

Fragebogen zur Evaluierung des BDSG

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Stand: 15. Januar 2021

Teil 1

I. Anwendungsbereich und Begriffsbestimmungen

1. Ist der Anwendungsbereich in § 1 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Nein. Es ist problematisch, dass durch das BDSG sowohl die Anpassungen an die DSGVO vorgenommen werden als auch die Umsetzung der JR-Richtlinie erfolgt. Dies führt zu einer unnötigen Verkomplizierung des Anwendungsbereichs des BDSG und zieht sich wie ein roter Faden durch die „Gemeinsamen Bestimmungen“ und zwingt dann zu einer weiteren Festlegung des jeweiligen Anwendungsbereichs der Teile 2 und 3. Eine Ausgliederung der Umsetzung der JR-Richtlinie in ein eigenständiges Gesetz dient der Rechtsklarheit (siehe Definitionskatalog) und der Anwendungsklarheit (Entbehrlichkeit der Abgrenzung von Teil 2 und 3).

2. Ist der Anwendungsbereich in § 45 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

In unserem Verband sind keine Auftragsverarbeiter i. S. d. der Richtlinie (EU) 2016/680 vertreten, daher verzichten wir auf eine entsprechende Kommentierung.

3. Sind die Begriffsbestimmungen in § 2 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Die Begriffsbestimmungen in § 2 BDSG sind aus unserer Sicht – jedenfalls teilweise – nicht normenklar und damit auch nicht praktikabel. Es gibt öffentliche Stellen, die nur teilweise am Wettbewerb teilnehmen und bei denen sich die Frage stellt, ob sie als nichtöffentliche Stelle gelten.

Eine Klarstellung könnte durch die Formulierung „ganz oder teilweise“ in Absatz 5 Satz 1 erreicht werden.

II. Rechtsgrundlagen für die Datenverarbeitung

1. Sind die Rechtsgrundlagen für die Datenverarbeitung in den §§ 3, 4, 22, 23 und 24 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

- Die Rechtsgrundlagen für die Datenverarbeitung in § 3 BDSG sind nur dann sachgerecht, praktikabel und normenklar geregelt, wenn die Aufgaben der öffentlichen Stellen in den jeweiligen Fachgesetzen so geregelt sind, dass die Aufgaben in den Fachgesetzen hinreichend genau beschrieben sind und somit die Erforderlichkeit beurteilbar ist.
- Mit Blick auf das Urteils des BVerwG vom 7. März 2019 (AZ. 6 C 2.18) ist klargestellt, dass § 4 BDSG im Anwendungsbereich der DSGVO nicht mehr angewendet werden darf. Dies muss gesetzlich durch die Streichung des § 4 BDSG im Teil „Gemeinsame Bestimmungen“ klargestellt werden. Hier

manifestiert sich die eingangs geäußerte Kritik an der gemeinsamen Anpassung an DSGVO und Umsetzung der JR-Richtlinie in einem Gesetz. Es sollte eine Anpassung an die DSGVO einerseits und Umsetzung der JR-Richtlinie in verschiedenen Gesetzen erfolgen und § 4 BDSG – wenn überhaupt – in dem Gesetz zur Umsetzung der JR-Richtlinie genannt werden.

- **Die Rechtsgrundlagen für die Datenverarbeitung in § 22 BDSG sind nicht sachgerecht, praktikabel und normenklar geregelt.**

a. Die Vorgaben in § 22 Abs. 2 BDSG enthalten teilweise dieselben Anforderungen wie Art. 32 DSGVO:

- Pseudonymisierung
 - Art. 32 Abs. 1 Buchst. a DSGVO: Pseudonymisierung und Verschlüsselung personenbezogener Daten
 - § 22 Abs. 2 Ziff. 6 BDSG: Pseudonymisierung personenbezogener Daten;
 - § 22 Abs. 2 Ziff. 7 BDSG: Verschlüsselung personenbezogener Daten
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
 - Art. 32 Abs. 1 Buchst. b, c DSGVO: die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
 - § 22 Abs. 2 Ziff. 8 BDSG: Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
 - Art. 32 Abs. 1 Buchst. d DSGVO: ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
 - § 22 Abs. 2 Ziff. 9 BDSG: zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Daher wird zur Erhöhung der Rechtssicherheit vorgeschlagen, auf die Wiederholung der Vorgaben der DSGVO zu verzichten, d.h. § 22 Abs. 2 Ziff. 6, 7, 8, 9 BDSG zu entfernen.

b. § 22 Abs. 2 Ziff. 1 beinhaltet die Vorgabe, die Verarbeitung besonderer Kategorien personenbezogener Daten so durchzuführen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt. Jede Verarbeitung personenbezogener Daten, welche nicht den Anforderungen der

Verordnung (EU) 2016/679 genügt, erfolgt rechtswidrig. Eine Aufforderung, sich an europäisches Recht zu halten, erscheint nicht zielführend. Daher wird empfohlen, § 22 Abs. 2 Ziff. 1 BDSG zu entfernen

- Die Erfordernis, ob die Vorgaben in § 22 Abs. 2 BDSG verpflichtend bei der Verarbeitung besonderer Kategorien personenbezogener Daten zu beachten sind, wird unterschiedlich ausgelegt. Einerseits ist der Wortlaut „können dazu insbesondere gehören“, was nahelegt, dass der Verantwortliche selbst entscheidet, ob er die Maßnahmen berücksichtigt. Andere Autoren leiten eine Pflicht zur Beachtung aus der Formulierung ab, d.h. der Verantwortliche muss ihrer Ansicht nach begründen, wenn er diese Vorgaben nicht berücksichtigt. Hier wäre vorteilhaft, den Wortlaut bzgl. der Berücksichtigung der Aufzählung an den Wortlaut der DSGVO anzugleichen, so dass hier die Kommentarliteratur zur DSGVO analog herangezogen werden kann.

Lösungsvorschlag: Löschung der Wiederholungen der DSGVO in § 22 Abs. 2 BDSG, zugleich Anpassung des Wortlautes an die DSGVO:

| Bundesdatenschutzgesetz | Änderungsvorschlag |
|--|---|
| <p>§ 22 Verarbeitung besonderer Kategorien personenbezogener Daten (2) In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:</p> <ol style="list-style-type: none"> 1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt, 2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind, 3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten, 4. Benennung einer oder eines Datenschutzbeauftragten, 5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen | <p>§ 22 Verarbeitung besonderer Kategorien personenbezogener Daten (2) In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein können dazu insbesondere gehören:</p> <ol style="list-style-type: none"> 1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt, 2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind, 3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten, |

| | |
|--|--|
| <p>Stelle und von Auftragsverarbeitern,</p> <ol style="list-style-type: none"> 6. Pseudonymisierung personenbezogener Daten, 7. Verschlüsselung personenbezogener Daten, 8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, 9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder 10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen. | <ol style="list-style-type: none"> 4. Benennung einer oder eines Datenschutzbeauftragten, 5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern, 6. Pseudonymisierung personenbezogener Daten, 7. Verschlüsselung personenbezogener Daten, 8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, 9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder 10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen. |
|--|--|

- Die **Rechtsgrundlagen** für die Datenverarbeitung in **§ 23 BDSG** sind **nur zum Teil sachgerecht, praktikabel und normenklar geregelt.**

- a. Die Regelung in Ziffer 5 ist nicht normenklar, da „schwerwiegenden Beeinträchtigung der Rechte einer anderen Person“ unklar ist. Daher wird vorgeschlagen, hier stattdessen auf die Erforderlichkeit zum Schutz lebenswichtiger Interessen einer anderen natürlichen Person abzustellen.
- b. In Ziffer 6 werden die Verarbeitungen „Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen“ genannt, die jedoch alle zu den Aufgaben der öffentlichen Stelle gehören, deren Erlaubnistatbestand in § 3 BDSG geregelt ist. Dies gilt auch „für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen“; handelt es sich nicht um einen Ausbildungs- oder Schulungsbetrieb, erscheint eine Zweckänderung der Verarbeitung nicht angebracht, handelt es sich um einen Ausbildungs- oder Schulungsbetrieb,

gehört die Verarbeitung zu den in § 3 BDSG geregelten Aufgaben der öffentlichen Stelle.

Lösungsvorschlag: Anpassung der Ziffer 5 und Streichung der Ziffer 6 in § 23 Abs. 1 BDSG:

| Bundesdatenschutzgesetz | Änderungsvorschlag |
|--|--|
| <p>§ 23 Verarbeitung zu anderen Zwecken durch öffentliche Stellen</p> <p>(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn</p> <ol style="list-style-type: none"> 1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde, 2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen, 3. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist, 4. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist, 5. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder 6. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von | <p>§ 23 Verarbeitung zu anderen Zwecken durch öffentliche Stellen</p> <p>(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn</p> <ol style="list-style-type: none"> 1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde, 2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen, 3. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist, 4. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuchs oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist, 5. sie zum Schutz lebenswichtiger Interessen einer anderen natürlichen Person zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist. oder 6. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der |

| | |
|---|---|
| <p>Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.</p> | <p>Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.</p> |
|---|---|

- Die **Rechtsgrundlagen für die Datenverarbeitung in § 24 BDSG** sind **nicht sachgerecht, praktikabel und normenklar geregelt.**

Eine Erforderlichkeit für die Regelung in § 24 Abs. 1 BDSG ist neben Art. 6 DSGVO nicht erkennbar. Ein Anwendungsbereich über die DSGVO hinaus kann sich im Regelungsgehalt des § 24 Abs. 2 BDSG ergeben, sodass die Regelung in § 24 BDSG in diesem Fall insgesamt hierauf beschränkt sein sollte.

2. Sind die Rechtsgrundlagen für die Datenübermittlung in § 25 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Die **Rechtsgrundlagen für die Datenübermittlung in § 25 BDSG** sind aus unserer Sicht **nicht sachgerecht, praktikabel und normenklar.**

- a. Eine Übermittlung stellt lediglich *eine* Form der Verarbeitung dar. Laut § 3 BDSG ist die „Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe“ erforderlich ist. Somit ist die Regelung von § 25 Abs. 1 BDSG bereits in § 3 BDSG enthalten. Die Regelung in Absatz 1 sollte daher entfernt werden.
- b. Auch § 25 Abs. 2 Ziff. 1 BDSG wird durch § 3 BDSG bereits geregelt und sollte daher entfernt werden.
- c. Die in § 25 Abs. 2 Ziff. 3 BDSG geregelte Übermittlung zur „Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche“ der öffentlichen Stelle gegenüber einer nichtöffentlichen Stelle gehört ebenfalls regelhaft zu den Aufgaben einer öffentlichen Stelle und wird somit bereits durch § 3 BDSG adressiert. Auch § 25 Abs. 2 Ziff. 3 BDSG sollte daher entfernt werden.

3. Sind die Regelungen in Bezug auf besondere Verarbeitungssituationen in den §§ 26 bis 31 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

- Die **Regelungen** in Bezug auf besondere Verarbeitungssituationen **in § 26 BDSG** sind aus unserer Sicht normenklar, aber **nicht sachgerecht und praktikabel.**

§ 26 BDSG stellt lediglich die Fortschreibung der § 32 BDSG a.F. dar. Alle bereits zu § 32 BDSG a.F. als ungelöst kritisierten Fragen zum Beschäftigtendatenschutz wie beispielsweise die Grenzen des Fragerechts des Arbeitgebers, die Datenerhebung über Bewerber im Internet oder auch die Speicherdauer von Bewerberdaten bleiben weiterhin ungelöst. Neue Ansätze wie Predictive Analytics oder auch Big Data Szenarien können mit den vorhandenen Regelungen nicht

rechtssicher begleitet werden. Sofern nicht jedenfalls in der nächsten Legislaturperiode ein eigenes Beschäftigungsdatenschutzgesetz verabschiedet wird, sollten die beschriebenen Klarstellungen bereits im BDSG berücksichtigt werden.

- Die **Regelungen** in Bezug auf besondere Verarbeitungssituationen in **§ 27 BDSG** sind aus unserer Sicht **nicht normenklar, sachgerecht und praktikabel**.
 - a. Die Öffnungsklausel in Art. 9 Abs. 4 DSGVO für nationale Gesetzgeber erfasst ausschließlich die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten, die Regelung in § 27 Abs. 1 BDSG betrifft aber alle in Art. 9 Abs. 1 DSGVO genannten besonderer Kategorien personenbezogener Daten und dürfte somit nicht europarechtskonform sein. Wir schlagen daher vor, zur Erhöhung der Rechtssicherheit für den Rechtsanwender den Erlaubnistatbestand auf die in Art. 9 Abs. 4 DSGVO genannten Datenkategorien zu beschränken.
 - b. Beschränkungen der Betroffenenrechte können nur entsprechend den in Art. 23 Abs. 1 DSGVO enthaltenen Vorgaben erfolgen, die Regelung in § 27 Abs. 2 BDSG erfüllt in der Allgemeinheit jedoch nicht die Anforderungen von Art. 23 Abs. 1 DSGVO. Zudem fehlt in § 27 Abs. 2 BDSG die Berücksichtigung von Art. 23 Abs. 2 DSGVO. Die Anwendung von § 27 Abs. 2 BDSG stellt daher eine Rechtsunsicherheit dar.

Eine Beschränkung wäre – unter Berücksichtigung, dass Art. 9. Abs. 4 DSGVO bzgl. § 27 Abs. 1 BDSG nur Regelungen hinsichtlich der Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten erlaubt – aus unserer Sicht nur unter Nutzung von Art. 23 Abs. 1 Buchst. e DSGVO im Sinne von „Forschungs- oder Statistikzwecke des allgemeinen öffentlichen Interesses Deutschlands“ sowie von „Forschungs- oder Statistikzwecke im Bereich der öffentlichen Gesundheit“ möglich, begleitet von Art. 23 Abs. 2 DSGVO adressierenden spezifischen Vorschriften.
 - c. Auch in § 27 Abs. 3 BDSG ist die Regelung auf die in Art. 9 Abs. 4 DSGVO genannten Datenkategorien anzupassen.

Lösungsvorschlag: Anpassung von § 27 BDSG

| Bundesdatenschutzgesetz | Änderungsvorschlag |
|---|--|
| <p style="text-align: center;">§ 27 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken</p> <p>(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss</p> | <p style="text-align: center;">§ 27 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken</p> <p>(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten besonderer Kategorien personenzbezogener Daten im Sinne des Artikels 9 Absatz 1 4 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an</p> |

der Verarbeitung erheblich überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) Die in den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

(4) Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

(2) Die in den Artikeln 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke **des allgemeinen öffentlichen Interesses oder im Bereich der öffentlichen Gesundheit** unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. ~~Das Recht auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.~~ **Werden die im dritten Kapitel der Verordnung (EU) 2016/679 beschriebenen Rechte eingeschränkt, so ist hiervon sowie von der Begründung der Erforderlichkeit der Einschränkung die zuständige Datenschutz-Aufsichtsbehörde der forschenden Stelle zu informieren, welche die Rechtmäßigkeit der Einschränkung prüft. Die Daten sind unverzüglich nach Erreichung des Zieles zu löschen, eine nachgewiesene Anonymisierung der personenbezogenen Daten gilt als Löschung.**

(3) Ergänzend zu den in § 22 Absatz 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete **genetische, biometrische oder Gesundheitsdaten** ~~besondere Kategorien personenbezogener Daten~~ im Sinne des Artikels 9 Absatz ~~1~~ **4** der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn,

| | |
|--|---|
| | <p>berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.</p> <p>(4) Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.</p> |
|--|---|

- Die **Rechtsgrundlagen** für die Datenübermittlung in **§ 28 BDSG** sind aus unserer Sicht **nicht sachgerecht, praktikabel und normenklar**.

Die Begründung ist analog dem Kommentar zu § 27 BDSG, dass der in Art. 9 Abs. 4 DSGVO enthaltene Erlaubnistatbestand für nationale Regelungen nicht alle in Art. 9 Abs. 1 DSGVO genannten Datenkategorien umfasst. Auch § 28 Abs. 1 BDSG muss daher angepasst werden.

Lösungsvorschlag: Anpassung von § 28 Abs. 1 BDSG

| Bundesdatenschutzgesetz | Änderungsvorschlag |
|---|---|
| <p>§ 28 Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken</p> <p>(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.</p> | <p>§ 28 Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken</p> <p>(1) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 44 der Verordnung (EU) 2016/679 zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.</p> |

- Die **Regelungen in § 29 Abs. 1 BDSG** sind aus unserer Sicht **nicht sachgerecht, praktikabel und normenklar**.

Eine Beschränkung der in Kapitel II DSGVO genannten Betroffenenrechte können nur entsprechend den in Art. 23 Abs. 1 DSGVO enthaltenen Vorgaben

erfolgen, die Regelung in § 29 Abs. 1 BDSG der Einschränkung aufgrund der „überwiegenden berechtigten Interessen eines Dritten“ genügt nicht den Anforderungen von Art. 23 Abs. 1 DSGVO. Aus unserer Sicht ist eine Einschränkung der Rechte für Dritte nur unter Nutzung von Art. 23 Abs. 1 Buchst. j DSGVO möglich.

Art. 34 DSGVO kennt keine Öffnungsklausel, sodass eine Einschränkung wohl nicht europarechtskonform erfolgen kann. Daher sollte auf diesen Abschnitt verzichtet werden.

Lösungsvorschlag: Anpassung von § 29 Abs. 1 BDSG

| Bundesdatenschutzgesetz | Änderungsvorschlag |
|---|---|
| <p>§ 29 Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten</p> <p>(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Die Pflicht zur Benachrichtigung gemäß Artikel 34 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 3 ist die betroffene Person nach Artikel 34 der Verordnung (EU) 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.</p> | <p>§ 29 Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten</p> <p>(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung die Durchsetzung zivilrechtlicher Ansprüche Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten verhindert würden, geheim gehalten werden müssen. Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, die Durchsetzung zivilrechtlicher Ansprüche insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, verhindert würden geheim gehalten werden müssen. Die Pflicht zur Benachrichtigung gemäß Artikel 34 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 3 ist die betroffene Person nach Artikel 34 der Verordnung (EU) 2016/679 zu benachrichtigen, wenn die Interessen</p> |

der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

- Die Regelung für die Datenübermittlung in **§ 30 Abs. 1 BDSG** sollte so formuliert sein, dass deutlicher hervortritt, dass es sich hierbei nicht um eine Rechtsgrundlage für eine Datenverarbeitung handelt.
- Die Rechtsgrundlagen für die Datenübermittlung in **§ 31 BDSG** sind aus unserer Sicht sachgerecht, praktikabel und normenklar. Gleichwohl bestehen Zweifel daran, dass diese Regelung von einer Öffnungsklausel umfasst ist.

4. Sind die Rechtsgrundlagen für die Datenverarbeitung in den §§ 48 bis 51 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

In unserem Berufsverband sind keine Auftragsverarbeiter i. S. d. der Richtlinie (EU) 2016/680 vertreten, daher nehmen wir von Ausführungen Abstand.

III. Datenschutzbeauftragte öffentlicher und nichtöffentlicher Stellen

1. Sind die Regelungen zu Datenschutzbeauftragten öffentlicher Stellen in den §§ 5 bis 7 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Ja.

2. Sind die Regelungen zu Datenschutzbeauftragten nichtöffentlicher Stellen in § 38 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Die **Regelungen zu Datenschutzbeauftragten nichtöffentlicher Stellen in § 38 BDSG** sind aus unserer Sicht praktikabel und normenklar, aber **nicht sachgerecht**.

- a. Die Gestaltung in §38 Abs. 1 Satz 1 BDSG erscheint aufgrund der geübten Praxis zu dieser Regelung tragfähig. Gleichwohl ist die Anhebung des Quorums von 10 auf 20 grundlegender Kritik ausgesetzt (siehe Antwort zu Frage III.3). Entscheidend hierfür ist neben der sachlichen Kritik auch, dass diese Anhebung untauglich war und ist, das damit verbundene Ziel der "Entbürokratisierung" zu erreichen.

Im Interesse der Normenklarheit wird angeregt, die Sätze 1 und 2 des Abs. 1 auf zwei Absätze zu verteilen.

- b. Wenngleich die Anzahl der mit der Verarbeitung befassten Personen ein Indiz für die Erforderlichkeit eines DSB ist, darf dies kein Ausschlusskriterium für die Erforderlichkeit darstellen, weshalb auch Kriterien definiert und vorgesehen sein müssen, dass unterhalb dieses Quorums ein DSB verpflichtend zu bestellen ist. Über die bereits in §38 Abs. 1 Satz 2 BDSG enthaltenen Aspekte hinaus sollte eine Erweiterung der Benennungspflicht vor allem unter folgenden Aspekten erfolgen:

- Die feste Zuordnung von mindestens 20 Personen für eine Benennungspflicht berücksichtigt nicht die Anzahl betroffener Personen und/oder verarbeiteter Datensätze. Gerade bei der digitalen Verarbeitung personenbezogener Daten kann z.B. ein Startup, welches nur 3 bis 5 Personen beschäftigt, eine sehr große Menge personenbezogener Daten von einer größeren Anzahl Personen verarbeiten, wohingegen in einer Schreinerei vielleicht 20 Beschäftigte die Daten von deutlich weniger Kunden und/oder Datensätze als das Startup verarbeiten.
 - Um der Zielsetzung des Art. 25 Abs. 1 DSGVO (“Privacy by design”) effektiv Rechnung tragen zu können, erscheint es geboten, nicht nur die Verantwortlichen, sondern auch die durch Art. 25 DSGVO mittelbar adressierten Hersteller der Produkte, Dienste und Anwendungen (z.B. Videoüberwachung mit Gesichtserkennung, medizinische Informationssysteme) zur Benennung eines DSB zu verpflichten. Denn Art. 25 Abs. 1 DSGVO nimmt formal die Verantwortlichen in die Pflicht, obgleich deren Erfüllung auch die vorgenannten Hersteller adressiert. Diese Pflicht sollte jedenfalls dann bestehen, wenn die Produkte, Dienste und Anwendungen ihren bestimmungsgemäßen Einsatz nach einer Datenschutz-Folgenabschätzung unterliegen. Dies würde dazu führen, dass die datenschutzrechtlichen Pflichten bereits bei Herstellung und nicht erst später (evtl. ohne Änderungsmöglichkeiten) Berücksichtigung finden werden. Dies könnte insbesondere einen Beitrag zur bürokratischen Entlastung von KMU bei der Durchführung einer Datenschutz-Folgenabschätzung leisten.
- c. Die aus dem Datenschutzrecht resultierenden Pflichten bestehen für Verantwortliche unabhängig von der Tatsache, ob ein Datenschutzbeauftragter benannt wurde oder nicht. Hingegen kennt ein Datenschutzbeauftragter die gesetzlichen Anforderungen und kann den Verantwortlichen bzgl. der Erfüllung der gesetzlichen Anforderungen beraten und unterstützen. Ehrlicherweise muss man davon ausgehen, dass eine hohe Anzahl von Unternehmen ohne benannten Datenschutzbeauftragten die gesetzlichen Anforderungen nicht kennen, folglich diese nicht umsetzen können und aus Unwissen gegen datenschutzrechtliche Bestimmungen verstoßen. Daher sollte auch aus dieser Sichtweise die Benennung eines Datenschutzbeauftragten auch an der Menge der von der Verarbeitung betroffenen Personen/Datensätze abhängig gemacht werden.

3. Mit dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG- EU) wurde in § 38 Absatz 1 Satz 1 BDSG die maßgebliche Zahl der Personen, ab der ein betrieblicher Datenschutzbeauftragter zu benennen ist, von 10 auf 20 angehoben. Angestrebt wurde damit vor allem eine Entlastung kleiner und mittlerer Unternehmen sowie ehrenamtlich tätiger Vereine.

a) Welche Wirkungen hat die Änderung des § 38 Absatz 1 Satz 1 BDSG nach Ihrer Kenntnis erzielt?

Durch die Anhebung des Benennungspflicht-Quorums ist für kleinere und mittlere Unternehmen im Ergebnis statt einer Entlastung ein zusätzliches Risiko für unternehmerische Fehlbewertung der Anforderungen entstanden, die gegebenenfalls erhebliche Nachteile mit sich bringt.

Durch den Wegfall des Datenschutzbeauftragten sind nicht die Aufwände für die Erfüllung der datenschutzrechtlichen Anforderungen durch den Verantwortlichen reduziert worden, hingegen fehlt jetzt die Kenntnis, wie man fachkundig und ressourcenschonend mit diesen Anforderungen umgeht. Die Anhebung des Quorums führt somit zu einer zusätzlichen Belastung der Unternehmensleitung.

b) Hat die Änderung der Norm nach Ihrer Kenntnis zu einer Erleichterung für Unternehmen und Vereine geführt?

Nein. Es haben sich keine Bürokratierleichterungen durch die Anhebung ergeben, da alle Erfordernisse aus der DSGVO weiterhin bestehen bleiben und beachtet werden müssen. Der DSB trägt aufgrund seiner Fachkompetenz zu einer Erleichterung in der Umsetzung bei.

IV. Zusammenarbeit, Zuständigkeiten und Befugnisse der Aufsichtsbehörden

1. Ist die Zusammenarbeit der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Die Zusammenarbeit der Aufsichtsbehörden ist im BDSG aus unserer Sicht normenklar, aber nicht sachgerecht und praktikabel geregelt.

Dem Föderalismus folgend, ist die Zuständigkeitsverteilung zwischen Bundesländern und Bund geboten. Damit einher gehen auch – wenngleich nicht stets und zu jedem Aspekt - unterschiedliche Auslegungen der DSGVO und des BDSG durch die Aufsichtsbehörden der Länder und des Bundes. Dies kann für Verantwortliche und Auftragsverarbeiter zur Folge haben, dass in einem Bundesland eine Verarbeitung nach Ansicht der dortigen Aufsichtsbehörde rechtskonform erfolgt, während sie in einem anderen Bundesland durch die dort zuständige Aufsichtsbehörde als rechtswidrig angesehen wird. Vor allem für Auftragsverarbeiter, die für Verantwortliche in unterschiedlichen Bundesländern tätig sind und somit indirekt mit verschiedenen Aufsichtsbehörden zusammenarbeiten müssen, hat dies Auswirkungen.

Wir fordern den Gesetzgeber auf, in Abstimmung mit den zuständigen Aufsichtsbehörden eine Gestaltung zu finden, welche diese Unsicherheit in der Rechtsanwendung ausschließt oder die Abweichung hinreichend transparent macht.

2. Sind die Zuständigkeiten der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Die Zuständigkeiten der Aufsichtsbehörden im BDSG sind aus unserer Sicht nicht sachgerecht, praktikabel und normenklar geregelt. Die Zuständigkeit der Aufsichtsbehörden ist bei bundeslandübergreifender Verarbeitung nicht geregelt. Eine Abstimmung zu einer einheitlichen Rechtsauslegung im konkreten Einzelfall für beteiligte Aufsichtsbehörden ist nicht vorgeschrieben. In § 17 BDSG wird zudem die Tatsache, dass der Bundesrat keinen Stellvertreter wählt, nicht berücksichtigt.

Lösungsvorschlag: Die Schaffung einer Regelung für eine federführende deutschen Aufsichtsbehörde ähnlich dem europäischen Recht für bundeslandübergreifende Verarbeitungen, damit Verantwortliche und Auftragsverarbeiter eine Aufsichtsbehörde als verbindlichen Ansprechpartner haben.

3. Hat sich aus Ihrer Sicht die Regelung in § 40 Absatz 2 BDSG bewährt, wonach sich, wenn der Verantwortliche oder Auftragsverarbeiter mehrere inländische Niederlassungen hat, die zuständige Aufsichtsbehörde entsprechend Artikel 4 Nummer 16 DSGVO nach der Hauptniederlassung bestimmt?

Nein, siehe Antworten zu den Fragen IV.1 und IV.2

4. Sind die Befugnisse der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

Nein, siehe Antworten zu den Fragen IV.1 und IV.2

5. Gibt es aus Ihrer Sicht neben den in den Fragen 1 bis 3 angesprochenen Aspekten Änderungsbedarf bei der Regelung der Datenschutzaufsicht im BDSG und wenn ja, worin besteht er?

Die Kernanliegen wurden vorstehend adressiert.

V. Betroffenenrechte

1. Sind die Regelungen zu den Betroffenenrechten in den §§ 32 bis 37 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

Die Regelungen zu den Betroffenenrechten in den §§ 32 bis 37 BDSG sind aus unserer Sicht nicht uneingeschränkt sachgerecht, praktikabel und normenklar.

Beschränkungen der Betroffenenrechte können nur entsprechend den in Art. 23 Abs. 1 DSGVO festgelegten Grenzen unter Beachtung der Maßgaben des Art. 23 Abs. 2 DSGVO. Der BvD regt eine Ausrichtung der Ausnahmen an diesen Regelungen an, um ein Mehr an Rechtssicherheit zu erreichen.

2. Sind die Regelungen zu den Betroffenenrechten in den §§ 55 bis 61 BDSG aus Ihrer Sicht normenklar? Sind sie aus Ihrer Sicht sachgerecht und praktikabel, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen?

In unserem Berufsverband sind keine Auftragsverarbeiter i. S. d. der Richtlinie (EU) 2016/680 vertreten, daher nehmen wir von Ausführungen Abstand.

VI. Pflichten der Verantwortlichen und Auftragsverarbeiter

In unserem Berufsverband sind keine Auftragsverarbeiter i. S. d. der Richtlinie (EU) 2016/680 vertreten, daher nehmen wir von Ausführungen zu diesem Fragenkomplex Abstand.

VII. Datenübermittlungen an Drittstaaten und an internationale Organisationen

In unserem Berufsverband sind keine Auftragsverarbeiter i. S. d. der Richtlinie (EU) 2016/680 vertreten, daher nehmen wir von Ausführungen zu diesem Fragenkomplex Abstand.

VIII. Haftung und Sanktionen

1. Sind die Regelungen zu Sanktionen in den §§ 41 bis 43 BDSG aus Ihrer Sicht sachgerecht und normenklar?

Die Regelungen zu Sanktionen in den §§ 41 bis 43 BDSG sind aus unserer Sicht nicht uneingeschränkt sachgerecht und normenklar.

Nach §41 Abs. 1 BDSG sind die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß anzuwenden. Die Bezugnahme auf insbesondere §§ 30, 130 OWiG ergibt Friktionen zu dem Art. 83 DSGVO zugrunde liegenden Unternehmensbegriff. Der BvD regt im Interesse der Rechtsklarheit eine klarstellende Überprüfung an.

2. In wie vielen Fällen haben nach Ihrer Kenntnis Landgerichte gemäß § 41 Absatz 1 Satz 3 BDSG über einen Einspruch gegen einen Bescheid über ein Bußgeld von mehr als 100.000 (einhunderttausend) Euro wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 DSGVO entschieden? (Bitte nach Jahren und Landgerichten aufschlüsseln)

Der BvD führt entsprechend seinen Verbandsaufgaben keine solche Aufstellung. Aufgrund der beruflichen Geheimhaltungspflichten sind die Mitglieder des BvD auch nicht ohne Weiteres berechtigt hierzu zu kommunizieren.

Der BvD regt an, dass eine Veröffentlichung der verhängten Bußgelder und Entscheidungen eingerichtet wird. Zu berücksichtigen ist jedoch, wie auch die aktuelle Rechtsprechung zeigt, dass hierdurch kein „Pranger-Effekt“ entsteht. Eine bundesweit gemeinsame, anonyme Veröffentlichung könnte diesen Effekt vermeiden, aber gleichwohl der erforderliche Erkenntnisgewinn aus den Entscheidungen zur Einheitlichkeit der Rechtsanwendung beitragen.

3. Sind die Regelungen zu Haftung und Sanktionen in den §§ 83 und 84 BDSG aus Ihrer Sicht sachgerecht und normenklar?

In unserem Berufsverband sind nicht in signifikantem Umfang Verarbeiter im Sinne des Teils des BDSG vertreten, daher nehmen wir von Ausführungen Abstand.

IX. Allgemein zu den Regelungen des BDSG

1. Wie bewerten Sie das BDSG insgesamt in Bezug auf die Sachgerechtigkeit, Praktikabilität und Normenklarheit der Bestimmungen?

Die DSGVO wird aufgrund ihrer Bürokratie-Aufwände und der damit verbundenen Kosten der Verantwortlichen kritisiert. Diese Bürokratie und diese Kosten bestehen unabhängig von der Benennung eines DSB. Denn die umfassenden Dokumentations-, Informations- und Prüfungspflichten der DSGVO bestehen unabhängig von der Benennung eines DSB. Mit anderen Worten: Der Verzicht auf die Benennung eines DSB bringt für die Verantwortlichen keine Entbürokratisierung. Eine hierauf ausgerichtete Ausgestaltung der Tätigkeit des DSB entlastet hingegen die Unternehmensleitung in KMU:

Die DSGVO bietet dem BDSG anders als im alten Datenschutzrecht besser die Möglichkeit, die Rolle des Datenschutzbeauftragten stärker als proaktiven Gestalter für das Unternehmen, weniger als reaktiven Überwacher auszugestalten. **Der BvD regt daher an, die Einbindung des Datenschutzbeauftragten in die Gestaltung der Verarbeitung personenbezogener Daten zu stärken und dem Datenschutzbeauftragten die Möglichkeit zu eröffnen, die Unternehmensleitung bei einzelnen Aufgaben nach der DSGVO zu entlasten.** Davon würden vor allem kleine und mittlere Unternehmen profitieren und es würde eine effektive Nutzung des Know-hows zur Gestaltung der Nutzung personenbezogener Daten erreicht werden.

Konkrete Ansätze zur effektiveren Einbindung von Datenschutzbeauftragten sieht der BvD in folgenden Maßnahmen:

- Anpassung der Meldepflicht bei Datenpannen: Meldungen von (Verdacht auf) Datenpannen an die Aufsichtsbehörden erst bei einem hohen Risiko. Meldung aller Vorgänge an den DSB, der zudem ein Register aller Vorfälle führt und die Abhilfemaßnahmen überwacht.
- Anpassung der Zuständigkeit bei der Datenschutz-Folgenabschätzung (DSFA): Die Erstellung der DSFA und die Beurteilung der Risiken sollte in den Händen des DSB liegen. Das Ergebnis wird dann von der Unternehmensleitung verbindlich festgestellt und die vorgesehenen Maßnahmen werden umgesetzt.
- Führen des Verzeichnisses der Verarbeitungstätigkeiten durch den DSB anstatt der ansonsten hierfür verantwortlichen Leitung des Verantwortlichen.

Der BvD fordert den Bundesgesetzgeber zudem auf, anlässlich der Evaluierung des BDSG klarzustellen, dass durch die Beratungsleistung externer Datenschutzbeauftragter bei der Wahrnehmung ihrer gesetzlichen Aufgaben gem. Art. 39 DSGVO im Rahmen ihrer Benennung keine Kollisionen zum RDG entsteht. Dem DSB ist durch die DSGVO eindeutig die Aufgabe der Beratung

zugewiesen. Das schließt nach dem Selbstverständnis der DSGVO zwangsweise die Beratung zu allen Aspekten des Datenschutzrechts ein, die datenschutzrechtliche Themen tangieren. Die in Deutschland geführte Diskussion, dass dies vermeintlich gegen das RDG verstößt, verhindert die proaktiv unterstützende Funktion des DSB im Unternehmen, obgleich diese in der DSGVO so vorgesehen ist. Eine Einschränkung der Tätigkeit des DSB bei der (datenschutz-)rechtlichen Beratung durch eine Vorschrift eines Mitgliedsstaates verstößt gegen die höherrangige Vorgabe zur Beratung durch eine europäische Verordnung.

Schließlich fordert der BvD den Gesetzgeber auf, von seinen Gestaltungsmöglichkeiten, insbesondere nach Art. 23 DSGVO Gebrauch zu machen, auf eine fokussierte anstatt bürokratisierte Dokumentationspflicht hinzuwirken. Die Hauptbelastung für die Unternehmen unter der DSGVO und BDSG ist nicht die Einhaltung der Zulässigkeit der Verarbeitung. Die als unnötige Bürokratie empfundenen Anforderungen der DSGVO und des BDSG liegen vielmehr in der Vielzahl unterschiedlicher Dokumentationspflichten, die sich inhaltlich auch noch überschneiden, aber nicht deckungsgleich sind. Dennoch ist jede dieser Dokumentationspflichten für sich mit einem Bußgeld bewehrt. Die Unternehmensleitung ist damit im Rahmen des Datenschutzes mehr damit beschäftigt, Dokumentationen stets aktuell zu halten, als sich mit der eigentlichen Frage der Zulässigkeit zu befassen.

2. Bestehen in Ihrer datenschutzrechtlichen Praxis Schwierigkeiten mit der Auslegung und Anwendung des BDSG? Wenn ja, welche Schwierigkeiten sind das und auf welche Regelungen des BDSG beziehen sie sich?

Die Schwierigkeiten wurden in den Fragen I. bis VIII. dargestellt.

Teil 2

X. Schutz- und Dokumentationspflichten bei Unterbleiben einer Information der betroffenen Person

Zu diesem Fragenkomplex liegen uns als BvD keine Informationen im signifikanten Umfang vor.

Impressum

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Budapester Straße 31, 10787 Berlin

E-Mail: bvd-gs@bvdnet.de

Telefon (030) 26 36 77 60

Telefax (030) 26 36 77 63

www.bvdnet.de

Stand: 15. Januar 2021