

# **Behördliche und betriebliche Datenschutzbeauftragte**

Stand: 09.10.2023



I. Pflicht zur Benennung eines Datenschutzbeauftragten.....	3
1. Voraussetzungen der DS-GVO .....	3
2. Voraussetzungen nach dem BDSG/HDSIG .....	6
3. Veröffentlichungs- und Mitteilungspflicht .....	6
4. Gemeinsame Datenschutzbeauftragte .....	7
5. Interne und externe Datenschutzbeauftragte .....	8
6. Datenschutzteam und Benennung juristischer Personen .....	8
7. Freiwillige Benennung.....	9
II. Persönliche Voraussetzungen des Datenschutzbeauftragten .....	9
1. Berufliche Qualifikation und Fachwissen .....	9
2. Fähigkeit zur Erfüllung der genannten Aufgaben .....	10
III. Aufgaben und Pflichten .....	10
1. Unterrichtung und Beratung .....	10
2. Überwachung der Einhaltung der DS-GVO, des BDSG und des HDSIG.....	10
3. Beratung und Überwachung im Zusammenhang mit der Datenschutz- Folgenabschätzung.....	11
4. Sensibilisierung und Schulung .....	11
5. Zusammenarbeit mit der Aufsichtsbehörde .....	12
6. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde .....	12
7. Risikoorientierte Aufgabenerfüllung .....	12
8. Erweiterung des Aufgabenkatalogs durch Vereinbarung.....	13
IV. Stellung des Datenschutzbeauftragten.....	13
1. Ordnungsgemäße und frühzeitige Einbindung .....	13
2. Bereitstellung erforderlicher Ressourcen .....	14
3. Weisungsfreiheit/Unabhängigkeit.....	15
4. Keine Benachteiligung: Abberufung und Kündigung .....	15
5. Unmittelbarer Berichtsweg zu der Geschäftsführung bzw. zu der höchsten Leitungsebene .....	16
6. Anrufungsrecht der betroffenen Person .....	16
7. Geheimhaltung, Vertraulichkeit und Zeugnisverweigerungsrecht .....	16
8. Kein Interessenkonflikt.....	17
9. Zusammenarbeit mit der Aufsichtsbehörde .....	17
10. Ausweitung der Privilegien auf Vertreter oder Datenschutzteam.....	17
V. Sanktionen und Haftung.....	18
1. Sanktionen.....	18
2. Haftungsverteilung zwischen Datenschutzbeauftragten und Unternehmen.....	18



Die zentralen Regelungen zu der Benennung, Stellung und zu den Aufgaben des Datenschutzbeauftragten<sup>1</sup> enthalten die Art. 37-39 der Datenschutzgrundverordnung (DS-GVO).<sup>2</sup> Neben diesen Vorschriften kommen für betriebliche Datenschutzbeauftragte die Regelungen des § 38 und des § 6 Abs. 4, Abs. 5 S. 2 und Abs. 6 des Bundesdatenschutzgesetzes (BDSG) ergänzend zur Anwendung. Für betriebliche Datenschutzbeauftragte füllen diese Vorschriften des BDSG die in der DS-GVO enthaltene Öffnungsklausel und Gestaltungsspielräume aus. Für Datenschutzbeauftragte von hessischen öffentlichen Stellen gelten neben den Vorschriften der DS-GVO die §§ 5-7 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG).<sup>3</sup> Neben der Ausfüllung der Öffnungsklausel und der Gestaltungsspielräume der DS-GVO enthalten die §§ 5-7 HDSIG Regelungen zur Benennung, Stellung und Aufgaben des Datenschutzbeauftragten auch für die Bereiche, in denen die DS-GVO sachlich nicht anwendbar ist, vgl. Art. 2 Abs. 2 DS-GVO. Dazu gehören Regelungen aus dem Anwendungsbereich der JI-RL<sup>4</sup> (Polizeibehörden, Allgemeine Ordnungsbehörden, Justizvollzugsbehörden) und die Datenverarbeitung zu Zwecken, die nicht in den Anwendungsbereich des Unionsrechts fallen (etwa die nationale Sicherheit gemäß Art. 4 Abs. 2 S. 3 des EU-Vertrages; Landesamt für Verfassungsschutz Hessen).

Bei der Rechtsfigur des Datenschutzbeauftragten handelt es sich um ein bereits vor der unmittelbaren Geltung der DS-GVO am 25.05.2018 bekanntes und bewährtes Instrument zur Wahrung des Datenschutzes in Deutschland.<sup>5</sup> Gleichwohl haben sich einige Änderungen ergeben. Dies sind etwa die Pflicht zu der Benennung eines Datenschutzbeauftragten auch für Auftragsverarbeiter; die Möglichkeit für öffentliche Stellen, einen externen Datenschutzbeauftragten zu benennen; sowie die Pflicht, die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der Aufsichtsbehörde mitzuteilen.

## **I. Pflicht zur Benennung eines Datenschutzbeauftragten**

### **1. Voraussetzungen der DS-GVO**

Der Verantwortliche und der Auftragsverarbeiter müssen gemäß Art. 37 Abs. 1 DS-GVO einen Datenschutzbeauftragten benennen, 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

---

<sup>1</sup> Aus Gründen der besseren Lesbarkeit wird das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

<sup>2</sup> Die Artikel 29 Datenschutzgruppe hat zu den genannten Rechtsvorschriften im Dezember 2016 das Working Paper 243 „Guidelines on Data Protection Officers (‘DPOs’)“ (WP 243) veröffentlicht, welches im April 2017 überarbeitet wurde. Die Artikel 29 Datenschutzgruppe war das unabhängige Beratungsgremium der EU-Kommission in Fragen des Datenschutzes. Seit dem 25.05.2018 ist an ihre Stelle der [Europäische Datenschutzausschuss \(EDSA\)](#) getreten. Die Working Paper sind abrufbar über die [Webseiten der Europäischen Kommission](#).

<sup>3</sup> Seit der unmittelbaren Geltung der DS-GVO am 25.05.2018 können die Landesgesetzgeber nicht mehr unterschiedliche Benennungspflichten für behördliche Datenschutzbeauftragte vorsehen. Einige Landesdatenschutzgesetze haben es daher bei den unmittelbar geltenden Bestimmungen der DS-GVO belassen und enthalten keine Aussage zu behördlichen Datenschutzbeauftragten. Hessen hat die Regelungen des BDSG weitgehend übernommen, vgl. §§ 5-7 HDSIG.

<sup>4</sup> 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 Rahmenbeschlusses 2008/977/JI des Rates. S. a. Erwägungsgrund 19 der DS-GVO.

<sup>5</sup> Vgl. die Regelungen der §§ 4f und 4g des Bundesdatenschutzgesetzes alter Fassung (BDSG a. F.), welche sowohl behördliche als auch betriebliche Datenschutzbeauftragte erfassen.

- 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 Art. 9 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO besteht.

Eine Frist zu der Benennung des Datenschutzbeauftragten ist gesetzlich nicht vorgesehen. Daher hat die Benennung unverzüglich zu erfolgen, wenn die jeweiligen Voraussetzungen vorliegen.

Behörden und öffentliche Stellen müssen immer einen Datenschutzbeauftragten benennen, wenn sie in den Anwendungsbereich der DS-GVO fallen.<sup>6</sup> Der hessische Gesetzgeber hat zudem von der Öffnungsklausel des Art. 37 Abs. 4 DS-GVO Gebrauch gemacht. Öffentliche Stellen müssen gemäß § 5 Abs. 1 HDSIG neben einem Datenschutzbeauftragten auch einen stellvertretenden Datenschutzbeauftragten benennen.<sup>7</sup>

Für Unternehmen und andere nicht-öffentliche Stellen greift die Pflicht zu der Benennung eines betrieblichen Datenschutzbeauftragten, wenn die unter Art. 37 Abs. 1 Buchstabe b oder Buchstabe c DS-GVO genannten Voraussetzungen erfüllt sind.

Die Begriffe „Kerntätigkeit“, „umfangreiche Verarbeitung“ sowie „regelmäßige und systematische Überwachung“ sind auslegungsbedürftig. Hilfestellung bei der Interpretation leisten sowohl die Erwägungsgründe der DS-GVO als auch das WP 243.<sup>8</sup>

Nach Erwägungsgrund 97 der DS-GVO bezieht sich der Begriff der **Kerntätigkeit** im privaten Sektor auf die Haupttätigkeit und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit eines Unternehmens. Entscheidend und im Einzelfall schwierig kann vor allem die Abgrenzung der beiden Begrifflichkeiten sein, da hierdurch die Benennungspflicht ausgelöst werden kann oder aber entfällt. Das WP 243 greift den Gedanken Haupt- und Nebentätigkeit auf und führt hierzu aus, dass hierunter Aktivitäten zu verstehen sind, welche entweder essentiell für die Erreichung der Ziele eines Unternehmens oder untrennbar mit diesem verbunden sind. Kerntätigkeit im Sinne der DS-GVO ist somit anzunehmen, wenn die Verarbeitung personenbezogener Daten primärer Geschäftszweck eines Unternehmens ist oder die Erfüllung des primären Geschäftszwecks ohne die Verarbeitung personenbezogener Daten nicht erreicht werden kann und es sich hierbei nicht um herkömmliche Unternehmensaufgaben handelt, welche unabhängig vom eigentlichen Geschäftszweck anfallen (z. B. aus dem Bereich der IT oder Personaldatenverwaltung). Als Beispiel für die Annahme der Kerntätigkeit nennt das WP 243 die Verarbeitung von Gesundheitsdaten durch Krankenhäuser. Zwar ist die Kerntätigkeit eines Krankenhauses die Gesundheitsversorgung. Diese kann aber ohne die Verarbeitung von personenbezogenen Gesundheitsdaten nicht gewährleistet werden.<sup>9</sup>

---

<sup>6</sup> Vgl. dazu für Gerichte im Rahmen ihrer justiziellen Tätigkeit Art. 55 Abs. 3 und Erwägungsgrund 20 der DS-GVO.

<sup>7</sup> Von der zu den Regelungen des (alten) Hessischen Datenschutzgesetzes (HDSG) vertretenen Ansicht, dass es sich hierbei um eine reine Abwesenheitsvertretung handelt, kann nicht mehr ausgegangen werden, s. a. *Wilmer*, in: Roßnagel, Kommentar HDSIG, § 5 Rn. 16.

<sup>8</sup> Vgl. Erwägungsgründe 97, 91 und 24 der DS-GVO und WP 243, S. 8 ff.

<sup>9</sup> Hinweise zu der Benennung von Datenschutzbeauftragten im Gesundheitsbereich sind auf meiner Webseite abrufbar:

<https://datenschutz.hessen.de/datenschutz/datenschutzbeauftragte/datenschutzbeauftragte-im-gesundheitswesen>

Der Begriff der **umfangreichen Verarbeitung** wird durch die DS-GVO selbst nicht definiert. Erwägungsgrund 91 der DS-GVO gibt aber zumindest drei Wertungskriterien für umfangreiche Verarbeitungsvorgänge an die Hand:

- Verarbeitung großer Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene,
- Betroffenheit einer großen Zahl von Personen,
- hohes Risiko für die Betroffenen, z. B. aufgrund der Verarbeitung sensibler Daten.

Berücksichtigt werden sollte in diesem Zusammenhang die in Erwägungsgrund 89 der DS-GVO zum Ausdruck kommende Wertung, dass insbesondere bei Verarbeitungsvorgängen, bei denen neue Technologien eingesetzt werden, von einem hohen Risiko für den Betroffenen auszugehen ist.

Nach dem WP 243 sollten zumindest die folgenden Überlegungen in eine Bewertung einfließen, ob eine „umfangreiche Verarbeitung“ anzunehmen ist:

- Anzahl der Betroffenen,
- Menge der betroffenen Datensätze/Vielzahl der Verarbeitungsprozesse,
- Dauer oder Permanenz der Datenverarbeitung,
- geographische Reichweite der Datenverarbeitung.

Das WP 243 nennt darüber hinaus einige Praxisbeispiele (etwa die regelmäßige Verarbeitung von Kundendaten durch Versicherungen oder Banken oder die Verarbeitung von personenbezogenen Daten im Zusammenhang mit verhaltensbasierter Werbung).

Zu der Frage der Auslegung der **regelmäßigen und systematischen Überwachung** können die Wertungen des Erwägungsgrundes 24 der DS-GVO herangezogen werden. Dazu zählen alle Fälle der Nachverfolgung von Internetaktivitäten und Profilbildung, wobei der Begriff nicht auf Anwendungsfälle im Bereich der Internetnutzung beschränkt ist.

Nach dem WP 243 kann der Begriff „regelmäßige Überwachung“ bei Vorliegen der nachfolgenden Kriterien erfüllt sein:

- fortlaufende oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommende Überwachung,
- immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretende Überwachung,
- ständig oder regelmäßig stattfindende Überwachung.

Der Begriff der „systematischen Überwachung“ ist nach dem WP 243 erfüllt, wenn die Überwachung

- systematisch,
- vereinbart, organisiert oder methodisch,
- im Rahmen eines allgemeinen Datenerfassungsplans, oder
- im Rahmen einer Strategie

erfolgt.

Als Beispiele werden u. a. der Betrieb eines Telekommunikationsnetzes, die Bereitstellung von Telekommunikationsdienstleistungen, datengetriebene Marketingaktivitäten oder Profilbildung/Scoring zu der Risikobewertung genannt.

## 2. Voraussetzungen nach dem BDSG/HDSIG

Das HDSIG wiederholt für behördliche Datenschutzbeauftragte die Regelung der generellen Benennungspflicht des Art. 37 Abs. 1 DS-GVO, vgl. § 5 Abs. 1 HDSIG.<sup>10</sup>

Für die Benennung betrieblicher Datenschutzbeauftragter hat der deutsche Gesetzgeber über die Öffnungsklausel des Art. 37 Abs. 4 S. 1 DS-GVO mit dem § 38 Abs. 1 BDSG eine nationale Sonderregelung geschaffen. Die Benennung ist (infolge einer Gesetzesänderung zum 26.11.2019) nunmehr erforderlich, wenn eine verantwortliche Stelle in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt. Mit der Heraufsetzung von 10 auf 20 Personen strebt der deutsche Gesetzgeber „vor allem eine Entlastung kleinerer und mittlerer Unternehmen sowie ehrenamtlich tätiger Vereine“ an.<sup>11</sup>

In Bezug auf die Anzahl der mit der Verarbeitung beschäftigten Personen ist die Arbeitnehmereigenschaft nicht entscheidend. Neben Vollzeitbeschäftigten sind daher z. B. auch Teilzeitbeschäftigte, Leiharbeiter, Auszubildende und Praktikanten, aber auch Inhaber, geschäftsführende Gesellschafter oder Vorstandsmitglieder bei der Kalkulation der 20 Personen zu berücksichtigen. Bei der Auslegung des Begriffs der automatisierten Verarbeitung personenbezogener Daten kann die Annahme genügen, dass die beschäftigten Personen einen personalisierten E-Mail-Account haben. Es ist also nicht erforderlich, dass die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten Kernaufgabe der beschäftigten Person ist.

Sind weniger als 20 Mitarbeiter mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine Benennungspflicht, wenn der Verantwortliche oder der Auftragsverarbeiter einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegt oder personenbezogene Daten geschäftsmäßig zu dem Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet, § 38 Abs. 1 S. 2 BDSG.

## 3. Veröffentlichungs- und Mitteilungspflicht

Ausweislich des Wortlautes „Benennung“, vgl. Art. 37 Abs. 7 DS-GVO, § 5 Abs. 5 HDSIG, ist eine schriftliche Bestellung des Datenschutzbeauftragten nicht erforderlich.<sup>12</sup> Die Benennung wird vor allem durch die Veröffentlichung der Kontaktdaten und die Mitteilung an die Aufsichtsbehörden in formeller Hinsicht vollzogen. Die Mitteilungs- und Veröffentlichungspflicht steht in einem engen Zusammenhang mit der Rolle des Datenschutzbeauftragten als zentrale Anlaufstelle für Betroffene, Verantwortliche, Auftragsverarbeiter und Aufsichtsbehörden und ist Ausdruck des in Art. 5 DS-GVO verankerten Transparenzgrundsatzes.<sup>13</sup> Sinn und Zweck der Veröffentlichungs- und Mitteilungspflicht ist, Betroffenen und Aufsichtsbehörden eine einfache, direkte und vertrauliche Kommunikation mit dem Datenschutzbeauftragten zu ermöglichen. Vor diesem Hintergrund sollten Kontaktmöglichkeiten sowohl innerhalb des Unternehmens (z. B. per E-Mail, Informationsrundschreiben, Intranet, Organigramm oder Aushang) als auch für Betroffene (z. B. Webseite, Kundeninformation) ausreichend kommuniziert werden.

---

<sup>10</sup> Hinweise zu dem schulischen Datenschutzbeauftragten sind auf meiner Webseite abrufbar: <https://datenschutz.hessen.de/datenschutz/datenschutzbeauftragte/hinweise-zum-schulischen-datenschutzbeauftragten>

<sup>11</sup> BT-Drucksache 19/11181, S. 19.

<sup>12</sup> S. zu der Benennung des Datenschutzbeauftragten auch [LAG Niedersachsen, Urteil vom 09.06.2020 – 9 Sa 608/19, ZD 2021 107 ff.](#)

<sup>13</sup> Vgl. hierzu vor allem Punkt III. 6. „Tätigkeit als Anlaufstelle für die Aufsichtsbehörden“ und Punkt IV. 6. „Anrufungsrecht der betroffenen Person“.



Meine Behörde stellt ein elektronisches Meldeverfahren zur Verfügung, über welches die verantwortlichen Stellen und Auftragsverarbeiter die gesetzlich vorgeschriebene Mitteilung der Kontaktdaten vornehmen können. Das Meldeformular finden Sie unter folgendem Link: <https://datenschutz.hessen.de/service/meldung-eines-datenschutzbeauftragten>

In diesem Zusammenhang ist darauf hinzuweisen, dass auch die Kontaktdaten eines freiwillig benannten Datenschutzbeauftragten mitzuteilen sind.

Für die zu veröffentlichen und mitzuteilenden Kontaktdaten spricht das WP 243 konkrete Empfehlungen aus. Bei den zu veröffentlichen Daten sollte die Bereitstellung der postalischen Adresse sowie einer entsprechend gewidmeten E-Mail-Adresse und Telefonnummer erfolgen. Nicht zwingend soll demgegenüber die Veröffentlichung oder Mitteilung des Namens des Datenschutzbeauftragten sein. Gleichwohl wird die Bekanntgabe des Namens gegenüber Beschäftigten empfohlen. Bei der Erfüllung der Meldepflicht gegenüber Aufsichtsbehörden sieht das WP 243 unter Beachtung der Aufgabe eines Datenschutzbeauftragten als Anlaufstelle der Aufsichtsbehörde die Mitteilung des Namens eines Datenschutzbeauftragten als erforderlich an.<sup>14</sup>

Auch wenn die schriftliche Bestellung nicht erforderlich ist, empfiehlt es sich, aus Gründen der Rechtssicherheit sowie vor dem Hintergrund von Nachweispflichten<sup>15</sup>, die Benennung zum Datenschutzbeauftragten in geeigneter Form zu dokumentieren. Denkbar sind z. B. eine Benennungsurkunde, ein Dienstleistungsvertrag, eine Ergänzung zu dem Arbeitsvertrag oder aber eine Kombination dieser Dokumente. Dabei sollte auf

- den Zeitpunkt der Wirksamkeit der Benennung,
- die vom Datenschutzbeauftragten übernommenen gesetzlichen und gegebenenfalls zusätzlich vertraglich vereinbarten Aufgaben,
- das zur Verfügung gestellte Zeitkontingent,
- die zur Verfügung gestellten Ressourcen,
- und bei Unternehmensgruppen auf die Aufzählung der konkreten Unternehmen etc.

eingegangen werden.

Hinsichtlich der Fortgeltung der vor der Geltung der DS-GVO unterzeichneten Bestellurkunden nach dem 25.05.2018 verändert sich jedenfalls der Regelungscharakter der Bestellurkunde. Die bis dato konstitutiv wirkende Unterzeichnung der Bestellurkunde kann fortan nur noch deklaratorische Wirkung entfalten, da die Schriftform nicht mehr erforderlich ist. Aufgrund der zuvor dargestellten Erwägungen kann es aber durchaus sinnvoll sein, an den bereits bestehenden schriftlichen Dokumenten festzuhalten. Bestehende Dokumente sollten aber in jedem Fall auf ihre Konformität mit den aktuellen gesetzlichen Bestimmungen überprüft werden.

#### **4. Gemeinsame Datenschutzbeauftragte**

Verantwortliche und Auftragsverarbeiter können einen Datenschutzbeauftragten für eine Unternehmensgruppe benennen, sofern dieser von jeder Niederlassung leicht erreicht werden kann, vgl. Art. 37 Abs. 2 DS-GVO. Eine separate Benennung für jedes einzelne Konzernunternehmen muss daher nicht erfolgen. Allerdings sollte allen Beteiligten klar sein, für welche konkreten Mitglieder einer Unternehmensgruppe ein benannter Datenschutzbeauftragter zuständig ist. Scheidet ein Unternehmen aus einer Unternehmensgruppe aus, welches die Anforderungen zu der Benennung eines Datenschutzbeauftragten erfüllt, sollte festgelegt sein, ob eine Zuständigkeit des

---

<sup>14</sup> WP 243, S. 12 f.

<sup>15</sup> Vgl. dazu Art. 24 Abs. 1 DS-GVO und Erwägungsgrund 74 der DS-GVO: Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind.

Konzerndatenschutzbeauftragten noch immer gegeben ist. Zugleich muss sichergestellt werden, wie bei Unternehmenstransaktionen (Mergers & Acquisitions) mit der Zuständigkeit im Gefüge einer Unternehmensgruppe umzugehen ist. Es ist empfehlenswert, entsprechende Fallkonstellationen bei der Benennung eines Datenschutzbeauftragten für eine Unternehmensgruppe vorab zu regeln.

Der Begriff der leichten Erreichbarkeit verlangt zum einen die Sicherstellung der persönlichen Kommunikation durch ausreichend verfügbare Kontaktmöglichkeiten, z. B. die Einrichtung eines Kontaktformulars auf der Webseite, Bereitstellung einer Telefonnummer und/oder E-Mail-Adresse, regelmäßige Sprechstunden für Beschäftigte. Zum anderen muss der Datenschutzbeauftragte in der Lage sein, mit Aufsichtsbehörden und Betroffenen sprachlich zu kommunizieren. Wenn nach deutschem Recht eine Pflicht zu der Benennung eines betrieblichen Datenschutzbeauftragten besteht, kann somit ein Konzerndatenschutzbeauftragter auch außerhalb Deutschlands für deutsche Niederlassungen benannt werden. Dies gilt z. B. auch, wenn ein Unternehmen mit Hauptsitz außerhalb der Europäischen Union am Ort des Hauptsitzes den Datenschutzbeauftragten auch für alle europäischen Tochterunternehmen benennt. Entscheidend ist, dass der Datenschutzbeauftragte aufgrund seiner Eigenschaften<sup>16</sup> sowie seiner Stellung im Unternehmen tatsächlich in der Lage ist für Betroffene und Aufsichtsbehörden persönlich als Ansprechpartner zur Verfügung zu stehen, d. h., mit ihnen zu kommunizieren und zu kooperieren und die ihm von der DS-GVO auferlegten Aufgaben zu erfüllen. Gleichwohl ist es empfehlenswert, dass der Datenschutzbeauftragte in der Europäischen Union/im Europäischen Wirtschaftsraum ansässig ist, da andernfalls die Erfüllung der übernommenen Aufgaben erheblich erschwert sein dürfte.

Auch Behörden und öffentliche Stellen können unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe einen gemeinsamen Datenschutzbeauftragten benennen, vgl. Art. 37 Abs. 3 DS-GVO, § 5 Abs. 2 HDSIG. Denkbar wäre beispielsweise die Benennung eines gemeinsamen Datenschutzbeauftragten für mehrere kleine Kommunen im Rahmen der interkommunalen Zusammenarbeit.

## 5. Interne und externe Datenschutzbeauftragte

Der Datenschutzbeauftragte kann sowohl Beschäftigter des Unternehmens/der öffentlichen Stelle sein als auch auf der Grundlage eines Dienstleistungsvertrages tätig werden, vgl. Art. 37 Abs. 6 DS-GVO, § 5 Abs. 4 HDSIG. Der Dienstleistungsvertrag kann mit einer Einzelperson oder einem Dienstleistungsunternehmen (juristischen Person) abgeschlossen werden. In der Praxis ist insbesondere darauf zu achten, dass der externe Datenschutzbeauftragte die gestellten Anforderungen erfüllt und den mit der Stellung des Datenschutzbeauftragten verbundenen Schutz genießt. Sowohl bei internen als auch bei externen Datenschutzbeauftragten empfiehlt es sich, die wichtigsten, mit der Benennung zu dem Datenschutzbeauftragten zusammenhängenden tatsächlichen und rechtlichen Folgen zu dokumentieren.<sup>17</sup> Bei der Bestellung externer Datenschutzbeauftragter ist insbesondere auf die Einhaltung der Verschwiegenheitsvorgaben hinzuweisen.<sup>18</sup>

## 6. Datenschutzteam und Benennung juristischer Personen

Neben der Benennung einer einzelnen Person ist es auch möglich, dass mehrere Personen gemeinsam die Aufgaben des Datenschutzbeauftragten wahrnehmen. Die Beauftragung eines Datenschutzteams kann geeignet sein, die Erfüllung der nach der DS-GVO obliegenden Aufgaben effizient zu gestalten. So kann beispielsweise vorhandenes Spezialwissen gezielt eingesetzt werden.

---

<sup>16</sup> Vgl. dazu vor allem Punkt II. „Persönliche Voraussetzungen des Datenschutzbeauftragten“.

<sup>17</sup> Vgl. zu dem Umfang der schriftlichen Dokumentation auch die weitergehenden Ausführungen unter Punkt I. 3. „Veröffentlichungs- und Mitteilungspflicht“.

<sup>18</sup> *Wilmer*, in: Roßnagel, Kommentar HDSIG, § 5 Rn. 28.



Die Übernahme der Aufgaben des Datenschutzbeauftragten durch ein Team kann aber auch zu erheblicher Rechtsunsicherheit führen, etwa wenn es um Fragen der Zuständigkeit, der Haftungsverteilung oder des Abberufungs- und Kündigungsschutzes geht. Fraglich könnte etwa sein, welchen Personen des Datenschutzteams die Privilegien des Art. 38 DS-GVO und der § 38 Abs. 2 in Verbindung mit § 6 Abs. 4, Abs. 5 S. 2 und Abs. 6 BDSG zustehen. Aus Gründen der Rechtssicherheit ist es daher unerlässlich, dass die Verantwortlichkeiten bei der Aufnahme der Tätigkeit klar zugewiesen und entsprechend dokumentiert werden. Generell empfiehlt es sich, einen „Hauptverantwortlichen“ für die Erfüllung der Aufgaben des Datenschutzbeauftragten zu benennen.

Zulässig ist auch die Benennung einer juristischen Person zum Datenschutzbeauftragten.<sup>19</sup> Dann ist es jedoch zwingend, dass die für die juristische Person handelnden und die Aufgaben des Datenschutzbeauftragten ausführenden Personen die Voraussetzungen der Art. 37-39 DS-GVO erfüllen.

## **7. Freiwillige Benennung**

Für den Fall, dass die Benennung eines Datenschutzbeauftragten nicht zwingend erforderlich ist, besteht für Unternehmen die Möglichkeit der freiwilligen Benennung eines Datenschutzbeauftragten, vgl. Art. 37 Abs. 4 S. 1 DS-GVO. Dann gelten die Vorschriften der Art. 37-39 DS-GVO. Zu berücksichtigen ist aber, dass die zu der DS-GVO hinzutretenden Privilegien des BDSG bzgl. des Abberufungs- und Kündigungsschutzes nach dem Wortlaut des § 38 Abs. 2 BDSG nur bei der verpflichtenden Benennung zur Anwendung gelangen.<sup>20</sup> Gleichwohl können die Parteien entsprechende vertragliche Vereinbarungen treffen. Auch hier empfiehlt sich die schriftliche Dokumentation.

Unternehmen, die weder verpflichtend einen Datenschutzbeauftragten benennen müssen noch freiwillig einen Datenschutzbeauftragten benennen wollen, haben zudem die Möglichkeit, interne Mitarbeiter oder externe Berater mit bestimmten Datenschutzaufgaben zu betrauen. In solchen Fällen muss jedoch sichergestellt werden, dass sowohl den Parteien als auch etwaigen Kommunikationspartnern (z. B. Beschäftigte, Betroffene, Aufsichtsbehörden etc.) klar ist, dass es sich bei der tätigen Person nicht um einen Datenschutzbeauftragten handelt.<sup>21</sup>

## **II. Persönliche Voraussetzungen des Datenschutzbeauftragten**

Der Datenschutzbeauftragte wird auf der Grundlage der folgenden drei Voraussetzungen benannt, vgl. Art. 37 Abs. 5 DS-GVO:

- (1) berufliche Qualifikation,
- (2) Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis,
- (3) Fähigkeit zur Erfüllung der in der DS-GVO, dem BDSG und dem HDSIG genannten Aufgaben.

### **1. Berufliche Qualifikation und Fachwissen**

Der Begriff der beruflichen Qualifikation wird gesetzlich nicht weiter definiert. Erforderlich sind Kenntnisse des nationalen und europäischen Datenschutzrechts sowie ein vertieftes Verständnis der DS-GVO.<sup>22</sup>

Auch im Hinblick auf das erforderliche Fachwissen fehlt eine genauere Beschreibung. Dieses sollte in einem angemessenen Verhältnis zu der Sensitivität, Komplexität und zu dem Umfang der Verarbeitungsvorgänge stehen. Die Bewertung systematischer Übermittlung personenbezogener Daten in Drittstaaten verlangt etwa ein tiefergehendes Fachwissen als ein gelegentlicher Datenaustausch innerhalb der Europäischen Union und des Europäischen

---

<sup>19</sup> WP 243, S. 14.

<sup>20</sup> [LAG Hamm, Urteil vom 06.10.2022 – 18 Sa 271/22, Rn. 20 ff.](#)

<sup>21</sup> WP 243, S. 6.

<sup>22</sup> WP 243, S. 13 f.

Wirtschaftsraums.<sup>23</sup> Neben der sicheren Anwendung der gesetzlichen Regelungen ist es für die Erfüllung der obliegenden Aufgaben unerlässlich, dass der Datenschutzbeauftragte organisatorische und vertiefte technische Kenntnisse hat.

## **2. Fähigkeit zur Erfüllung der genannten Aufgaben**

Neben der beruflichen und der fachlichen Qualifikation ist im Zusammenhang mit der Fähigkeit zu der Erfüllung der in der DS-GVO genannten Aufgaben erforderlich, dass der Datenschutzbeauftragte ein hohes Maß an persönlicher Integrität und Berufsethik mitbringt.<sup>24</sup> Personen, die in der Vergangenheit bereits Datenschutzverstöße begangen oder Verschwiegenheitspflichten verletzt haben, kommen damit als Datenschutzbeauftragte nicht in Betracht.

## **III. Aufgaben und Pflichten**

Die Kernaufgaben des Datenschutzbeauftragten lassen sich wie folgt zusammenfassen, vgl. Art. 39 DS-GVO und § 7 HDSIG:

- (1) Unterrichtung und Beratung,
- (2) Überwachung der Einhaltung der DS-GVO und anderer Datenschutzvorschriften der Union bzw. der Mitgliedsstaaten (des BDSG, HDSIG und sonstiger Vorschriften über den Datenschutz), Zuweisung von Zuständigkeiten,
- (3) Sensibilisierung und Schulung,
- (4) Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung,
- (5) Zusammenarbeit mit der Aufsichtsbehörde,
- (6) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde.

### **1. Unterrichtung und Beratung**

Die Unterrichtungs- und Beratungspflicht, vgl. Art. 39 Abs. 1 Buchstabe a DS-GVO, § 7 Abs. 1 S. 1 Nr. 1 HDSIG, verlangt, dass der Datenschutzbeauftragte über einschlägige datenschutzrelevante Vorschriften und Vorgänge informiert und darüber hinaus Mittel und Wege zu der Behandlung bestehender datenschutzrechtlicher Probleme vorschlägt. Die Pflicht besteht gegenüber der obersten Unternehmens- oder Behördenebene, aber auch gegenüber Beschäftigten, die Verarbeitungen durchführen. Es besteht eine enge Verbindung zwischen der Unterrichtungs- und Beratungspflicht und dem Recht des Datenschutzbeauftragten, unmittelbar der höchsten Management- oder Leitungsebene zu berichten, vgl. Art. 38 Abs. 3 S. 3 DS-GVO, § 6 Abs. 3 S. 2 HDSIG.

### **2. Überwachung der Einhaltung der DS-GVO, des BDSG und des HDSIG**

Der Datenschutzbeauftragte kontrolliert die Einhaltung des einschlägigen nationalen und europäischen Datenschutzrechts durch Behörden bzw. Unternehmen, vgl. Art. 39 Abs. 1 Buchstabe b DS-GVO, § 7 Abs. 1 S. 1 Nr. 2 HDSIG. Behördliche Datenschutzbeauftragte müssen insbesondere auch die Bestimmungen des HDSIG berücksichtigen.

Falls ein betrieblicher Datenschutzbeauftragter/Konzerndatenschutzbeauftragter für mehrere Niederlassungen innerhalb Europas tätig ist, müssen ihm die wesentlichen nationalen Sonderregelungen der Mitgliedsstaaten, in denen er als Datenschutzbeauftragter benannt ist, bekannt sein. Darüber hinaus können, je nach Betätigung des Unternehmens, Kenntnisse bereichsspezifischen Datenschutzrechts erforderlich sein.<sup>25</sup>

Neben der Kontrolle der Wahrung des Datenschutzrechts obliegt dem Datenschutzbeauftragten auch die Überwachung der Einhaltung der Strategien bzw. Regeln

---

<sup>23</sup> Vgl. zu dem erforderlichen Fachwissen im Falle eines Konzerndatenschutzbeauftragten auch die weitergehenden Ausführungen unter Punkt III. 2. „Überwachung der Einhaltung der DS-GVO, des BDSG und des HDSIG“.

<sup>24</sup> WP 243, S. 14.

<sup>25</sup> Vgl. dazu auch die Ausführungen unter Punkt II. 1. „Berufliche Qualifikation und Fachwissen“.

und Richtlinien, die sich Unternehmen oder Behörden selbst auferlegen. Hierzu können z. B. Betriebsvereinbarungen, Handlungsanweisungen, Dienstvereinbarungen, Industriestandards, Code of Conducts usw. gehören.

Schließlich erstreckt sich die Kontrollbefugnis des Datenschutzbeauftragten auch auf die gewählte interne Zuständigkeitsverteilung. Der Datenschutzbeauftragte kann daher auch Einfluss auf die organisatorische Umsetzung des Datenschutzrechts nehmen.

### **3. Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung**

Bei der Überwachung und Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung, vgl. Art. 39 Abs. 1 Buchstabe c DS-GVO, § 7 Abs. 1 S. 1 Nr. 3 HDSIG, handelt es sich um einen Sonderfall der allgemeinen Beratungs- und Überwachungspflicht des Datenschutzbeauftragten. Während sich die Überwachungsverpflichtung des Datenschutzbeauftragten im Rahmen der Durchführung der Datenschutz-Folgenabschätzung eindeutig dem gesetzlichen Wortlaut entnehmen lässt, besteht nach dem Wortlaut der DS-GVO (das HDSIG verzichtet auf diesen Passus) eine Beratungspflicht des Datenschutzbeauftragten nur „auf Anfrage“ des Verantwortlichen. Die Vorschrift kann daher so interpretiert werden, dass es dem Verantwortlichen freistünde, den Rat des Datenschutzbeauftragten in Anspruch zu nehmen oder nicht. Die Formulierung des Art. 35 Abs. 2 DS-GVO, nach welcher der Verantwortliche bei der Durchführung der Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten einzuholen hat, steht hierzu jedoch im Widerspruch.

Letztlich ist unabhängig von der rechtlichen Beurteilung die Hinzuziehung des Datenschutzbeauftragten aus rein praktischen Gründen dringend zu empfehlen, da dieser aufgrund seiner Erfahrung und seines Fachwissens wichtige Denkanstöße geben kann. Vor diesem Hintergrund empfiehlt es sich auch, den Datenschutzbeauftragten bereits bei der Frage, ob für eine Datenverarbeitung eine Datenschutz-Folgenabschätzung zu erfolgen hat, einzubeziehen.

### **4. Sensibilisierung und Schulung**

Datenschutzverstöße (etwa das Versenden von E-Mails mit offenem Empfängerkreis oder das Herunterladen von Schadsoftware durch versehentliches Öffnen von Spam-Nachrichten) sind häufig auf ein fehlendes Bewusstsein der handelnden Mitarbeiter zurückzuführen.<sup>26</sup> Der Aufgabe des Verantwortlichen oder Auftragsverarbeiters, Mitarbeiter zu sensibilisieren und zu schulen, vgl. Art. 39 Abs. 1 Buchstabe b DS-GVO, § 7 Abs. 1 S. 1 Nr. 2 HDSIG, kommt somit besondere Bedeutung zu. Für eine wirkungsvolle Datenschutzorganisation ist es daher unerlässlich, dass die mit der Verarbeitung personenbezogener Daten beschäftigten Personen ihrer Arbeitsplatzbeschreibung entsprechend geschult, regelmäßig an die Einhaltung datenschutzrechtlicher Vorschriften erinnert und über akute Gefahren informiert werden.

Welche Anforderungen an eine Schulungsmaßnahme sowie an weitergehende Sensibilisierungen zu stellen sind, richtet sich nach den Umständen des Einzelfalles. Für die Organisation und effektive Ausgestaltung einer Schulungsmaßnahme können z. B. die folgenden Erwägungen eine Rolle spielen:

- Kerntätigkeit der Mitarbeiter erfordert die Verarbeitung personenbezogener Daten (z. B. Mitarbeiter der IT, Personalabteilung, des Marketings oder des Vertriebs),
- Umfang der Verarbeitung personenbezogener Daten,
- Verarbeitung sensibler Daten,

---

<sup>26</sup> Dies zeigen zahlreiche Studien, vgl. etwa Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2022 ([https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?\\_\\_blob=publicationFile&v=6](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6)), S. 11 ff.

- Zugang- und Zugriffsmöglichkeiten zu personenbezogenen Daten,
- Anwendung bereichsspezifischen Datenschutzrechts,
- Dokumentation/Teilnehmernachweis.

Nach dem Wortlaut der DS-GVO und des HDSIG obliegt dem Datenschutzbeauftragten nur die Überwachung, dass ausreichend Sensibilisierungen und Schulungen stattgefunden haben. Es empfiehlt sich aber, dem Datenschutzbeauftragten die Durchführung von Sensibilisierungen und Schulungsmaßnahmen als Aufgabe zu übertragen.

### **5. Zusammenarbeit mit der Aufsichtsbehörde**

Der Datenschutzbeauftragte ist ausdrücklich zu der Zusammenarbeit mit der Aufsichtsbehörde verpflichtet, vgl. Art. 39 Abs. 1 Buchstabe d DS-GVO, § 7 Abs. 1 S. 1 Nr. 4 HDSIG. Er wird somit zu der zentralen Anlaufstelle für Betroffene, Verantwortliche, Auftragsverarbeiter und Aufsichtsbehörden. Die Kooperationspflicht ist nicht gleichbedeutend mit einer Verpflichtung des Datenschutzbeauftragten zu der sofortigen Meldung von Datenschutzverstößen gegenüber der Aufsichtsbehörde. Die gegenüber Aufsichtsbehörden bestehenden Pflichten zu der Meldung von Datenschutzverstößen sind abschließend geregelt, vgl. insbesondere Art. 33 DS-GVO.

Der Datenschutzbeauftragte ist in erster Linie interne Kontrollinstanz und sollte aufgrund der gegenüber dem Unternehmen oder der Behörde bestehenden Treuepflicht zunächst intern versuchen, Maßnahmen zu der Beseitigung von Datenschutzverstößen zu ergreifen. Das besondere Vertrauensverhältnis erfordert es, dass datenschutzrechtliche Fragen und Probleme zwischen den Parteien offen kommuniziert werden und beiderseits an rechtskonformen und konstruktiven Lösungen gearbeitet wird. Nur so kann der Datenschutzbeauftragte den übernommenen Aufgaben gerecht werden und zu dem „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ effektiv beitragen.

Sofern sich der Datenschutzbeauftragte, z. B. zu dem Zwecke der Beratung im Zusammenhang mit der Anwendung der DS-GVO, an die Aufsichtsbehörde wendet, erfolgt die Tätigkeit jeder Aufsichtsbehörde für den Datenschutzbeauftragten unentgeltlich, Art. 57 Abs. 3 DS-GVO. Aufgaben der zuständigen Aufsichtsbehörden sind die Kontrolle und die Beratung in Fragen des Datenschutzes. Um diese Aufgaben effizient erfüllen zu können, ist es wichtig, dass die Datenschutzbeauftragten den Sachverhalt und die Rechtsfragen so weit wie möglich zunächst selbst konkretisieren und prüfen. Bei juristisch geschulten Datenschutzbeauftragten wird zunächst eine juristische Eigeneinschätzung erwartet. Bei verbleibenden konkreten Zweifelsfragen können sich die Datenschutzbeauftragten an die zuständige Aufsichtsbehörde wenden, in dem sie das Ergebnis ihrer Prüfung mit dem entscheidenden Sachverhalt und den wesentlichen Argumentationslinien darlegen.

### **6. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde**

Bei der Tätigkeit als Anlaufstelle für die Aufsichtsbehörden, vgl. Art. 39 Abs. 1 Buchstabe e DS-GVO, § 7 Abs. 1 S. 1 Nr. 5 HDSIG, handelt es sich um einen Unterfall der Kooperationspflicht. Der Datenschutzbeauftragte ist danach Anlaufstelle für alle im Zusammenhang mit der Verarbeitung stehenden Fragen, einschließlich vorheriger Konsultationen im Rahmen der Datenschutz-Folgenabschätzung. Die Aufsichtsbehörden haben insbesondere die Möglichkeit, sich direkt an den Datenschutzbeauftragten zu wenden, ohne vorab etwa den Geschäftsführer oder Behördenleiter des Verantwortlichen oder Auftragsverarbeiters kontaktieren zu müssen. Darüber hinaus besteht auf Anfrage der Aufsichtsbehörden eine Beratungspflicht des Datenschutzbeauftragten zu allen sonstigen Fragen.

### **7. Risikoorientierte Aufgabenerfüllung**

Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art und den Umfang, die Umstände und Zwecke der Verarbeitung berücksichtigt, vgl. Art. 39 Abs. 2 DS-

GVO, § 7 Abs. 3 HDSIG. Damit wird nicht nur ein Aufgabenkatalog beschrieben, sondern dem Datenschutzbeauftragten auch eine Maxime zu der Aufgabenerfüllung mitgegeben.

Der Datenschutzbeauftragte trifft somit Abwägungsentscheidungen, die in einem angemessenen Verhältnis zu den Risiken stehen müssen, welche durch die Verarbeitungsvorgänge entstehen. Dabei hat er einen Ermessensspielraum. Eine Pflichtverletzung ist dann gegeben, wenn der Datenschutzbeauftragte diesen überschreitet oder aber keine ausreichende Abwägungsentscheidung trifft. Empfehlenswert wäre daher z. B. die Erstellung eines an den Umständen des Unternehmens oder der Behörde orientierten Aufgabenkatalogs, der an Hand einer Gegenüberstellung der Verarbeitungsaktivitäten und den zu erwartenden Risiken Aufgaben-Priorisierungen vornimmt. Zu Nachweiszwecken ist grundsätzlich anzuraten, die eingestellten Überlegungen einer Abwägungsentscheidung entsprechend der aufgestellten Maxime zu dokumentieren.

### **8. Erweiterung des Aufgabenkatalogs durch Vereinbarung**

Den Behörden und Unternehmen steht es frei, die Rolle des Datenschutzbeauftragten strategischer und proaktiver auszugestalten, als dies gesetzlich vorgesehen ist. Die Vorschriften enthalten keine abschließende Aufgabenzuweisung. Weitere Pflichten, wie beispielsweise die Pflicht zu der Führung des Verzeichnisses von Verarbeitungstätigkeiten, die generelle Beantwortung von Auskunfts- und Löschungsersuchen durch den Datenschutzbeauftragten oder die Durchführung von Schulungsmaßnahmen können daher zusätzlich vereinbart werden. Wie bereits erwähnt, empfiehlt es sich, die über den gesetzlich vorgesehenen Aufgabenkatalog weitergehend vereinbarten Aufgaben schriftlich festzuhalten.

## **IV. Stellung des Datenschutzbeauftragten**

Die unabhängige und organisatorisch herausgehobene Stellung des Datenschutzbeauftragten, vgl. Art. 38 DS-GVO, §§ 6 und 7 Abs. 2 HDSIG, ist für eine wirkungsvolle Tätigkeit von ausschlaggebender Bedeutung, da dieser andernfalls den zuvor beschriebenen Aufgaben und Pflichten nur schwerlich gerecht werden kann. Der europäische Gesetzgeber hat daher Regelungen geschaffen, welche sich mit der organisatorischen Stellung des Datenschutzbeauftragten beschäftigen und diesem bestimmte Privilegien einräumen. Das HDSIG übernimmt, sofern die DS-GVO nicht anwendbar ist, für behördliche Datenschutzbeauftragte gleichlautende Regelungen und ergänzt die bereits in der DS-GVO angelegten Privilegien für Datenschutzbeauftragte.

Insgesamt können folgende Themenkreise zu der Stellung des Datenschutzbeauftragten in Behörden und Unternehmen zusammengefasst werden:

- ordnungsgemäße und frühzeitige Einbindung,
- Bereitstellung erforderlicher Ressourcen,
- Weisungsfreiheit und Unabhängigkeit,
- keine Benachteiligung: Abberufungs- und Kündigungsschutz,
- unmittelbarer Berichtsweg zu der höchsten Führungsebene,
- Anrufungsrecht der betroffenen Personen,
- kein Interessenkonflikt,
- Zusammenarbeit mit der Aufsichtsbehörde.

### **1. Ordnungsgemäße und frühzeitige Einbindung**

Verantwortliche und Auftragsverarbeiter müssen den Datenschutzbeauftragten ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einbinden, vgl. Art. 38 Abs. 1 DS-GVO, § 6 Abs. 1 HDSIG. Die Vorschrift ist für die Erfüllung der Aufgaben des Datenschutzbeauftragten zwingend erforderlich, da dieser andernfalls seinen Beratungs- und Überwachungsaufgaben nicht gerecht werden kann.



Erfahrungen zeigen, dass Datenschutzbeauftragte häufig zu spät in neue, datenschutzrechtlich relevante Projekte (z. B. Einführung eines Personalinformationssystems oder Einsatz neuer Analyse-Software im Bereich des Digitalmarketings) eingebunden werden. Dies führt unter Umständen zu erheblichen praktischen Problemen für Unternehmen und Behörden, z. B.

- kann sich die Einführung einer neuen IT verzögern, da datenschutzrechtlich notwendige Verträge (z. B. Abschluss von Auftragsdatenverarbeitungsverträgen o. ä.) nachträglich geschlossen werden müssen,
- können Projektkosten steigen, da datenschutzrechtlich notwendiger Programmieraufwand (z. B. Löschungen und Zugriffsbeschränkungen) bei der Planung nicht berücksichtigt wurde,
- kann beschaffte Software nicht genutzt werden, weil dies gegen Bestimmungen des Datenschutzrechts verstößt.

Die Sicherstellung der frühzeitigen Einbindung des Datenschutzbeauftragten erfordert einen in der Praxis leicht zu realisierenden Mechanismus, der von der Größe der Organisation, der Komplexität der Strukturen sowie weiterer Faktoren (z. B. Matrixstrukturen in einer Unternehmensgruppe) abhängig sein kann. Mögliche Lösungsansätze zu der Sicherstellung der frühzeitigen Einbindung können z. B. sein:

- generelle Einbindung des Datenschutzbeauftragten, bevor Budgetfreigaben einer bestimmten Größenordnung erteilt werden,
- regelmäßige Teilnahme an Führungskreistreffen (abhängig von Unternehmensstruktur, z. B. Vorstand, Geschäftsführer, höchste Managementebene),
- regelmäßige Abstimmung mit Bereichen, die intensiv personenbezogene Daten verarbeiten (z. B. Personal, IT, Marketing und Vertrieb),
- regelmäßige Treffen mit IT und Informationssicherheitsbeauftragten,
- Teilnahme an Betriebsratssitzungen/Personalvertretungssitzungen, sofern die Einführung neuer IT vorgestellt oder der Abschluss von Betriebsvereinbarungen in Betracht gezogen wird.

## **2. Bereitstellung erforderlicher Ressourcen**

Verantwortliche und Auftragsverarbeiter sind verpflichtet, den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen, vgl. Art. 38 Abs. 2 DS-GVO, § 6 Abs. 2 HDSIG. Dazu sind diesem insbesondere erforderliche Ressourcen zur Verfügung zu stellen, Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen zu gewähren und erforderliche Ressourcen zu der Erhaltung seines Fachwissens zur Verfügung zu stellen.

Im Zusammenhang mit der Pflicht des Verantwortlichen oder Auftragsverarbeiters zu der Unterstützung und Bereitstellung der erforderlichen Ressourcen sind z. B. die folgenden Themenkomplexe zu berücksichtigen<sup>27</sup>:

- aktive Unterstützung des Datenschutzbeauftragten durch die Geschäftsführung (z. B. Vorstandsebene),
- Einräumung eines ausreichenden Zeitkontingentes, damit der Datenschutzbeauftragte seine Aufgaben angemessen erfüllen kann (ggf. Freistellung von anderen Tätigkeiten),
- angemessene Unterstützung durch Bereitstellung von finanziellen Mitteln, Infrastrukturen und ggf. Personal (abhängig von der Größe und der Struktur des Unternehmens kann es erforderlich sein, mehrere Personen mit Datenschutzaufgaben zu betrauen),<sup>28</sup>

<sup>27</sup> Vgl. dazu auch die Ausführungen im WP 243, S. 16 f.

<sup>28</sup> Vgl. dazu auch Punkt I. 6. „Datenschutzteam und Benennung juristischer Personen“ und IV. 10. „Ausweitung der Privilegien auf Vertreter oder Datenschutzteam“.





- Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen, sofern und soweit dies zu der Erfüllung seiner Aufgaben tatsächlich erforderlich ist (z. B. im Zusammenhang mit Kontrollmaßnahmen),
- neben der ohnehin bestehenden Veröffentlichungs- und Mitteilungspflicht: Offizielle Vorstellung des Datenschutzbeauftragten gegenüber der Belegschaft;
- Zugang zu anderen Abteilungen (z. B. Vertrieb, Personal, Recht, IT und Sicherheit), um ggf. hierüber Unterstützung oder Anregungen zu erhalten,
- regelmäßige Weiterbildungsmaßnahmen/Bereitstellung erforderlicher Fachliteratur in dem zu der Aufgabenerfüllung notwendigen Umfang,
- Bereitstellung von Informationen über das Unternehmen, soweit ein entsprechender datenschutzrechtlicher Zusammenhang besteht (z. B. Organigramm, Geschäftsverteilungsplan, Planungsunterlagen, Konzepte oder Richtlinien).

Grundsätzlich gilt: Je komplexer, vielfältiger und sensibler die Datenverarbeitungsvorgänge sind, desto mehr Ressourcen müssen von dem Verantwortlichen oder Auftragsverarbeiter zur Verfügung gestellt werden.

### **3. Weisungsfreiheit/Unabhängigkeit**

Die Weisungsfreiheit des Datenschutzbeauftragten ist Kernstück seiner Unabhängigkeit, vgl. Art. 38 Abs. 3 S. 1 und Erwägungsgrund 97 der DS-GVO, § 6 Abs. 3 HDSIG. Diese ist beschränkt auf solche Handlungen, die sich auf die Ausübung seiner Aufgaben als Datenschutzbeauftragter beziehen.

Unternehmen und Behörden dürfen dem Datenschutzbeauftragten gegenüber somit keine Weisungen in seiner Funktion als Datenschutzbeauftragter erteilen. Deshalb sind z. B. Vorgaben zu der Erreichung eines bestimmten Ziels, zu der Art und Weise der Bearbeitung von Beschwerden oder zu dem Austausch mit Aufsichtsbehörden unzulässig. Andererseits gibt die Weisungsfreiheit dem Datenschutzbeauftragten aber auch keine über die Erfüllung seiner Aufgaben hinausgehenden Befugnisse.

### **4. Keine Benachteiligung: Abberufung und Kündigung**

Neben der Weisungsfreiheit wird die Unabhängigkeit des Datenschutzbeauftragten auch dadurch gewährleistet, dass dieser aufgrund der Ausübung seiner Tätigkeit nicht abberufen oder benachteiligt werden darf, vgl. Art. 38 Abs. 3 S. 2 DS-GVO. Das Verbot der Abberufung oder Benachteiligung ist auf solche Fälle begrenzt, in denen diese als Reaktion auf die Ausübung der Tätigkeiten als Datenschutzbeauftragter erfolgen sollen. Zulässig ist eine befristete Benennung des Datenschutzbeauftragten, soweit diese durch einen sachlichen, angemessenen Grund gerechtfertigt ist.

Die DS-GVO selbst kennt keinen Sonderabberufungs- oder Kündigungsschutz. Der deutsche Gesetzgeber verstärkt jedoch für verpflichtend zu benennende betriebliche Datenschutzbeauftragte die Unabhängigkeit, vgl. § 38 Abs. 2 in Verbindung mit § 6 Abs. 4 BDSG.<sup>29</sup> Abberufungen sind nur in entsprechender Anwendung des § 626 BGB möglich und Kündigungen sind nur aus wichtigem Grund zulässig. Darüber hinaus ist die Kündigung des Arbeitsverhältnisses nach dem Ende der Tätigkeit als Datenschutzbeauftragter innerhalb eines Jahres nach der Abberufung unzulässig, es sei denn, die kündigende Stelle ist zu der Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt.

Im Fall der freiwilligen Benennung besteht dagegen kein besonderer Abberufungs- oder Kündigungsschutz, sofern dieser nicht vertraglich zwischen den Parteien vereinbart wird. Bei der Benennung eines externen Datenschutzbeauftragten sollte durch vertragliche Vereinbarungen sichergestellt werden, dass dem von dem Gesetzgeber gewollten

---

<sup>29</sup> Unionsrechtskonforme Regelungen: [EuGH, Urteil vom 22.06.2022 – C-534/20, Rn. 31 ff.](#); [BAG, Urteil vom 25.08.2022 – 2 AZR 225/20](#).

Benachteiligungsschutz (z. B. durch Vereinbarung von festen Vertragslaufzeiten mit gewisser Dauer) ausreichend Rechnung getragen wird.

Für behördliche Datenschutzbeauftragte sieht das HDSIG dagegen – anders als auf Bundesebene, vgl. § 6 Abs. 4 BDSG – keinen Sonderabberufungs- oder Kündigungsschutz vor. Diese unterliegen lediglich einem allgemeinen, tätigkeitsbezogenen Abberufungsverbot.<sup>30</sup>

### **5. Unmittelbarer Berichtsweg zu der Geschäftsführung bzw. zu der höchsten Leitungsebene**

Datenschutzbeauftragte verfügen über einen unmittelbaren Berichtsweg zu der Geschäftsführung bzw. zu der höchsten Leitungsebene der öffentlichen Stelle, vgl. Art. 38 Abs. 3 S. 3 DS-GVO, § 6 Abs. 3 S. 2 HDSIG. Das direkte Berichtsrecht steht im Zusammenhang mit der Beratungs- und Überwachungspflicht des Datenschutzbeauftragten. Dieses gewährleistet, dass der Datenschutzbeauftragte tatsächlich Gehör findet.

Um für den unmittelbaren Berichtsweg ein Bewusstsein innerhalb von Unternehmen und Behörden zu schaffen und um dem Grundsatz der Transparenz zu entsprechen, empfiehlt es sich, die Stellung des Datenschutzbeauftragten innerhalb der verantwortlichen Stelle und dessen direktes Berichtsrecht transparent im Organigramm des Unternehmens oder der Behörde darzustellen.

### **6. Anrufungsrecht der betroffenen Person**

Der Datenschutzbeauftragte ist Ansprechpartner der betroffenen Person für sämtliche Fragen des Datenschutzes. Betroffene haben das Recht, sich direkt an den Datenschutzbeauftragten zu wenden und ihn zu konsultieren, sofern es um die Verarbeitung ihrer personenbezogenen Daten und die Wahrnehmung ihrer Rechte geht, vgl. Art. 38 Abs. 4 DS-GVO, § 6 Abs. 4 HDSIG.

### **7. Geheimhaltung, Vertraulichkeit und Zeugnisverweigerungsrecht**

Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedsstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung und Vertraulichkeit gebunden, vgl. Art. 38 Abs. 5 DS-GVO. Datenschutzbeauftragte sind zu der Verschwiegenheit über die Identität der betroffenen Person sowie über die Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet. Die Verschwiegenheitspflicht entfällt, soweit der Betroffene den Datenschutzbeauftragten hiervon befreit, vgl. § 38 Abs. 2 in Verbindung mit § 6 Abs. 5 S. 2 BDSG bzw. § 6 Abs. 4 S. 3 und S. 4 HDSIG.

Der betriebliche Datenschutzbeauftragte ist zudem gegenüber dem Arbeitgeber über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrates zulassen, zu der Verschwiegenheit verpflichtet, § 79a S. 4 des Betriebsverfassungsgesetzes (BetrVG). Die Verschwiegenheitspflicht gemäß § 38 Abs. 2 in Verbindung mit § 6 Abs. 5 S. 2 BDSG gilt hinsichtlich der von dem Betriebsrat verarbeiteten personenbezogenen Daten auch gegenüber dem Arbeitgeber, § 79a S. 5 BetrVG. Die Verschwiegenheitspflicht für den behördlichen Datenschutzbeauftragten ist in § 42 S. 4 und S. 5 des Hessischen Personalvertretungsgesetzes (HPVG) geregelt. Danach ist dieser gegenüber der Dienststelle zu der Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Personalrats zulassen. Die Verschwiegenheitspflicht gemäß § 6 Abs. 4 S. 3 und S. 4 HDSIG gilt auch im Hinblick auf das Verhältnis des Datenschutzbeauftragten zur Dienststelle.

Darüber hinaus erstrecken das BDSG und das HDSIG die Pflicht zu der Wahrung der Geheimhaltung und Vertraulichkeit auf das Zeugnisverweigerungsrecht, vgl. § 6 Abs. 6 BDSG und § 6 Abs. 5 HDSIG. Dem Datenschutzbeauftragten sowie den ihm unterstellten Beschäftigten steht somit ein Zeugnisverweigerungsrecht zu, wenn sie i. R. ihrer Tätigkeit Kenntnis von Daten erhalten, für die bei der betroffenen Person aus beruflichen Gründen ein

<sup>30</sup> *Wilmer*, in: Roßnagel, Kommentar HDSIG, § 6 Rn. 21.

Zeugnisverweigerungsrecht besteht. Über die Ausübung des Zeugnisverweigerungsrechts entscheidet dabei grundsätzlich die Person, der das Zeugnisverweigerungsrecht zusteht. Eine Ausnahme besteht jedoch für den Fall, dass die Entscheidung des Rechteinhabers nicht in absehbarer Zeit herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Datenschutzbeauftragten reicht, unterliegen Akten und andere Schriftstücke auch dem Beschlagnahmeverbot.

Dem Datenschutzbeauftragten ist es jedoch auch bei Bestehen einer Verpflichtung zu der Verschwiegenheit und Geheimhaltung nicht verboten, die Aufsichtsbehörden zu kontaktieren und deren Rat einzuholen.

### **8. Kein Interessenkonflikt**

Neben den Aufgaben, die mit der Benennung einhergehen, kann der Datenschutzbeauftragte auch andere Aufgaben und Pflichten wahrnehmen. Verantwortlicher und Auftragsverarbeiter haben aber sicherzustellen, dass zusätzlich wahrgenommene Tätigkeiten nicht zu einem Interessenkonflikt führen, vgl. Art. 38 Abs. 6 S. 2 DS-GVO, § 7 Abs. 2 HDSIG.

Interessenkonflikte bei betrieblichen Datenschutzbeauftragten bestehen regelmäßig, wenn etwa die Benennung des Geschäftsführers oder eines nahen Verwandten des Personalleiters, des Marketing- oder Vertriebsleiters, des IT-Leiters oder eines Beschäftigten der IT- oder Personalabteilung, wenn dieser in der Lage ist, Datenverarbeitungsprozesse zu bestimmen oder wesentlich zu beeinflussen, zum Datenschutzbeauftragten erfolgen soll. Daneben wird in der Regel auch bei anderen unternehmensweiten Tätigkeiten wie etwa IT-Sicherheitsbeauftragter oder Compliance-Beauftragter ein Interessenkonflikt anzunehmen sein. Problematisch ist die Benennung eines Datenschutzbeauftragten, welcher zugleich Mitglied bzw. Vorsitzender des Betriebsrates ist.<sup>31</sup> Dahingehend ist letztlich immer eine Einzelfallbetrachtung vorzunehmen, ob und inwiefern Entscheidungsbefugnisse über Zweck und Mittel der Verarbeitung bestehen. Um Interessenkonflikte möglichst zu vermeiden, empfiehlt es sich, die strukturelle Organisation mit den jeweiligen Aufgaben und Kompetenzen innerhalb einer Richtlinie eindeutig festzulegen und etwaige Interessenkonflikte von vornherein zu regeln.

Bei behördlichen Datenschutzbeauftragten besteht regelmäßig ein Interessenkonflikt bei der Behördenleitung, bei dem Bürgermeister einer Gemeinde sowie bei herausgehobenen Leitungstätigkeiten (insbesondere bei der Leitung der Personalabteilung und bei der Leitung der IT-Abteilung). Die Benennung von Mitgliedern des Personalrates ist aufgrund der Kontrollpflichten des behördlichen Datenschutzbeauftragten gegenüber dem Personalrat ebenfalls kritisch zu bewerten.<sup>32</sup> Grundsätzlich zulässig ist die Tätigkeit im Justizariat ohne Leitungsfunktion sowie die Leitung des Rechnungsprüfungsamtes.

### **9. Zusammenarbeit mit der Aufsichtsbehörde**

Die ausdrückliche Befugnis zu der direkten Kommunikation mit der Aufsichtsbehörde, vgl. Art. 39 Abs. 1 Buchstabe d und Buchstabe e DS-GVO, § 7 Abs. 1 S. 1 Nr. 4 und Nr. 5 HDSIG, dient der Stärkung der Position des Datenschutzbeauftragten innerhalb des Unternehmens bzw. der Behörde.

### **10. Ausweitung der Privilegien auf Vertreter oder Datenschutzteam**

Sofern bei einem Unternehmen neben dem Datenschutzbeauftragten auch freiwillig ein stellvertretender Datenschutzbeauftragter benannt wird oder mehrere Personen die Aufgaben des Datenschutzbeauftragten gemeinsam wahrnehmen, stellt sich die Frage, ob und in welchem Umfang die Privilegien des benannten Datenschutzbeauftragten auch auf diese Personen anzuwenden sind. Die DS-GVO und das BDSG treffen hierfür keine Regelungen.

---

<sup>31</sup> EuGH, Urteil vom 09.02.2023 – [C-453/21](#) (X-FAB Dresden GmbH & Co. KG/FC); [BAG, Urteil vom 06.06.2023 – 9 AZR 383/19](#).

<sup>32</sup> S. Fn. 31.

Da weder die DS-GVO noch das BDSG die Pflicht zu der Benennung eines stellvertretenden Datenschutzbeauftragten kennt, erfolgt die Benennung eines Stellvertreters bei betrieblichen Datenschutzbeauftragten auf freiwilliger Basis und kann daher einer freiwilligen Benennung gleichgestellt werden.<sup>33</sup> Dies hat zur Folge, dass zwar die Regelungen zum Datenschutzbeauftragten der DS-GVO, aber nicht der für betriebliche Datenschutzbeauftragte nach dem BDSG bestehende Sonderabberufungs- und Kündigungsschutz anwendbar ist. Den Parteien steht es jedoch frei, etwa den Sonderkündigungsschutz vertraglich zu vereinbaren.

Jedenfalls dann, wenn grundsätzlich eine Pflicht zu der Benennung besteht, der Vertretungsfall eintritt und der stellvertretende Datenschutzbeauftragte auch tatsächlich die Aufgaben des Datenschutzbeauftragten wahrnimmt, ist davon auszugehen, dass dem stellvertretenden Datenschutzbeauftragten auch die durch das BDSG gewährten Rechte zustehen.<sup>34</sup>

Für behördliche Datenschutzbeauftragte normiert § 5 Abs. 1 HDSIG eine Pflicht zur Benennung eines Vertreters des Datenschutzbeauftragten. Da es sich hierbei nicht um eine reine Abwesenheitsvertretung handelt, gelten auch für den Stellvertreter die mit der Aufgabewahrnehmung einhergehenden Privilegien.

Sofern ein Team mit der Erfüllung der Aufgaben des Datenschutzbeauftragten betraut wird, sollte jedes Mitglied die Anforderungen der Art. 37-39 DS-GVO erfüllen und durch die Regelungen zu der Stellung des Datenschutzbeauftragten geschützt sein. In jedem Fall empfiehlt es sich, die Aufgabenverteilung klar zu dokumentieren und in diesem Rahmen auch zu klären, ob und in welchem Umfang die Rechte des Datenschutzbeauftragten auf ein Mitglied des Datenschutzteams Anwendung finden.

## **V. Sanktionen und Haftung**

### **1. Sanktionen**

Verstöße gegen die Bestimmungen zum Datenschutzbeauftragten können mit Geldbußen von bis zu 10.000.000 € oder im Falle eines Unternehmens von bis zu zwei Prozent seines gesamten weltweit erzielten Jahresumsatzes sanktioniert werden, je nachdem, welcher Betrag höher ist, vgl. Art. 83 Abs. 4 Buchstabe a DS-GVO. Nach dem in Art. 83 DS-GVO verwendeten weiten und am europäischen Kartellrecht orientierten funktionalen Unternehmensbegriff ist als Unternehmen jede wirtschaftliche Tätigkeit ausübende Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung anzusehen.<sup>35</sup> Somit kann ggf. nicht nur ein einzelnes konzernangehöriges Unternehmen, sondern ein ganzer Konzern im Rahmen der Verhängung einer Geldbuße zu der Berechnung des maßgeblichen Unternehmensumsatzes herangezogen werden.

Die DS-GVO sieht eine Öffnungsklausel zu der Verhängung von Geldbußen gegenüber Behörden und öffentlichen Stellen vor, vgl. Art. 83 Abs. 7 DS-GVO. Das HDSIG schließt jedoch die Verhängung von Bußgeldern gegen Behörden und öffentliche Stellen aus, vgl. § 36 Abs. 2 HDSIG.

### **2. Haftungsverteilung zwischen Datenschutzbeauftragten und Unternehmen**

Der umfangreiche Aufgabenkatalog des Datenschutzbeauftragten, insbesondere die Überwachung der Einhaltung der gesetzlichen Bestimmungen, geht grundsätzlich nicht mit einer weitergehenden Haftung und Verantwortlichkeit einher. Dieser ist nicht persönlich verantwortlich, wenn ein Verstoß gegen datenschutzrechtliche Bestimmungen festgestellt wird. Die Einhaltung des Datenschutzes ist vielmehr die unternehmerische Pflicht des

---

<sup>33</sup> Vgl. dazu auch die Ausführungen unter Punkt I. 7. „Freiwillige Benennung“.

<sup>34</sup> [BAG, Urteil vom 27.07.2017 – 2 AZR 812/16.](#)

<sup>35</sup> Vgl. [EuGH, Urteil vom 12.07.1984, Rs. 170/83.](#)

Verantwortlichen bzw. Auftragsverarbeiters und nicht diejenige des Datenschutzbeauftragten.<sup>36</sup>

Die DS-GVO verlagert somit die Pflicht zu der Einhaltung datenschutzrechtlicher Regelungen nicht einseitig auf die Datenschutzbeauftragten. Vielmehr werden dem Verantwortlichen und dem Auftragsverarbeiter explizit Aufgaben zugewiesen, durch die der Datenschutzbeauftragte in die Lage versetzt werden soll, seine Aufgaben zu erfüllen. Verantwortlich im Sinne des Art. 4 Nr. 7 DS-GVO bleibt daher in erster Linie der Verantwortliche oder der Auftragsverarbeiter.

Unabhängig von der Frage der Umsetzungsverantwortung obliegt dem Datenschutzbeauftragten gleichwohl die Erfüllung der in der DS-GVO, dem BDSG und dem HDSIG genannten Aufgaben, so dass ggf. auch eine persönliche Haftung des Datenschutzbeauftragten in Betracht kommen kann. Der Datenschutzbeauftragte sollte daher eigenständig Beratungs- und Überwachungsmaßnahmen dokumentieren, um nachweisen zu können, dass er die ihm obliegenden Aufgaben ordnungsgemäß erfüllt.

---

<sup>36</sup> S. a. [OLG München, Urteil vom 27.10.2021 – 20 U 7051/20](#), nach dem der Datenschutzbeauftragte nicht „Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO ist.