes Risiko in sich birgt, und er dem Verantwortlichen bzw. dem Auftragsverarbeiter eine Datenschutz-Folgenabschätzung empfiehlt, der Verantwortliche bzw. der Auftragsverarbeiter diese Einschätzung des DSB jedoch nicht teilt. In einem solchen Fall ist es nicht zulässig, den DSB wegen seiner diesbezüglichen Empfehlung abzuberufen.

Strafen können verschiedenerlei Formen annehmen und unmittelbarer oder mittelbarer Natur sein. Denkbar sind beispielsweise eine ausbleibende oder verspätet erfolgende Beförderung, die Verwehrung einer beruflichen Fortentwicklung oder der Ausschluss von Leistungen, die anderen Beschäftigten gewährt werden. Dabei ist es nicht erforderlich, dass solche Strafen tatsächlich verhängt werden: Ihr bloße Androhung reicht aus, solange diese dazu dient, den DSB aus im Zusammenhang mit seiner Tätigkeit stehenden Gründen zu bestrafen.

Als normale Management-Regel und wie dies bei jedem anderen Beschäftigten oder Fremdmitarbeiter nach geltendem nationalem Vertrags-, Arbeits- oder Strafrecht der Fall wäre, kann ein DSB jederzeit von Rechts wegen aus Gründen abberufen werden, die nicht im Zusammenhang mit der Erfüllung seiner Pflichten als DSB stehen (beispielsweise wegen Diebstahls, physischer, psychischer oder sexueller Belästigung oder einem vergleichbarem groben Fehlverhalten).

In diesem Zusammenhang ist anzumerken, dass die DS-GVO keine Angaben dazu enthält, wie und wann ein DSB abberufen oder durch eine andere Person ersetzt werden darf. Je stabiler allerdings der Vertrag eines DSB ist und je mehr Garantien gegen eine ungerechtfertigte Abberufung bestehen, desto wahrscheinlicher ist es, dass er in unabhängiger Weise agieren kann. Daher würde es die WP29 begrüßen, wenn von Seiten der Einrichtungen hierauf zielende Anstrengungen unternommen würden.

### 3.5. Interessenkonflikte

Nach Artikel 38 Absatz 6 können *DSB „andere Aufgaben und Pflichten wahrnehmen“*. Die betreffende Einrichtung hat allerdings dafür Sorge zu tragen, dass *„derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen“*.

Die Abwesenheit eines Interessenkonflikts ist eng mit dem Erfordernis einer unabhängigen Tätigkeit verknüpft. DSB dürfen zwar auch andere Funktionen wahrnehmen, aber nur mit Aufgaben und Pflichten betraut werden, die zu keinen Interessenkonflikten mit ihrer Tätigkeit als DSB führen. Diese Vorgabe bringt insbesondere mit sich, dass der DSB innerhalb einer Einrichtung keine Position innehaben kann, welche es mit sich bringt, dass er die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt. Aufgrund der jeder Einrichtung eigenen strukturellen Unterschiede ist diese Frage fallweise zu betrachten.

Als Faustregel lassen sich zu den mit Interessenkonflikten einhergehenden Positionen innerhalb der Einrichtung solche des leitenden Managements zählen (wie etwa Leiter des Unternehmens, Leiter des operativen Geschäftsbereichs, Finanzvorstand, leitender medizinischer Direktor, Leiter der Marketingabteilung, Leiter der Personalabteilung

oder Leiter der IT-Abteilung), jedoch auch hierarchisch nachgeordnete Positionen, wenn die betreffenden Funktionen oder Aufgabenfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen. Auch können Interessenkonflikte auftreten, wenn z. B. ein externer DSB aufgefordert wird, den Verantwortlichen oder den Auftragsverarbeiter in datenschutzrelevanten Rechtssachen vor Gericht zu vertreten.

Je nach Tätigkeiten, Größe und Struktur der Einrichtung kann es für Verantwortliche bzw. Auftragsverarbeiter ratsam sein,

- die Positionen zu benennen, die mit der Funktion eines DSB unvereinbar sind,
- zur Vermeidung von Interessenkonflikten diesbezügliche interne Richtlinien aufzustellen
- eine allgemeine Erläuterung potenzieller Interessenkonflikte vorzunehmen
- zu erklären, dass sich der DSB in Bezug auf seine Funktion in keinem Interessenkonflikt befindet und auf diese Weise das Bewusstsein für diese Anforderung zu schärfen
- in die internen Richtlinien der Einrichtung Sicherungsvorkehrungen aufzunehmen und dafür Sorge zu tragen, dass die Stellenausschreibung für die Position eines DSB bzw. der betreffende Dienstleistungsvertrag zwecks Vermeidung von Interessenkonflikten hinreichend genau und präzise formuliert wird. In diesem Zusammenhang ist zu beachten, dass Interessenkonflikte je nachdem, ob der DSB intern oder extern rekrutiert wird, unterschiedliche Formen annehmen können.

## 4 Aufgaben des DSB

### 4.1. Überwachung der Einhaltung der DS-GVO

Artikel 39 Absatz 1 Buchstabe b überträgt dem DSB unter anderem die Pflicht zur Überwachung der Einhaltung der DS-GVO. ErwG 97 besagt ferner, dass *„der Verantwortliche oder der Auftragsverarbeiter bei der*

*Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person unterstützt werden"* sollte.

Im Rahmen dieser Überwachungspflicht sind DSB insbesondere befugt,

- Informationen zur Ermittlung von Datenverarbeitungstätigkeiten zu sammeln,
- die Einhaltung der Vorgaben bei Datenverarbeitungstätigkeiten zu analysieren und zu kontrollieren,
- den Verantwortlichen oder den Auftragsverarbeiter zu unterrichten und zu beraten und ihm Empfehlungen zu unterbreiten.

Überwachung der Einhaltung bedeutet nicht, dass der DSB im Fall der Nichteinhaltung persönlich zur Verantwortung gezogen werden kann. Aus der DS-GVO geht klar hervor, dass es Sache des Verantwortlichen – und nicht des DSB – ist, *„geeignete technische und organisatorische Maßnahmen [umzusetzen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt"* (Artikel 24 Absatz 1). Die Einhaltung der datenschutzrechtlichen Bestimmungen fällt somit in den Aufgabenbereich des Verantwortlichen und nicht in den des DSB.

## 4.2. Die Funktion des DSB bei einer Datenschutz-Folgenabschätzung

Gemäß Artikel 35 Absatz 1 ist es Sache des Verantwortlichen – und nicht des DSB –, erforderlichenfalls eine Datenschutz-Folgenabschätzung („DS-Folgenabschätzung") durchzuführen. Allerdings kann der DSB eine überaus wichtige und nützliche Rolle spielen, indem er dem Verantwortlichen Hilfestellung leistet. Dem Grundsatz eines „eingebauten Datenschutzes" folgend sieht Artikel 35 Absatz 2 ausdrücklich vor, dass der Verantwortliche bei der Durchführung einer Datenschutz-Folgenabschätzung (im Folgenden „DS-Folgenabschätzung") den Rat des DSB einholt. Artikel 39 Absatz 1 Buchstabe c wiederum überträgt den DSB die Pflicht, *„Beratung – auf Anfrage – im Zusammenhang mit der [DS-Folgenabschätzung] und Überwachung ihrer Durchführung gemäß Artikel 35"* zu leisten.

Die WP29 empfiehlt, dass der Verantwortliche den DSB insbesondere[35] dann zurate zieht, wenn es um die Frage geht,

- ob eine DS-Folgenabschätzung durchgeführt werden sollte oder nicht
- welche Methodik bei der Durchführung einer solchen DS-Folgenabschätzung angewandt werden sollte
- ob diese DS-Folgenabschätzung intern oder extern erfolgen sollte
- welche Sicherheitsvorkehrungen (einschließlich technischer und organisatorischer Maßnahmen) getroffen werden sollten, um bestehenden Bedrohungen der Rechte und Interessen der Betroffenen zu begegnen
- ob eine solche Datenschutz-Folgenabschätzung ordnungsgemäß durchgeführt worden ist und ob die daraus gezogenen Schlussfolgerungen (bezüglich der Frage, ob die Datenverarbeitung fortgesetzt werden sollte oder nicht und welche Sicherheitsvorkehrungen gegebenenfalls getroffen werden sollten) im Einklang mit der DS-GVO stehen

Falls der Verantwortliche der Empfehlung des DSB nicht zustimmt, ist in der Dokumentation zu der DS-Folgenabschätzung ausdrücklich schriftlich zu begründen, warum der Empfehlung nicht Folge geleistet wurde[36].

Die WP29 empfiehlt ferner, dass der Verantwortliche – beispielsweise im Vertrag des DSB und auch in an die Beschäftigten, die Unterneh-

---

[35] In Artikel 39 Absatz 1 sind die Aufgaben der DSB aufgeführt, demnach haben sie *„zumindest“* die im Folgenden genannten Aufgaben wahrzunehmen. Daher hindert den Verantwortlichen nichts daran, dem DSB Aufgaben zu übertragen, die über die in Artikel 39 Absatz 1 ausdrücklich erwähnten Aufgaben hinausgehen, oder solche Aufgaben zu präzisieren.

[36] Artikel 24 Absatz 1 besagt: *„Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen* ***und den Nachweis dafür erbringen zu können****, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert“.*

mensleitung und etwaige sonstige Interessenträger gerichteten Mitteilungen – die Aufgaben, die der DSB in Bezug auf die Durchführung der DS-Folgenabschätzung zu erfüllen hat, und deren Umfang genau darlegt.

### 4.3. Zusammenarbeit mit der Aufsichtsbehörde und Tätigkeit als Anlaufstelle

Nach Artikel 39 Absatz 1 Buchstaben d und e obliegt dem DSB die *„Zusammenarbeit mit der Aufsichtsbehörde“* und die *„Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen“*.

Diese Aufgaben zeugen von der in der Einführung zu diesen Leitlinien erwähnten Funktion des DSB als „Mittler“. Der DSB handelt als Anlaufstelle, um den Zugang der Aufsichtsbehörden zu Dokumenten und Informationen zur Erfüllung der Aufgaben nach Artikel 57 und die Ausübung ihrer Untersuchungs-, Abhilfe-, Genehmigungs- und beratenden Befugnisse nach Artikel 58 zu erleichtern. Wie bereits erwähnt, ist der DSB nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden (Artikel 38 Absatz 5). Allerdings verbietet die Wahrung der Geheimhaltung oder der Vertraulichkeit es dem DSB nicht, die Aufsichtsbehörden zu Rate zu ziehen. Laut Artikel 39 Absatz 1 Buchstabe e kann der DSB die Aufsichtsbehörde gegebenenfalls zu allen sonstigen Fragen konsultieren.

### 4.4. Risikobasierter Ansatz

Artikel 39 Absatz 2 sieht vor, dass der DSB *„dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung [trägt], wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt“*.

Dieser Artikel bezieht sich auf einen allgemeinen, auf dem gesunden Menschenverstand basierenden Grundsatz, der für viele Aspekte der Alltagstätigkeit eines DSB von Belang sein kann. Im Wesentlichen verpflichtet er den DSB, seine Tätigkeiten nach Priorität zu ordnen und

seine Anstrengungen auf Fragen zu konzentrieren, von denen größere Bedrohungen für den Datenschutz ausgehen. Dies bedeutet keineswegs, dass er die Überwachung der Vorschrifteneinhaltung bei vergleichsweise weniger risikobehafteten Datenverarbeitungsvorgängen vernachlässigen sollte, sondern besagt, dass er sich in erster Linie auf die Bereiche konzentrieren sollte, von denen ein höheres Risiko ausgeht.

Dieser selektive, pragmatische Ansatz soll DSB dabei helfen, Verantwortliche darüber zu beraten, nach welcher Methodik bei einer DS-Folgenabschätzung vorgegangen werden sollte, welche Bereiche einer internen oder externen Datenschutzprüfung unterzogen werden sollten, welche internen Schulungsmaßnahmen für leitende oder sonstige mit Datenverarbeitungstätigkeiten befasste Mitarbeiter durchgeführt werden sollten und welchen Datenverarbeitungsvorgängen mehr Zeit und Ressourcen gewidmet werden sollten.

## 4.5. Die Funktion des DSB bei der Führung von Verzeichnissen

Nach Artikel 30 Absatz 1 und Absatz 2 ist es Sache der Verantwortlichen oder der Auftragsverarbeiter - und nicht der DSB -, *„ein Verzeichnis aller Verarbeitungstätigkeiten [zu führen], die ihrer Zuständigkeit unterliegen“* bzw. *„ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung [zu führen]“*.

In der Praxis erstellen DSB oftmals Inventarlisten und führen Register der Verarbeitungsvorgänge auf der Grundlage der Informationen, die ihnen von den verschiedenen für die Verarbeitung personenbezogener Daten zuständigen Bereichen ihrer Einrichtung vorgelegt werden. Dieses Vorgehen ist in zahlreichen aktuellen einzelstaatlichen Rechtsvorschriften und in den geltenden Datenschutzbestimmungen der EU-Organe und -Einrichtungen[37] festgeschrieben worden.

Artikel 39 Absatz 1 sieht eine Liste von Aufgaben vor, die der DSB als Mindestanforderung wahrzunehmen hat. Den Verantwortlichen bzw.

[37] Artikel 24 Absatz 1 Buchstabe d der Verordnung (EG) 45/2001.

den Auftragsverarbeiter hindert somit nichts daran, den DSB die Aufgabe zu übertragen, unter der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters ein Verzeichnis der Verarbeitungsvorgänge zu führen. Ein solches Verzeichnis sollte als eines der Instrumente angesehen werden, die den DSB in die Lage versetzen, die ihm in Bezug auf die Überwachung der Vorschrifteneinhaltung und in Bezug auf die Unterrichtung und Beratung des Verantwortlichen bzw. des Auftragsverarbeiters obliegenden Aufgaben wahrzunehmen.

In jedem Falle sollte das nach Artikel 30 zu führende Verzeichnis auch als ein Instrument angesehen werden, das den Verantwortlichen und die Aufsichtsbehörde in die Lage versetzt, sich bei Bedarf einen Überblick über sämtliche in einer Einrichtung erfolgenden Tätigkeiten der Verarbeitung personenbezogener Daten zu verschaffen. Es stellt von daher eine unverzichtbare Voraussetzung für die Vorschrifteneinhaltung und somit eine wirksame Maßnahme zur Rechenschaftslegung dar.

### 5 Anhang zu den DSB-Leitlinien: Was Sie wissen müssen

[…]

*[Hier nicht abgedruckt]*

## 5. Sonstige relevante Muster zum Datenschutzbeauftragten

*Koreng/Lachenmann*, Formularhandbuch Datenschutzrecht, 2. Auflage 2018, B. II., Verträge mit externen Datenschutzbeauftragten

- Dienstvertrag mit einem externen Datenschutzbeauftragten
- Beratungsvertrag mit einem Dienstleistungsunternehmen
- Aufhebungsvertrag der Parteien

# Stichwortverzeichnis

## A

Abberufungs- und Kündigungsschutz ..... 68
Altbestellungen ..... 38
Anspruch auf Einbindung..... 63
Anwalt der betroffenen Personen ... 55
Art.-29-Datenschutzgruppe ..... 102
Aufsichtsbehörde ..... 54
Ausbildung ..... 67

## B

Befristung ..... 30
Benachteiligungsverbot ..... 72
Benennung Datenschutzbeauftragter
- Altbestellungen ..... 38
- Anforderungen ..... 30
- Arztpraxen, Apotheken etc. ..... 28
- Befristung ..... 30
- Form ..... 30
- Freiwillig ..... 29
- Juristische Person ..... 34
- Mitbestimmungsrecht ..... 32
- Muster ..... 87
- Öffnungsklausel ..... 23
- Verpflichtende ..... 22

Beratungspflicht ..... 49
Betriebsrat ..... 51

## D

Datenschutzbeauftragter
- Anforderungen ..... 39
- Arztpraxen, Apotheken etc. ..... 28
- Aufgaben ..... 48
- Ausbildung..... 67
- Einvernehmliche Beendigung der Benennung..... 71
- Extern ..... 33
- Fachwissen ..... 40
- Fähigkeit zur Aufgabenerfüllung.....43
- Gemeinsamer.....37
- Haftung .....74
- Interessenkonflikte .....44
- Juristische Person.....34
- Kontaktdaten .....32
- Meldung an Aufsicht .....33
- Niederlegung des Amtes .....71
- Öffnungsklausel.....23
- Organisatorische Stellung .....61
- Pflicht zur Benennung .....22
- Rechtsstellung.....60
- Ressourcen.....63
- Schwellenwert.....23
- Strafbarkeit .....80
- Tätigkeitsbericht .....58
- Unternehmensfusion .....72
- Verband.....37
- Zeitbudget.....65

Datenschutz-Folgenabschätzung.....53
Datenschutzkonferenz.....95

## E

Europäischer Datenschutzausschuss .....102
Externer Datenschutzbeauftragter
- Allgemein .....33
- Gewerbesteuer .....35

## F

Fachwissen .....40
Fortbildung .....67

## G

Garantenstellung.....51, 77, 80
Gemeinsamer Datenschutzbeauftragter .....37
Gewerbesteuer.....35

## H

Haftung des Datenschutz-
beauftragten ..... 74
Hinwirken auf den Datenschutz
Rechtsdienstleistungsgesetz
(RDG) ..... 42

## I

Interessenkonflikt ..... 44

## J

Juristische Person ..... 34

## K

Kontaktdaten
Veröffentlichung/Mitteilung ..... 32
Konzerndatenschutzbeauftragter
Allgemein..... 33, 34
Benennung ..... 37
Leichte Erreichbarkeit..... 37
Neueinführung ..... 70
Sprache..... 37
Kündigungsschutz ..... 68

## M

Meldung Datenschutzbeauftragter . 33

## O

Öffnungsklausel ..... 23

## P

Probezeit..... 70

## Q

Qualifikation ..... 40

## R

Rechtsanwälte ..... 36
Rechtsdienstleistungsgesetz (RDG) . 42
Ressourcen ..... 63
Risikoorientierte Tätigkeit ..... 57

## S

Stellenbeschreibung
Allgemein ..... 31
Muster..... 89
Strafbarkeit..... 80

## T

Tätigkeitsbericht..... 58

## U

Überwachung
Allgemein ..... 50
Betriebsrat..... 51
Unabhängigkeit.....57, 61
Unternehmensfusion..... 72
Unterrichtungspflicht ..... 49

## V

Verschwiegenheitspflicht ..... 56

## W

Weisungsfreiheit..... 61

## Z

Zeitbudget ..... 65
Zugang zu Verarbeitungsvor-
gängen und Daten ..... 63

## Wie Sie noch mehr erfahren

**Gesellschaft für Datenschutz und Datensicherheit e.V.**

Heinrich-Böll-Ring 10
53119 Bonn
Telefon (0228) 96 96 75 00
Telefax (0228) 96 96 75 25
E-Mail: info@gdd.de
Internet: www.gdd.de

# >> GDD-Support für Wirtschaft, Verwaltung, Wissenschaft und Politik

Die GDD tritt für die Prinzipien der Selbstkontrolle und Selbstregulierung auf dem Gebiet des Datenschutzes ein. Sie unterstützt die politische Willensbildung durch fachlichen Rat.

Bei der Umsetzung der datenschutzrechtlichen Vorgaben bietet die GDD folgende Leistungen:

- >> Beratung in Einzelfragen
- >> Schulungen und Praktikerforen
- >> Online-Datenbanken, u.a.:
  GDD-Rechtsprechungsarchiv
  GDD-Literaturarchiv
- >> GDD-Praxis-Ratgeber
- >> Fachzeitschrift „Recht der Datenverarbeitung (RDV)“
- >> Fachpublikationen
- >> Erfahrungsaustausch

Gesellschaft für Datenschutz und Datensicherheit e.V.