



Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

214.7.40

Vorschläge zur Änderung des Berliner Datenschutzgesetzes (BlnDSG)

(Stand: 6. Februar 2026)

**Berliner Beauftragte für Datenschutz
und Informationsfreiheit (BlnBDI)**

Alt-Moabit 59-61, 10555 Berlin
Eingang: Alt-Moabit 60

Telefon: 030 13889-0
Telefax: 030 215 50 50

Sprechzeiten: Mo.-Fr. 10-15 Uhr,
Do. 10-18 Uhr, oder nach Vereinbarung

E-Mail: mailbox@datenschutz-berlin.de
Website: www.datenschutz-berlin.de



		Inwieweit einer Religionsgemeinschaft nach deutschem Staatskirchenrecht der Status einer Körperschaft des öffentlichen Rechts verliehen wurde, spielt dabei für den Verordnungsgeber keine Rolle. Erfüllt damit eine Religionsgemeinschaft, der die Körperschaftsrechte verliehen worden sind, die Voraussetzungen des Art. 91 Abs. 1 DSGVO nicht, so sind die Regelungen der Verordnung vorbehaltlos auf diese anzuwenden. Für diesen Fall ergibt sich jedoch bisher keine Zuständigkeit der BlnBDI aus dem BlnDSG. Öffentlich-rechtliche Religionsgemeinschaften sind mangels Eingliederung in die Staatsorganisation wie es bei einer K. d. ö. R. im verwaltungs- und staatsorganisatorischen Sinne der Fall wäre¹ nicht als öffentliche Stelle i. S. d. § 8 Abs. 1, 2 Abs. 1 oder des § 2 Abs. 1 BDSG einzuordnen. Auch eine Bewertung als nicht-öffentliche Stelle iSd § 8 Abs. 2 iVm § 40 BDSG schließt sich, anders als bei rein privat-rechtlich (z. B. als e. V.) verfassten Religionsgemeinschaften, aus.²
--	--	--

¹ BVerfGE 139, BVERFGE Jahr 139 Seite 321, bei juris Rn. 91 f., m.w.N.

² vgl. VG Hannover, Urt. v. 30.11.2022 – 10 A 1195/21, BeckRS 2022, 34588, Rn. 54.

§ 6 Abs. 2 Die in Absatz 1 genannten Aufgaben der oder des Datenschutzbeauftragten beziehen sich nicht auf die Verarbeitung von personenbezogenen Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit und durch den Rechnungshof im Rahmen seiner unabhängigen Tätigkeit.	§ 6 Abs. 2 Die in Absatz 1 genannten Aufgaben der oder des Datenschutzbeauftragten beziehen sich nicht auf die Verarbeitung von personenbezogenen Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit und durch den Rechnungshof im Rahmen seiner unabhängigen Tätigkeit.	Die Vorschriften ist nicht mit der DSGVO zu vereinbaren. Art. 55 Abs. 1 DSGVO geht von einer umfassenden Kontrollbefugnis der Aufsichtsbehörde aus und sieht lediglich Ausnahmen für Gerichte vor.
§ 8 Abs. 3 Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist nicht zuständig für die Aufsicht über die von den Gerichten im Rahmen ihrer justiziellen Tätigkeit oder über die vom Rechnungshof in unabhängiger Tätigkeit vorgenommenen Verarbeitungen personenbezogener Daten.	§ 8 Abs. 3 Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist nicht zuständig für die Aufsicht über die von den Gerichten im Rahmen ihrer justiziellen Tätigkeit oder über die vom Rechnungshof in unabhängiger Tätigkeit vorgenommenen Verarbeitungen personenbezogener Daten.	

(Neuer Absatz)	§ 8 Absatz 5 (neu) (5) Soweit die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit nach den Absätzen 1 bis 4 für die Durchsetzung der Verordnung (EU) 2016/679 zuständig ist, ist sie oder er auch zuständige Behörde im Sinne von Artikel 22 Absatz 4 Satz 1 der Verordnung (EU) 2024/900 für die Überwachung der Anwendung des Artikels 20 der Verordnung (EU) 2024/900.	Der neue Absatz regelt die Zuständigkeit für die datenschutzrelevanten Vorgaben in Artikel 20 der Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung (TTPW-VO), die gemäß Artikel 30 Absatz 2 Satz 1 TTPW-VO bereits ab dem 10. Oktober 2025 gelten. Artikel 22 Absatz 1 Satz 1 TTPW-VO regelt, dass die Aufsichtsbehörden nach Artikel 51 DSGVO oder der Europäische Datenschutzbeauftragte nach Artikel 52 der Verordnung (EU) 2018/1725 in ihrem jeweiligen Zuständigkeitsbereich für die Überwachung der Anwendung der Artikel 18 und 19 TTPW-VO verantwortlich sind. Den mitgliedstaatlichen Zuständigkeitsrahmen nach Artikel 51 DSGVO hat der deutsche Bundes- und die Landesgesetzgeber mit den Vorgaben nach §§ 9 Absatz 1 und 40 Absatz 1 BDSG sowie denen der Landesdatenschutzgesetzen für die föderale Aufsichtsverteilung gefüllt. Wir gehen davon aus, dass der europäische Gesetzgeber bei den Datenschutzvorgaben der TTPW-VO die bereits etablierten DSGVO-Zuständigkeiten übernehmen wollte. Hiervon
-----------------------	--	--

		geht auch die Bundesregierung aus (vgl. den Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung (Politische-Werbung-Transparenz-Gesetz - PWTG), S. 28). Artikel 22 Absatz 4 Satz 1 TTPW-VO sieht jedoch vor, dass jeder Mitgliedstaat eine oder mehrere zuständige Behörden benennt, die für die Anwendung und Durchsetzung der in Artikel 22 Absätzen 1 und 3 TTPW-VO nicht genannten Aspekte der TTPW-VO zuständig ist. Nicht geregelt ist in Artikel 22 Absätzen 1 und 3 TTPW-VO die Zuständigkeit für die Überwachung des Artikels 20 TTPW-VO. Die Aufsichtszuständigkeit für Artikel 20 TTPW-VO ist somit zwingend von den Mitgliedstaaten zu treffen. Bei Artikel 20 TTPW-VO handelt es sich um eine Übermittlungspflicht, die sich auf die von den Datenschutzbehörden sowieso zu überwachende Vorgabe des Artikels 19 TTPW-VO bezieht. Es erscheint daher sachgerecht, dass die Überwachung der Anwendung von Artikel 20 TTPW-VO ebenfalls von unserer Behörde übernommen wird. Die
--	--	--

		Bundesregierung hat in ihrem Entwurf eines Durchführungsgesetzes (§ 2 Abs. 1 PWTG-E) bisher nur die Zuständigkeit der BfDI für Art. 20 TTPW-VO im Rahmen ihrer sonstigen datenschutzrechtlichen Zuständigkeit vorgesehen, was vom Bundesrat bereits kritisiert worden ist (vgl. BR-Drs. 766/25 (Beschluss), S. 1 f.). Auch wir wünschen uns eine einheitliche Regelung über Zuständigkeit und Befugnisse im PWTG sowohl für BfDI als auch die Landesdatenschutzbehörden. Es ist momentan jedoch unklar, ob im PWTG als Bundesgesetz auch die Zuständigkeit der Landesdatenschutzbehörden für Art. 20 TTPW-VO im weiteren Gesetzgebungsprozess aufgenommen werden wird, weshalb wir vorsichtshalber eine entsprechende Zuständigkeitsregelung im BlnDSG vorschlagen.
§ 13 (2) Stellt die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit bei Datenverarbeitungen durch öffentliche Stellen zu Zwecken außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 Verstöße gegen die Vorschriften dieses	§ 13 (2) Stellt die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit bei Datenverarbeitungen durch öffentliche Stellen zu Zwecken außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 Verstöße gegen die Vorschriften dieses	Gemäß Art. 47 Abs. 2 der JI-Richtlinie müssen die Aufsichtsbehörden <u>wirksame</u> Abhilfebefugnisse erhalten. Demzufolge sollten die Datenschutzaufsichtsbehörden im Anwendungsbereich der JI-Richtlinie über dieselben Kompetenzen verfügen, die ihnen auch durch die DS-GVO eingeräumt werden. Die Umsetzung der entsprechenden

Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie oder er dies gegenüber dem Verantwortlichen und fordert diesen zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden angemessenen Frist auf. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit getroffen worden sind.	Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so <u>gelten die Befugnisse gemäß Art. 58 der Verordnung der (EU) 2016/679 entsprechend.</u> - beanstandet sie oder er dies gegenüber dem Verantwortlichen und fordert diesen zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden angemessenen Frist auf. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthal-	Befugnisse wäre jederzeit gerichtlich überprüfbar, ggf. auch in Rahmen des vorläufigen Rechtsschutzes. Es wird insoweit auch auf das Vertragsverletzungsverfahren der Europäischen Kommission gegen Deutschland verwiesen – INFR (2022/2030), weil Deutschland hinsichtlich wirksamer Abhilfebefugnisse seinen Verpflichtungen aus der JI-Richtlinie nicht nachgekommen ist.
---	---	--

Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen. (3) Sofern in den Fällen des Absatzes 1 Satz 2 und Absatz 2 Satz 1 die beanstandeten Verstöße oder Mängel auch unter Berücksichtigung der Stellungnahme weiterhin bestehen, kann [...]	ten, die auf Grund der Beanstandung der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit getroffen worden sind. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen. (3) Sofern in den Fällen des Absatzes 1 Satz 2 und Absatz 2 Satz 1 die beanstandeten Verstöße oder Mängel auch unter Berücksichtigung der Stellungnahme weiterhin bestehen, kann [...]	
--	---	--

§ 13a (Neue Vorschrift)	§ 13a Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann Maßnahmen, die sie oder er innerhalb der gesetzlichen Befugnisse trifft, mit Zwangsmitteln nach den Bestimmungen des Verwaltungsvollstreckungsgesetzes durchsetzen. Dabei kann sie oder er die Zwangsmittel für jeden Fall der Nichtbefolgung androhen. Die Höhe des Zwangsgeldes beträgt bis zu 50.000 Euro.	Die vorgeschlagene Norm entspricht § 17 Abs. 1 des Finanzdienstleistungsaufsichtsgesetzes (FinDAG). Ohne diese Ergänzung ist eine effektive Datenschutzaufsicht im öffentlichen Bereich nicht möglich, da die BlnBDI zwar Anordnungen gegen öffentliche Stellen treffen, diese aber letztlich im Zweifel nicht durchsetzen kann. Dies ergibt sich aus § 17 Bundesverwaltungsvollstreckungsgesetz (VwVG), der auch für Berlin anwendbar ist. Dort heißt es: „Gegen Behörden und juristische Personen des öffentlichen Rechts sind Zwangsmittel unzulässig, soweit nicht etwas Anderes bestimmt ist.“
§ 15 Abs. 1 (1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck, als demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ist auf Grund von Artikel 6 Absatz 4 Satz 1 1. Halbsatz der Verordnung (EU) 2016/679 in Verbindung mit den in Artikel 23 Absatz 1	§ 15 Abs. 1 (1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck, als demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ist auf Grund von Artikel 6 Absatz 4 Satz 1 1. Halbsatz der Verordnung (EU) 2016/679 in Verbindung mit den in Artikel 23 Absatz 1	Das Abgeordnetenhaus von Berlin ist offenbar bei der Schaffung des § 15 BlnDSG davon ausgegangen, dass Art. 6 Abs. 4 Halbsatz 1 DSGVO eine Öffnungsklausel enthält, die es erlaubt, gesetzliche Regelungen aufzunehmen, die die zweckändernde Verarbeitung erlauben. Unabhängig von der in der Literatur unterschiedlich bewerteten Frage, ob es sich bei Art. 6 Abs. 4 Halbsatz 1

der Verordnung (EU) 2016/679 genannten Zielen zulässig, wenn 1. sie zum Schutz lebenswichtiger Interessen einer natürlichen Person erforderlich und die betroffene Person aus rechtlichen oder tatsächlichen Gründen nicht in der Lage ist, die Einwilligung zu erteilen; 2. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für	der Verordnung (EU) 2016/679 genannten Zielen zulässig, wenn 1. sie zum Schutz lebenswichtiger Interessen einer natürlichen Person erforderlich ist <u>und der Schutz der lebenswichtigen Interessen die mit der zweckändernden Verarbeitung verbundenen Nachteile überwiegt.</u> betroffene Person aus rechtlichen oder tatsächlichen Gründen nicht in der Lage ist, die Einwilligung zu erteilen; 2. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer unmittelbar drohenden Gefahr für	DSGVO um eine solche Öffnungsklausel handelt, ist es allerdings notwendig, Art. 6 Abs. 4 DSGVO im Zusammenhang mit Art. 6 Abs. 2 und 3 DSGVO zu betrachten, d. h. die Tatbestände des § 15 Abs. 1 BlnDSG sind am strengen Maßstab der Ziele des Art. 23 Abs. 1 DSGVO zu messen. Da diese nicht bei allen Tatbeständen erfüllt sind, ergibt sich folgender Änderungsbedarf: Die Einwilligung kommt als Rechtsgrundlage im öffentlichen Bereich idR nicht in Betracht, da sich die Grenzen zulässiger Datenverarbeitung sich nach den gesetzlichen Aufgaben bestimmen und damit auch die Datenverarbeitung auf gesetzlichen Grundlagen zu stützen ist. Es ist davon auszugehen, dass es hier eher um den antizipierten Willen des Betroffenen gehen soll, so dass die Norm entsprechend abzuändern ist. Der Verantwortliche hat die Abwägungsentscheidung zu treffen und im Rahmen der Rechenschaftspflicht zu dokumentieren. Es lässt sich der Gesetzesbegründung nicht entnehmen, was unter den erheblichen Nachteilen für das Gemeinwohl zu verstehen ist. Da Art. 23 Abs. 1 DSGVO diesen
---	---	---

die öffentliche Sicherheit oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist;	die öffentliche Sicherheit oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist;	Begriff auch nicht verwendet, lässt sich dieser Zweck insoweit nicht unter die in Art. 23 Abs. 1 DSGVO genannten Alternativen subsumieren. Die Alternative ist daher zu streichen.
3. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden erforderlich erscheint;	3. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden <u>für die übermittelnde Stelle</u> erforderlich erscheint <u>ist</u>;	Anhaltspunkte für Ordnungswidrigkeiten werden nicht von Art. 23 Abs. 1 lit. d DSGVO umfasst, so dass zweckändernde Verarbeitungen für den Zweck der Verfolgung von Ordnungswidrigkeiten nicht in Betracht kommen und zu streichen sind. Die zweckändernde Verarbeitung steht unter dem Vorbehalt der Erforderlichkeit, die immer aus der Sicht der übermittelnden Stelle zu bewerten ist. Die Norm ist daher entsprechend klarstellend zu ergänzen. Nicht entscheidend ist, dass ob die Daten für die Erfüllung der gesetzlichen Aufgaben der Strafverfolgungsbehörden erforderlich sind. Dies kann auch nicht geregelt werden.
4. die Daten aus allgemein zugänglichen Quellen erhoben werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit	4. die Daten aus allgemein zugänglichen Quellen erhoben werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit	Die Regelung begegnet erheblicher Kritik, die bereits im Gesetzgebungsverfahren von der BlnBDI (Wortprotokoll zur 11. Sitzung des Ausschusses für Kommunikationstechnologie und Datenschutz, 14.5.2018, S. 41) vorgetragen

nicht schutzwürdige Interessen der betroffenen Person offensichtlich entgegenstehen;	nicht schutzwürdige Interessen der betroffenen Person offensichtlich entgegenstehen;	worden ist. Die Norm ist zu streichen, da sie mit den Vorgaben des Art. 23 DSGVO nicht vereinbar ist. Die Zulässigkeit der zweckändernden Verarbeitung muss sich nach dem konkreten Zweck der Weiterverarbeitung richten, der zu beschreiben wäre. Hier knüpft die Zulässigkeit der zweckändernden Verarbeitung jedoch an die Art der Daten, nämlich „allgemein zugängliche Daten“ an. Dies ist nicht mit den Vorgaben des Art. 23 DSGVO nicht vereinbar.
5. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der internen Revision, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient; der Zugriff auf personenbezogene Daten ist insoweit nur zulässig, als er für die Ausübung dieser Befugnisse erforderlich ist;	5. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der internen Revision, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient; der Zugriff auf personenbezogene Daten ist insoweit nur zulässig, als er für die Ausübung dieser Befugnisse erforderlich ist;	Die Regelung ist zu streichen. Nach § 11 Abs. 4 Satz 1 und 2 BlnDSG aF lag eine Verarbeitung zu „anderen Zwecken“ nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen etc. diene, so dass davon auszugehen war, dass die Verarbeitung zu den genannten Zwecken mit dem Erhebungszweck vereinbar war. Es ist nicht ersichtlich, warum hiervon in der Neufassung des BlnDSG abgewichen wurde, da eine enge Verbindung zwischen den Zwecken, für die personenbezogene Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung bestand (Art. 6 Abs. 4 Satz 1 lit. a

6. sie zu Aus- und Fortbildungszwecken erforderlich ist und schutzwürdige Belange der betroffenen Person dem nicht entgegenstehen; zu Test- und Prüfungszwecken dürfen personenbezogene Daten nicht verarbeitet werden. Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ord-	6. sie zu Aus- und Fortbildungszwecken erforderlich ist und schutzwürdige Belange der betroffenen Person dem nicht entgegenstehen; zu Test- und Prüfungszwecken dürfen personenbezogene Daten nicht verarbeitet werden. Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ord-	DSGVO). Es besteht insoweit kein Bedarf für die Regelung in § 15 Abs. 1 Satz 1 Nr. 5 BlnDSG. Im Unterschied zur bisherigen Regelung in § 11 Abs. 4 Satz 2 BlnDSG a.F. geht die Vorschrift davon aus, dass eine Verarbeitung zu einem anderen Zweck vorliegt. Die Norm lässt sich nicht unter die in Art. 23 Abs. 1 Nr. 6 lit. e DSGVO genannten Tatbestände subsumieren, so dass eine entsprechende Regelung nicht getroffen werden kann und zu streichen ist. Zu prüfen wäre in der Praxis ggf., ob sich eine Vereinbarkeit mit den ursprünglichen Zwecken begründen lässt. Allerdings muss hier eine strenge Prüfung der Verhältnismäßigkeit erfolgen. Die Verantwortlichen haben die Erforderlichkeit darzulegen und schutzwürdige Belange dürfen nicht entgegenstehen, wobei ein strenger Prüfungsmaßstab anzulegen ist. Die Regelung ist zu streichen, da es sich hier um ein Verbot für die Weiterverarbeitung ergibt, da sich das Verarbeitungsverbot bereits aus der DSGVO ergibt und es insoweit der Klarstellung nicht bedarf. Eine Regelungskompetenz hierfür besteht ebenfalls nicht.
---	---	--

nungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verarbeitet werden.	nungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verarbeitet werden.	
§ 15 Abs. 2 (2) Absatz 1 Satz 1 Nummer 2 und 3 findet keine Anwendung, wenn die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis unterliegen und sie der datenverarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind.	§ 15 Abs. 2 (2) Absatz 1 Satz 1 Nummer 2 und 3 findet keine Anwendung, wenn die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis unterliegen und sie der datenverarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind. <u>Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der verantwortlichen Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- und</u>	Die zweckändernde Weiterverarbeitung auf der Grundlage der in Absatz 1 Satz 1 der Norm genannten Tatbestände begegnet angesichts der Schutzbedürftigkeit der einem Berufs- oder Amtsgeheimnis unterliegenden Daten erheblichen Bedenken. In Anlehnung an die in anderen Bundesländern bestehenden Regelungen sollte die vorgeschlagene Änderung übernommen werden (vgl. § 9 Abs. 5 Datenschutzgesetz Nordrhein-Westfalen, § 7 Abs. 4 Datenschutzgesetz Rheinland-Pfalz).

	<u>Amtspflicht übermittelt worden, findet Absatz 1 keine Anwendung.</u>	
§ 15 Abs. 4 (4) Sind personenbezogene Daten derart verbunden, dass ihre Trennung nach verschiedenen Zwecken auch durch Vervielfältigen und Unkenntlichmachung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, so tritt an die Stelle der Trennung ein Verwertungsverbot nach Maßgabe des Absatzes 1 für die Daten, die nicht dem Zweck der jeweiligen Verarbeitung dienen.	§ 15 Abs. 4 (4) Sind personenbezogene Daten derart verbunden, dass ihre Trennung nach verschiedenen Zwecken auch durch Vervielfältigen und Unkenntlichmachung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, so tritt an die Stelle der Trennung ein Verwertungsverbot nach Maßgabe des Absatzes 1 für die Daten, die nicht dem Zweck der jeweiligen Verarbeitung dienen, <u>sofern schutzwürdige Interessen der betroffenen Personen an der Geheimhaltung nicht entgegenstehen.</u>	Die Vorschrift enthält neben dem unverhältnismäßig hohen Aufwand für die Trennung nach verschiedenen Zwecken keine weiteren Voraussetzungen für die Zulässigkeit. Da aber durchaus schutzwürdige Interessen der betroffenen Personen an der Geheimhaltung bestehen können, ist die Regelung nicht sachgerecht. Schutzwürdige Interessen können z. B. vorliegen, wenn besondere Kategorien personenbezogener Daten betroffen sind und eine Offenlegung Nachteile für die Betroffenen mit sich bringen können. Um den schutzwürdigen Interessen der Betroffenen Rechnung zu tragen, sollte in Anlehnung an z. B. § 67 d Abs. 2 SGB X eine Verpflichtung zur Prüfung entgegenstehender schutzwürdiger bzw. berechtigter Interessen aufgenommen werden. Die Vorschrift erscheint im Übrigen im Kontext der übrigen Regelungen des § 15 BlnDSG fremd. Es handelt sich gerade nicht um eine originäre Verarbeitungsbefugnis zu anderen Zwecken, sondern vielmehr um eine besondere

		Übermittlungsbefugnis. Da der Gesetzgeber darauf verzichtet hat, gesonderte Regelungen für die Übermittlung personenbezogener Daten durch öffentliche Stellen in das Gesetz aufzunehmen und eine § 15 Abs. 4 entsprechende Vorschrift auch in der Vorgängerregelung in § 11 Abs. 3 BlnDSG aF enthalten war, lässt sich die Aufnahme der Regelung in das Gesetz erklären. Es sollte allerdings geprüft werden, ob ein praktischer Bedarf für die Schaffung einer gesonderten Regelung für Datenübermittlungen im öffentlichen Bereich (vergleichbar der Regelung anderer Landesdatenschutzgesetze, z. B. § 22 Hessisches Datenschutzgesetz) besteht.
§ 15 Abs. 5 (5) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen	§ 15 Abs. 5 (5) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen <u>des § 15 Abs. 1 Satz 1 vorliegen</u>	Rechtsdogmatisch kann eine Ausnahme vom Verarbeitungsverbot nach Art. 9 Abs. 1 DSGVO nur in den Fällen des Art. 9 Abs. 2 DSGVO in Betracht kommen. Eine zweckändernde Verarbeitung besonderer Kategorien personenbezogener Daten setzt voraus, dass eine der in § 15 Abs. 1 Satz 1 geregelten Fallkonstellationen vorliegt und zusätzlich die Voraussetzungen des Art. 9 Abs. 2 DSGVO oder § 14 Abs. 1 oder 2 erfüllt sind, da die in Art. 6 Abs. 4 Halbsatz 1 DSGVO genannten Voraussetzungen für eine

gen nach § 14 Abs. 2 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 14 Abs. 1 vorliegen.	<u>und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder § 14 Absatz 1 und 2 erfüllt ist.</u>	mitgliedsstaatliche Regelung zur zweckändernden Verarbeitung erfüllt sein müssen.
§ 20a Die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen ist zulässig, wenn diese vom Abgeordnetenhaus, dessen verfassungsmäßigen Organen, seinen Mitgliedern oder den Fraktionen des Abgeordnetenhauses im Rahmen ihrer Aufgaben verlangt werden. Personenbezogene Daten dürfen für diese Institutionen zur Erfüllung ihrer Aufgaben nur verarbeitet werden, wenn nicht überwiegende private Interessen an der Geheimhaltung zwingend entgegenstehen. Diese Befugnis gilt auch für be-	§ 20a Die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen ist zulässig, wenn diese vom Abgeordnetenhaus, dessen verfassungsmäßigen Organen, seinen Mitgliedern oder den Fraktionen des Abgeordnetenhauses im Rahmen ihrer Aufgaben verlangt werden. Personenbezogene Daten dürfen für diese Institutionen zur Erfüllung ihrer Aufgaben nur verarbeitet werden, wenn nicht überwiegende private Interessen an der Geheimhaltung zwingend entgegenstehen. Diese Befugnis gilt auch für be-	Die Einbeziehung besonderer Kategorien personenbezogener Daten i. S. v. Art. 9 Abs. 1 steht nicht im Einklang mit Art. 9 Abs. 2 lit. g DSGVO. Es gibt keine angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte, da es im Abgeordnetenhaus an einer unabhängigen Datenschutzkontrollinstanz fehlt.

sondere Kategorien personen-bezo- gener Daten i. S. v. Art. 9 Abs. 1 der Verordnung (EU) 2016/679.	sondere Kategorien personenbezo- gener Daten i. S. v. Art. 9 Abs. 1 der Verordnung (EU) 2016/679	
§ 24 Abs. 1 Nr. 2 (1) Unbeschadet von § 17 Absatz 4 besteht das Recht der betroffenen Person auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 nicht, sofern die Erteilung der Auskunft hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten muss. Ein Fall des Satzes 1 liegt insbesondere vor, wenn die Erteilung der Auskunft 1. die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes erhebliche Nachteile bereiten würde,	§ 24 Abs. 1 Nr. 2 (1) Unbeschadet von § 17 Absatz 4 besteht das Recht der betroffenen Person auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 nicht, sofern die Erteilung der Auskunft hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten muss. Ein Fall des Satzes 1 liegt insbesondere vor, wenn die Erteilung der Auskunft 1. die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes erhebliche Nachteile bereiten würde,	§ 24 Abs. 1 Nr. 2 BlnDSG weitet die Beschränkungstatbestände hinsichtlich des Auskunftsrechts aus Art. 15 DSGVO auf einfache Ordnungswidrigkeiten aus. Diese Beschneidung des zentralen Betroffenenrechts der DSGVO und der damit verbundene empfindliche Grundrechtseingriff erscheint jedoch unverhältnismäßig. § 24 Abs. 1 Nr. 2 BlnDSG dürfte in seiner gegenwärtigen Formulierung auch die zugrundeliegende Öffnungsklausel des Art. 23 Abs. 1 lit. d DSGVO überdehnen, in der keine Ordnungswidrigkeiten genannt werden. Es bestehen daher erhebliche Zweifel an der Unionsrechtskonformität der Regelung (ähnliche Bedenken dürften sich gegen die entsprechende Regelung in § 23 Abs. 1 Nr. 2 BlnDSG ergeben). In der Praxis spielt der Beschränkungstatbestand zudem offenbar keine Rolle und wird nicht angewendet (vgl. AGH, Drs. 18/4107, 6).

2. die Verfolgung von Straftaten und Ordnungswidrigkeiten gefährden würde oder	2. die Verfolgung von Straftaten und Ordnungswidrigkeiten gefährden würde oder	
§ 28 Gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 sowie Stellen, die nach § 2 Absatz 3 den Bestimmungen dieses Gesetzes unterliegen, werden keine Geldbußen verhängt.	§ 28 Gegen öffentliche Stellen im Sinne des § 2 Absatz 1 und 2 sowie Stellen, die nach § 2 Absatz 3 den Bestimmungen dieses Gesetzes unterliegen, werden keine Geldbußen verhängt, sofern diese Stellen keine Unternehmen im Sinne von Art. 101, 102 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) sind.	Die bisherige Regelung des § 28 BlnDSG ist aufgrund des Anknüpfungspunkts der Privilegierung des § 28 BlnDSG an öffentliche Stellen gemäß § 2 Abs. 6 Satz 1 BlnDSG, die als Unternehmen am Wettbewerb teilnehmen, unionsrechtswidrig. Die Öffnungsklausel des Art. 83 Abs. 7 DSGVO für öffentliche Stellen und Behörden umfasst für die Mitgliedstaaten nur Regelungsmöglichkeiten, die das Sanktionsregime der Art. 83 Abs. 4-6 DSGVO nicht unterlaufen. Die Bußgeldtatbestände des Art. 83 Abs. 4-6 DSGVO ermöglichen vor dem Hintergrund des Erwägungsgrunds 150 Satz 3 DSGVO Bußgelder direkt gegen Unternehmen i. S. v. Art. 101, 102 AEUV, unabhängig davon, ob die Unternehmen

		privat- oder öffentlich-rechtlich ausgestaltet³ sind.⁴ Öffentlich-rechtliche Unternehmen sind europarechtlich weder als Behörden oder öffentliche Stellen, sondern als Unternehmen einzustufen.⁵ Als Unternehmen gelten sie danach, wenn sie sich entsprechend der EuGH-Rechtsprechung zum funktionalen Unternehmensbegriff nicht hoheitlich betätigen und eine Trennung der Sphären der wirtschaftlichen Betätigung und der Ausübung hoheitlicher Befugnisse möglich ist.⁶
--	--	--

³ Nach dem EuGH ist unter „Unternehmen“ im EU-Kartellrecht jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung, zu verstehen, EuGH Urt. v. 11.7.2006 – C-205/03 P, Slg 2006, I-6295 Rn. 25 – FENIN m. w. N.

⁴ So auch LG Bonn Urt. v. 11.11.2020 – 29 OWi 1/20, BeckRS 2020, 35663 Rn. 21 ff.; Interdiözesanes Datenschutzgericht, Beschl. v. 12.7.2021 – IDSG 21/2020; DSK Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder v. 3.4.2019; a. A. LG Berlin Beschl. v. 18.2.2021 – (526 OWi LG) 212 Js-OWi 1/20 (1/20), BeckRS 2021, 2985 Rn. 11 ff.; öBVwG Urt. v. 26.11.2020 – W258 2227269-1/14E Punkt 3.1 ff.; diese Frage der Anwendbarkeit des funktionalen Unternehmensbegriffs im Rahmen des Art. 83 DSGVO vor dem Hintergrund des § 41 BDSG iVm §§ 30, 130 OWiG wurde vom Kammergericht dem EuGH (C-807/21 – Deutsche Wohnen) zur Vorabentscheidung vorgelegt, vgl. KG Beschl. v. 6.12.2021 – 3 Ws 250/21, BeckRS 2021, 39748.

⁵ Vgl. HK-BayDSG/Dieterle Art. 22 Rn. 10 f. mit Verweis auf EuGH Urt. v. 12.7.2012 – C-138/11, EuZW 2012, 835 Rn. 35 ff. – Compass-Datenbank GmbH/Österreich; BayLfD Aktuelle Kurz-Information 17; i. E. wohl auch Kohn ZD 2019, 498 (499); i. E. auch Kühling/Buchner/Bergt DS-GVO Art. 83 Rn. 27; Ehmann ZD 2017, 201 (202).

⁶ Vgl. EuGH Urt. v. 12.7.2012 – C-138/11, EuZW 2012, 835 Rn. 35 ff. – Compass-Datenbank GmbH/Österreich.

		Eine wirtschaftliche Tätigkeit ist insofern jede Tätigkeit, die darin besteht, Güter oder Dienstleistungen auf einem bestimmten Markt anzubieten.⁷ Hoheitlich sind Tätigkeiten, die nach ihrer Art, ihrem Gegenstand und den für sie geltenden Regeln mit der Ausübung hoheitlicher Befugnisse zusammenhängen.⁸ Zu den wirtschaftlichen Tätigkeiten gehören regelmäßig alle wirtschaftlichen Kerntätigkeiten von öffentlich-rechtlichen Unternehmen (z. B. Betrieb und Verwaltung eines Flughafens durch eine staatliche Flughafengesellschaft,⁹ das klassische Bankgeschäft¹⁰ einer Landesbank, die Versorgung von Patient:innen durch staatliche Krankenhäuser,¹¹ Kommunikationsleistungen von staatlichen Kommunikationsunternehmen, die Stromlieferung durch staatliche Elektrizitätsversorgungsunternehmen
--	--	---

⁷ EuGH Urt. v. 3.3.2011 – C-437/09, BeckRS 2011, 80182 Rn. 42 m. w. N.

⁸ EuG Urt. v. 16.7.2014 – T-309/12, BeckRS 2014, 81173 Rn. 56 – „Zweckverband Tierkörperbeseitigung“; Immenga/Mestmäcker/Mestmäcker/Schweitzer AEUV Art. 107 Abs. 1 Rn. 17; LMR/Kersting/Meyer-Lindemann/Schwensfeier/Knauff GWB § 185 Abs. 1 Rn. 46.

⁹ Vgl. EuGH Urt. v. 19.12.2012 – C-288/11 P – Mitteldeutscher Flughafen ua/Kommission.

¹⁰ Vgl. BeckOK DatenschutzR/Schild BDSG § 2 Rn. 43.

¹¹ Vgl. EU-Kommission Bekanntmachung der Kommission zum Begriff der staatlichen Beihilfe im Sinne des Artikels 107 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union 2016/C 262/01 Rn. 26; HK-BayDSG/Dieterle Art. 22 Rn. 12; Ehmann ZD 2017, 201 (202).

		oder der Transport von Passagieren durch staatliche Verkehrsunternehmen). Nicht schon alleine ausschlaggebend für die Einstufung als hoheitliche Tätigkeit ist dabei, ob die als Unternehmen agierende öffentliche Stelle eine rechtliche oder tatsächliche Monopolstellung am jeweiligen Markt (z. B. bei der Wasserversorgung) hat.¹² Die EU-Kommission und die EU-Gerichte interpretieren die hoheitliche Tätigkeit sehr eng und lassen darunter beispielsweise die Armee- oder Polizeitätigkeiten, Flugsicherung und Flugverkehrskontrolle, Seeverkehrskontrolle und -sicherheit, Überwachungstätigkeiten zur Bekämpfung der Umweltverschmutzung, Organisation, Finanzierung und Durchsetzung von Haftstrafen, Erschließung und Revitalisierung öffentlichen Geländes durch öffentliche Stellen und Erhebung von Unternehmensdaten für öffentliche Zwecke auf der Grundlage einer Meldepflicht der Unternehmen fallen.¹³ Ebenso agieren öffentliche Bildungs- und
--	--	--

¹² Vgl. BayLfD Aktuelle Kurz-Information 17 mit Verweis auf EuG Urt. v. 16.7.2014 – T-309/12, BeckRS 2014, 81173 Rn. 58 ff. – Zweckverband Tierkörperbeseitigung; a. A. wohl Gola/Heckmann/Schulz BDSG § 2 Rn. 27; ErfK/Franzen BDSG § 2 Rn. 4; differenzierend nach rechtlichen und tatsächlichen Monopolstellungen Taeger/Gabel/Arning/Rothkegel BDSG § 2 Rn. 94.

¹³ Mit Rechtsprechungsnachweisen EU-Kommission Bekanntmachung der Kommission zum Begriff der staatlichen Beihilfe im Sinne des Artikels 107 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union 2016/C 262/01 Rn. 17; Dausen/Ludwigs EU-WirtschaftsR-HdB/Götz H.III. Rn. 70.

		Forschungseinrichtungen sowie Kulturstätten in der Regel hoheitlich.¹⁴ Insofern ist nicht das deutsche datenschutzrechtliche Verständnis der öffentlichen Stellen, die als Unternehmen am Wettbewerb teilnehmen, maßgeblich, sondern die Frage, ob es sich bei der datenverarbeitenden Stelle des Landes Berlins um ein Unternehmen nach unionsrechtlichem Maßstab handelt. Wenn eine öffentliche Stelle nach § 2 Abs. 6 Satz 1 BlnDSG nicht als Wettbewerbsunternehmen anzusehen ist, bedeutet dies somit nicht in jedem Fall, dass sie auch umfassend von der Bußgeldprivilegierung profitieren kann, die § 28 BlnDSG bisher hinsichtlich der Ahndungsmöglichkeit nach Art. 83 DSGVO unionsrechtswidrig vorsieht.
§ 29 (4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder	§ 29 (4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder	Das bisherige sehr weite Beweisverwendungsverbot des § 29 Abs. 4 BlnDSG ist zumindest hinsichtlich Unternehmen europarechtswidrig.

¹⁴ Vgl. EU-Kommission Bekanntmachung der Kommission zum Begriff der staatlichen Beihilfe im Sinne des Artikels 107 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union 2016/C 262/01 Rn. 28 ff.

eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Straf- oder Bußgeldverfahren gegen die meldepflichtige oder benachrichtigende Person oder deren in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung der meldepflichtigen oder benachrichtigenden Person verwendet werden.	eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Straf- oder Bußgeldverfahren gegen die meldepflichtige oder benachrichtigende Person oder deren in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung der meldepflichtigen oder benachrichtigenden Person verwendet werden. <u>Sofern der jeweilige Verantwortliche kein Unternehmen gemäß Art. 101, 102 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) ist, darf eine Meldung nach Artikel 33 der Verordnung (EU)</u>	Es umfasst grundsätzlich die Verwendung der konkreten Datenpannenmeldung bzw. -benachrichtigung nach Art. 33, 34 DSGVO als Beweis für ein Straf- oder Bußgeldverfahren (sog. Verwertungsverbot) sowie der dadurch erhaltenen Informationen als Spurenansatz für weitere Ermittlungen (sog. Fernwirkung)¹⁵ oder für die Begründung eines Anfangsverdachts (sog. Frühwirkung).¹⁶ Es ist davon auszugehen, dass dieses weite Verwendungsverbot im Hinblick auf die nach Art. 33 und 34 DSGVO geforderten rein tatsächlichen Angaben zumindest bei Bußgeldverfahren gegen Unternehmen i. S. v. Art. 101, 102 AEUV gegen das EU-Recht verstößt, da solche Angaben nach der Rechtsprechung des EuGH nicht unter das
---	--	--

¹⁵ Kommt durch die Formulierung „verwendet“ statt „verwertet“ zum Ausdruck, vgl. zu § 97 Abs. 1 S. 3 InsO BT-Drs. 12/7302, 166; OLG Düsseldorf Beschl. v. 1.6.2016 – 2 Ws 299/16, BeckRS 2016, 127246 Rn. 15; LG Stuttgart Beschl. v. 21.7.2000 – 11 Qs 46/00, NZI 2001, 498; LG Potsdam Beschl. v. 24.4.2007 – 27 Ns 23/06, BeckRS 2009, 5070.

¹⁶ Vgl. SJTK/Schwartmann/Burkhardt BDSG § 43 Rn. 13 m. w. N.; a. A. im Hinblick auf Erwägungsgrund 87 S. 3 DSGVO weniger streng, Datenpannenmeldungen bzw. -benachrichtigungen seien auch verwertbar, sofern die aus diesen hervorgehenden Erkenntnisse hypothetisch auch bei einer direkten Prüfung durch die Aufsichtsbehörde bzw. im Rahmen einer Beschwerde erkannt worden wäre, HBfDI 47. Tätigkeitsbericht 2018, 172; HK-HDSIG/Rost § 37 Rn. 35.

	<u>2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 in einem Straf- oder Bußgeldverfahren gegen die meldepflichtige oder benachrichtigende Person oder deren in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung der meldepflichtigen oder benachrichtigenden Person verwendet werden.</u>	Verbot der Selbstbezeichnung fallen ¹⁷ und die Mitgliedstaaten mangels Öffnungsklausel ¹⁸ keine Verfahrensvorschriften schaffen dürfen, die die unionsweit einheitliche Durchsetzung und Effektivität (effet utile) der DSGVO untergraben. ¹⁹ Der Vergleich mit dem nationalen Datenschutzrecht anderer Mitgliedstaaten der EU zeigt, dass bisher – soweit ersichtlich – kein anderer Mitgliedstaat ein solches Beweisverwendungsverbot, das auch in der deutschen Literatur im Hinblick auf die Unionsrechtskonformität Kritik erfährt, ²⁰ eingeführt hat und die anderen EU-Aufsichtsbehörden in der Praxis insofern auch keine Einschränkungen vornehmen. ²¹ Nicht zuletzt sieht auch Erwägungsgrund 87 Satz 3 DSGVO ausdrücklich vor, dass die
--	--	---

¹⁷ Vgl. EuGH Urt. v. 18.10.1989 – 374/98, BeckRS 2004, 71022 Rn. 37 ff.; EuG Urt. v. 8.7.2004 – T-50/00, BeckRS 2004, 70472 Rn. 47.

¹⁸ Für § 43 Abs. 4 BDSG berufen sich die Gesetzgebenden auf Art. 83 Abs. 8 DSGVO, BT-Drs. 18/11325, 109.

¹⁹ Vgl. ausführlich Kühling/Buchner/Bergt BDSG § 43 Rn. 11 ff. m. w. N.

²⁰ Ausführlich zum Meinungsstand Kühling/Buchner/Bergt BDSG § 43 Rn. 11 ff.

²¹ Vgl. insofern im Hinblick auf die anerkannten europäischen Grundsätze eine Anpassung der nationalen Gesetze erwartend HK-HDSIG/Rost § 36 Rn. 33, § 37 Rn. 38 f.

		Aufsichtsbehörden die Datenpannenmeldungen bzw. -benachrichtigungen zum Anlass von Maßnahmen gegen die Meldenden nehmen dürfen. ²²
§ 29a (Neue Vorschrift)	§ 29a Ordnungswidrigkeiten bei Verstößen gegen Artikel 20 Verordnung (EU) 2024/900 (1) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2024/900 in der Fassung vom 13. März 2024 verstößt, indem er vorsätzlich oder fahrlässig entgegen Artikel 20 der Verordnung (EU) 2024/900 als Verantwortlicher keine geeigneten Maßnahmen ergreift, um auf Ersuchen von Interessenten im Einklang mit Artikel 17 Absatz 2 die Informationen nach Artikel 19 kostenlos zu übermitteln.	Wir gehen davon aus, dass der Bundesgesetzgeber eine Bußgeldvorschrift in Umsetzung von Artikel 25 Absatz 1 TTPW-VO für Verstöße gegen Artikel 20 TTPW-VO nicht erlassen wird (wie er es bundesweit aber z. B. sonst auch bei § 28 Absatz 1 Nummer 13 TDDDG in Umsetzung von Artikel 15a Absatz 1 Satz 1 Richtlinie (EU) 2002/58/EG getan hat). Der Regierungsentwurf enthält im Gegensatz zu früheren Entwürfen in § 14 Absatz 1 PWTG-E keinen eigenen Bußgeldtatbestand mehr für Verstöße gegen Artikel 20 TTPW-VO. Dies wurde vom Bundesrat in seiner Stellungnahme leider nicht kritisiert (vgl. BR-Drs. 766/25 (Beschluss)). Der Bundesgesetzgeber scheint davon auszugehen, dass die Befugnisse (u.a. Anordnung und Zwangsgeldverhängung) der BfDI in § 8 PWTG-E als Sanktion oder andere Maßnahmen ausreichend sind.

²² Kühling/Buchner/Bergt BDSG § 43 Rn. 13 m. w. N.

	(2) ¹Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 300.000 Euro geahndet werden. ²Gegenüber einer juristischen Person oder Personenvereinigung mit einem Gesamtumsatz von mehr als fünf Millionen Euro kann abweichend von Satz 1 in Verbindung mit § 30 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten eine Ordnungswidrigkeit nach Absatz 1 mit einer Geldbuße von bis zu 6 Prozent des Gesamtumsatzes geahndet werden. ³Gesamtumsatz nach Satz 2 ist die Summe aller Umsatzerlöse, die die juristische Person oder Personenvereinigung in dem der Behördenentscheidung vorausgegangenen Geschäftsjahr weltweit erzielt hat. ⁴Der Gesamtumsatz kann geschätzt werden.	Wir halten ein Absehen von einem Bußgeldtatbestand für verfehlt, da Artikel 25 Absatz 1 TTPW-VO klar die Schaffung von Vorschriften über Sanktionen bzw. andere Maßnahmen von den Mitgliedstaaten verlangt, die für Sponsoren oder Anbieter politischer Webdienstleistungen bei Verstößen gegen Artikel 20 TTPW-VO erforderlich sind. Für eine wirksame Durchsetzung des Artikel 20 TTPW-VO dürfte in der Praxis nach unserer Auffassung jedoch einer Bußgeldvorschrift notwendig sein und nicht bloß eine Anordnungs befugnis, da letztere entgegen Artikel 25 Absatz 1 Satz 2 TTPW-VO wenig Abschreckungswirkung für große Unternehmen haben dürfte. Bei Artikel 20 TTPW-VO greift der One-Stop-Shop auf europäischer Ebene nicht, sodass wir für die Durchsetzung als Behörde auch unmittelbar für die größten international agierenden Plattformbetreibern, die ihre deutsche Hauptniederlassung in Berlin haben, zuständig wären. Zumal § 8 PWTG-E in der derzeitigen Ausgestaltung nur Befugnisse der BfDI, nicht aber der Landesdatenschutzbehörden regelt, sodass wir diese Maßnahmen nicht ergreifen dürften bei Verstößen gegen Artikel 20 TTPW-VO.
--	--	--

	(3) § 17 Absatz 2 des Gesetzes über Ordnungswidrigkeiten ist nicht anzuwenden. (4) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit, sofern sie oder er nach § 8 Absatz 5 für die Durchsetzung der Verordnung (EU) 2024/900 in der Fassung vom 13. März 2024 zuständig ist.	Vorsichtshalber empfehlen wir daher dem Berliner Landesgesetzgeber, selber eine entsprechende Bußgeldvorschrift zu erlassen. Bei den restlichen Vorgaben, insbesondere dem Bußgeldrahmen, haben wir uns an § 14 Absatz 2, 3, 5 bis 7 PWTG orientiert.
§ 43 Abs. 7 Satz 3 (7) ³Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit zu erteilen, soweit nicht die zustän-	§ 43 (7) ³Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der oder dem Berliner Beauftragten für Datenschutz und Informationsfreiheit zu erteilen, soweit nicht die zustän-	Ein Grund für die Beschränkung einer möglichen Auskunftserteilung an die oder den BlnBDI ist nicht ersichtlich. Die bzw. der BlnBDI ist eine unabhängige oberste Landesbehörde, deren Beschäftigte zur strikten Geheimhaltung der ihnen dienstlich bekannt gewordenen Informationen verpflichtet sind. Die bisherige Regelung kann zu Fällen führen, in denen Betroffene die Einschränkung ihres

dige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eine Landes gefährdet würde.	dige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eine Landes gefährdet würde.	Auskunftsrechts durch eine unabhängige Datenschutzaufsichtsbehörde kontrollieren lassen kann. Dies verstößt gegen die europarechtlichen Vorgaben (vgl. Erwägungsgrund 48 JI-Richtlinie sowie Art. 17 JI-Richtlinie).
§ 45 (2) ¹Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des § 43 Absatz 6 und des § 44 Absatz 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.	§ 45 (2) ¹Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des § 43 Absatz 6 und des § 44 Absatz 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde. <u>²Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung.</u> ³Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität erforderlich ist. <u>⁴Der Verantwortliche unterrichtet die</u>	Die bisherigen Laufzeiten von teilweise vielen Monaten für die Bearbeitung der Anträge von Betroffenen sind unzureichend. Gemäß Erwägungsgrund 40 Satz 2 JI-Richtlinie sollte der Verantwortliche verpflichtet werden, den Antrag der betroffenen Person unverzüglich zu beantworten. Erwägungsgrund 43 Satz 1 JI-Richtlinie sieht weiterhin vor, das Recht auf Auskunft solle „problemlos“ geltend gemacht werden können. Eine zügige Bearbeitungsdauer von Anträgen Betroffener ist für die wirksame Durchsetzung eines effektiven Selbstschutzes unabdingbar. Die vorgesehenen Fristen laufen gleich mit den bereits in der Praxis bewährten Vorgaben in der DSGVO (vgl. Art. 12 Abs. 3 DSGVO).

	<u>betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung.</u>	
§ 46 (Neue Vorschrift)	§ 46 (neu) (2) ¹ Mit den Aufgaben aus Abs. 1 ist eine besondere Stelle der Gerichtsbarkeit betraut, soweit personenbezogene Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit verarbeitet werden. Für die Rechtsstellung der Mitglieder dieser besonderen Stelle und ihre Befugnisse gelten § 10 Abs. 1 bis Abs. 5 BlnDSG und § 13 Abs. 2 bis Abs. 6, Abs. 8 BlnDSG entsprechend. Der Senat wird ermächtigt, den besonderen Stellen durch Rechtsverordnung weitere Aufgaben zu übertragen, soweit	Art. 8 GRCh verpflichtet die Mitgliedsstaaten, die Einhaltung von Datenschutzvorschriften durch eine unabhängige Stelle überwachen zu lassen. In Erwägungsgrund 80 JI-Richtlinie wird hinsichtlich der Kontrolle der von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Datenverarbeitung, für die die Aufsichtsbehörden nicht zuständig sind, insoweit klargestellt, dass diese Datenverarbeitung in jedem Fall stets der unabhängigen Überwachung unterliegt. Diese europarechtlich verpflichtende Vorgabe findet sich für Gerichte bisher nicht im 3. Teil des BlnDSG. Der Vorschlag ist angelehnt an Erwägungsgrund 20 DSGVO, der vorsieht, mit der Aufsicht über Datenverarbeitungsvorgänge der Gerichte besondere Stellen im Jus-

	sie die Verarbeitung personenbezogener Daten durch Strafgerichte im Rahmen ihrer justiziellen Tätigkeit betreffen.	tizsystem des Mitgliedstaats zu betrauen, die insbesondere die Einhaltung der datenschutzrechtlichen Vorschriften sicherstellen, Richter:innen und Staatsanwält:innen für ihre datenschutzrechtlichen Pflichten sensibilisieren und Beschwerden in Bezug auf Datenverarbeitungsvorgänge bearbeiten. Die Dienstaufsicht über den oder die Präsidenten des jew. Gerichtes ist hierfür unzureichend, da dort neben datenschutzrechtlichen auch andere Erwägungen eine entscheidende Rolle spielen können. Der gerichtliche Instanzenzug garantiert nicht die institutionelle, funktionelle und materielle Unabhängigkeit der aufsichtsführenden Stelle und kennt kein isoliertes Beschwerderecht, was Art. 8 Abs. 3 GrCh jeweils vorsieht.²³ Neben rechtlichem Sachverstand sollte in der zu schaffenden Stelle auch technischer Sachverstand verstetigt werden. Der bisherige Absatz 2 wird Absatz 3.
--	---	--

²³ Vgl. Jarass GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta Art. 8 Rn. 22; Stern/Sachs/Johlen, 1. Aufl. 2016, GRCh Art. 8 Rn. 64.

§ 55 Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 3 Satz 1 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.	§ 55 Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 3 Satz 1 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.	Diese Regelung ist nicht mit den Vorgaben des Art. 28 der JI-Richtlinie zu vereinbaren und daher europarechtswidrig. Abgesehen davon, dass diese Begriffe äußerst dehnbar sind, weil jede Stelle dazu neigt, ihre Maßnahmen für äußerst dringlich zu halten, wird damit eine zweifelhafte und Rechtsgüter gefährdende Datenverarbeitung trotz aller Bedenken ermöglicht, bevor die Prüfung durch die Aufsichtsbehörde abgeschlossen ist. Und dies, obwohl die zur Prüfung vorgesehene 6- (max. 10-) Wochenfrist ohnehin schon extrem kurz bemessen ist und in einer digitalisierten Welt eine Rechtsverletzung bereits erhobener Daten kaum wieder rückgängig gemacht werden kann.
§ 58 ¹Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den	§ 58 ¹Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den	§ 58 Satz 1 BlnDSG dient der Umsetzung von Art. 6 JI-RL, der vorgibt, dass: „Die Mitgliedstaaten sehen vor, dass der Verantwortliche gegebenenfalls und so weit wie möglich zwischen den

verschiedenen Kategorien betroffener Personen zu unterscheiden.	verschiedenen Kategorien betroffener Personen <u>klar</u> zu unterscheiden.	personenbezogenen Daten verschiedener Kategorien betroffener Personen klar unterscheidet, darunter: [...]“ Das Wort „klar“ hat es nicht in die Umsetzung des § 58 Satz 1 BlnDSG geschafft, ²⁴ sollte jedoch zur Hervorhebung richtlinienkonform nachträglich aufgenommen werden, da die klare Unterscheidung eine höhere Anforderung stellt als die bloße Unterscheidung.
§ 59 ² Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen.	§ 59 ² Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist , Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen.	§ 59 BlnDSG dient der Umsetzung von Art. 7 Abs. 1 JI-RL. ²⁵ In Art. 7 Abs. 1 JI-RL wird die Unterscheidungspflicht zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten nur anhand der Möglichkeit, nicht der Angemessenheit eingeschränkt. § 59 Satz 2 ist deshalb richtlinienkonform dahingehend anzupassen, dass die Angemessenheit als Befreiung von der Kenn-

²⁴ Vgl. dazu Gola/Heckmann/Scheurer BDSG § 72 Rn. 6; Sydow/Marsch/Johannes/Weinhold DS-GVO BDSG § 72 Rn. 3; Sydow/Johannes/Weinhold BDSG § 72 Rn. 3; HK-LDSG NRW/Johannes/Weinhold § 42 Rn. 3.

²⁵ Abgeordnetenhaus von Berlin Drs. 18/1033, 111.

		zeichnungspflicht nicht länger als weiteres Einschränkungsmerkmal vorgesehen wird. ²⁶ Die Ausnahme der Angemessenheit führt zu einer Abwägung im Einzelfall, die das Unionsrecht so gerade nicht vorsieht.
§ 60 (1) ¹Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden.	§ 60 (1) ¹Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig, <u>unvollständig</u> oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden.	Der Berliner Gesetzgeber hat bewusst davon abgesehen, in § 60 Abs. 1 Satz 1 BlnDSG entsprechend der Vorgabe in Art. 7 Abs. 2 JI-RL aufzunehmen, dass unvollständige personenbezogene Daten nicht übermittelt oder bereitgestellt werden sollen.²⁷ Die Übernahme dieser Regelung würde nach Ansicht der Gesetzgeber dazu führen, dass eine Datenübermittlung gerade zu dem Zweck der Vervollständigung unvollständiger Daten ausgeschlossen wäre, so dass darauf verzichtet wurde.²⁸ Dieser Argumentation ist mit einer richtlinienkonformen Anpassung des

²⁶ Vgl. ebenfalls kritisch Auernhammer/Herbst BDSG § 73 Rn. 12; Gola/Heckmann/Scheurer BDSG § 73 Rn. 11; Kühling/Buchner/Schwichtenberg BDSG § 73 Rn. 6.

²⁷ Abgeordnetenhaus von Berlin Drs. 18/1033, 111; BT-Drs. 18/11325, 119.

²⁸ Abgeordnetenhaus von Berlin Drs. 18/1033, 111; BT-Drs. 18/11325, 119.

		§ 60 Abs. 1 Satz 1 BlnDSG entgegenzutreten.²⁹ Die Begründung des Berliner Gesetzgebers überzeugt nicht, da das dargestellte Szenario einen Ausnahmefall darstellt und mittels teleologischer Reduktion in der Anwendung eines gänzlich umgesetzten § 60 Abs. 1 Satz 1 BlnDSG berücksichtigt werden kann.³⁰ Zwar können auch unvollständige Daten für die betroffenen Personen positiv sein (zB entlastende Beweise),³¹ im Standardfall führt die Übermittlung unvollständiger Daten aber häufig zu Problemen in bearbeiteten Vorgängen. Nicht nur leidet unter ihr allgemein die Qualität der Datenbestände, auch können Personen aufgrund fehlender Identifizierungsmerkmale verwechselt werden. Verfehlt ist insofern der zum Teil vertretene Ansatz, unvollständige Daten hilfsweise als Unterfall unrichtiger Daten zu verstehen,³² da allein die Unvollständigkeit von Daten nicht zwangsläufig den Rückschluss auf
--	--	---

²⁹ Vgl. HK-BDSG/Johannes/Weinhold § 74 Rn. 23; i. E. auch BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 74 Rn. 23; Gola/Heckmann/Marnau BDSG § 74 Rn. 13; Paal/Pauly/Paal BDSG § 74 Rn. 5.

³⁰ Insofern für § 74 BDSG einen Ausnahmetatbestand vorschlagend BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 74 Rn. 23; Gola/Heckmann/Marnau BDSG § 74 Rn. 13; Paal/Pauly/Paal BDSG § 74 Rn. 5.

³¹ Vgl. BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 74 Rn. 23.

³² Vgl. Auernhammer/Herbst BDSG § 74 Rn. 7; BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 74 Rn. 23; HK-BDSG/Johannes/Weinhold § 74 Rn. 23.

		ihre Unrichtigkeit zulässt; z. B. sind Tag und Monat des Geburtstags einer natürlichen Person ohne das Geburtsjahr nicht falsch, sondern unvollständig.
§ 60 (1) ² Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen.	§ 60 (1) ² Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich <u>durchführbar</u> ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen.	Die Beschränkung der Überprüfungspflicht in § 60 Abs. 1 Satz 2 BlnDSG auf das, was mit „angemessenem Aufwand möglich“ ist, ist als europarechtswidrig einzustufen, da Art. 7 Abs. 2 S. 2 JI-RL nur eine Begrenzung hinsichtlich der Durchführbarkeit der Überprüfung („soweit durchführbar“) und nicht hinsichtlich der Angemessenheit enthält. ³³ Statt einer Kosten-Nutzen-Abwägung (insbesondere hinsichtlich der personellen Kapazitäten der jeweiligen Behörde) haben die Verantwortlichen die Überprüfung richtlinienkonform ausschließlich dann nicht durchzuführen, wenn die Überprüfung technisch-organisatorisch nicht möglich ist. ³⁴
§ 60 Abs. 1 Satz 3	§ 60 Abs. 1 Satz 3	§ 60 Abs. 1 Satz 3 BlnDSG ist richtlinienkonform dahingehend anzupassen, dass die Angemessenheit kein Kriterium

³³ Kritisch auch BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 74 Rn. 28; Gola/Heckmann/Marnau BDSG § 74 Rn. 2, 18; Kühling/Buchner/Schwichtenberg BDSG § 74 Rn. 3; Paal/Pauly/Paal BDSG § 74 Rn. 6; a. A. HK-DSG NRW/Johannes/Weinhold § 44 Rn. 24; insofern auf Erwägungsgrund 53 S. 1 JI-RL abstellend, der allerdings Ausführungen zu „geeigneten“ technischen und organisatorischen Maßnahmen enthält, HK-LDSG RhPf/Braun § 62 Rn. 22 ff.

³⁴ Vgl. BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 74 Rn. 28; Gola/Heckmann/Marnau BDSG § 74 Rn. 18; a. A. HK-DSG NRW/Johannes/Weinhold § 44 Rn. 24.

Bei jeder Übermittlung personenbezogener Daten hat er zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.	Bei jeder Übermittlung personenbezogener Daten hat er zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.	für die Pflicht ist, weil Art. 7 Abs. 2 Satz 3 JI-RL nur die Ausnahme der Unmöglichkeit („nach Möglichkeit“) vorsieht. ³⁵ Das Unionsrecht sieht gerade keine Abwägung im Einzelfall vor, sondern lediglich eine Beschränkung hinsichtlich der Möglichkeit.
§ 61 Abs. 3 Satz 2 Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt worden, ist auch dies dem Empfänger mitzuteilen.	§ 61 Abs. 3 Satz 2 Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt worden, ist auch dies <u>unverzüglich</u> dem Empfänger mitzuteilen.	Die Mitteilungen nach § 61 Abs. 3 Satz 2 BlnDSG haben im Hinblick auf die Regelung des Art. 7 Abs. 3 S. 1 JI-RL richtlinienkonform „unverzüglich“ zu erfolgen. ³⁶ Dieses zeitliche Element fehlt bisher unionsrechtswidrig in § 61 Abs. 3 Satz 2 BlnDSG.
§ 63	§ 63	Hinter der unionsrechtlichen Vorgabe bleibt § 63 BlnDSG vom Wortlaut zurück, da Art. 48 JI-RL von den Mitglied-

³⁵ Kritisch auch BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 74 Rn. 30; Gola/Heckmann/Marnau BDSG § 74 Rn. 20; Kühling/Buchner/Schwichtenberg BDSG § 74 Rn. 3; a. A. nur eine enge Auslegung der Angemessenheit fordernd HK-DSG NRW/Johannes/Weinhold § 44 Rn. 26; HK-LDSG RhPf/Braun § 62 Rn. 32; wohl auch Paal/Pauly/Paal BDSG § 74 Rn. 6a.

³⁶ Vgl. BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 75 Rn. 6.

Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.	¹Der Verantwortliche hat zu ermöglichen <u>und zu fördern</u>, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können. <u>²§ 5 Absatz 5 Satz 2 gilt für die zur Entgegennahme dieser Meldungen betraute Stelle entsprechend.</u>	staaten nicht nur die Ermöglichung, sondern auch die Förderung der Enthüllung von Missständen (Whistleblowing) fordert, so dass § 63 BlnDSG entsprechend richtlinienkonform anzupassen ist.³⁷ Die Pflicht der Verantwortlichen nach § 63 BlnDSG, zu fördern, dass ihnen vertrauliche Meldungen über in ihrem Verantwortungsbereich erfolgende Datenschutzverstöße zugeleitet werden können, soll das vertrauliche Melden von Datenschutzverstößen gegenüber den Behörden erleichtern und absichern und damit die Aufklärung von Verstößen gegen das Datenschutzrecht erleichtern.³⁸ Die schlanke Struktur des § 63 enthält nur einen Satz mit einer vagen Vorgabe, ohne dass die konkret zu treffenden Maßnahmen der Förderung und des Schutzes von Meldungen über Datenschutzverstöße gesetzlich vorgegeben werden. Die Gesetzgebenden haben insofern leider nicht die unionsrechtlich zulässige (vgl. Art. 1 Abs. 3 JI-RL)
---	---	--

³⁷ Vgl. Kühling/Buchner/Schwichtenberg BDSG § 77 Rn. 2; HK-BDSG/Johannes/Weinhold § 77 Rn. 2; HK-DSG NRW/Franck § 66 Rn. 2; Hornung/Schindler/Schneider ZIS 2018, 566 (569); a. A. wohl BeckOK DatenschutzR/Burghardt/Reinbacher BDSG § 77 Rn. 4; Gola/Heckmann/Scheurer BDSG § 77 Rn. 2; LDSG RhPf/Braun § 65 Rn. 11.

³⁸ Vgl. Paal/Pauly/Paal BDSG § 77 Rn. 2; HK-BDSG/Johannes/Weinhold § 77 Rn. 1.

		Möglichkeit wahrgenommen, organisatorische Mindeststandards festzulegen. Zumindest eine Verschwiegenheitspflicht sollte etabliert werden. ³⁹
§ 65 Abs. 3 (Krae) ¹Der Verantwortliche hat die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit jährlich über Übermittlungen zu unterrichten, die auf Grund einer Beurteilung nach Absatz 1 Nummer 2 erfolgt sind. ²In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.	§ 65 Abs. 3 ¹Der Verantwortliche hat die Berliner Beauftragte oder den Berliner Beauftragten für Datenschutz und Informationsfreiheit jährlich über Übermittlungen zu unterrichten, die auf Grund einer Beurteilung nach Absatz 1 Nummer 2 erfolgt sind. <u>²Fehl- anzeige ist erforderlich.</u> ³In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.	Bei teleologischer Betrachtung ergibt sich, dass die Unterrichtungspflicht auch die Pflicht zur Fehlanzeige umfasst. Nur so ist gewährleistet, dass die Aufsichtsbehörde einen tatsächlichen Überblick über die Zahl der Übermittlungen in Drittländer erhält und etwaige, versehentlich ausgebliebene Meldungen nicht fälschlicherweise als unterbliebene Übermittlungen gewertet werden. Dem entspricht auch die Verwendung des unbestimmten Artikels im Gesetz. Ein anderes Verständnis könnte zudem dazu führen, dass sämtliche nicht meldende Stellen im Zweifel durch die Aufsichtsbehörde kontaktiert werden müssten, was dem proaktiven Charakter dieser Unterrichtungspflicht klar widerspricht.

³⁹ Vgl. z. B. die entsprechende Anwendung der Verschwiegenheitspflichten der Datenschutzbeauftragten in Art. 36 S. 2, Art. 12 Abs. 2 BayDSG für die zur Entgegennahme der Meldungen betraute Stelle.

§ 71 Abs. 3 Die Artikel 13, 14, 15 und 19 der Verordnung (EU) 2016/679 sind nicht anzuwenden.	§ 71 Abs. 3 Artikel 13, 14, 15 und 19 der Verordnung (EU) 2016/679 sind <u>ist</u> nicht anzuwenden.	Die Berliner Gesetzgebenden gingen wie die Bundesgesetzgebenden davon aus, dass die Vergabe öffentlicher Auszeichnungen und Ehrungen als außergerichtlicher Gunstbeweis, den die öffentliche Stelle der Person gewährt, die sie für auszeichnungswürdig hält, eine Tätigkeit ist, die nicht in den Anwendungsbereich des Unionsrechts fällt und damit auch nicht in den der DSGVO nach Art. 2 Abs. 2 lit. a DSGVO.⁴⁰ Für diese Fälle finden daher gemäß § 2 Abs. 9 die DSGVO und Teile 1 und 2 des BlnDSG entsprechend Anwendung, soweit nicht Abweichendes geregelt ist.⁴¹ Der Annahme der Unanwendbarkeit der DSGVO ist allerdings zu widersprechen, da die Kompetenz der EU nach Art. 16 Abs. 2 AEUV und damit auch Art. 2 Abs. 2 lit. a DSGVO die Regelung eines einheitlichen europäischen Datenschutzniveaus umfasst und entsprechende Ausnahmen hiervon gemäß der Rechtsprechung des EuGH⁴² restriktiv zu handhaben sind.⁴³ Zu den Ausnahmen dürften z. B.
---	--	--

⁴⁰ Abgeordnetenhaus von Berlin Drs. 18/1033, 114; vgl. zu § 86 BDSG: BT-Drs. 19/4674, 211.

⁴¹ Abgeordnetenhaus von Berlin Drs. 18/1033, 114.

⁴² Vgl. EuGH Urt. v. 9.7.2020 - C-272/19, ZD 2020, 577 Rn. 68.

⁴³ Vgl. ausführlich Kühling/Buchner/Schwichtenberg BDSG § 86 Rn. 2.

		Tätigkeiten im Rahmen der nationalen Sicherheit wie die Verarbeitung durch Streitkräfte oder Nachrichtendienste der Mitgliedstaaten gehören.⁴⁴ Der EuGH hat mittlerweile auch festgestellt, dass die DSGVO auf die Verarbeitung personenbezogener Daten durch die Ausschüsse der mitgliedstaatlichen Parlamente Anwendung findet und Art. 2 Abs. 2 lit. a DSGVO nicht greift.⁴⁵ Mit der Verarbeitung personenbezogener Daten im Rahmen der Vorbereitung und Durchführung von Auszeichnungen und Ehrungen gehen durch die zum Teil umfangreiche Verarbeitung personenbezogener Daten Eingriffe in Art. 7 und 8 GRCh sowie diverse Risiken für die Rechte und Freiheiten der betroffenen Personen einher, z. B. bei Verarbeitung unrichtiger personenbezogener Daten, dem Entzug von Orden oder der (ungewollten) Veröffentlichung der Ablehnung einer Auszeichnung oder Ehrung.⁴⁶ Dementsprechend sind keine ausreichenden Gründe ersichtlich, im Rahmen des § 71
--	--	--

⁴⁴ Vgl. Art. 4 Abs. 2 S. 3 EUV; Taeger/Gabel DS-GVO Art. 2 Rn. 14 m. w. N.; zu Datenverarbeitungen mit dem Ziel, lediglich die nationale Sicherheit eines Drittstaats zu schützen, die unter die DSGVO fallen, s. EuGH Urt. v. 16.7.2020 – C-311/18, GRUR-RS 2020, 16082 Rn. 80 ff.

⁴⁵ EuGH Urt. v. 9.7.2020 – C-272/19, ZD 2020, 577 Rn. 66 ff.; vorsichtshalber die DSGVO auf die gesamte Verarbeitung durch die mitgliedstaatlichen Parlamente anwendbar sehend BeckOK DatenschutzR/Bäcker DS-GVO Art. 2 Rn. 9e; aA Grzeszick/Schwartzmann/Mühlenbeck NVwZ 2020, 1491.

⁴⁶ Vgl. Sydow ZD 2019, 189 (190).

		die Vorgaben der DSGVO zu ignorieren, so dass die Zulässigkeit von Abweichungen der Berliner Gesetzgebung an den Öffnungsklauseln der DSGVO zu messen ist.⁴⁷ Die Betroffenenrechte nach Art. 12 ff. DSGVO können nicht einfach durch mitgliedstaatliches Recht ausgeschlossen werden.⁴⁸ Ohne die nach § 71 Abs. 3 BlnDSG ausgeschlossenen Betroffenenrechte besteht die Gefahr, dass die betroffenen Personen hinsichtlich der Verarbeitung ihrer Daten hilflos gestellt sind. Sollte es z. B. dazu kommen, dass im Rahmen der Vorbereitungsphase entschieden wird, die Auszeichnung oder Ehrung nicht zu verleihen, wird die betroffene Person ohne Information nach Art. 13-14 DSGVO davon in der Regel niemals erfahren oder jedenfalls bei Kenntnis darüber nicht über ihr Auskunftsrecht nach Art. 15 DSGVO in Erfahrung bringen können, welche Informationslage und Gründe zur Ent-
--	--	---

⁴⁷ Vgl. Kühling/Buchner/Schwichtenberg BDSG § 86 Rn. 2.

⁴⁸ Kritisch zum Ausschluss der Betroffenenrechte auch Kühling/Buchner/Schwichtenberg BDSG § 86 Rn. 6; HK-BDSG/Braun § 86 Rn. 29 ff., 37 ff.; Sydow ZD 2019, 189.

		scheidung geführt haben und welche Daten zu ihnen gespeichert wurden.⁴⁹ Im Hinblick auf den Ausschluss nach § 71 Abs. 3 ist daher genau zu prüfen, ob dies durch Öffnungsklauseln in der DSGVO gedeckt ist. Das dürfte nur hinsichtlich Art. 14 DSGVO der Fall sein, da hierfür Art. 14 Abs. 5 lit. c DSGVO eine Öffnungsklausel für die Mitgliedstaaten vorsieht, die vorliegend durch die strenge Zweckbindung nach § 71 Abs. 1 Satz 2 BlnDSG erfüllt sein dürfte. Art. 13, 15⁵⁰ und 19 DSGVO finden daher uneingeschränkt auch im Rahmen des § 71 BlnDSG Anwendung und müssen von den verarbeitenden Stellen beachtet werden, insbesondere durch eine Datenschutzerklärung bei Erhebung personenbezogener Daten unmittelbar bei den betroffenen Personen (sinnvollerweise mit der Einräumung eines das Verfahren abbrechenden Widerspruchsrechts⁵¹) und durch Auskünfte an diese.
--	--	--

⁴⁹ Vgl. BeckOK DatenschutzR/Hilgers BDSG § 86 Rn. 10.

⁵⁰ Vgl. so i. E. auch im Hinblick auf Art. 8 Abs. 2 S. 2 GRCh Weichert Stellungnahme LDSG BW, 4; einschränkend, die Anwendung der Informationspflichten und das Auskunftsrecht nur bei Ordensentziehungen und Rücknahmen von Annahmegenehmigungen fordernd HK-BDSG/Braun § 86 Rn. 33.

⁵¹ Vgl. HK-BDSG/Braun § 86 Rn. 26.