



Landesbeauftragte
für Datenschutz
und Akteneinsicht

Datenschutzbeauftragte – rechtliche Anforderungen

Stand: September 2025

**Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht**
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Telefax: 033203 356-49
E-Mail: Poststelle@LDA.Brandenburg.de

www.LDA.Brandenburg.de

Inhaltsverzeichnis

1	Fallkonstellationen, in denen eine Datenschutzbeauftragte bzw. ein Datenschutzbeauftragter benannt werden muss	4
1.1	Öffentliche Stellen des Landes Brandenburg	4
1.2	Nicht öffentliche Stellen – Art und Umfang der Verarbeitung im Rahmen der Kerntätigkeit ..	5
1.3	Nicht öffentliche Stellen – umfangreiche Verarbeitung besonderer Kategorien von Daten im Rahmen der Kerntätigkeit	6
1.4	Nicht öffentliche Stellen – mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt	7
1.5	Nicht öffentliche Stellen – Erfordernis einer Datenschutz-Folgenabschätzung	8
1.6	Nicht öffentliche Stellen – geschäftsmäßige Verarbeitung zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung	8
1.7	Muster zur Prüfung, ob eine Benennungspflicht besteht	9

2	Auswahlkriterien für die Benennung von Datenschutzbeauftragten	9
----------	---	----------

3	Benennung interner oder externer Datenschutzbeauftragter	10
3.1	Zeitpunkt der Benennung	10
3.2	Benennung im Rahmen einer Arbeitnehmerüberlassung und Möglichkeit der Befristung	10
3.3	Benennung einer juristischen Person als externe Datenschutzbeauftragte	11
3.4	Veröffentlichung der Kontaktdaten der bzw. des Datenschutzbeauftragten	11
3.5	Meldung der Kontaktdaten an die Aufsichtsbehörde	12
3.6	Stellung der bzw. des Datenschutzbeauftragten	12
3.7	Freiwillige Benennung von Datenschutzbeauftragten	13

4	Interessenkonflikte	13
4.1	IT-Sicherheitsbeauftragte	13
4.2	Betriebsrats- bzw. Personalratsmitglied	14

5	Ressourcen der Datenschutzbeauftragten	15
----------	---	-----------

6	Benennung mehrerer Datenschutzbeauftragter für einen Verantwortlichen	15
----------	--	-----------

7	Gemeinsame Datenschutzbeauftragte	16
<hr/>		
8	Gleichzeitiges Tätigwerden der bzw. des Datenschutzbeauftragten für andere Verantwortliche	16
<hr/>		
9	Abberufung und Kündigungsschutz	17
<hr/>		
10	Aufgaben und Pflichten der bzw. des Datenschutzbeauftragten	18
<hr/>		
11	Haftung der bzw. des Datenschutzbeauftragten	20
<hr/>		
12	Weitere Informationen	20
<hr/>		
13	Verzeichnis der Gesetze	21

1 Fallkonstellationen, in denen eine Datenschutzbeauftragte bzw. ein Datenschutzbeauftragter benannt werden muss

Bereits vor Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO)¹ gab es in Deutschland sowohl bei öffentlichen als auch bei nicht öffentlichen Stellen die Pflicht zur Benennung (damals Bestellung) von Datenschutzbeauftragten. Diese Pflicht wird seit dem 25. Mai 2018 durch Artikel 37 Absatz 1 DS-GVO europaweit festgeschrieben. Den Mitgliedstaaten wird durch eine Öffnungsklausel zusätzlich die Möglichkeit gegeben, ergänzende Regelungen zur Benennungspflicht vorzusehen. Deutschland hat von dieser Öffnungsklausel durch die Regelungen in § 5 Bundesdatenschutzgesetz (BDSG) für öffentliche Stellen des Bundes und § 38 BDSG für nicht öffentliche Stellen Gebrauch gemacht. Für die in der Hoheit der Bundesländer liegende Umsetzung der Vorgaben der Richtlinie (EU) 2016/680 in Bezug auf die vom Anwendungsbereich der Datenschutz-Grundverordnung nicht umfasste Datenverarbeitung durch die Polizei sowie den Justiz- und Maßregelvollzug hat Brandenburg entsprechende Regelungen für Datenschutzbeauftragte in den §§ 31 ff. Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG)² getroffen.

Nach enger Auslegung des Wortlauts von Artikel 37 Absatz 1 DS-GVO müssten sowohl der Verantwortliche als auch der Auftragsverarbeiter eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten benennen, auch wenn entweder nur der Verantwortliche oder nur der Auftragsverarbeiter die Voraussetzungen zur Benennung einer Datenschutzbeauftragten bzw. eines Datenschutzbeauftragten erfüllt. Nach Sinn und Zweck des Gesetzes legt die Artikel-29-Datenschutzgruppe in Nr. 2.2 ihrer [Leitlinien in Bezug auf Datenschutzbeauftragte \(„DSB“\)](#) (WP 243 rev.01) diese Norm allerdings einschränkend aus. Danach ist nur derjenige benennungspflichtig, der die Kriterien für eine Benennungspflicht erfüllt. Das kann dazu führen, dass in bestimmten Fällen nur der Verantwortliche oder nur der Auftragsverarbeiter, in anderen Fällen beide benennungspflichtig sind.

1.1 Öffentliche Stellen des Landes Brandenburg

Alle Behörden im Sinne des § 1 Nummer 2 Verwaltungsverfahrensgesetz für das Land Brandenburg und sonstige öffentliche Stellen des Landes Brandenburg, soweit sie vom Anwendungsbereich der Datenschutz-Grundverordnung umfasst sind, trifft die Pflicht zur Benennung einer Datenschutzbeauftragten bzw. eines Datenschutzbeauftragten gemäß Artikel 37 Absatz 1 Buchstabe a DS-GVO unabhängig von der Zahl der mit der Datenverarbeitung befassten Personen und dem Umfang der Datenverarbeitung.

Eine Datenverarbeitung ist gemäß Artikel 4 Nummer 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung

1 Die Fundstellen der in dieser Handreichung zitierten Gesetze werden unter Gliederungsnummer 13 aufgeführt.

2 Anders als die Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz spricht das Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz nicht von „Datenschutzbeauftragten“ und deren „Benennung“, sondern von „behördlichen Datenschutzbeauftragten“ und deren „Bestellung“. Für die Zwecke der Handreichung sind diese Unterschiede im Wortlaut unerheblich; zur besseren Lesbarkeit wird ausschließlich die erstgenannte Ausdrucksweise verwendet.

oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Hauptausnahme der Anwendbarkeit der Datenschutz-Grundverordnung ist gemäß Artikel 2 Absatz 2 Buchstabe d DS-GVO die Datenverarbeitung durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Vom europarechtlichen Begriff der Straftaten sind auch Ordnungswidrigkeiten mit umfasst. Das bedeutet, dass beispielsweise Staatsanwaltschaften, Polizei und Ordnungsbehörden, soweit sie personenbezogene Daten für die o. g. Zwecke verarbeiten, formal keine Verpflichtung zur Benennung einer Datenschutzbeauftragten bzw. eines Datenschutzbeauftragten nach Artikel 37 Absatz 1 Buchstabe a DS-GVO trifft.

Für die Polizei und den Justiz- und Maßregelvollzug des Landes Brandenburg ist in diesen Fällen eine Benennungspflicht einer Datenschutzbeauftragten bzw. eines Datenschutzbeauftragten in § 31 BbgPJMDSG geregelt. Die bzw. der Datenschutzbeauftragte nach § 31 Absatz 1 BbgPJMDSG ist unabhängig von der Zahl der mit der Datenverarbeitung befassten Personen und der Art und dem Umfang der Datenverarbeitung zu benennen.

Da Staatsanwaltschaften, Polizei und Ordnungsbehörden aber personenbezogene Daten nicht ausschließlich zu den o. g. Zwecken verarbeiten, sondern auch personenbezogene Daten im Anwendungsbereich der Datenschutz-Grundverordnung verarbeiten (beispielsweise interne Datenverarbeitungsprozesse in Bezug auf Beschäftigtendaten), resultiert für diese Fälle dennoch eine Verpflichtung zur Benennung einer Datenschutzbeauftragten bzw. eines Datenschutzbeauftragten nach Artikel 37 Absatz 1 Buchstabe a DS-GVO. Faktisch haben also auch diese Behörden – zumindest für die in den Anwendungsbereich der Datenschutz-Grundverordnung fallenden Datenverarbeitungen – eine Benennungspflicht nach Artikel 37 Absatz 1 Buchstabe a DS-GVO. Eine solche Pflicht trifft auch die Gerichte. Zwar müssen sie – vergleichbar zu den obigen Ausführungen – im Rahmen ihrer justiziellen Tätigkeiten formal keine Datenschutzbeauftragte bzw. keinen Datenschutzbeauftragten benennen. Allerdings handeln auch Gerichte nicht ausschließlich justiziell, sodass für die anderen Datenverarbeitungen dennoch eine Benennungspflicht nach Artikel 37 Absatz 1 Buchstabe a DS-GVO besteht.

1.2 Nicht öffentliche Stellen – Art und Umfang der Verarbeitung im Rahmen der Kerntätigkeit

Nicht öffentliche Stellen haben eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten gemäß Artikel 37 Absatz 1 Buchstabe b DS-GVO zu benennen, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke umfangreiche regelmäßige und systematische Überwachungen von betroffenen Personen erforderlich machen. Die Anzahl der mit der Datenverarbeitung beschäftigten Personen ist unerheblich, wenn die Pflicht bereits wegen Art und Umfang der Verarbeitung im Rahmen der Kerntätigkeit besteht.

Die Kerntätigkeit ist die Haupttätigkeit eines Unternehmens, die es untrennbar prägt. Entsprechend Erwägungsgrund 97 DS-GVO gehören zu den Kerntätigkeiten alle Vorgänge, die fester Bestandteil der Haupttätigkeit des Unternehmens sind. Dies meint die wichtigsten Arbeitsabläufe, die zur Erreichung der Ziele des Verantwortlichen oder des Auftragsverarbeiters erforderlich sind. Die Haupttätigkeit der

nicht öffentlichen Stelle muss zur Erfüllung des Artikels 37 Absatz 1 Buchstabe b DS-GVO auf die Überwachung natürlicher Personen gerichtet sein. Diese Überwachung muss fortlaufend oder wiederholt (regelmäßig), einer Strategie folgend bzw. methodisch (systematisch) sein und viele Personen oder große Mengen an personenbezogenen Daten betreffen oder zeitlich bedeutend oder geografisch ausgedehnt (umfangreich) sein (vgl. zu diesen und weiteren Erfordernissen Nr. 2.1.3 in WP 243 rev.01). Beispiele für eine solche Überwachung von Personen und damit Auslöser für die Pflicht zur Benennung einer Datenschutzbeauftragten bzw. eines Datenschutzbeauftragten sind das personenbezogene Nachvollziehen von Internetaktivitäten, die Erstellung von Profilen und das Betreiben einer Auskunft, einer Detektei oder einer Partnervermittlung.³

1.3 Nicht öffentliche Stellen – umfangreiche Verarbeitung besonderer Kategorien von Daten im Rahmen der Kerntätigkeit

Nach Artikel 37 Absatz 1 Buchstabe c DS-GVO haben nicht öffentliche Stellen ebenfalls eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten zu benennen, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DS-GVO besteht.

Besondere Kategorien personenbezogener Daten sind gemäß Artikel 9 DS-GVO die rassische und ethnische Herkunft, die politische Meinung, die religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit. Ebenfalls hierunter fallen die genetischen und biometrischen Daten zur Identifizierung einer natürlichen Person sowie sämtliche Gesundheitsdaten und Daten zur sexuellen Orientierung einer Person. Die Begrifflichkeiten „genetische Daten“, „biometrische Daten“ und „Gesundheitsdaten“ werden in Artikel 4 Nummer 13 bis 15 DS-GVO legaldefiniert.

Die Kerntätigkeit meint auch hierbei wieder die in diesem Zusammenhang stehenden wichtigsten Arbeitsabläufe, die zur Erreichung des Ziels erforderlich sind. Hinsichtlich der Kerntätigkeit wird auf die Ausführungen unter Punkt 1.2 verwiesen. Klassische Beispiele für Kerntätigkeiten, die in der Verarbeitung besonderer Kategorien von Daten liegen, sind bei Ärztinnen bzw. Ärzten oder Physiotherapeutinnen bzw. Physiotherapeuten zu finden. Sie verarbeiten personenbezogene Daten ihrer Patientinnen bzw. Patienten, um Diagnosen und ggf. Medikationen etc. nachhalten und die Behandlungsleistungen abrechnen zu können. Damit gehört die Datenverarbeitung untrennbar zur Behandlungstätigkeit und folglich zur Kerntätigkeit. Die Anzahl der mit der Datenverarbeitung beschäftigten Personen ist unerheblich, sofern umfangreich besondere Kategorien von Daten verarbeitet werden. Insbesondere Kliniken und Abrechnungsdienste dürfte die Benennungspflicht nach Artikel 37 Absatz 1 Buchstabe c DS-GVO treffen.

Ob eine Verarbeitung als umfangreich zu klassifizieren ist, hängt von verschiedenen Faktoren ab. Ausschlaggebend ist die Menge der verarbeiteten personenbezogenen Daten, ob eine Verarbeitung auf regionaler, nationaler oder supranationaler Ebene erfolgt (geografischer Aspekt), die Anzahl der betroffenen Personen (absolute Zahl oder in Prozent zur relevanten Bezugsgröße) und die Dauer der Verarbeitung (zeitlicher Aspekt), siehe schon Punkt 1.2. Sind mehrere Faktoren als hoch zu bewerten, so spricht dies für eine umfangreiche Verarbeitung. Hierbei ist auch Erwägungsgrund 91 DS-GVO ergänzend zu be-

3 Kühling/Buchner, DS-GVO/BDSG, 3. Auflage 2020, Art. 37 Rn. 20, 23 mit weiteren Nachweisen.

achten, wonach eine Verarbeitung von Patienten- oder Mandantendaten durch eine einzelne Ärztin bzw. einen einzelnen Arzt, sonstige Angehörige eines Gesundheitsberufs oder eine Rechtsanwältin bzw. einen Rechtsanwalt regelmäßig keine die Benennungspflicht auslösende umfangreiche Datenverarbeitung darstellt. Anders verhält es sich hingegen, wenn die Praxis eine hohe, über das für vergleichbare Praxen übliche Maß deutlich hinausgehende Menge an personenbezogenen Daten verarbeitet.

Die Frage, ob die Kerntätigkeit in der umfangreichen Verarbeitung von sensiblen personenbezogenen Daten besteht, ist nicht immer eindeutig zu klären. Im Zweifel empfiehlt sich die (freiwillige) Benennung einer Datenschutzbeauftragten bzw. eines Datenschutzbeauftragten, um präventiv einer Verletzung der Pflichten nach der Datenschutz-Grundverordnung vorzubeugen.

1.4 Nicht öffentliche Stellen – mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt

Soweit sich in einer nicht öffentlichen Stelle in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, ist die nicht öffentliche Stelle nach § 38 Absatz 1 Satz 1 BDSG verpflichtet, unabhängig von Art und Umfang der verarbeiteten personenbezogenen Daten, eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten zu benennen. Hinsichtlich der Personenzahl hat der Gesetzgeber zur Entlastung kleinerer Unternehmen und Vereine die Personenzahl im Jahr 2019 von 10 auf 20 Personen erhöht. Sofern bereits zuvor eine Datenschutzbeauftragte bzw. ein Datenschutzbeauftragter benannt war, empfiehlt es sich, diese bzw. diesen beizubehalten, auch wenn die Personenzahl nunmehr unterschritten wird. Dies dient schließlich auch der Entlastung der verantwortlichen Stelle in Bezug auf datenschutzrechtliche Fragestellungen.

Die Wortwahl „in der Regel“ meint, dass die beschäftigte Personenanzahl auf Dauer nicht unterschritten wird. Kurzzeitige Schwankungen bleiben hierbei unberücksichtigt.

Der Begriff „ständig“ ist weit auszulegen. Lediglich dann, wenn bei Beschäftigten die Datenverarbeitung einen völlig untergeordneten Anteil der auszuübenden Tätigkeit einnimmt, müssen diese nicht hinzugechnet werden.

„Beschäftigte Personen“ sind nicht nur fest oder befristet Angestellte, sondern beispielsweise auch Praktikantinnen bzw. Praktikanten, freie Mitarbeiterinnen bzw. Mitarbeiter, Leiharbeiterinnen bzw. Leiharbeiter, Volontärinnen bzw. Volontäre und Auszubildende. Dabei ist es irrelevant, ob es sich um Voll- oder Teilzeitbeschäftigte handelt. Angehörige der Geschäftsleitung werden hiervon jedoch nicht erfasst.

Auch der Begriff „automatisierte Verarbeitung“ ist weit zu verstehen und erfasst jede Form der Verarbeitung mittels des gesteuerten, selbständig ablaufenden, technisch unterstützten Verfahrens einer Datenverarbeitungsanlage, wie beispielweise PC, Smartphone, Scanner etc.

Zwar sollen durch das Erfordernis, dass mindestens 20 Personen mit der Datenverarbeitung beschäftigt sein müssen, kleinere Unternehmen der Privatwirtschaft grundsätzlich hinsichtlich ihres bürokratischen Aufwandes entlastet werden. Dennoch empfiehlt es sich, bei Unsicherheiten auch ohne eine gesetzliche Verpflichtung eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten zu benennen, auszubilden bzw. zu schulen und der Person feste Aufgaben, die die Verarbeitung personenbezogener Daten betreffen, aufzuerlegen, um präventiv der Verletzung des Schutzes personenbezogener Daten vorzubeu-

gen. Auch wenn keine Datenschutzbeauftragte bzw. kein Datenschutzbeauftragter zwingend zu benennen ist, sind Verantwortliche bzw. Auftragsverarbeiter zur Einhaltung sämtlicher datenschutzrechtlicher Regelungen verpflichtet (siehe hierzu im Einzelnen Punkt 3.7).

1.5 Nicht öffentliche Stellen – Erfordernis einer Datenschutz-Folgenabschätzung

Unabhängig von der Anzahl der mit der Datenverarbeitung beschäftigten Personen müssen nicht öffentliche Stellen eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten gemäß § 38 Absatz 1 Satz 2 BDSG benennen, wenn die nicht öffentliche Stelle eine automatisierte Verarbeitung vornimmt, die gemäß Artikel 35 DS-GVO eine Datenschutz-Folgenabschätzung erfordert.

Gemäß Artikel 35 Absatz 1 DS-GVO muss eine Datenschutz-Folgenabschätzung dann durchgeführt werden, wenn nach der Art, dem Umfang, den Umständen und den Zwecken der Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Wann dies im Einzelfall gegeben ist, lässt sich Artikel 35 Absatz 3 DS-GVO sowie der nach Artikel 35 Absatz 4 DS-GVO seitens der Aufsichtsbehörde erstellten und veröffentlichten Liste von Verarbeitungsvorgängen entnehmen. Diese Liste ist auf unserer Seite [Auslegungshilfen der Landesbeauftragten](#) hinterlegt. Im Zweifel kann darüber hinaus bei der Aufsichtsbehörde nachgefragt werden.

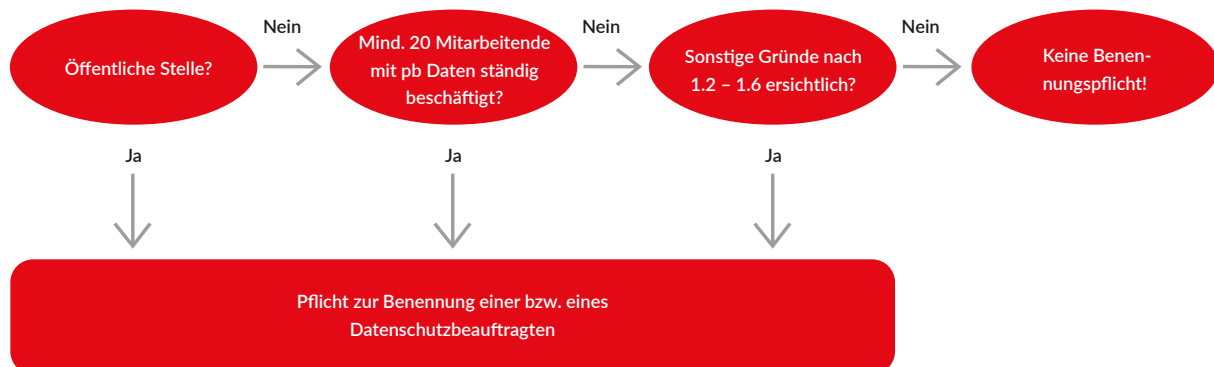
Auch die [Leitlinien zur Datenschutz-Folgenabschätzung \(DSFA\) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“](#) der Artikel-29-Datenschutzgruppe enthält hierzu hilfreiche Ausführungen. Die Fallkonstellationen, in denen eine Datenschutz-Folgenabschätzung erforderlich ist, decken sich weitgehend mit den in Artikel 37 Absatz 1 Buchstabe b und c DS-GVO ohnehin niedergeschriebenen Verpflichtungen, eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten zu benennen. Dennoch soll § 38 Absatz 1 Satz 2 BDSG als Auffangtatbestand für diejenigen Fälle dienen, die nicht schon von den Regelungen des Artikels 37 Absatz 1 Buchstabe b und c DS-GVO erfasst sind. Der Inhalt der Datenschutz-Folgenabschätzung richtet sich im Übrigen nach Artikel 35 Absatz 7 DS-GVO.

1.6 Nicht öffentliche Stellen – geschäftsmäßige Verarbeitung zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung

Zuletzt haben nicht öffentliche Stellen, die personenbezogene Daten zum Zweck der (ggf. anonymisierten) Übermittlung oder zum Zweck der Markt- und Meinungsforschung automatisiert verarbeiten, zwingend eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten zu benennen. Dies ergibt sich aus § 38 Absatz 1 Satz 2 BDSG.

Hierunter fallen beispielsweise Marktforschungsinstitute und Auskunfteien. Grund für diese doch sehr allgemeine Regelung ist die hohe Zahl der verarbeiteten personenbezogenen Daten und die sehr risikoreiche Verarbeitung durch Übermittlung der Daten.

1.7 Muster zur Prüfung, ob eine Benennungspflicht besteht



Vorlage der Darstellung entnommen aus Kühling/Klar/Sackmann – Datenschutzrecht, 4. Auflage, S. 288.

2 Auswahlkriterien für die Benennung von Datenschutzbeauftragten

Gemäß Artikel 37 Absatz 5 DS-GVO/§ 31 Absatz 1 BbgPJMDSG sind an die Auswahl der bzw. des Datenschutzbeauftragten bestimmte Anforderungen zu stellen. Hierbei spielen die berufliche Qualifikation und insbesondere das datenschutzrechtliche Fachwissen sowie die Fähigkeit/Eignung, die ihr bzw. ihm obliegenden Aufgaben nach Artikel 39 DS-GVO/§ 33 BbgPJMDSG zu erfüllen, eine Rolle. Datenschutzbeauftragte müssen in der Lage sein, die sie benennende Stelle und deren Beschäftigte, die mit der Verarbeitung personenbezogener Daten befasst sind, hinsichtlich ihrer Pflichten zu unterrichten und zu beraten. Die Gesetzeslage sieht vor, dass Datenschutzbeauftragte, unabhängig davon, ob sie für eine öffentliche oder eine nicht öffentliche Stelle benannt werden, hinreichend qualifiziert sein sollen. Das erforderliche Niveau des Fachwissens sollte sich hierbei insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die vom Verantwortlichen verarbeiteten personenbezogenen Daten richten, vgl. Erwägungsgrund 93 Satz 2 DS-GVO. Damit wird ein risikobasierter Ansatz verfolgt: Je schutzbedürftiger die Daten sind, desto höhere Anforderungen sind an die Qualifikation und Fachkunde der bzw. des Datenschutzbeauftragten zu stellen. Die Person sollte in der Regel zum Zeitpunkt der Benennung mit dem Datenschutzrecht bereits vertraut sein. Sollte dies in Ausnahmefällen nicht (vollständig) realisierbar sein, muss sich das notwendige Wissen durch entsprechende Schulungen zeitnah nach der Benennung angeeignet werden.

Es empfiehlt sich, eine Person auszuwählen, die mit den internen Abläufen, Funktionen und Strukturen der Stelle vertraut ist. Ihr muss bekannt sein, welche Aufgaben Datenschutzbeauftragten nach Artikel 39 DS-GVO/§ 33 BbgPJMDSG zukommen, und sie muss befähigt sein, diese Aufgaben zu erfüllen. Neben dem datenschutzrechtlichen Fachwissen sind hierfür sowohl Zuverlässigkeit als auch die Fähigkeit der konstruktiven Zusammenarbeit und – im Fall von Datenschutzverletzungen – die Bereitschaft zur Konfrontation mit der Geschäftsleitung vonnöten.⁴ Dies erfordert eine hohe Sozialkompetenz.

4 Vergleiche Kühling/Buchner, DS-GVO/BDSG, 3. Auflage 2020, Art. 37 Rn. 35 mit weiteren Nachweisen.

3 Benennung interner oder externer Datenschutzbeauftragter

Der Verantwortliche sollte zur besseren Nachweisbarkeit eine Benennungsurkunde erstellen. Diese sollte gewisse Mindestregelungen treffen und den Zeitraum der Beauftragung festlegen. Die bzw. der Datenschutzbeauftragte sollte die Benennung auf der Benennungsurkunde schriftlich bestätigen. Datenschutzbeauftragte können gemäß Artikel 37 Absatz 6 DS-GVO prinzipiell sowohl Beschäftigte der öffentlichen oder nicht öffentlichen Stelle sein (interne Datenschutzbeauftragte) als auch auf Grundlage eines Dienstleistungsvertrags für öffentliche und nicht öffentliche Stellen tätig werden (externe Datenschutzbeauftragte).

Im Anwendungsbereich des Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetzes ist eine Benennung externer Datenschutzbeauftragter allerdings nicht gestattet, da § 31 Absatz 1 BbgPJMDSG ausschließlich von „Bediensteten“ der Behörde spricht.

3.1 Zeitpunkt der Benennung

Gesetzlich sind keine Benennfristen normiert. Die Benennung hat daher unverzüglich mit Entstehung der Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragten zu erfolgen. Die Dauer der Benennung legt der Verantwortliche fest. Es ist sowohl eine befristete als auch unbefristete Benennung möglich.⁵

3.2 Benennung im Rahmen einer Arbeitnehmerüberlassung und Möglichkeit der Befristung

Eine Benennung der bzw. des Datenschutzbeauftragten im Rahmen einer Arbeitnehmerüberlassung ist grundsätzlich im Rahmen der Anwendbarkeit des Arbeitnehmerüberlassungsgesetzes (AÜG) möglich, sofern kein Ausschluss nach § 1 Absatz 3 AÜG o. Ä. vorliegt. Es gilt zu beachten, dass gemäß § 1 Absatz 1 Buchstabe b AÜG eine Leiharbeit nur für den Zeitraum von 18 Monaten möglich ist.

Die Wahrnehmung der Funktion der bzw. des Datenschutzbeauftragten kann im Rahmen einer befristeten Anstellung oder über einen fest bestimmten Zeitraum erfolgen. Hierbei sollte jedoch der Grundgedanke beachtet werden, dass sich eine Befristung nicht immer anbietet. Denn Datenschutzbeauftragte sollten fest im Unternehmen integriert sein und zu ihrer Person sollte ein Vertrauensverhältnis bestehen, das sich ggf. erst nach einer gewissen Zeitspanne aufbaut. Zudem sollten Datenschutzbeauftragte mit den internen Abläufen vertraut sein; auch unterliegen sie im Rahmen ihrer beruflichen Tätigkeit einem gewissen Kündigungsschutz. Unter Berücksichtigung dieser Umstände ist es vorzugswürdig, eine Person langfristig mit der Funktion der bzw. des Datenschutzbeauftragten zu betrauen. Insbesondere die Kenntnis der internen Abläufe dürfte ausschlaggebend für eine erfolgreiche Aufgabenerfüllung sein. Eine Arbeitnehmerüberlassung ist daher zwar nicht der geeignetste, aber dennoch ein gangbarer Weg.

⁵ Vergleiche dazu 3.2.

3.3 Benennung einer juristischen Person als externe Datenschutzbeauftragte

Die Benennung einer juristischen Person als externe Datenschutzbeauftragte ist gesetzlich nicht geregelt, allerdings möglich, sofern folgende Kriterien, die in Nr. 5.7 in WP 243 rev.01 dargelegt sind, erfüllt werden:

- Alle Mitarbeiterinnen und Mitarbeiter der juristischen Person, welche die Aufgaben der bzw. des Datenschutzbeauftragten wahrnehmen, müssen die in der Datenschutz-Grundverordnung vorgesehenen Anforderungen erfüllen.
- Es hat im Dienstleistungsvertrag eine klare Aufgabenverteilung innerhalb des externen Datenschutzbeauftragten-Teams zu erfolgen.
- Eine einzelne Person ist als primäre Ansprechperson für die verantwortliche Stelle und die Kundinnen und Kunden zu benennen.

Gemäß § 31 Absatz 1 BbgPJMDSG können nur Bedienstete die Rolle der bzw. des Datenschutzbeauftragten bekleiden. Eine juristische Person kann an dieser Stelle folglich nicht benannt werden.

3.4 Veröffentlichung der Kontaktdaten der bzw. des Datenschutzbeauftragten

Gemäß Artikel 37 Absatz 7 DS-GVO sind die Kontaktdaten der bzw. des Datenschutzbeauftragten zu veröffentlichen. Zu den Kontaktdaten zählen die Anschrift und Kontaktmöglichkeiten via Telefon oder E-Mail. Handelt es sich um interne Datenschutzbeauftragte, ist für deren postalische Erreichbarkeit die Anschrift der verantwortlichen Stelle anzugeben.

Der Name der bzw. des Datenschutzbeauftragten zählt nicht zu den Kontaktdaten, die verpflichtend anzugeben sind. Es empfiehlt sich oftmals, diesen dennoch anzugeben, da das Vertrauen der Beschwerdeführerinnen und Beschwerdeführer hierdurch gestärkt wird und sie sich dann eher geneigt sehen, das Unternehmen oder die Behörde über die bzw. den Datenschutzbeauftragten zu konsultieren, anstatt sich direkt an die Aufsichtsbehörde zu wenden. Die Entscheidung, ob die Angabe des Namens als Kontaktdaten unter den gegebenen Umständen erforderlich oder hilfreich ist, liegt im Ermessen der verantwortlichen Stelle.

Da Datenschutzbeauftragte die entscheidende Kontaktperson sowohl für datenschutzrechtliche Anfragen von Beschäftigten der verantwortlichen Stelle als auch von externen Personen sind, genügt ein Aushang ihrer Kontaktdaten im Eingangsbereich der Behörde oder des Unternehmens nicht. Vielmehr empfiehlt sich eine gut sichtbare Veröffentlichung der Kontaktdaten auf der Internetseite, beispielsweise im Rahmen der Datenschutzerklärung.

Im Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz ist eine Veröffentlichung der Kontaktdaten der bzw. des Datenschutzbeauftragten nicht vorgesehen. Sie empfiehlt sich aus den o. g. Gründen aber auch in diesem Bereich.

3.5 Meldung der Kontaktdaten an die Aufsichtsbehörde

Gemäß Artikel 37 Absatz 7 DS-GVO teilen Verantwortliche oder Auftragsverarbeiter die Kontaktdaten der bzw. des Datenschutzbeauftragten der Aufsichtsbehörde mit. Diese Meldung kann gegenüber der Landesbeauftragten über ein speziell eingerichtetes [Online-Formular](#) erfolgen.

Die Mitteilungspflicht gegenüber der Aufsichtsbehörde liegt nach Artikel 37 Absatz 7 DS-GVO bei den Verantwortlichen bzw. Auftragsverarbeitern. Daher ist eine Meldung allein durch die bzw. den Datenschutzbeauftragten nach dem Wortlaut der Verordnung nicht ausreichend, um die Pflicht der verantwortlichen Stelle zu erfüllen. Die verantwortliche Stelle kann ihre Verpflichtung aber an die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten delegieren, sodass eine Meldung im Auftrag und in Vollmacht der verantwortlichen Stelle möglich ist. Gegenüber der Aufsichtsbehörde ist aufgrund der direkten Kontaktaufnahme die Nennung des Namens der bzw. des Datenschutzbeauftragten wünschenswert, wenn auch vom Gesetz nicht gefordert.

Auf dem Meldeformular sind die E-Mail-Adresse oder Telefonnummer der bzw. des Datenschutzbeauftragten anzugeben sowie die Anschrift, sollte diese von derjenigen der meldepflichtigen Stelle abweichen.

Gemäß § 31 Absatz 3 BbgPJMDSG ist bei der Meldung durch Polizei-, sowie Justizvollzugs- und Maßregelvollzugsbehörden auch der Name der bzw. des Datenschutzbeauftragten verpflichtend mit anzugeben.

3.6 Stellung der bzw. des Datenschutzbeauftragten

Datenschutzbeauftragte berichten gemäß Artikel 38 Absatz 3 Satz 3 DS-GVO unmittelbar der höchsten Managementebene der verantwortlichen Stelle. Aus dieser Stellung ist aber nicht die Notwendigkeit abzuleiten, die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten der höchsten Managementebene direkt zu unterstellen. Datenschutzbeauftragte können rein organisatorisch einer anderen Abteilung im Unternehmen unter- bzw. zugeordnet sein, solange sich diese Ordnung nicht auf die direkte Berichtsmöglichkeit zur höchsten Managementebene auswirkt.⁶ Dennoch empfiehlt sich eine direkte Unterstellung unter die höchste Managementebene, um die besondere Autorität der bzw. des Datenschutzbeauftragten auch im Organigramm abbilden zu können.⁷

Hierbei ist hervorzuheben, dass Datenschutzbeauftragte gemäß Artikel 38 Absatz 3 Satz 1 DS-GVO/§ 32 Absatz 3 BbgPJMDSG in der Ausübung ihrer Aufgaben keiner Weisung durch die sie benennende Stelle unterliegen. Aufgrund der Weisungsfreiheit der bzw. des Datenschutzbeauftragten ist eine inhaltliche Beeinflussung bezüglich der Ausübung der Aufgaben durch die verantwortliche Stelle untersagt.

Die verantwortliche Stelle muss es der bzw. dem Datenschutzbeauftragten zudem gemäß Artikel 38 Absatz 2 DS-GVO/§ 32 Absatz 2 BbgPJMDSG ermöglichen, datenschutzrechtliche Kenntnisse durch Schulungen und Weiterbildungen zu erlangen und zu vertiefen. Ein weiteres wichtiges Merkmal ist, dass Datenschutzbeauftragten Zugang zu allen personenbezogenen Daten und den damit verbundenen Verarbeitungsvorgängen zu gewähren ist.

⁶ BeckOK DatenschutzR/Moos, 33. Edition 1. November 2019, DS-GVO Art. 38 Rn. 26 mit weiteren Nachweisen.

⁷ Kühling/Buchner, DS-GVO/BDSG, 3. Auflage 2020, Art. 38, Rn. 25 mit weiteren Nachweisen.

3.7 Freiwillige Benennung von Datenschutzbeauftragten

Auch wenn keine Benennungspflicht besteht, kann eine Datenschutzbeauftragte bzw. ein Datenschutzbeauftragter gemäß Artikel 37 Absatz 4 DS-GVO i. V. m. § 38 Absatz 2 BDSG durch die verantwortliche Stelle benannt werden. Hierbei sind die Anforderungen des Kapitels IV Abschnitt 4 DS-GVO gleichermaßen zu berücksichtigen wie bei der verpflichtenden Benennung. Einzige Ausnahme hiervon ist das Privileg des Kündigungsschutzes: Nach § 38 Absatz 2 BDSG findet der Kündigungsschutz nach § 6 Absatz 4 BDSG bei freiwillig benannten Datenschutzbeauftragten keine Anwendung.

4 Interessenkonflikte

Gemäß Artikel 38 Absatz 6 DS-GVO darf die Aufgabenübernahme der bzw. des Datenschutzbeauftragten nicht im Interessenkonflikt mit einer anderweitig übernommenen Aufgabe bei der verantwortlichen Stelle stehen. Dies ist insbesondere bei der Benennung intern bereits beschäftigter Personen zu berücksichtigen.

Im Wesentlichen besteht ein Interessenkonflikt immer dann, wenn Datenschutzbeauftragte sich selbst kontrollieren müssten. Dies kann beispielsweise dadurch geschehen, dass sie Aufgaben als beschäftigte Person in der verantwortlichen Stelle wahrnehmen, die die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen. Dies ist häufig in Leitungspositionen der Fall. Da sie in ihrer anderen Rolle als Datenschutzbeauftragte gemäß Artikel 38 Absatz 2 DS-GVO alle Datenverarbeitungen der verantwortlichen Stelle kontrollieren können, würde dies zu einer Überprüfung ihrer eigenen Arbeit als beschäftigte Person der verantwortlichen Stelle führen. Die hierfür erforderliche Objektivität ist zumindest fraglich. Vor einer Beauftragung sollte daher immer geprüft werden, ob eine Interessenkollision durch Ausschluss verschiedener Aufgabenbereiche verhindert werden kann.

Ein möglicher Interessenkonflikt nach Artikel 38 Absatz 6 DS-GVO kann entstehen, wenn Datenschutzbeauftragte gleichzeitig als Leiterin bzw. Leiter der Personalabteilung eingesetzt würden. Bei Mitarbeiterinnen und Mitarbeitern in hierarchisch nachgeordneten Positionen ist die Frage möglicher Interessenkonflikte hingegen im Einzelfall zu prüfen und kann nicht pauschal beantwortet werden.

Ebenso ist ein Interessenkonflikt bei Personen anzunehmen, die die IT-Abteilung leiten oder Administrationstätigkeiten ausüben und damit Einfluss auf die Verarbeitung der personenbezogenen Daten haben. Doch auch die Geschäftsführung, die schließlich durch die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten beraten werden soll, die Gesellschafterinnen und Gesellschafter eines Unternehmens und nahe Angehörige der Geschäftsführung scheiden als Datenschutzbeauftragte in der Regel aus. In diesen Fällen liegt ein wirtschaftliches Interesse der bzw. des Datenschutzbeauftragten am Unternehmenserfolg nahe, sodass auch hier die Objektivität ihrer bzw. seiner Arbeit gefährdet sein kann.

4.1 IT-Sicherheitsbeauftragte

Wie oben dargelegt, ist ein Interessenkonflikt anzunehmen, sofern gleichzeitig zur Funktion der bzw. des Datenschutzbeauftragten administrative Aufgaben in der IT wahrgenommen werden.

Dies bezieht sich insbesondere auf die Fallkonstellation, in denen sich die Aufgaben der bzw. des IT-Sicherheitsbeauftragten mit den durch die bzw. den Datenschutzbeauftragten zu prüfenden Verarbeitungspersonenbezogener Daten überschneiden. Dann ist die Besetzung der bzw. des IT-Sicherheitsbeauftragten und der bzw. des Datenschutzbeauftragten in Personalunion regelmäßig als Interessenkonflikt zu bewerten. Dies wird insbesondere an der Aufgabe der bzw. des IT-Sicherheitsbeauftragten, ein Sicherheitskonzept zu verfassen, das die bzw. der Datenschutzbeauftragte anschließend überprüfen muss, deutlich.

Eine mögliche Besetzung beider Ämter in Personalunion ist zwar denkbar, wenn voraussehbare Konflikte durch konkrete Aufgabenübertragungen an Dritte vermieden werden. Hierbei ist jedoch zu berücksichtigen, dass der Aufgabenkatalog der Datenschutzbeauftragten unionsrechtlich vorgegeben und damit unabdingbar ist. Aufgaben können nur an anderer Stelle, d. h. bei der bzw. dem IT-Sicherheitsbeauftragten verschoben werden. Zudem sollten die Schnittstellen zwischen beiden Rollen klar definiert und dokumentiert werden sowie auf beiden Seiten Berichtswege zur Leitungsebene existieren. Daneben muss die bzw. der IT-Sicherheitsbeauftragte ausreichend Ressourcen zur Erfüllung beider Aufgaben besitzen.⁸

4.2 Betriebsrats- bzw. Personalratsmitglied

Eine weitere Problemstellung ist eröffnet, wenn ein Personalrats- oder Betriebsratsmitglied im eigenen Haus gleichzeitig die Rolle der bzw. des Datenschutzbeauftragten übernehmen soll. Der Interessenkonflikt resultiert u. a. daraus, dass auch die Datenverarbeitung des Personal- oder Betriebsrats der Kontrolle der bzw. des Datenschutzbeauftragten unterliegt.

Mitgliedern des Personal- bzw. Betriebsrates stehen Mitbestimmungsrechte im Personalwesen zu. Sie sind auch in Personalentscheidungen eingebunden.

Das Mitglied eines Betriebsrates unterliegt gemäß § 79 Betriebsverfassungsgesetz (BetrVG) einer strengen Geheimhaltungspflicht. Hieraus kann sich eine Vielzahl von Interessenkollisionen ergeben. Ein Beispiel ist, dass Datenschutzbeauftragte gemäß Artikel 38 Absatz 2 DS-GVO zur Kontrolle aller Datenverarbeitungen befugt sind. Hiervon sind auch die Datenverarbeitungen des Betriebsrats umfasst. Darüber hinaus muss die verantwortliche Stelle ihnen den Zugang zu personenbezogenen Daten zur Verfügung stellen, was auch ein umfassendes Einsichtsrecht in Personalakten ermöglicht. Ein solches Einsichtsrecht steht dem Betriebsrat gemäß § 83 Absatz 1 Satz 2 BetrVG nur mit Einwilligung der betroffenen Person zu. Datenschutzbeauftragte müssten sich somit nicht nur im Rahmen der eigenen Datenverarbeitung selbst kontrollieren, sondern auch Informationen, die sie in ihrer Eigenschaft als Datenschutzbeauftragte erhalten haben, in der Funktion als Betriebsratsmitglied wieder vergessen. Aus diesem weitergehenden Umgang mit Personalaktendaten können sich somit Interessenkonflikte ergeben.

Eine Interessenkollision besteht aus den gleichen Gründen bei einer Personalunion von Personalratsmitglied und der bzw. dem Datenschutzbeauftragten. Die Rechte des Personalrats nach §§ 63 bis 69 Personalvertretungsgesetz für das Land Brandenburg (PersVG) eröffnen diesem einen weiten Zugriff auf und Umgang mit personenbezogenen Daten der Mitarbeiterinnen und Mitarbeiter. Ebenso wie beim Betriebsrat stehen dem Personalrat Einsichtsrechte in die Personalakten aber nur mit Einwilligung der be-

⁸ Siehe Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-2, IT-Grundschutz-Methodik“, Version 1.0, S. 42f.

troffenen Person gemäß § 60 Absatz 3 Satz 2 PersVG zu. Datenschutzbeauftragte hingegen können nach Artikel 38 Absatz 2 DS-GVO von der verantwortlichen Stelle im Rahmen ihrer Aufgabenerfüllung Zugang zu allen personenbezogenen Daten verlangen und somit auch Einsicht in die Personalakten erhalten. Zudem können Datenschutzbeauftragte die Datenverarbeitung des Personalrats nach § 94 Absatz 1 PersVG uneingeschränkt kontrollieren, was zu einer Kontrolle der eigenen Arbeit führen würde.

5 Ressourcen der Datenschutzbeauftragten

Verantwortliche und Auftragsverarbeiter sollen die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten gemäß Artikel 38 Absatz 2 DS-GVO/§ 32 Absatz 2 Brandenburgisches Polizei- Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) bei der Erfüllung der Aufgaben aus Artikel 39 DS-GVO/§ 33 BbgPJMDSG unterstützen. Diese Unterstützungspflicht umfasst auch die Bereitstellung von Ressourcen. Ressourcen können zum einen materieller Natur sein, wie beispielsweise Hilfspersonal, EDV-Anlagen, Einrichtungen, Gerätschaften, Literatur und sonstige Mittel, die zur Aufgabenerfüllung und Erlangung von Fachwissen erforderlich sind. Auch die Bereitstellung geeigneter Räumlichkeiten ist hierunter zu fassen. Damit Datenschutzbeauftragte ihre Geheimhaltungspflicht gemäß Artikel 38 Absatz 5 DS-GVO einhalten können, ist es erforderlich, dass sie zumindest zeitweise auf ein ausschließlich durch sie genutztes Büro oder andere geeignete Räumlichkeiten, wie einen Besprechungsraum, zurückgreifen können. Insbesondere in größeren Organisationen sollte zudem die Einrichtung eines ganzen Datenschutzteams, das der bzw. dem Datenschutzbeauftragten bei der Erfüllung der Aufgaben behilflich ist, angestrebt werden.

Zum anderen sind Datenschutzbeauftragten Fortbildungen zur Erhaltung ihres Fachwissens zu gewähren und es muss ihnen genügend Zeit für die Erfüllung der Aufgaben eingeräumt werden. Dies kann bedeuten, dass je nach Umfang der Tätigkeit und Ausgestaltung des Unternehmens oder der Behörde eine Vollzeitstelle für die Erfüllung der Aufgaben der bzw. des Datenschutzbeauftragten zu schaffen ist. Wir empfehlen in jedem Fall, Datenschutzbeauftragten die Rolle nicht als sogenanntes „Rucksackprojekt“ zu übertragen, sondern zu überprüfen, welche Kapazitäten ihnen realistisch zur Verfügung stehen. Eine Anstellung in Vollzeit ist zumindest in größeren Institutionen erstrebenswert.

6 Benennung mehrerer Datenschutzbeauftragter für einen Verantwortlichen

Bereits der Gesetzeswortlaut führt in Artikel 37 Absatz 1 DS-GVO/§ 31 Absatz 1 BbgPJMDSG aus, dass die verantwortliche Stelle „einen“ Datenschutzbeauftragten bzw. „eine“ Datenschutzbeauftragte zu benennen hat. Für eine einzige Person spricht auch die Stellung der bzw. des Datenschutzbeauftragten nach Artikel 38 DS-GVO/§ 32 BbgPJMDSG. Datenschutzbeauftragte dienen als konkrete Anlaufstelle für alle datenschutzrechtlichen Fragen. Sie sind in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden und in ihrer Aufgabenerfüllung weisungsunabhängig. Zu diesen Grundsätzen würde es im Widerspruch stehen, wenn zwei Personen gleichzeitig als Datenschutzbeauftragte auftreten. Auch die Einrichtung eines Datenschutzteams hat nicht zur Folge, dass mehrere Personen Datenschutzbeauftragte werden. Vielmehr wird das Team zur Unterstützung der bzw. des Datenschutzbeauftragten eingesetzt.

Unabhängig hiervon sollte aber die Benennung einer Stellvertretung für Zeiten der Abwesenheit der bzw. des Datenschutzbeauftragten (beispielsweise wegen Urlaubs oder Krankheit) erfolgen. Die Rechte der Stellvertretung sind jedoch abgeschwächt, sofern die Vertretungssituation nicht eintritt, da die Benennung einer bzw. eines stellvertretenden Datenschutzbeauftragten gesetzlich nicht erforderlich ist. Insofern gelten in diesem Fall die gleichen Vorgaben wie bei einer bzw. einem freiwillig benannten Datenschutzbeauftragten. Tritt der Vertretungsfall ein, genießt die Stellvertretung den gleichen Schutz wie die bzw. der Datenschutzbeauftragte (vgl. Punkt 9). Die Stellvertretung nimmt im Vertretungsfall die gleichen Aufgaben wahr.

Von der obigen Regel, dass zwei Personen nicht „gleichrangig“ als Datenschutzbeauftragte benannt werden können, kann eine Ausnahme gemacht werden, wenn die Aufgabenbereiche klar voneinander getrennt sind – etwa wenn unterschiedliche Gesetze, die unterschiedliche Datenverarbeitungen regeln, jeweils die Benennung einer bzw. eines Datenschutzbeauftragten verlangen. So kann eine öffentliche Stelle beispielsweise eine Person als Datenschutzbeauftragte bzw. Datenschutzbeauftragten für Datenverarbeitungen, die in den Anwendungsbereich der Datenschutz-Grundverordnung fallen, benennen und daneben eine andere Person als Datenschutzbeauftragte bzw. Datenschutzbeauftragten für Datenverarbeitungen benennen, die in den Anwendungsbereich des Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetzes fallen. Die Stelle muss in diesem Fall für beide Datenschutzbeauftragte die Kontaktdaten veröffentlichen und diese der Aufsichtsbehörde mitteilen.

7 Gemeinsame Datenschutzbeauftragte

Die Benennung einer bzw. eines gemeinsamen Datenschutzbeauftragten durch eine Unternehmensgruppe ist nach Artikel 37 Absatz 2 DS-GVO zulässig, sofern die bzw. der Datenschutzbeauftragte von jeder Niederlassung aus leicht erreicht werden kann. Zu der vom Gesetz verlangten örtlichen Erreichbarkeit kommt hinzu, dass für die Kommunikation mit der bzw. dem Datenschutzbeauftragten keine technischen oder sprachlichen Barrieren bestehen dürfen.

Behörden und andere öffentliche Stellen können nach Artikel 37 Absatz 3 DS-GVO unter Berücksichtigung der Organisationsstruktur und ihrer Größe eine gemeinsame Datenschutzbeauftragte bzw. einen gemeinsamen Datenschutzbeauftragten für Zweigstellen der Behörden oder Stellen benennen.

Auch § 31 Absatz 2 BbgPJMDSG eröffnet den dortigen Verantwortlichen die Möglichkeit, unter Berücksichtigung von Organisationsstruktur und Größe eine gemeinsame Datenschutzbeauftragte bzw. einen gemeinsamen Datenschutzbeauftragten für die Zweigstellen der Behörden oder Stellen zu benennen.

8 Gleichzeitiges Tätigwerden der bzw. des Datenschutzbeauftragten für andere Verantwortliche

Nach Artikel 37 Absatz 6 DS-GVO besteht die Möglichkeit für Verantwortliche im Anwendungsbereich der Datenschutz-Grundverordnung, externe Datenschutzbeauftragte zu benennen, auch wenn diese bereits Datenschutzbeauftragte – gleich, ob intern oder extern – für eine oder mehrere andere Stellen sind. Externe Datenschutzbeauftragte erfüllen ihre Aufgaben auf der Grundlage eines Dienstleistungsvertrags. Dabei müssen sie – ebenso wie interne Datenschutzbeauftragte – die Anforderungen nach Artikel 37 Ab-

satz 5 DS-GVO erfüllen, ihre Stellung muss nach Artikel 38 DS-GVO gesichert werden und sie müssen in der Lage sein, die Aufgaben nach Artikel 39 DS-GVO zu erfüllen. Eine leichte Erreichbarkeit der bzw. des Datenschutzbeauftragten von beiden bzw. allen Standorten aus wird vorausgesetzt.

Da auch externe Datenschutzbeauftragte datenschutzrechtlich als Teil der sie benennenden Verantwortlichen anzusehen sind, muss die Organisation dies innerhalb ihrer Arbeitsabläufe berücksichtigen. Insbesondere dürfen externe Datenschutzbeauftragte nicht selbst als Verantwortliche für diejenigen personenbezogenen Daten agieren, die sie als externe Datenschutzbeauftragte verarbeiten.⁹ Das bedeutet, dass beispielsweise Übermittlungen personenbezogener Daten zwischen dem Verantwortlichen, für den die bzw. der externe Datenschutzbeauftragte auf Grundlage eines Dienstleistungsvertrags tätig wird, und dem eigenen Unternehmen der bzw. des externen Datenschutzbeauftragten nicht möglich sind.

9 Abberufung und Kündigungsschutz

Sind interne Datenschutzbeauftragte eines Unternehmens ordnungsgemäß benannt, ist eine Abberufung nur noch möglich, wenn die Voraussetzungen nach § 38 Absatz 2 BDSG i. V. m. § 6 Absatz 4 Satz 2 BDSG i. V. m. § 626 Bürgerliches Gesetzbuch (BGB) vorliegen. Für interne Datenschutzbeauftragte der Behörden und öffentlichen Stellen des Landes Brandenburg – mit Ausnahme derjenigen im Anwendungsbereich des Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetzes – gilt § 6 Absatz 4 BDSG analog, da das Bundesdatenschutzgesetz mangels Regelungskompetenz auf die Behörden des Landes ansonsten nicht anwendbar ist.

Für die Abberufung interner Datenschutzbeauftragter gelten somit die zivilrechtlichen Regelungen der fristlosen Kündigung aus wichtigem Grund (§ 626 BGB) entsprechend. Als wichtiger Grund ist beispielsweise Diebstahl, physische, psychische oder sexuelle Belästigung oder vergleichbares grobes Fehlverhalten erfasst.¹⁰ Wegen der Erfüllung ihrer Aufgaben dürfen interne Datenschutzbeauftragte aber nicht abberufen werden, vgl. Artikel 38 Absatz 3 Satz 2 DS-GVO/§ 32 Absatz 4 BbgPJMSDG. Es darf also kein Zusammenhang zwischen der Abberufung und der Art und Weise der Aufgabenwahrnehmung bestehen. Es wäre daher unzulässig, interne Datenschutzbeauftragte abzuberaufen, weil sie in datenschutzrechtlichen Belangen anderer Meinung als die Geschäftsleitung sind. Zerwürfnisse zwischen der bzw. dem Datenschutzbeauftragten und der verantwortlichen Stelle scheiden als wichtiger Grund nach § 626 BGB aus.

Interne Datenschutzbeauftragte unterliegen darüber hinaus einem besonderen Kündigungsschutz, der ein Jahr nach Ende ihrer Tätigkeit als Datenschutzbeauftragte nachwirkt. Dies ist selbstverständlich nur dann der Fall, wenn sie zuvor nicht als Vollzeitdatenschutzbeauftragte tätig waren. Ihr Arbeitsverhältnis als Beschäftigte bzw. Beschäftigter der verantwortlichen Stelle darf gemäß § 6 Absatz 4 Satz 2 BDSG in dieser Zeitspanne nicht von dem Verantwortlichen gekündigt werden. Ausnahmen hiervon bestehen nur bei Vorliegen von Tatsachen, die eine Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist rechtfertigen. Mangels entsprechender Rechtsgrundlagen bedeutet eine unbefristete Anstellung interner Vollzeitdatenschutzbeauftragter regelmäßig einen Kündigungsschutz bis zum Eintritt in

⁹ Kühling/Buchner, DS-GVO BDSG, 3. Auflage 2020, Art. 37, Rn. 36 mit weiteren Nachweisen.

¹⁰ Vergleiche die „Leitlinien in Bezug auf Datenschutzbeauftragte („DSB)“, Arbeitspapier WP 243 rev.01, deutsch, Stand: 5. April 2017, der Artikel-29-Datenschutzgruppe Nr. 3. 4.

den Ruhestand. Wird die Funktion niedergelegt (was jederzeit einvernehmlich geschehen kann), haben interne Datenschutzbeauftragte jedoch dem Unternehmen bzw. der Behörde genügend Zeit einzuräumen, eine neue Datenschutzbeauftragte bzw. einen neuen Datenschutzbeauftragten zu benennen.

Bei externen Datenschutzbeauftragten gilt ebenfalls, dass sie nicht aufgrund der Erfüllung ihrer Aufgaben abberufen werden dürfen. Die Schutzvorschrift des § 6 Absatz 4 BDSG, die für den internen Datenschutzbeauftragten gilt, ist für externe Datenschutzbeauftragte aber nicht anwendbar. Für ihre Abberufung und damit der Beendigung des Dienstleistungsvertrags muss demnach kein wichtiger Grund bestehen. Der Wortlaut des § 6 Absatz 4 Satz 1 BDSG differenziert zwar nicht zwischen externen und internen Datenschutzbeauftragten. Es könnte also vertreten werden, dass auch externe Datenschutzbeauftragte nur bei Vorliegen der Voraussetzungen des § 626 BGB (u. a. dem Vorliegen eines wichtigen Grundes) abberufen werden dürfen. Andererseits lässt sich aus der Gesetzesbegründung zum Bundesdatenschutzgesetz entnehmen, dass es sich bei § 6 Absatz 4 BDSG um eine arbeitsrechtliche Regelung handelt.¹¹ Damit soll sie wohl nicht auf externe Datenschutzbeauftragte anwendbar sein, da diese keine Beschäftigten des Verantwortlichen sind. Zudem bestehen Zweifel, ob die Öffnungsklausel des Artikels 37 Absatz 4 DS-GVO für die Benennung von Datenschutzbeauftragten es erlaubt, durch nationales Recht für externe Datenschutzbeauftragte strengere Abberufungsvoraussetzungen zu schaffen.

Bei externen Datenschutzbeauftragten endet das Vertragsverhältnis gleichzeitig mit dem Widerruf der Ernennung durch den Verantwortlichen. Die Niederlegung der Funktion durch externe Datenschutzbeauftragte dürfte regelmäßig mit einer Kündigung des Vertragsverhältnisses einhergehen.

Datenschutzbeauftragte im Anwendungsbereich des Brandenburgischen Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetzes genießen nach § 32 Absatz 4 Satz 2 BbgPJMD SG den gleichen Kündigungsschutz wie Mitglieder des Personalrats. Dies bedeutet, dass ihnen ebenfalls erst nach Ablauf eines Jahres nach Beendigung der Tätigkeit als Datenschutzbeauftragte gekündigt werden darf, es sei denn, es liegt ein wichtiger Grund vor, der die verantwortliche Stelle zur fristlosen Kündigung berechtigt, vgl. § 15 Kündigungsschutzgesetz.

10 Aufgaben und Pflichten der bzw. des Datenschutzbeauftragten

Nach Artikel 39 DS-GVO/§ 33 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMD SG) haben Datenschutzbeauftragte gegenüber der Geschäftsleitung und den Beschäftigten Unterrichts-, Beratungs-, Überwachungs- und Kontrollpflichten. Daneben arbeiten sie mit der Aufsichtsbehörde zusammen, gehen datenschutzrechtlichen Anfragen, Hinweisen und Beschwerden nach und beraten die von der Datenverarbeitung betroffenen Personen. Die gesetzlich genannten Aufgaben sind nicht abschließend.

Im Rahmen ihrer Überwachungspflichten nach Artikel 39 Absatz 1 Buchstabe b DS-GVO/§ 33 Nummer 2 BbgPJMD SG kontrollieren Datenschutzbeauftragte die Einhaltung der Vorschriften der Datenschutz-Grundverordnung/der Rechtsvorschriften zur Umsetzung der JI-Richtlinie sowie die Strategien/Maßnahmen der verantwortlichen Stelle zum Schutz personenbezogener Daten. Hiervon ist die Kontrolle insbesondere der internen Richtlinien und Vorgaben des Verantwortlichen erfasst, die sich auf die Zuweisung

¹¹ Bundestags-Drucksache 18/11325, S. 82.

von Verarbeitungszuständigkeiten sowie Sensibilisierungen und Schulungen des mit der Verarbeitung personenbezogener Daten betrauten Personals beziehen. Sensibilisierungen und Schulungen müssen durch die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten nicht selbst erfolgen. Sie können ihr bzw. ihm von der verantwortlichen Stelle aber als Aufgabe im Rahmen ihrer Kapazitäten übertragen werden. Dies ist wegen ihrer Fachkompetenz und der Kenntnis interner Vorgänge zu empfehlen. Schulungsmaßnahmen richten sich hinsichtlich ihres Umfangs und ihrer Art jeweils nach dem vorliegenden Einzelfall.

Eine weitere wesentliche Aufgabe ist die Beratung der verantwortlichen Stelle – auf Anfrage – bei der Vornahme der Datenschutz-Folgenabschätzung nach Artikel 35 Absatz 2 DS-GVO/§ 21 Absatz 3 BbgPJMDSG.

Datenschutzbeauftragte müssen die Geschäftsleitung über datenschutzrelevante Vorgänge informieren und bei festgestellten Mängeln im Ablauf Mittel und Wege zur Verbesserung bzw. Problemlösungen vorschlagen.

Zudem arbeiten Datenschutzbeauftragte mit den Aufsichtsbehörden zusammen. Sie sind wesentliche Ansprechpersonen für die Aufsichtsbehörden, wenn es datenschutzrechtliche Belange zu klären gilt.

Die Aufgabenerfüllung der bzw. des Datenschutzbeauftragten nach Artikel 39 Absatz 2 DS-GVO richtet sich nach den Risiken der Verarbeitung für die betroffenen Personen. Es gilt die Forderung: Je kritischer die Art, je größer der Umfang, je risikoreicher die Umstände und je weiter die Zwecke der Datenverarbeitung, desto sorgfältiger die Prüfung.¹² Datenschutzbeauftragte müssen das Risiko für jeden Einzelfall konkret bewerten. Zum Zweck der Nachweisbarkeit sollte diese Bewertung ausreichend dokumentiert werden.

Datenschutzbeauftragte sind nach Artikel 38 Absatz 5 DS-GVO i. V. m. § 38 Absatz 2 BDSG i. V. m. § 6 Absatz 5 Satz 2 BDSG/§ 32 Absatz 5 BbgPJMDSG zur Verschwiegenheit verpflichtet. Die Verschwiegenheitsverpflichtung trifft sie teilweise auch gegenüber der verantwortlichen Stelle selbst, nämlich dann, wenn die betroffene Person im Vertrauen auf die Geheimhaltung ihrer personenbezogenen Daten auf die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten zugeht und sie bzw. ihn nicht ausdrücklich von der Verschwiegenheit entbindet. Die Verschwiegenheitsverpflichtung trägt dazu bei, dass Datenschutzbeauftragte Kenntnis von Missständen erhalten und somit ihre Aufgaben erfüllen können.¹³

Im Fall des Auskunftersuchens nach Artikel 15 DS-GVO und anderer Betroffenenrechte ist eine Geheimhaltung der Identität der betroffenen Person gegenüber der verantwortlichen Stelle aber nicht möglich, da diese die Rechtspflicht zur Auskunftserteilung trifft und hierfür die Kenntnis der Daten zur betroffenen Person und von der Geltendmachung der Rechte erforderlich ist.

Datenschutzbeauftragte sind verpflichtet, Verstöße gegen den Schutz personenbezogener Daten dem Verantwortlichen zu melden. Sie sind bei der Durchführung einer Datenschutz-Folgenabschätzung hinzuzuziehen.

12 Kühling/Buchner, DS-GVO/BDSG, 3. Auflage 2020, Art. 39, Rn. 23 mit weiteren Nachweisen.

13 Kühling/Buchner, DS-GVO/BDSG, 3. Auflage 2020, Art. 38, Rn. 38.

11 Haftung der bzw. des Datenschutzbeauftragten

Datenschutzbeauftragte übernehmen nach dem Aufgabenkatalog des Artikels 39 DS-GVO/§ 33 Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz (BbgPJMDSG) zahlreiche Aufgaben. Angesichts der hohen Bußgelder gemäß Artikel 83 DS-GVO, die Unternehmen bei datenschutzrechtlichen Verstößen drohen, stellt sich die Frage, ob Datenschutzbeauftragte Adressaten einer möglichen Geldbuße nach Artikel 83 DS-GVO sein können.

Dies ist nicht der Fall, da Datenschutzbeauftragte Teil der verantwortlichen Stelle sind und somit gegenüber betroffenen Personen nicht als eigenständige Verantwortliche oder Auftragsverarbeiter fungieren. Die Beachtung des Datenschutzes bleibt die unternehmerische Pflicht der verantwortlichen Stelle, für die die Datenschutzbeauftragten arbeiten. Sie kontrollieren die Einhaltung der Normen, haben aber keine datenschutzrechtliche Verantwortung. Diese verbleibt bei der verantwortlichen Stelle. Umso wichtiger ist es für die verantwortliche Stelle, eine voll vertrauenswürdige und qualifizierte Person für diese besondere Rolle auszuwählen und ihr die notwendigen Ressourcen zur Verfügung zu stellen.

Hinsichtlich einer möglichen zivilrechtlichen Haftung der Datenschutzbeauftragten ist zu differenzieren:

Vertragliche Schadenersatzpflichten gegenüber den betroffenen Personen existieren nicht, da es sich bei den nach Artikel 38 Absatz 4 DS-GVO vorgenommenen Beratungen nicht um schuldrechtliche Verpflichtungen der bzw. des Datenschutzbeauftragten handelt.¹⁴

Eine deliktische Haftung der bzw. des Datenschutzbeauftragten gegenüber den von der Datenverarbeitung betroffenen Personen ist hingegen in einigen Fällen denkbar. Beispielsweise dann, wenn die bzw. der Datenschutzbeauftragte die verantwortliche Stelle aktiv falsch berät oder Überwachungsmaßnahmen unterlässt und dies zu einem Schaden für die betroffenen Personen führt. Auch bei einer Verletzung ihrer Verschwiegenheitspflicht machen sich Datenschutzbeauftragte im Rahmen der zivilrechtlichen persönlichen deliktischen Haftung nach § 823 Absatz 2 BGB haftbar.¹⁵ In eng umgrenzten Fällen kann dies nach § 203 Absatz 4 Strafgesetzbuch strafrechtliche Konsequenzen haben. Die Schweigepflicht gilt über die Dauer der Funktionsausübung unbegrenzt hinaus.

12 Weitere Informationen

Antworten auf weitere Fragen liefert neben den bereits erwähnten Quellen auch das [Kurzpapier Nr. 12: Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern](#) der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder.

Auch wir stehen Ihnen selbstverständlich gerne für die Beantwortung von Fragen zur Verfügung.

¹⁴ Kühling/Buchner, DS-GVO/BDSG, 3. Auflage 2020, Art. 37, Rn. 52 mit weiteren Nachweisen.

¹⁵ Kühling/Buchner, DS-GVO/BDSG, 3. Auflage 2020, Art. 37, Rn. 54.

13 Verzeichnis der Gesetze

- Arbeitnehmerüberlassungsgesetz in der Fassung der Bekanntmachung vom 3. Februar 1995 (BGBl. I S. 158), das zuletzt durch Artikel 55 des Gesetzes vom 23. Oktober 2024 (BGBl. 2024 I Nr. 323) geändert worden ist
- Betriebsverfassungsgesetz in der Fassung der Bekanntmachung vom 25. September 2001 (BGBl. I S. 2518), das zuletzt durch Artikel 1 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 248) geändert worden ist
- Brandenburgisches Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz vom 19. Juni 2019 (GVBl. I Nr. 43)
- Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist
- Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 1 des Gesetzes vom 17. Juli 2025 (BGBl. 2025 I Nr. 163) geändert worden ist
- 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 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35)
- Kündigungsschutzgesetz in der Fassung der Bekanntmachung vom 25. August 1969 (BGBl. I S. 1317), das zuletzt durch Artikel 2 des Gesetzes vom 14. Juni 2021 (BGBl. I S. 1762) geändert worden ist
- Personalvertretungsgesetz für das Land Brandenburg vom 15. September 1993 (GVBl. I/93, [Nr. 20], S. 358), zuletzt geändert durch Artikel 3 des Gesetzes vom 20. September 2018 (GVBl. I/18, [Nr. 21], S. 4).
- 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 (ABl. L 119 vom 4.5.2016, S. 89; L 127 vom 23.5.2018, S. 9; L 74 vom 4.3.2021, S. 36)
- Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nr. 351) geändert worden ist
- Verwaltungsverfahrensgesetz für das Land Brandenburg vom 7. Juli 2009 (GVBl. I S. 262, 264), das zuletzt durch Artikel 6 des Gesetzes vom 8. Mai 2018 (GVBl. I Nr. 8, S. 4) geändert worden ist