bitkom

Auf einen Blick

BDSG-Evaluierung

Ausgangslage

Für das am 25. Mai 2018 in Kraft getretene neue Bundesdatenschutzgesetz ist eine Evaluierung vorgesehen. Diese Evaluierung führt das Bundesministerium des Innern, für Bau und Heimat durch.

Bitkom-Bewertung

Wir begrüßen die Evaluierung des BDSG und die damit einhergehende Überprüfung des nationalen Datenschutzrahmens. Wir setzen uns im Zuge der Überprüfung des nationalen Datenschutzrahmens für stärkere Harmonisierung, Abbau föderaler Unterschiede, verbesserten Rechtsschutz durch Anpassungen an der Schnittstelle zum OWiG und Rechtssicherheit für Anwender und Betroffene ein.

Das Wichtigste

Im Bitkom sind neue Anbieter genauso wie Mitglieder mit großer Nähe zu den klassischen Diensten vertreten. Unser Papier zeichnet daher mögliche Kompromisslinien vor:

- **Abbau föderaler Unterschiede**
  Zwar wurde auf der EU Ebene mit der Datenschutz-Grundverordnung (DS-GVO) ein EU-weit gültiger Rahmen geschaffen, um die geltenden Datenschutzgesetze zu harmonisieren, aber speziell im Bereich des Gesundheitssektors wurden viele gesetzliche Regelungen noch nicht überarbeitet bzw. in den Bundesländern unterschiedlich gestaltet. Es ist nunmehr an den lokalen Gesetzgebern und den Aufsichtsbehörden in den Mitgliedsstaaten, die Möglichkeiten der in der DS-GVO verankerten Öffnungsklauseln mit Bedacht zu nutzen und hierbei bestehende Unzulänglichkeiten und Widersprüche zu beseitigen.

- **Einheitlichkeit der Aufsichtsbehördlichen Interpretation fördern**
  Aus den unterschiedlichen Interpretationen der Landesaufsichtsbehörden resultiert eine Komplexität, die sowohl für kleine und mittelständische Unternehmen (KMU) als auch Unternehmen mit Niederlassungen bzw. Kunden in mehreren Bundesländern Herausforderungen bedeuten. Die unterschiedliche Interpretation der DS-GVO durch die Behörden behindert Wachstum, da für jeden Geltungsbereich rechtlicher Rat eingeholt werden muss und evtl. Produkte verändert werden müssen. Rechtsunsicherheit führt zudem dazu, dass innovative Projekte gar nicht erst angegangen werden.

- **Bitkom-Zahl**

56 Prozent

Jedes 2. Unternehmen verzichtet aus Datenschutzgründen auf Innovationen (lt. einer Studie von Bitkom Research).

Stellungnahme

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Zusammenfassung

Das Datenschutzrecht berührt in der heutigen digitalen Wirtschaft nahezu alle Geschäftsbereiche. Der mit der Datenschutzgrundverordnung (DS-GVO) geschaffene Rechtsrahmen zum Schutz der Grundrechte der Betroffenen kann zugleich Prozesse und Innovationen ermöglichen und die digitale Souveränität Europas stärken. Das kann jedoch nur gelingen, wenn die Auslegung ausbalanciert ist, die nationalstaatlichen Abweichungen gering gehalten und vor allem eine rechtssichere Anwendung ermöglicht wird. Daneben muss endlich das wichtigste Versprechen der DS-GVO eingelöst werden: Ein einheitlicher Rechtsrahmen für die gesamte EU. Das muss auch für die innerdeutsche Anwendung und Auslegung der Datenschutzvorschriften gelten.

Wir begrüßen daher die Evaluierung des BDSG und setzen uns im Zuge der Überprüfung des nationalen Datenschutzrahmens für stärkere Harmonisierung, Abbau föderaler Unterschiede und Rechtssicherheit für Anwender und Betroffene ein. Detaillierte Anmerkungen und unsere Antworten auf den Fragenkatalog des Bundesministeriums des Innern, Bau und Heimat finden sich untenstehend.

Aus unserer Sicht ist neben der Evaluierung des gesetzlichen Rahmens ein weiterer Aspekt essentiell: Die Ziele der Harmonisierung und Rechtssicherheit müssen auch für die Auslegung durch die Aufsichtsbehörden gelten. Die bisherige Struktur der Datenschutzaufsicht ist jedoch auf 18 unterschiedliche Behörden angelegt, was zu Auslegungsdifferenzen führt, die durch mehr Vereinheitlichung und bundesweit harmonisierte Auslegungshilfen zukünftig vermindert werden müssen. Konkrete Vorschläge um dieses Ziel zu erreichen hat der Bitkom bereits im Positionspapier zur Struktur der Aufsichtsbehörden in Deutschland zusammengefasst.[1] Daneben sind die verfahrensrechtlichen Regelungen, insbesondere für das Ordnungswidrigkeitenverfahren dringend verbesserungsbedürftig.

[1] https://www.bitkom.org/Bitkom/Publikationen/Struktur-der-Datenschutzaufsichtsbehoerden-in-Deutschland.

Antworten zum Fragenkatalog und Detailanmerkungen zum Datenschutzrahmen:

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

Der Umstand, dass es für die Verantwortlichen nicht nur das BDSG zu beachten gilt, sondern auch noch 16 unterschiedliche Landesdatenschutzgesetze sowie zahlreiche weitere Landesgesetze (z.B. Landeskrankenhausgesetze) mit Datenschutzregelungen, führt jeweils dazu, dass der Prüfaufwand im Vergleich zu anderen EU Ländern erheblich komplexer ist und einheitliche Datenschutzlösungen für Deutschland im Einzelfall nicht verwendet werden können. So verbietet das Landesdatenschutzgesetz in Rheinland Pfalz (§ 19 IV) öffentlichen Auftraggebern (z.B. Unikliniken) ausnahmslos den Einsatz von Dienstleistern, die nicht in den territorialen Anwendungsbereich der DS-GVO fallen. Es ist daher aus unserer Sicht dringend erforderlich, dass hier ein bundesweit einheitlicher Ansatz entwickelt wird.

Bitkom ist bewusst, dass die Lösung dieses Problems aufgrund der sich hieraus ergebenden Fragen zur Gesetzgebungskompetenz des Bundes/der Länder innerhalb Deutschlands eine Herausforderung ist. Dennoch ist dies eines des dringlichsten Probleme des Datenschutzrahmens in Deutschland und wir sehen hierin einen Nachteil gegenüber anderen EU-Ländern, insbesondere aufgrund der durchaus relevanten Verschärfungen gegenüber der DS-GVO.

Wir halten eine Streichung des § 4 BDSG wegen der festgestellten Europarechtswidrigkeit nach BVerwG Urteil vom 27.03.2019, 6 C 2.18 für erforderlich.

In § 22 BDSG sollte im Wortlaut eine eindeutigere Klärung erfolgen, ob Art. 9 Abs. 2 DS-GVO die zentrale Befugnisnorm zur Verarbeitung besonderer Kategorien personenbezogener Daten ist mit der Folge, dass § 22 BDSG bei der Ausfüllung der Öffnungsklauseln eine subsidiäre Auffangfunktion hat.

Im Kontext von § 22 BDSG sollte die Verarbeitungsmöglichkeit von Gesundheitsdaten aus unserer Sicht grundsätzlich überprüft und erweitert ermöglicht werden, um innovative Geschäftsmodelle zu fördern. So sollte zB umfassend evaluiert werden, ob die Verarbeitung auch im Rahmen der Durchführung des Versicherungsvertrages erlaubt

werden kann. Dazu sollte im BDSG ein entsprechender gesetzlicher Erlaubnistatbestand geschaffen werden.

Beispiel: Verträge, bei denen die Verarbeitung von Gesundheitsdaten des Betroffenen wesentlicher Bestandteil der Erbringung der vertraglich vereinbarten Leistung durch den verantwortlichen Vertragspartner ist, z. B. in der privaten Krankenversicherung oder der Lebensversicherung. Für die Verarbeitung der Gesundheitsdaten ist trotz des geschlossenen Vertrages zusätzlich die Einwilligung des Betroffenen gemäß Art. 9 Abs. 1 DS-GVO erforderlich. Diese ist gemäß Art. 7 Abs. 3 DS-GVO durch den Betroffenen jederzeit widerruflich. Widerruft aber der Betroffene seine Einwilligung und ist die Verarbeitung der Gesundheitsdaten für die Erbringung der Leistung durch den Vertragspartner zwingend erforderlich, kann der Vertragspartner diese Leistung nicht erbringen. Der Vertrag kann dann nicht erfüllt und muss rückabgewickelt werden. Der Betroffene hat durch diese datenschutzrechtliche Anforderung eine Möglichkeit, sich durch den Widerruf der Einwilligung von einem Vertrag zu lösen, von dem er sich nach den zivilrechtlichen Regelungen nicht mehr lösen könnte. Hier werden die Grundsätze des Vertragsrechts durch das Datenschutzrecht unterlaufen.

Entsprechend könnte in § 22 BDSG ergänzt werden, dass die Verarbeitung besonderer Kategorien von Daten zulässig ist, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder für die Durchführung des Vertrags mit dem Betroffenen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist.

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

In § 26 Absatz 1 Satz 2 BDSG sollte nach den Wörtern "Zur Aufdeckung von Straftaten" die Wörter "oder anderer schwerer Pflichtverletzungen " sowie nach den Wörtern "eine Straftat" die Wörter "oder eine andere schwere Pflichtverletzung" eingefügt werden.

Begründung: In § 26 Absatz 1 Satz 2 BDSG ist eine Datenverarbeitung "zur Aufdeckung von Straftaten" möglich. Nicht geregelt ist bislang die Frage, ob die Norm auch bei gewichtigen Vertragspflichtverletzungen, die keine Straftat darstellen, Anwendung finden kann. In der betrieblichen Praxis spielt die Verarbeitung von personenbezogenen Daten in vielen Fällen eine Rolle, in denen es um eine außerordentliche Kündigung des Arbeitsverhältnisses aus wichtigem Grund im Sinne von § 626 Absatz 1 BGB geht. Hierzu besteht bereits eine umfangreiche Kasuistik. Für den praktisch bedeutsamen Bereich der verhaltensbedingten Gründe kommt es jedoch nicht auf die strafrechtliche Wertung an. Es ist vielmehr auf das

Gewicht des Kündigungsgrundes und die Qualität der Pflichtverletzung abzustellen. Ist der Anwendungsbereich der zulässigen Datenverarbeitung auf "Straftaten" beschränkt, wird ein wichtiger Bereich im betrieblichen Bereich der Pflichtverletzungen nicht erfasst. Darüber hinaus werden Arbeitgeber dem Risiko ausgesetzt, als juristische Laien beurteilen zu müssen, ob eine mögliche Pflichtverletzung strafrechtlichen Charakter hat. Die Änderung nimmt inhaltlich die ständige Rechtsprechung des Bundesarbeitsgerichts auf. Das Bundesarbeitsgericht hat bereits zu § 32 BDSG a.F. eine Datenerhebung nicht nur bei einem Verdacht einer strafbaren Handlung sondern auch zur Aufdeckung "anderer schwerer Verfehlungen" als zulässig angesehen (zuletzt: BAG, 22. September 2016 - 2 AZR 848/15 Rn. 28). Diese Auslegung ergibt sich jedoch nicht unmittelbar aus dem Gesetzeswortlaut. Auch engere Auslegungen haben in der Rechtsprechung Niederschlag gefunden (zum Beispiel LAG BW, 20. Juli 2016 - 4 Sa 61/15, Rn. 92). Im Hinblick auf diese Rechtsunsicherheit erscheint eine gesetzgeberische Klarstellung erforderlich.

Aus unserer Sicht sind der § 26 Absatz 2 Satz 3 BDSG und die dort genannten Formvorschriften nicht erforderlich, sodass wir eine Streichung des Satzes 3 vorschlagen.

Bezüglich § 27 BDSG wäre eine Klarstellung sinnvoll, dass die Forschungstätigkeit von Unternehmen für die Produktentwicklung (Hardware, Software, KI, Services) als wissenschaftliche Forschung im Sinne des Gesetzes gilt.

Die bisherigen Erfahrungen zeigen, dass es hierzu bisher divergierende Auffassungen gibt. Der daraus resultierenden Rechtsunsicherheit könnte durch eine Klarstellung abgeholfen werden.

Beispiel: Ein Unternehmen trainiert bspw. einen Algorithmus mit personenbezogenen Daten, um ein Produkt zu entwickeln, welches bessere Therapiemöglichkeiten für die Behandlung von Krebs oder Covid19 ermöglichen soll. Für solche und ähnliche Fälle sollte klargestellt sein, dass es sich ebenfalls um privilegierte Forschung i.S.d. § 27 BDSG handelt.

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

Für den Fall, dass ein*e Konzern-DSB bestellt ist, sollte die Klarstellung erfolgen, dass der Verantwortliche seiner Mitteilungspflicht nach Art. 37 DS-GVO gerecht wird, wenn die Benennung des Konzern-DSB durch Mitteilung bei der Datenschutzaufsichtsbehörde erfolgt, die die Zuständigkeit für die Hauptniederlassung des Unternehmens hat.

4. Zu § 34 BDSG - Auskunftsrecht der betroffenen Person

Über Art. 23 DS-GVO besteht die Möglichkeit, den sehr umfangreichen und unbestimmten Auskunftsanspruch nach Art. 15 DS-GVO einzuschränken, wovon mit § 34 BDSG zum Teil Gebrauch gemacht wurde. Über § 34 BDSG sollte jedoch zu Art. 15 DS-GVO noch mehr Rechtssicherheit geschaffen werden: Zum Gegenstand der Auskunft sollte eine Konkretisierung und zur Art der Auskunft eine Klarstellung erfolgen. Auch sollte der Missbrauch von Auskunftsansprüchen durch den Betroffenen gegen den Verantwortlichen ausgeschlossen sein.

Der bisher sehr umfangreiche und unbestimmte Auskunftsanspruch nach Art. 15 DS-GVO, § 34 BDSG führt in Kombination mit einer möglichen Bußgeldbewehrung und eventueller Schadensersatzansprüche zu erheblicher Rechtsunsicherheit. Die Rechtsprechung hat mit dem Urteil des OLG Köln vom 26.07.2019, Az. 20 U 75/18 einen Auskunftsanspruch des Betroffenen bejaht, der – neben Stammdaten- und sonstigen in Unternehmen üblicherweise strukturiert geführten Datensätzen – sämtliche persönlichen Informationen und Merkmale umfasst, unabhängig davon, wie sie niedergelegt sind und in welchem Kontext sie sich befinden, z.B. in händischen Notizen, E-Mails einschließlich interner Verteiler etc. Ein solch nahezu unbedingter Auskunftsanspruch wird auch zu einer Ausforschung in einem zivilrechtlichen Streit führen.

Hierdurch werden beispielsweise die differenzierten Vorschriften der §§ 421 ff. ZPO über die Vorlage von Urkunden durch den Gegner und die Beweiswürdigung sowie Beweiserleichterung umgangen und das in Staaten des common law bekannte Element der „Discovery“, der umfassenden Ausforschung, eingeführt, ohne dem Auskunftsverpflichteten den Schutz zu gewähren, der selbst in Staaten mit umfassender vorgerichtlicher Ausforschung üblich ist. Auch bleiben die Rechte der betroffenen Personen, die die Daten erstellt haben, und deren Gedanken und Bewertungen in ihnen verkörpert sind, entgegen Art. 15 Abs. 4 DS-GVO außer Betracht.

In § 34 BDSG könnten an geeigneter Stelle die Ausschlussgründe ergänzt werden, um Gründe, an denen die Auskunftsdatenschutz- und persönlichkeitsrechtsfremden Zwecken dienen soll – insbesondere an Stellen, in denen arbeitsrechtliche Streitigkeiten im Vordergrund stehen.[2]

[2] Hierfür sprechen auch bisherigen Aussagen der Aufsichtsbehörden und Rechtsprechung: „Mit dem Recht auf Auskunft sollen ausschließlich Datenschutzziele verfolgt werden“., S. 27, https://www.lda.bayern.de/media/baylda_report_09.pdf

Außerdem soll der Verantwortliche nach Art. 15 Abs. 1 i.V.m. Abs. 3 S. 1 DS-GVO eine „Kopie der personenbezogenen Daten“ zur Verfügung stellen. Der Begriff der „Kopie“ nach Art. 15 Abs. 3 DS-GVO ist aufgrund einer fehlenden Legaldefinition oder mangels Konkretisierungen in den Erwägungsgründen so unbestimmt, dass Verantwortliche derzeit nicht wissen können, wie sie einem Antrag auf eine Kopie personenbezogener Daten entsprechen sollen. Dieser Rechtunsicherheit sollte durch eine Klarstellung und Definition abgeholfen werden.

5. Zu § 35 BDSG - Recht auf Löschung

§ 35 BDSG regelt Ausnahmen des Rechts auf Löschung nach Artikel 17 DS-GVO für den Fall, dass die Datenverarbeitung nicht automatisiert erfolgt, wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und das Interesse der betroffenen Person an der Löschung als gering anzusehen ist. Auch hier wird der Anwendungsbereich für diese Ausnahme geringer, da immer weniger Daten nicht automatisiert verarbeitet werden, obwohl gerade im Rahmen der Digitalisierung ein weiterer Bedarf nach Ausnahmen für die Löschpflicht besteht.

In vielen Unternehmen müssen große Mengen von Daten von Millionen von Kunden verarbeitet werden. Dies muss IT-gestützt erfolgen, da eine manuelle Verarbeitung dieser Datenmengen nicht mehr möglich ist. Aus historischen, geografischen und technischen Gründen wird häufig nicht nur ein IT-System verwendet, sondern eine große Anzahl spezialisierter, unterschiedlicher und miteinander verbundener IT-Systeme. In der Praxis ist es deshalb häufig sehr schwierig, die Verpflichtung zur Löschung personenbezogener Daten ohne übermäßige Verzögerung in den IT-Systemen zu erfüllen. Die Löschpflicht sollte deshalb zumindest dort eingeschränkt sein, wo es automatische Löschläufe gibt, die regelmäßig nach bestimmten Zeitabläufen durchgeführt werden und dies z.B. durch weitere Sicherungsmaßnahmen, wie bspw. Sperren der Daten abgesichert werden kann.

6. § 37 BDSG - Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Gemäß § 37 Nr. 1 BDSG können Entscheidungen, bei denen dem Begehren des Betroffenen stattgegeben wird, automatisiert erfolgen. Automatisierte Entscheidungen, bei denen dem Begehren des Betroffenen nicht vollumfänglich stattgegeben wird, sind bisher nur in der Krankenversicherung ohne Einwilligung des Betroffenen möglich. Eine solche

„Der Auskunftsanspruch dient lediglich dem Schutz ideeller Interessen der betroffenen Person, den vom Kläger reklamierten Vermögensbezug weist er nicht auf.“ (BVerwG, Urteil vom 16.09.2020 - BVerwG 6 C 10.19).

Regelung wäre jedoch auch wichtig für Fälle, in denen Versicherungsleistungen an Dritte, die nicht Vertragspartner des Versicherers sind erfolgen.

Das Einholen einer Einwilligung gestaltet sich in der Praxis häufig schwierig, wenn der Betroffene nicht schon Vertragspartner ist, sondern wie in der Kraftfahrzeughaftpflicht-, der Privathaftpflicht oder Vermögensschadenhaftpflichtversicherung, ein Dritter. Auch hier haben die Geschädigten jedoch ein Interesse an serviceorientierten und schnellen Prozessen, die häufig so nur automatisiert möglich sind.

Im Rahmen des BDSG a.F. gab es hier eine praxisorientierte und auch wieder im BDSG erstrebenswerte Lösung mit § 6a Abs. 2 Nr. 2 BDSG a.F.: Eine automatisierte Entscheidung mit der dem Begehren des Betroffenen nicht stattgegeben wurde war auch dann möglich, wenn „die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert“.

Art. 22 legt sogar die Bewertung nahe, dass positive Entscheidungen ohnehin gar nicht erfasst sein sollen. Insbesondere Absatz 1 spricht insoweit von „erheblichen Beeinträchtigung“ und legt daher nahe, dass nur automatisierte Entscheidungen erfasst sein sollten, die den Betroffenen belasten. Vor diesem Hintergrund sollte erwogen werden, den § 37 BDSG zu streichen um diese Bewertung im nationalen Recht zu spiegeln.

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

Grundsätzlich sind die Regelungen normenklar, sie werden jedoch von Aufsichtsbehörden überschießend ausgelegt, und sie verkürzen den Rechtsschutz für (im ordnungswidrigkeitenrechtlichen Sinne) Betroffene und Beschuldigte in nicht vertretbarer Weise. Sie schaffen eine nicht vertretbare Sanktionslücke, indem sie öffentliche Stellen von der Sanktionierung durch Bußgelder ausnehmen; dies hat schon zu nahezu rechtsfreiem Raum bei den öffentlichen Stellen geführt. So werden die Regelungen in Art. 83 Abs. 4 und 5 DS-GVO zu den Geldbußen nicht als Obergrenze für ein Bußgeld verstanden („bis zu 2 bzw. 4 % des weltweit erzielten Jahresumsatzes“). Vielmehr vertritt die DSK im Entwurf eines Bußgeldkonzepts für Verstöße gegen die DS-GVO vom 14.10.2019 die Auffassung, dass „in einem modernen Unternehmenssanktionsrecht mit erheblichen maximalen Bußgeldbeträgen, das sich zugleich an eine Vielfalt unterschiedlich großer Unternehmen richtet, der Umsatz eines Unternehmens eine geeignete, sachgerechte und faire Anknüpfung zur Sicherstellung der Wirksamkeit,

Verhältnismäßigkeit und Abschreckung darstellt." Die Auswirkungen dieses aus unserer Sicht fehlerhaften Verständnisses zeigen sich zum Teil bereits in der Sanktionierungspraxis.

Bitkom hat zum Bußgeldkonzept bereits umfassend Stellung bezogen, sodass wir an dieser Stelle auf unsere Detailkritik in unserer Stellungnahme verweisen.[3] Wir halten es für erforderlich, dass auch politisch das Fehlverständnis hinsichtlich der Sanktionierung adressiert wird.

Der Verweis auf das OWiG nimmt den Betroffenen eine Tatsacheninstanz, da als Rechtsmittel gegen Urteile der Amts- und Landgerichte nur die Rechtsbeschwerde gegeben ist. Betroffene sehen sich damit im datenschutzrechtlichen Ordnungswidrigkeitenverfahren, obwohl ihnen Sanktionen in exorbitanter Höhe drohen, mit einem verkürzten Rechtsweg konfrontiert. Gepaart mit den Beweiserleichterungen des Ordnungswidrigkeitenverfahrens, die auf Massendelikte wie Verkehrsdelikte ausgerichtet sind, werden Betroffene in die Lage gebracht, in ihrer Verteidigung von dem Zweckmäßigkeitsdenken der erkennenden Gerichte abhängig zu sein.

Die Auskunftspflichten der DS-GVO gegenüber Aufsichtsbehörden höhlen zudem die Selbstbelastungsfreiheit aus. Die scheinbare Selbstbelastungsfreiheit bei Angaben, zu denen Verantwortliche und Auftragsverarbeiter gegenüber Aufsichtsbehörden verpflichtet sind, ist wertlos, da die Aufsichtsbehörden die daraus gewonnen Erkenntnisse durch Parallelermittlungen legitimieren können und so eine uneingeschränkte Verwertung möglich wird.

Die Regelung des § 43 Abs. 3 BDSG stellt Behörden und öffentliche Stellen von jeder wirksamen Sanktion frei. Wie auch ein Unternehmen oder eine natürliche Person, würde aber auch eine Behörde diszipliniert, wenn ihr ein Teil der in ihren Haushaltstiteln ausgebrachten Mittel nicht für die geplanten Zwecke zur Verfügung steht, weil er als Bußgeld abgeführt werden muss.

8. 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?

Zum Umgang mit personenbezogenen Daten bestehen insbesondere praktische Schwierigkeiten bei den Grenzen des Anwendungsbereichs des BDSG bzw. der DS-GVO,

[3] https://www.bitkom.org/Bitkom/Publikationen/Stellungnahme-zum-Bussgeldkonzept-der-Datenschutzkonferenz

wenn es um die Anonymisierung personenbezogener Daten geht. Bisher gibt es keine klaren Informationen zu den technischen Methoden, mit denen Daten BDSG- bzw. DS-GVO-konform anonymisiert werden können.

Die Anonymisierung personenbezogener Daten ist im Unternehmensalltag ein wichtiges praxisrelevantes Instrument zur Wahrung der Datenschutzrechte der Betroffenen. Sie ist eine Alternative zur Löschung von Daten, da technische Restriktionen, z.B. im Zusammenhang mit relationalen Datenbanken, dazu führen können, dass die physische Löschung von Daten oftmals nur mit Unwägbarkeiten realisierbar ist. Außerdem können durch Anonymisierung unternehmenswichtige Informationen auf aggregierter Basis für weitere übergreifende unternehmensinterne Zwecke weiterverwendet werden.

Die DS-GVO enthält in Erwägungsgrund 26 eine Erläuterung der Anonymisierung, die darauf abstellt, ob eine Person noch identifizierbar ist: „Um festzustellen, ob eine natürliche Person noch identifizierbar ist, sollten alle Mittel berücksichtig werden, die von dem Verantwortlich oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren." Dabei sollten „alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbaren Technologien und technologischen Entwicklungen zu berücksichtigen sind." Die DS-GVO verlangt damit also keine absolute Anonymisierung derart, dass eine erneute Identifizierung für alle unmöglich sein müsste. Um eine solche relative oder faktische Anonymisierung zu erreichen, wurden verschiedene Methoden entwickelt, wie beispielsweise k-Anonymität, l-Diversität oder „Differential Privacy", die aufgrund der schnell fortschreitenden technischen Entwicklungen ständig weiter entwickelt werden.

Eine klare Aussage dazu, welche standardisierten Anonymisierungsmethoden verwendet werden können, um die Anforderungen an die Anonymisierung von personenbezogenen Daten nach dem BDSG bzw. der DS-GVO zu erfüllen, würde zur Erhöhung der Transparenz für Unternehmen beitragen und dabei das Vertrauen der Betroffenen in die Anonymisierung von Daten erheblich steigern.

Auch zu diesem Themenkomplex möchten wir auf unsere früheren Detailanmerkungen im Rahmen der Konsultation des BfDI zur Anonymisierung und unseren Leitfaden zur Anonymisierung und Pseudonymisierung von Daten verweisen.[4]

[4] https://www.bitkom.org/Bitkom/Publikationen/BfDI-Konsultation-zur-Anonymisierung und https://www.bitkom.org/Bitkom/Publikationen/Anonymisierung-und-Pseudonymisierung-von-Daten-fuer-Projekte-des-maschinellen-Lernens

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

In § 26 BDSG ist die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses geregelt. Als Rechtsgrundlagen finden sich in Absatz 1 die Regelungen zur Durchführung des Beschäftigungsverhältnisses und in Absatz 2 die Regelungen zur Verarbeitung aufgrund einer Einwilligung. Zur Rechtsgrundlage des berechtigten Interesses (Art. 6 Abs. 1 lit. f DS-GVO) finden sich jedoch keine ergänzenden Ausführungen, was Rechtsunsicherheiten hervorgerufen hat.

Aus unserer Sicht wäre eine klarstellende Ergänzung in § 26 BDSG hilfreich, die die Anforderungen an einer Verarbeitung von Beschäftigtendaten aufgrund berechtigten Interesses konkretisieren würde.

10. Sind die weiteren Bestimmungen über Datenübermittlungen an Drittstaaten und an internationale Organisationen in den §§ 79 bis 81 BDSG normenklar?

Grundsätzlich fehlen klarere und einheitliche Vorgaben (u.a. durch die Aufsichtsbehörden), zum genauen Umgang mit Datenübermittlungen an Drittstaaten. Beispiel: EU-Standarddatenschutzklauseln sind je nach Anwendungsfall (z.B. Auftragsverarbeiter mit Sitz in der EU und Subverarbeiter im Drittland vs. Auftragsverarbeiter und Subverarbeiter mit Sitz im Drittland) in verschiedenen Konstellationen zu vereinbaren. Dazu gibt es verschiedene und/oder keine öffentlichen Angaben der Aufsichtsbehörden. Im Nachgang des Urteils des EuGH (Schrems II) ist der korrekte Umgang jedoch umso bedeutender geworden. Soweit sich dieses Problem mit der Einführung neuer Standarddatenschutzklauseln der EU-Kommission nicht erledigt und keine bundeseinheitliche Vorgabe besteht, wäre eine gesetzliche Klärung wünschenswert.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.