Bundesministerium
des Innern, für Bau
und Heimat

Evaluierung des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

Impressum

Herausgeber
Bundesministerium des Innern, für Bau und Heimat, 11014 Berlin
Internet: www.bmi.bund.de

Stand
Oktober 2021

Weitere Publikationen der Bundesregierung zum Herunterladen und zum Bestellen finden Sie ebenfalls unter: www.bundesregierung.de/publikationen

Inhalt

Abkürzungsverzeichnis

a. F.	alte Fassung
BDSG	Bundesdatenschutzgesetz
AGG	Allgemeines Gleichbehandlungsgesetz
BAnz	Bundesanzeiger
BfDI	Bundesbeauftragte oder Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BfJ	Bundesamt für Justiz
BFStrMG	Bundesfernstraßenmautgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BKAG	Bundeskriminalamtgesetz
BMI	Bundesministerium des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
DSAnpUG-EU	Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU)
2. DSAnpUG-EU	Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU)
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung)
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

EDSA	Europäischer Datenschutzausschuss
EU	Europäische Union
EU-GRCh	Charta der Grundrechte der Europäischen Union
EuGH	Gerichtshof der Europäischen Union
EUZBLG	Gesetz über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union
FinDAG	Finanzdienstleistungsaufsichtsgesetz
GG	Grundgesetz
GWB	Gesetz gegen Wettbewerbsbeschränkungen
IRG	Gesetz über die internationale Rechtshilfe in Strafsachen
KSchG	Kündigungsschutzgesetz
OWiG	Gesetz über Ordnungswidrigkeiten
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StrEG	Gesetz über die Entschädigung für Strafverfolgungsmaßnahmen
VwGO	Verwaltungsgerichtsordnung
VwVG	Verwaltungsvollstreckungsgesetz (Bund)
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

1. Einleitung

Mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung, DSGVO) wurde das Datenschutzrecht in der Europäischen Union (EU) weitgehend einheitlich geregelt. Die DSGVO löste die bis dahin geltende Datenschutz-Richtlinie (Richtlinie 95/46/EG) durch eine in allen Mitgliedstaaten der EU unmittelbar geltende Verordnung ab. Sie schaffte auf diese Weise ein einheitliches Schutzniveau für das Recht aller EU-Bürgerinnen und -Bürger auf den Schutz ihrer personenbezogenen Daten.

Gleichzeitig erließ der Unionsgesetzgeber mit der Richtlinie (EU) 2016/680 einen Rechtsakt, der die Verarbeitung personenbezogener Daten durch Behörden zum Zweck der Strafverfolgung und -vollstreckung harmonisiert.

In diesem Zusammenhang bestand für den deutschen Gesetzgeber unmittelbarer Handlungsbedarf:

- Das in Deutschland bis dahin geltende Bundesdatenschutzgesetz (BDSG a. F.)[1], das seinerzeit zur Umsetzung der Richtlinie 95/46/EG erlassen worden war, wurde mit dem Geltungsbeginn der DSGVO am 25. Mai 2018 in weiten Teilen unanwendbar.
- Die DSGVO enthält viele Öffnungsklauseln, die entweder Regelungsaufträge an die Mitgliedstaaten richten oder dem nationalen Gesetzgeber Möglichkeiten geben, in einzelnen Bereichen von Regelungen der DSGVO abzuweichen oder ergänzende Regelungen zu treffen.
- Die Richtlinie (EU) 2016/680 war in deutsches Recht umzusetzen.

Vor diesem Hintergrund wurde das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU[2]) erlassen. Mit dem DSAnpUG-EU wurden die im Hinblick auf die DSGVO erforderlichen gesetzlichen Anpassungen sowie die Umsetzung der Richtlinie (EU) 2016/680 für den Bereich des Bundes im Sinne einer allgemeinen Regelung in einem neuen Bundesdatenschutzgesetz (BDSG) vorgenommen. Auf diese Weise wurde ein Ineinandergreifen der DSGVO und der Richtlinie (EU) 2016/680 mit dem stark ausdifferenzierten deutschen Datenschutzrecht sichergestellt.

[1] Bundesdatenschutzgesetz a. F. in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66); abrufbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl103s0066.pdf (zuletzt abgerufen am 1. September 2021).

[2] Vgl. BGBl. I S. 2097, abrufbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf (zuletzt abgerufen am 1. September 2021).

Durch die DSGVO und das sie ergänzende neu gefasste BDSG, das auch für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen Anwendung findet, die außerhalb des Anwendungsbereichs des Unionsrechts liegen, ergab sich auch hinsichtlich der bestehenden bereichsspezifischen Datenschutzregelungen des Bundes Änderungsbedarf. Diesem wurde durch Änderungen in fünf Stammgesetzen Rechnung getragen.

Das DSAnpUG-EU soll ausweislich der Gesetzesbegründung spätestens drei Jahre nach Inkrafttreten des Gesetzes evaluiert werden.[3] Hieraus ergibt sich der Auftrag zur Evaluierung des Gesetzes an das für das DSAnpUG-EU federführende Bundesministerium des Innern, für Bau und Heimat (BMI).

Das BMI hat diese Evaluierung durchgeführt und stellt die Ergebnisse in diesem Bericht dar.

2. Evaluierungsgegenstand

Gegenstand und Ziel der Evaluierung sind für das DSAnpUG-EU nicht gesetzlich festgelegt. Da das BDSG den Kern des DSAnpUG-EU bildet, wurde der Untersuchungsgegenstand der Evaluierung auf das BDSG beschränkt.

Das BDSG wurde in der Form evaluiert, die es durch das Zweite Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (2. DSAnpUG-EU)[4] erhalten hat.

3. Konzeption der Evaluierung

Eine Evaluierung soll einen Zusammenhang zwischen Ziel und Zweck einer Regelung und den tatsächlich erzielten Wirkungen sowie den damit verbundenen Kosten herstellen. Wichtigstes Evaluierungskriterium ist dabei die Zielerreichung.

Ziel der Neuregelungen des BDSG war es, die aufgrund der Öffnungsklauseln der DSGVO bestehenden Gestaltungsmöglichkeiten im deutschen Recht zu nutzen, an die Mitgliedstaaten gerichtete Regelungsaufträge der DSGVO aufzugreifen und die Richtlinie (EU) 2016/680 umzusetzen. Gleichzeitig sollten diese Regelungen für die Normanwender praktikabel und verständlich und damit anwenderfreundlich sein.

Die Teile 1 und 2 des BDSG treffen punktuelle Regelungen, die insbesondere Regelungsaufträge und Öffnungsklauseln der DSGVO erfüllen und nutzen. Teil 3 des BDSG dient der Umsetzung der Richtlinie (EU) 2016/680, die EU-weite Mindestanforderungen für Daten-

[3] BT-Drs. 18/11325, S. 78.
[4] Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 20. November 2019 (BGBl. I 2019 S. 1626); abrufbar unter http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl119s1626.pdf (zuletzt abgerufen am 1. September 2021).

verarbeitungen im Bereich der polizeilichen Gefahrenabwehr und der Strafverfolgung regelt. Teil 4 des BDSG trifft spezifischere Regelungen für Datenverarbeitungen außerhalb des Anwendungsbereichs der DSGVO und der Richtlinie (EU) 2016/680 und führt dabei im Wesentlichen Bestimmungen fort, die bereits im früheren BDSG geregelt waren.

Ziel der Evaluierung ist es, die Sachgerechtigkeit, Praktikabilität und Normenklarheit des BDSG zu überprüfen. Daneben hat das Statistische Bundesamt den Erfüllungsaufwand, der durch die Neuregelung des BDSG entstanden ist, nachgemessen.

Zu beachten war, dass sowohl die DSGVO als auch die Richtlinie (EU) 2016/680 einen eigenen Evaluierungsmechanismus vorsehen, der die Kommission verpflichtet, die Bestimmungen der DSGVO und der Richtlinie alle vier Jahre zu bewerten und zu überprüfen. Gegenstand der vorliegenden Evaluierung sind deshalb nur die Regelungen des BDSG, nicht aber die der DSGVO oder der Richtlinie (EU) 2016/680.

Evaluiert wurde auf der Grundlage einer Befragung von Normanwendern, da sich die Sachgerechtigkeit, Praktikabilität und Normenklarheit vor allem vom Empfängerhorizont, also dem Horizont der Normanwender, beurteilen lassen.

Hierzu wurde ein Fragebogen mit zehn Fragekomplexen und insgesamt 32 Fragen (siehe Anlage) entwickelt, mit dem die Sachgerechtigkeit, Praktikabilität und Normenklarheit der Regelungen des BDSG aus Sicht der Normanwender erfragt wurden.

Um eine möglichst umfassende Evaluierungsgrundlage zu gewinnen, wurden sowohl private als auch öffentliche Normanwender befragt. Adressaten des Fragebogens waren die 17 Datenschutzaufsichtsbehörden der Länder sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), öffentliche Stellen des Bundes, die Fachressorts der Länder sowie 88 Spitzenverbände der Wirtschaft und weitere Akteure im Bereich des Datenschutzes.

Das Statistische Bundesamt hat den Erfüllungsaufwand nachgemessen. Zur Ermittlung der tatsächlichen Kosten für die Erfüllung von Schutz- und Dokumentationspflichten bei Unterbleiben einer Information der betroffenen Person wurden die Verbände gebeten, einen zweiten Teil des Fragebogens an ihre Mitgliedsunternehmen zu versenden, in dem der Aufwand für die Erfüllung dieser Pflichten erfragt wurde. Vereinzelt ergaben sich hieraus auch Antworten auf Teil 1 des Fragebogens.

4. Art und Inhalt der Rückmeldungen

Von den 88 beteiligten Verbänden und Institutionen haben 31 eine Stellungnahme abgegeben, durch die insgesamt mehrere Millionen Unternehmen repräsentiert werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat gemeinschaftlich Stellung genommen, daneben hat eine Landesdatenschutzaufsichtsbehörde eine eigene Stellungnahme abgegeben. Als Ergänzung zur Stellungnahme der DSK haben der BfDI eine eigene und daneben 16 Landesdatenschutzaufsichtsbehörden eine

gemeinsame Stellungnahme abgegeben. Auch die beteiligten Bundesbehörden sowie neun Fachressorts der Länder, die teilweise angegeben haben, die Ressorts ihrer Landesregierung und teilweise auch die Wirtschaft umfassend beteiligt zu haben, haben den Fragebogen beantwortet.

Inhaltlich fokussieren sich die Stellungnahmen oftmals auf wenige Themen, die für die jeweils antwortenden Akteure besonders relevant sind, nur vereinzelt wurden alle Fragen beantwortet. Daraus folgt, dass die meisten Rückmeldungen zu zahlreichen Vorschriften des BDSG keine Aussagen enthalten.

Die Stellungnahmen gehen zum einen auf Sachgerechtigkeit und Praktikabilität der Vorschriften des BDSG ein. Teilweise werden inhaltliche Änderungen vorgeschlagen. Zum anderen werden Unklarheiten berichtet und Änderungsvorschläge zur Verbesserung der Normenklarheit gemacht.

In den Rückmeldungen werden zudem teilweise Zweifel an der DSGVO-Konformität verschiedener Regelungen geäußert. Diese Rückmeldungen betreffen nicht im engeren Sinn die Sachgerechtigkeit, Praktikabilität und Normenklarheit von Normen des BDSG. Auch zu diesen Rückmeldungen wird im Evaluationsbericht Stellung genommen.

Teilweise betreffen die Stellungnahmen nicht das BDSG, sondern Regelungen der DSGVO oder des Fachrechts. Darauf wird nur eingegangen, wenn ein Bezug zu Regelungen des BDSG besteht.

5. Empirische Analyse und Bewertung der zu evaluierenden Regelungen

5.1. Anwendungsbereich des Gesetzes und gemeinsame Begriffsbestimmungen – §§ 1 und 2 BDSG

5.1.1. Zielsetzung und Gegenstand der Regelungen

Die §§ 1 und 2 BDSG dienen dem Ziel, das Ineinandergreifen der DSGVO und der Richtlinie (EU) 2016/680 mit dem stark ausdifferenzierten deutschen Datenschutzrecht zu gewährleisten. Damit werden die Regelungen der DSGVO in einzelnen Bereichen innerhalb eines neu gefassten BDSG spezifiziert, die Richtlinie (EU) 2016/680 umgesetzt sowie die Vorgaben für Datenverarbeitungen öffentlicher Stellen außerhalb des Anwendungsbereichs der DSGVO und der Richtlinie (EU) 2016/680 verankert. Entsprechend der Regelungssystematik des BDSG a. F. wird ein datenschutzrechtliches Vollregime im Geltungsbereich des Grundgesetzes (GG) geschaffen[5].

Dabei bestimmt § 1 BDSG den Anwendungs- und Geltungsbereich für öffentliche und nichtöffentliche Stellen des Bundes und der Länder (Absätze 1 und 4), das Verhältnis zu anderen Rechtsvorschriften des Bundes (Absätze 2 und 3), stellt den Anwendungsvorrang der DSGVO (Absatz 5) noch einmal klar, legt fest, welche Drittstaaten den EU-Mitgliedstaaten gleichgestellt sind (Absätze 6 und 7) und regelt die entsprechende Anwendung für Datenverarbeitungen öffentlicher Stellen außerhalb des Anwendungsbereichs der DSGVO und der Richtlinie (EU) 2016/680 (Absatz 8).

§ 2 BDSG nimmt die Begriffsbestimmung und Abgrenzung öffentlicher Stellen des Bundes und der Länder sowie nichtöffentlicher Stellen vor. Zudem bestimmt § 2 BDSG, welche öffentlichen Stellen und nichtöffentlichen Stellen unter den Anwendungsbereich nach § 1 BDSG fallen.

5.1.2. Empirische Ergebnisse und Bewertung

Nach den Rückmeldungen werden die Regelungen als überwiegend gelungen und grundsätzlich sachgerecht, praktikabel und normenklar beurteilt.

5.1.2.1. Rückmeldungen zu § 1

Abgrenzungsschwierigkeiten bei der Anwendbarkeit des BDSG im Verhältnis zu anderen Normen

Seitens der Länder wird lediglich vereinzelt darauf hingewiesen, dass Schwierigkeiten bei der Abgrenzung bestünden, wann die datenschutzrechtlichen Vorgaben der Länder und

[5] BT-Drs. 18/11325, S. 69

wann das BDSG anzuwenden seien. Dies betrifft zum einen gemeinsame Einrichtungen des Bundes und kommunaler Träger und zum anderen die Frage, wann der Anwendungsbereich des BDSG für Gerichte eröffnet sei.

Da die meisten Länder diesbezüglich keine Probleme sehen, ist insoweit eine Änderung des BDSG aus Sicht des BMI nicht zwingend erforderlich. Bei gemeinsamen Einrichtungen des Bundes und kommunaler Träger stellt sich die Frage nach dem anwendbaren Recht zudem nicht nur hinsichtlich des Datenschutzes, sondern allgemein als Abgrenzung zwischen Bundes- und Landesrecht, sodass eine Insellösung im BDSG nicht angezeigt erscheint.

Die Regelung zur Anwendbarkeit des BDSG auf die Organe der Rechtspflege in § 2 Absatz 1 BDSG entspricht § 1 Absatz 2 Nummer 2b BDSG a. F. und wird im BDSG weitergeführt. Nach den eingegangenen Rückmeldung hat sich die Regelung insgesamt bewährt. Eine Änderung hält das BMI daher nicht für erforderlich.

Ausschließliche Anordnung der Anwendung des BDSG durch öffentliche Stellen der Länder in den Landesdatenschutzgesetzen

In diesem Kontext wird angeregt, § 1 Absatz 1 Nummer 2 BDSG derart zu ändern, dass zukünftig Anordnungen zur Anwendung des BDSG durch öffentliche Stellen der Länder ausschließlich in den Landesdatenschutzgesetzen zu treffen seien.

Einer entsprechenden Änderung der Regelung bedarf es aus Sicht des BMI jedoch nicht. § 1 Absatz 1 Nummer 2 BDSG, der der Regelung zum Anwendungsbereich in § 1 Absatz 1 Nummer 2 BDSG a. F. entspricht, hat sich nach den Rückmeldungen zur Evaluierung in der Praxis im Allgemeinen bewährt und dient so auch der fortwährenden Rechtssicherheit.

Hinsichtlich § 1 Absatz 1 Satz 2 BDSG wird aus der Wirtschaft empfohlen, die Formulierung „(...) oder gespeichert werden sollen (...)“ ersatzlos zu streichen, da dies zu weitgehend sei und von der Praxis übersehen werden könne. Die Formulierung in § 1 Absatz 1 Nummer 2 BDSG entspricht allerdings dem in Artikel 2 Absatz 1 DSGVO festgelegten sachlichen Anwendungsbereich der DSGVO und kann daher nicht gestrichen werden.

Streichung des Satzteils „des Bundes“ in § 1 Absatz 2 BDSG

Zudem wird seitens eines Landes gewünscht, dass die Länder im Rahmen ihrer Gesetzgebungskompetenz befugt sein sollen, auch für die vom Anwendungsbereich des BDSG erfassten nichtöffentlichen Stellen, insbesondere im Krankenhausbereich, abweichende Datenschutzregelungen zu treffen. Dazu wird vorgeschlagen, in § 1 Absatz 2 BDSG den Zusatz „des Bundes“ zu streichen, um klarzustellen, dass nicht nur Rechtsvorschriften des Bundes, sondern auch solche der Länder den Auffangregelungen im BDSG vorgehen.

Für eine solche Änderung sieht das BMI jedoch keinen zwingenden Bedarf. Die Gesetzgebungskompetenzen von Bund und Ländern richten sich nach den Regelungen des GG. Für nichtöffentliche Stellen ergibt sich die Gesetzgebungskompetenz des Bundes weiterhin als Annex aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft). Eine bundesgesetzliche Regelung des Datenschutzes ist zur Wahrung der Rechtseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich, weil andernfalls zu befürchten wäre, dass unterschiedliche landesrechtliche Regelungen erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Dies würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden können.[6]

Soweit es hier zu einem Spannungsverhältnis mit der Wahrnehmung von Aufgaben der öffentlichen Verwaltung kommt, die in die Kompetenz der Länder fallen, wird dies durch die differenzierten Bestimmungen in § 2 BDSG aufgefangen. Hierbei ist insbesondere § 2 Absatz 4 Satz 2 BDSG zu nennen, nach dem nichtöffentliche Stellen dann als öffentliche Stellen zu betrachten sind, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen.

Streichung § 1 Absatz 4 Satz 2 Nummer 1 BDSG

Hinsichtlich der Regelung des räumlichen Anwendungsbereichs für nichtöffentliche Stellen wird aus dem Kreis der Länder angeregt, § 1 Absatz 4 Satz 2 Nummer 1 BDSG anzupassen, da hier eine Konstellation denkbar sei, bei der zwar das BDSG, nicht aber die DSGVO anwendbar wäre. Dies sei dann der Fall, wenn zwar keine Niederlassung des Verantwortlichen oder eines Auftragsverarbeiters in der EU bestehe und auch kein Angebot von Waren oder Dienstleistungen gegenüber Personen in der EU bzw. keine Verhaltensbeobachtung erfolge (Artikel 3 DSGVO), der Verantwortliche aber Daten in Deutschland verarbeite. Dies sei möglicherweise unionsrechtswidrig.

Aus Sicht des BMI besteht kein zwingender Bedarf, die Regelung entsprechend zu ändern. Zwar lässt die DSGVO den Ort der Datenverarbeitung bei der Bestimmung ihres Anwendungsbereichs außer Acht. Soweit jedoch eine Datenverarbeitung nicht in den Anwendungsbereich der DSGVO fällt, entfaltet diese auch keine Sperrwirkung. Für die Wirkung einer nationalen Regelung enthält die DSGVO insoweit keine Vorgaben.

Klarstellung des Inlandsbezugs bei § 1 Absatz 4 Satz 2 Nummer 3 BDSG

Aus der Wirtschaft wird vereinzelt eine Klarstellung hinsichtlich § 1 Absatz 4 Satz2 Nummer 3 BDSG dahingehend gewünscht, dass die Regelung nur insoweit greife, wie auch ein Inlandsbezug der Datenverarbeitung bestehe.

[6] So auch schon die Gesetzesbegründung: BT-Drs. 18/11325, S. 71.

Das BMI wird eine Klarstellung der Regelung prüfen, um eindeutig zum Ausdruck zu bringen, dass das BDSG nur anwendbar ist, wenn ein Inlandsbezug der Datenverarbeitung besteht.

Umformulierung § 1 Absatz 4 Satz 3 BDSG zur Hervorhebung, dass nichtöffentliche Stellen adressiert sind

Die Datenschutzaufsichtsbehörden regen an, § 1 Absatz 4 Satz 3 BDSG 1. Halbsatz wie folgt zu fassen: *„Sofern dieses Gesetz auf nichtöffentliche Stellen gemäß Satz 2 keine Anwendung findet, …“.* Ziel dieses Vorschlages ist es, keinen Zweifel darüber aufkommen zu lassen, dass damit nicht die Fälle nach Satz 1 gemeint sind, also die Anwendung des BDSG auf öffentliche Stellen.

Zwar ist dies aus der Systematik bereits erkennbar, das BMI wird aber prüfen, ob eine entsprechende Umformulierung vorgenommen werden soll.

5.1.2.2. Rückmeldungen zu § 2 BDSG

Die Regelung des § 2 BDSG wird in den Rückmeldungen weitgehend als gelungen bezeichnet, insbesondere Absatz 1 und Absatz 2. Es werden aber auch Änderungswünsche vorgebracht.

Ergänzung von § 2 Absatz 3 BDSG um Regelbeispiele oder weitere Tatbestandsmerkmale

Zu § 2 Absatz 3 BDSG wird von Abgrenzungsschwierigkeiten berichtet. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass in der Praxis die Auslegung des § 2 Absatz 3 Satz 1 Nummer 1 BDSG zu Problemen führe und eine Konkretisierung durch den Gesetzgeber hilfreich wäre.

Allerdings weisen die Aufsichtsbehörden selbst darauf hin, dass solche Fälle bislang durch Abstimmung zwischen den beteiligten Aufsichtsbehörden sachgerecht gelöst werden konnten. Dabei werde ein weiter Auslegungsspielraum hinsichtlich der Tatbestandsmerkmale „Aufgaben der öffentlichen Verwaltung“ und „über den Bereich eines Landes hinaus tätig werden“ gesehen.

Aus der Forschung wird zudem angeregt, § 2 Absatz 3 BDSG um Regelbeispiele zu ergänzen.

Angesichts der Vielzahl der möglichen Fallkonstellationen, die die Norm erfassen soll, erscheint es aus Sicht des BMI nicht angezeigt, einzelne Anwendungsfälle durch Regelbeispiele hervorzuheben und so eventuell Rechtsunklarheit im Hinblick auf andere Fallgestaltungen hervorzurufen. Da die Praktikabilität der Norm in den Rückmeldungen überwiegend nicht bemängelt wurde, erscheint eine Änderung der Vorschrift nicht zwingend.

Nichtöffentliche Stellen nur bei Wahrnehmung ihrer Kerntätigkeit als öffentliche Stellen im Sinne des § 2 Absatz 4 Satz 2 BDSG behandeln

§ 2 Absatz 4 BDSG regelt die Voraussetzungen, unter denen nichtöffentliche Stellen aufgrund ihrer Wahrnehmung von hoheitlichen Aufgaben wie öffentliche Stellen behandelt werden. Dabei macht der Wortlaut schon deutlich, dass die Vorschrift nicht nur auf Beliehene anzuwenden ist, weswegen eine entsprechende Klarstellung – wie von einem Land angeregt – nicht erforderlich ist. Zu diesem Absatz wird von Seiten der Wirtschaft und der Länder vorgeschlagen, dass nur solche Personen und privaten Betriebe als öffentliche Stelle im Sinne des BDSG qualifiziert werden sollten, deren Kerntätigkeit in der Wahrnehmung hoheitlicher Aufgaben liegt. Hier sei insbesondere die starke Belastung von Kleinstbetrieben zu reduzieren, wenn sie als Beliehene tätig werden.

Es erscheint nachvollziehbar, dass die Pflicht zur Bestellung eines Datenschutzbeauftragten für Kleinstbetriebe, die in einem untergeordneten Teil ihrer Tätigkeit als Beliehene tätig werden, einen verhältnismäßig hohen Aufwand darstellt. Inwieweit für diese Betriebe Erleichterungen geschaffen werden können, wird das BMI weiter prüfen.

Ergänzung des § 2 Absatz 5 Satz 1 BDSG um „ganz oder teilweise“

§ 2 Absatz 5 BDSG regelt, wann und inwieweit eine öffentliche Stelle ausnahmsweise als nichtöffentliche Stelle behandelt werden soll. Hier wird darauf hingewiesen, dass öffentliche Stellen gelegentlich nur teilweise am Wettbewerb teilnehmen und es dann unklar sei, wie diese zu bewerten seien. Dabei wird eine Ergänzung des § 2 Absatz 5 Satz 1 BDSG um die Formulierung „ganz oder teilweise“ vorgeschlagen, um klarzustellen, dass sie dann als nichtöffentliche Stelle zu behandeln seien.

Einer solchen Änderung bedarf es aus Sicht des BMI jedoch nicht. Nach Absatz 5 soll eine öffentliche Stelle nur soweit als nichtöffentliche Stelle behandelt werden, wie sie aus Wettbewerbsgründen dazu verpflichtet ist. Dies spiegelt die aktuelle Regelung wider, die darauf abstellt, dass eine Behandlung als nichtöffentliche Stelle nur insoweit gelten soll, wie sie als öffentlich-rechtliches Unternehmen am Wettbewerb teilnimmt. Ist dies nur teilweise der Fall, dann gilt dies nur für den entsprechenden Teil der Tätigkeit.

Legaldefinitionen von „Verschlüsselung“, „Stand der Technik“ und „Anonymisierung “

Zudem wird vereinzelt angeregt, dass Legaldefinitionen der Begriffe „Verschlüsselung“ „Stand der Technik“ und „Anonymisierung“ eingeführt werden sollen.

Die Unsicherheiten, die im Hinblick darauf bestehen, wann Daten so anonymisiert sind, dass eine betroffene Person nicht mehr identifiziert werden kann, sind zwar nachvollziehbar. Gleichwohl wäre aus Sicht des BMI der richtige Regelungsstandort für die Definition datenschutzrechtlicher Begriffe die DSGVO und nicht der allgemeine Teil des BDSG, da sich diese Definition nur auf Verarbeitungsvorgänge nach dem BDSG beziehen würde.

Dies würde zwar etwa im Hinblick auf die Pflicht nach § 27 Absatz 3 BDSG zur Anonymisierung von Daten, die zu Forschungszwecken erhoben wurden, weiterhelfen, zu sonstigen Anonymisierungsvorgängen, die sich nach der DSGVO richten, jedoch nicht.

Der Gesetzgeber hat bewusst davon abgesehen, in § 2 BDSG datenschutzrechtliche Begriffe zu definieren und hat hier nur solche Begriffe definiert, die nicht spezifisch datenschutzrechtlich sind. Mit Artikel 4 DSGVO besteht hingegen ein Katalog an datenschutzrechtlichen Begriffen, die dem gemeinsamen Verständnis der DSGVO zugrunde liegen. Der Begriff „Anonymisierung" wird im BDSG nicht definiert, im Erwägungsgrund 26 der DSGVO wird aber der Begriff „anonyme Informationen" erläutert.

5.1.3. Schlussfolgerung

Aus den Rückmeldungen wird deutlich, dass der für das BDSG gewählte integrative Ansatz, die auf die DSGVO und die Richtlinie (EU) 2016/680 bezogenen Regelungen in einem Gesetz zu vereinen und dafür Teile des Gesetzes gewissermaßen „vor die Klammer zu ziehen", zwar überwiegend als gelungen angesehen wird, dennoch aber die daraus folgende Komplexität zum Teil als unübersichtlich wahrgenommen wird. Die eingegangenen Änderungsvorschläge dienen vor allem der Klarstellung. Teilweise werden aber auch inhaltliche Veränderungen vorgeschlagen. Das BMI wird Folgendes weiter prüfen:

- eine Klarstellung der Regelung in § 1 Absatz 4 Satz 2 Nummer 3 BDSG, um ggf. eindeutig zum Ausdruck zu bringen, dass das BDSG nur anwendbar ist, wenn ein Inlandsbezug der Datenverarbeitung besteht;
- ob eine Umformulierung des § 1 Absatz 4 Satz 3 BDSG vorgenommen werden soll, um ggf. deutlich zu machen, dass die Norm nur nichtöffentliche Stellen adressiert;
- ob für Betriebe, die nur vereinzelt hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, der Umfang der Verpflichtungen, die das BDSG an öffentliche Stellen stellt, verringert werden sollte.

5.2. Rechtsgrundlagen für die Datenverarbeitung – §§ 3 und 4 BDSG

5.2.1. Zielsetzung und Gegenstand der Regelungen

Mit den §§ 3 und 4 BDSG hat der Gesetzgeber Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch öffentliche Stellen und für die Videoüberwachung öffentlich zugänglicher Räume geschaffen.

Die Regelung des § 3 BDSG dient dem Ziel, für die Fälle, in denen keine bereichsspezifische Verarbeitungsbefugnis besteht, eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen zur Verfügung zu stellen. Es handelt sich um eine allgemeine subsidiäre Rechtsgrundlage im Sinne einer Generalklausel, welche insbesondere im Falle geringer Eingriffsintensität, also bei weniger grundrechtsintensiven Datenverarbeitungen, in Betracht kommt. Sie kann sowohl im Geltungsbereich der Richtlinie (EU) 2016/680 als auch im Geltungsbereich der DSGVO angewandt werden. Soweit die Vorschrift für Datenverarbeitungen im Anwendungsbereich der DSGVO gilt, beruht sie auf der Öffnungsklausel des Artikels 6 Absatz 1 Buchstabe e DSGVO.

§ 4 BDSG regelt die Zulässigkeit der Videoüberwachung öffentlich zugänglicher Räume.

5.2.2. Empirische Ergebnisse und Bewertung

Die Regelungen der §§ 3 und 4 BDSG werden in den Rückmeldungen überwiegend für sachgerecht, praktikabel und normenklar gehalten. Insbesondere zu § 3 BDSG werden aber Unklarheiten bezüglich dessen Anwendungsbereich berichtet.

5.2.2.1. Rückmeldungen und Bewertung zu § 3 BDSG

Von behördlicher Seite wird teilweise von Anwendungsschwierigkeiten hinsichtlich § 3 BDSG berichtet. Das Verhältnis zu Artikel 6 Absatz 1 Buchstabe e DSGVO, dem die Norm im Wesentlichen entspreche, sei unklar. Auch § 3 BDSG setze voraus, dass eine andere Rechtsnorm die öffentliche Aufgabe beschreibe. Es bestehe die Schwierigkeit, den Anwendungsbereich der Auffangvorschrift nicht zu überdehnen, um das Recht auf informationelle Selbstbestimmung zu wahren.

§ 3 BDSG setzt den Regelungsgehalt von Artikel 6 Absatz 1 Buchstabe e DSGVO für den Bereich der öffentlichen Stellen des Bundes in das deutsche Recht um. Dies ist aufgrund von Artikel 6 Absatz 3 DSGVO erforderlich, da die Rechtsgrundlagen für die in Artikel 6 Absatz 1 Buchstabe e DSGVO genannten Verarbeitungen durch das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, festgelegt werden. Die Vorschrift des § 3 BDSG wurde vor diesem Hintergrund als subsidiäre, allgemeine Rechtsgrundlage für Datenverarbeitungen mit geringer Eingriffsintensität in die Rechte der betroffenen Person

geschaffen[7] und hat als datenschutzrechtliche Auffangnorm eine nicht zu unterschätzende praktische Relevanz für die öffentliche Verwaltung. Dies gilt insbesondere im Hinblick auf wenig grundrechtssensible Datenverarbeitungen, für die keine spezialgesetzliche Datenverarbeitungsnorm existiert und für die es auch nicht angezeigt erscheint, eine solche zu schaffen. Ein praktischer Anwendungsfall ist etwa das Notieren von Name, Adresse und Geburtsdatum beim Einlass von Besuchern. Maßstab bei der Beurteilung, ob eine Datenverarbeitung auf § 3 BDSG gestützt werden kann, sollte stets die Intensität des Eingriffs in die informationelle Selbstbestimmung sein.

5.2.2.2. Rückmeldungen und Bewertung zu § 4 BDSG

Im Rahmen der Rückmeldungen sowohl aus dem behördlichen Bereich als auch aus der Wirtschaft wird angeregt, den Wortlaut des § 4 BDSG an die Rechtsprechung des Bundesverwaltungsgerichts[8] (BVerwG) anzupassen. Das BVerwG hatte – im Rahmen eines Obiter Dictums – ausgeführt, aufgrund der unmittelbaren Anwendbarkeit der DSGVO sei für die Regelung kein Raum, soweit sie die Videoüberwachung durch Private regele, ohne dass gesetzlich die Voraussetzungen des Artikels 6 Absatz 1 Unterabsatz 1 Buchstabe e (bzw. c) DSGVO geschaffen würden. § 4 BDSG in seiner jetzigen Fassung könne nicht auf die Öffnungsklausel des Artikels 6 Absatz 1 Unterabsatz 1 Buchstabe e DSGVO gestützt werden. Private könnten nur dann eine öffentliche Aufgabe wahrnehmen, wenn ihnen die Befugnis, auf personenbezogene Daten im öffentlichen Interesse oder als Ausübung öffentlicher Gewalt zuzugreifen, im Wege eines Übertragungsakts verliehen worden sei (wie z. B. bei Beliehenen). Die Videoüberwachung Privater sei derzeit vielmehr ausschließlich auf Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DSGVO zu stützen.

Es wird deshalb vielfach vorgeschlagen, den Anwendungsreich des § 4 BDSG gesetzlich auf Videoüberwachungen durch öffentliche Stellen zu beschränken.

Demgegenüber wird teilweise auch vorgetragen, es handele sich bei § 4 BDSG um eine sachgerechte Regelung, für die trotz des Urteils des Bundesverwaltungsgerichts noch ein eingeschränkter Anwendungsbereich verbleibe und die insbesondere für hochfrequentierte Risikobereiche weiterhin Bedeutung habe.

Die Videoüberwachung durch Private leistet aus Sicht des BMI einen wichtigen Beitrag zur Gewährleistung der öffentlichen Sicherheit und zur Erhöhung der Sicherheit und des Sicherheitsgefühls der Bevölkerung.

Die Bedenken auch des Bundesverwaltungsgerichts an der Norm machen es aus Sicht des BMI jedoch erforderlich, die rechtlichen Grundlagen der Videoüberwachung durch nichtöffentliche Stellen im BDSG neu zu prüfen und die Regelung gegebenenfalls anzupassen.

[7] BT-Drs. 18/11325, S. 81.
[8] BVerwG, Urteil vom 27. März 2019 – Az. 6 C 2.18.

5.2.3. Schlussfolgerungen

Im Ergebnis haben sich die Regelungen der §§ 3 und 4 BDSG – trotz der punktuell an ihnen geäußerten Kritik – weitgehendbewährt. Lediglich hinsichtlich § 4 BDSG wird das BMI eine Änderung prüfen.

5.3. Rechtsgrundlagen für die Datenverarbeitung – Verarbeitung besonderer Kategorien personenbezogener Daten und Verarbeitung zu anderen Zwecken – §§ 22 bis 25 BDSG

Mit den §§ 22 bis 25 BDSG hat der Gesetzgeber unter Nutzung der Öffnungsklauseln der Artikel 6 und 9 DSGVO spezifische Rechtsgrundlagen für die Verarbeitung personenbezogener Daten geschaffen.

5.3.1. Zielsetzung und Gegenstand der Regelungen

Die Regelung des § 22 BDSG dient unter Rückgriff auf die Öffnungsklauseln des Artikels 9 Absatz 2 Buchstabe b, g, h und i DSGVO dem Ziel, für die Fälle, in denen keine bereichsspezifische Verarbeitungsbefugnis besteht, festzulegen, unter welchen Voraussetzungen die Verarbeitung besonderer Kategorien personenbezogener Daten ausnahmsweise zulässig ist. Die Vorschrift orientiert sich an den Regelungen des BDSG a. F.

Die Regelung des § 23 BDSG schafft für öffentliche Stellen im Rahmen der jeweiligen Aufgabenerfüllung eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch denselben Verarbeiter zu anderen – mit dem ursprünglichen Zweck nicht kompatiblen – Zwecken (zweckändernde Weiterverarbeitung).

Artikel 6 Absatz 4 DSGVO verlangt für die Datenverarbeitung im Falle fehlender Zweckkompatibilität entweder eine Einwilligung oder eine (mitgliedstaatliche) Rechtsgrundlage. Eine solche allgemeine Rechtsgrundlage stellt § 23 BDSG für die Weiterverarbeitung durch öffentliche Stellen dar. Sie orientiert sich an den Regelungen im BDSG a. F.

Die Regelung des § 24 BDSG dient der Schaffung einer Rechtsgrundlage für die Weiterverarbeitung personenbezogener Daten durch nichtöffentliche Stellen. Sie orientiert sich an den Regelungen im BDSG a. F.

Mit der Regelung des § 25 BDSG ist eine Rechtsgrundlage für die Übermittlung personenbezogener Daten durch öffentliche Stellen geschaffen worden, soweit diese von den Zwecken der ursprünglichen Erhebung abweichen. Absatz 1 regelt die Voraussetzungen der Datenübermittlung an öffentliche Stellen und Absatz 2 die Datenübermittlung an nichtöffentliche Stellen. Die Regelung entspricht den Vorschriften im BDSG a. F.

5.3.2. Empirische Ergebnisse und Bewertung

5.3.2.1. Rückmeldungen und Bewertung zu § 22 BDSG

Normwiederholung und mangelnde Bestimmtheit

Vereinzelt werden größere Teile des § 22 BDSG insbesondere unter Hinweis darauf kritisiert, dass vielfach lediglich der Normtext der DSGVO, insbesondere des Artikels 9 DSGVO, wiederholt würde. Teilweise stoßen zumindest einzelne Nummern der Absätze 1 und 2

des § 22 BDSG unter Hinweis auf mangelnde Bestimmtheit bzw. fehlende – über Artikel 9 oder Artikel 32 DSGVO hinausgehender – Spezifizierung auf Kritik.

Entgegen dieser Kritik besteht für die Auffang-Datenverarbeitungsbefugnis des § 22 BDSG ein beträchtliches praktisches Bedürfnis, welches sich nicht zuletzt im Zuge der Corona-Pandemie mehrfach gezeigt hat. Die Norm erweist sich zudem auch als unionsrechtskonform. Sie stützt sich auf die Öffnungsklauseln des Artikels 9 Absatz 2 Buchstabe b, h, i und g DSGVO. Auch die Tatsache, dass die Norm allgemein gehalten ist und – anders als dies bei bereichsspezifischen Vorschriften des Gesundheitsrechts der Fall ist – verstärkt die Begrifflichkeiten des Artikels 9 DSGVO in Bezug nimmt, liegt in der Natur einer solchen Generalklausel. Im Hinblick auf Absatz 1 ist zudem zu berücksichtigen, dass für eine zulässige Datenverarbeitung auch die Voraussetzungen des Absatzes 2 vorliegen müssen. Es wird mithin entgegen mancher Kritik nicht lediglich der Gesetzestext des Artikels 9 Absatz 2 DSGVO wiederholt.

Aufnahme einer Verarbeitungsbefugnis für Gesundheitsdaten zu Versicherungszwecken

Mitunter wird vorgeschlagen, eine Verarbeitungsbefugnis für Gesundheitsdaten zu Versicherungszwecken in die Regelung des § 22 BDSG aufzunehmen.

Dies erscheint indes mangels geeigneter Öffnungsklausel in Artikel 9 Absatz 2 DSGVO nur schwer zu verwirklichen. Wenngleich nachvollziehbar erscheint, dass der – derzeit praktizierte – Rückgriff auf die Einwilligung aufgrund deren Widerruflichkeit ein „Sonderkündigungsrecht durch die Hintertür“ schaffen kann, sieht das BMI für eine Ergänzung des § 22 BDSG im gewünschten Sinne mangels einer tragfähigen Öffnungsklausel keine Grundlage.

5.3.2.2. Rückmeldungen und Bewertung zu § 23 BDSG

§ 23 Absatz 1 Nummer 2 BDSG

§ 23 Absatz 1 Nummer 2 BDSG erlaubt die Datenverarbeitung durch öffentliche Stellen zur Überprüfung der Angaben der betroffenen Person, wenn tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen. Die Regelung wird teilweise mit dem Hinweis kritisiert, dass sie nicht in jeder Hinsicht den Anforderungen des Artikels 6 Absatz 4 i. V. m. Artikel 23 Absatz 1 DSGVO genüge.

Die Vorschrift schafft die Möglichkeit, die Richtigkeit von Daten, die öffentliche Stellen gespeichert haben, zu überprüfen. Sie dient dem Grundsatz der Rechtmäßigkeit der Verwaltung und damit dem Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses des Bundesrepublik Deutschland. Sie stützt sich damit auf die Öffnungsklausel des Artikels 23 Absatz 1 Unterabsatz 1 Buchstabe e DSGVO.

5.3.2.3. Rückmeldungen und Bewertung zu § 24 BDSG

Zweckändernde Weiterverarbeitung nach allgemeiner Interessenabwägung

Aus der Wirtschaft wird vereinzelt der Wunsch geäußert, § 24 BDSG dahingehend zu ergänzen, dass eine zweckändernde Weiterverarbeitung (analog Artikel 6 Unterabsatz 1 Absatz 1 Buchstabe f DSGVO) nach Durchführung einer allgemeinen Interessenabwägung zulässig sein soll.

Diesem Anliegen kann schon deshalb nicht entsprochen werden, da für eine solch weitgehende allgemeine Verarbeitungsbefugnis keine Öffnungsklausel in der DSGVO existiert.

Datenherausgabe an Ermittlungsbehörden

Zudem wird in den Rückmeldungen aus der Wirtschaft vereinzelt gebeten, in § 24 BDSG klarzustellen, dass eine Datenherausgabe an Ermittlungsbehörden zulässig ist.

Es wird darauf hingewiesen, dass genau dies in § 24 Absatz 1 Nummer 1 Alternative 2 BDSG geregelt ist.

5.3.2.4. Rückmeldungen und Bewertung zu § 25 BDSG

Streichung des § 25 BDSG

Teilweise wird die Ansicht vertreten, es bedürfe der Regelung des § 25 Absatz 2 Nummer 1 BDSG nicht, vielmehr könne eine Datenübermittlung zur Aufgabenerfüllung – weitgehend voraussetzungslos – bereits auf § 3 BDSG gestützt werden.

Hierzu ist darauf hinzuweisen, dass § 25 BDSG im Verhältnis zu § 3 BDSG eine Spezialvorschrift ist und an die Datenübermittlung durch öffentliche Stellen spezifische und durchaus auch höhere Anforderungen stellt als § 3 BDSG. Sofern die Datenverarbeitung zur Aufgabenwahrnehmung der übermittelnden oder empfangenden Stelle erforderlich ist, ist die maßgebliche Regelung mithin § 25 BDSG. Dabei regelt Absatz 1 die Anforderungen einer Datenübermittlung an öffentliche Stellen und Absatz 2 die Anforderungen einer Datenübermittlung an nichtöffentliche Stellen. § 25 Absatz 2 Nummer 1 BDSG bestimmt, dass die Datenübermittlung zur Aufgabenerfüllung erforderlich sein muss und die Anforderungen des § 23 BDSG einzuhalten sind.

Interessenabwägung im Rahmen des § 25 Absatz 2 Satz 1 Nummer 2 BDSG nicht ausschließlich durch übermittelnde Stelle

Aus dem behördlichen Bereich wird teilweise angeregt, die Regelung des § 25 Absatz 2 Satz 1 Nummer 2 BDSG zu überdenken, denn es sei nicht sachgerecht, die (unter Umständen durchaus schwierige) Interessenabwägung in Gänze der übermittelnden Stelle aufzubürden.

Die Prüfung, ob die Voraussetzungen für eine Datenübermittlung vorliegen, obliegt stets dem Verantwortlichen. Dies macht gerade seine Verantwortlichkeit aus. Eine Änderung des § 25 Absatz 2 Satz 1 Nummer 2 BDSG ist daher aus Sicht des BMI nicht angezeigt.

§ 25 Absatz 2 Satz 1 Nummer 3 BDSG – Einschränkung nur für zivilrechtliche Ansprüche

Die Regelung des § 25 Absatz 2 BDSG wird in Rückmeldungen aus der Wirtschaft ausdrücklich als sachgerechte und rechtssichere Rechtsgrundlage für Datenübermittlungen angesehen. Von anderer Seite wird teilweise vorgeschlagen, die Regelung des § 25 Absatz 2 Satz 1 Nummer 3 BDSG – entsprechend der Öffnungsklausel des Artikels 6 Absatz 4 i. V. m. Artikel 23 Absatz 1 Buchstabe j DSGVO – auf zivilrechtliche Ansprüche zu beschränken.

Zwar ist die Öffnungsklausel des Artikels 23 Absatz 1 Buchstabe j DSGVO auf die Beschränkung von Betroffenenrechten zugunsten der Durchsetzung zivilrechtlicher Ansprüche bezogen. § 25 Absatz 2 Satz 1 Nummer 3 BDSG ist aber zum Schutz der Rechte anderer Personen, namentlich der die Daten verarbeitenden nichtöffentlichen Stellen, erforderlich und stützt sich damit auf die Öffnungsklausel des Artikels 23 Absatz 1 Buchstabe i DSGVO. Eine Datenübermittlung darf indes nur erfolgen, wenn tatsächliche Anhaltspunkte bestehen, dass die Rechtsdurchsetzung tatsächlich gefährdet wird.

5.3.3. Schlussfolgerungen

Die Rückmeldungen zu den §§ 22 bis 25 BDSG stellen die Sachgerechtigkeit, Praktikabilität und Normenklarheit nicht grundsätzlich in Frage. Es werden lediglich vereinzelt Änderungen vorgeschlagen, die aus Sicht des BMI nicht erforderlich erscheinen.

5.4. Rechtsgrundlagen für die Datenverarbeitung – besondere Verarbeitungssituationen - §§ 26 bis 29 BDSG

5.4.1. Zielsetzung und Gegenstand der Regelungen

Mit den §§ 26 bis 29 BDSG hat der Gesetzgeber im Bereich des Beschäftigtendatenschutzes, der Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken sowie zu im öffentlichen Interesse liegenden Archivzwecken die Öffnungsklauseln des Kapitels IX der DSGVO genutzt.

Die Öffnungsklausel des Artikels 88 DSGVO lässt nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext zu. Mit § 26 BDSG hat der Gesetzgeber hiervon Gebrauch gemacht. § 26 BDSG führt in weiten Teilen die spezialgesetzliche Regelung des § 32 BDSG a. F. fort.

§ 27 BDSG trifft im Hinblick auf die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken Aussagen zur Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 DSGVO (Absatz 1 und 3), Beschränkung von Betroffenenrechten (Absatz 2) und Veröffentlichung von Daten zu Forschungszwecken (Absatz 4).

§ 28 BDSG enthält im Hinblick auf die Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken Aussagen zur Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 DSGVO (Absatz 1) und zur Beschränkung von Betroffenenrechten (Absatz 2 bis 4).

§ 29 BDSG trifft Aussagen zur Datenverarbeitung in Bereichen, in denen Geheimhaltungspflichten des Verantwortlichen bzw. Auftragsverarbeiters bestehen. Die Absätze 1 und 2 beschränken aus Artikel 13, 14, 15 und 34 DSGVO resultierende Rechte bzw. Pflichten. Absatz 3 regelt Untersuchungsbefugnisse und Geheimhaltungspflichten der Aufsichtsbehörden.

5.4.2. Empirische Ergebnisse und Bewertung

5.4.2.1. Rückmeldungen und Bewertung zu § 26 BDSG

In den zahlreichen Stellungnahmen, die den Beschäftigtendatenschutz thematisieren, wird § 26 BDSG überwiegend als sach- und praxisgerecht beurteilt, wenngleich zum Teil einzelne Änderungen der Vorschrift angeregt werden. Teilweise wird auch für die Einführung eines eigenen Beschäftigtendatenschutzgesetzes plädiert.

Einführung eines Beschäftigtendatenschutzgesetzes

Von manchen Verbänden wird vorgeschlagen, ein über die geltenden Regelungen hinausgehendes Beschäftigtendatenschutzgesetz einzuführen, das umfassende Regelungen zum

Beschäftigtenverhältnis u. a. zum Fragerecht des Arbeitgebers, zur Videoüberwachung im Beschäftigungskontext und zur Zulässigkeit ärztlicher Untersuchungen und Eignungstests enthalten soll. Auch die Datenschutzbehörden halten eine Konkretisierung der Regelungen zum Beschäftigtendatenschutz – innerhalb des BDSG oder in einem eigenen Gesetz für hilfreich. Für die Vielzahl spezifischer Verarbeitungssituationen entstünden aus dem weiten Interpretationsspielraum des § 26 BDSG Unklarheiten für alle Beteiligten über die Zulässigkeit verschiedener Datenverarbeitungen.

Demgegenüber sprechen sich andere Verbände explizit gegen die Einführung eines eigenständigen Beschäftigtendatenschutzgesetzes aus. Ganz überwiegend werden in den Rückmeldungen die Regelungen zum Beschäftigtendatenschutzgesetz nicht problematisiert.

Aus den Rückmeldungen ergibt sich in einer Gesamtschau aus Sicht des BMI derzeit kein zwingender Bedarf für ein eigenes, umfassendes Beschäftigtendatenschutzgesetz. Für die Beurteilung der Frage, ob und inwieweit über den aktuellen § 26 BDSG hinaus konkretisierende Regelungen zum Beschäftigtendatenschutz geschaffen werden sollten, muss auch die Entscheidung des Gerichtshofs der Europäischen Union (EuGH) zu dem Vorlageverfahren des Verwaltungsgerichts Wiesbaden in der Rechtssache C-34/21 abgewartet werden. Dieses wird die Frage klären, ob die dem § 26 BDSG ähnliche Regelung des hessischen Landesdatenschutzgesetzes eine spezifischere Regelung im Sinne des Artikel 88 Absatz 1 DSGVO darstellt.

Verarbeitung zur Aufdeckung von Straftaten

Nach § 26 Absatz 1 Satz 2 BDSG setzt die Verarbeitung personenbezogener Daten von Beschäftigten u. a. voraus, dass zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat. Es wird kritisiert, dass die Formulierung „zu dokumentierende tatsächliche Anhaltspunkte“ zu Rechtsunsicherheit führe und fraglich sei, ob § 26 Absatz 1 Satz 2 BDSG eine Datenverarbeitung zu präventiver oder repressiver Kontrolle ohne Straftatenbezug (z. B. bei anderweitigen gravierenden Pflichtverletzungen durch Beschäftigte) erlaube.

§ 26 Absatz 1 Satz 2 BDSG entspricht § 32 Absatz 1 Satz 2 BDSG a. F. Zu seiner Auslegung kann deshalb die umfangreiche (höchstrichterliche) Rechtsprechung und Literatur herangezogen werden. Danach ist insbesondere unstreitig, dass der Verdacht einer Straftat vorliegen muss, also z. B. der Verdacht einer Ordnungswidrigkeit nicht genügt und auch präventive Maßnahmen des Arbeitgebers nicht auf § 26 Absatz 1 Satz 2 BDSG gestützt werden können.[9] Eine klarstellende gesetzliche Regelung erscheint deshalb nicht erforderlich.

[9] Siehe nur Simitis/Hornung/Spiecker-*Seifert*, Datenschutzrecht, Kommentar, 1. Auflage 2019, Artikel 88 Rn. 160 f.

Freiwilligkeit der Einwilligung

§ 26 Absatz 2 Satz 2 BDSG bestimmt, wann im Regelfall von der Freiwilligkeit einer Einwilligung ausgegangen werden kann. Seitens der Wirtschaft wird der Wunsch geäußert, stattdessen umgekehrt zu normieren, in welchen Fällen eine Beeinträchtigung der Freiwilligkeit anzunehmen ist.

In welchen Fällen die Einwilligung nicht als freiwillig erteilt gilt, ergibt sich bereits aus den Erwägungsgründen der DSGVO (Erwägungsgrund 43). Des Weiteren kann in einem Umkehrschluss aus dem bestehenden § 26 Absatz 2 Satz 2 BDSG im Wege der Auslegung ermittelt werden, wann Zweifel an der Freiwilligkeit einer Einigung bestehen könnten. Einer Änderung der Regelung bedarf es deshalb aus Sicht des BMI nicht.

Elektronische Einwilligung

§ 26 Absatz 2 Satz 3 BDSG regelt: „*Die Einwilligung hat schriftlich oder elektronisch zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.*"

Teilweise wird bemängelt, es sei unklar, ob die Formulierung „schriftlich oder elektronisch" im Sinne der § 126 BGB („Schriftform") und § 126a BGB („Elektronische Form") zu verstehen sei oder auch in Textform (§ 126b BGB) eingewilligt werden könne.

Im Rahmen des 2. DSAnpUG-EU wurden in § 26 Absatz 2 Satz 3 BDSG die Wörter „bedarf der Schriftform" durch die Wörter „hat schriftlich oder elektronisch zu erfolgen" ersetzt. In der Gesetzesbegründung heißt es: *„Die Änderung ... erleichtert die Voraussetzungen, unter denen im Beschäftigungsverhältnis eine Einwilligung eingeholt werden kann. ... Da die Einwilligung elektronisch erfolgen kann, genügt es beispielsweise, dass der Arbeitgeber sie als E-Mail abspeichert."*[10] Der Gesetzgeber hat bewusst darauf verzichtet, den Wortlaut der Formvorschriften des § 126 BGB („Schriftform") und des § 126a BGB („Elektronische Form") zu wählen. Weder der Gesetzeswortlaut noch die Gesetzesbegründung lassen daher insoweit einen Interpretationsspielraum zu: § 26 Absatz 2 Satz 3 BDSG bestimmt nicht, dass die §§ 126 und 126a BGB anzuwenden sind.

Begriffsbestimmung des Beschäftigten

§ 26 Absatz 8 Satz 2 BDSG sieht vor, wer als Beschäftigter im Sinne des BDSG gilt. Die Norm bewirkt, dass das BDSG in allen Phasen eines Beschäftigungsverhältnisses Anwendung findet, also auch vor seiner Begründung und nach Beendigung. Es wird mitunter in Frage gestellt, ob es dieser Geltungsregelung bedarf.

Aus Gründen der Rechtsklarheit sieht das BMI § 26 Absatz 8 Satz 2 BDSG weiterhin als erforderlich an. Die Regelung ist zudem wortgleich mit § 6 Absatz 1 Satz 2 des Allgemeinen

[10] BT-Drs. 19/11181, S. 19.

Gleichbehandlungsgesetzes (AGG). Zu diesem besteht bereits eine reiche Kasuistik, die zur Auslegung des § 26 BDSG herangezogen werden kann.[11]

Rechtsgrundlage für Verarbeitung zu Zwecken der Datenschutzkontrolle, Innenrevision, Datensicherung und Sicherung des ordnungsgemäßen Betriebes von Datenverarbeitungssystemen

Teilweise wird vorgeschlagen, eine Rechtsgrundlage zur Verarbeitung personenbezogener Daten zu Zwecken der Datenschutzkontrolle, den Tätigkeiten der Innenrevision sowie zur Datensicherung und Sicherung des ordnungsgemäßen Betriebs von Datenverarbeitungssystemen zu schaffen.

Eine Regelungslücke besteht hier indes nicht, da § 26 BDSG die Erlaubnistatbestände der DSGVO nur verdrängt, soweit spezifischere Regelungen im Beschäftigungskontext einschlägig sind.[12] Arbeitgeber können nach überwiegender Auffassung neben § 26 BDSG auf die allgemeinen Erlaubnistatbestände des Artikels 6 Absatz 1 DSGVO zurückgreifen.[13] Relevant im hier angesprochenen Kontext ist vor allem die Datenverarbeitung zur Wahrung berechtigter Interessen (Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DSGVO).

Datenübermittlung im Konzern

Für Datenübermittlungen zwischen konzernangehörigen Unternehmen gelten dieselben Datenschutzbestimmungen wie für Übermittlungen zwischen voneinander unabhängigen Unternehmen.[14] Es wird seitens der Wirtschaft angeregt, erleichternde Regelungen zur Übermittlung personenbezogener Daten innerhalb von Konzernen zu schaffen.

Einen zwingenden Bedarf für eine solche Regelung sieht das BMI nicht. Zwar sehen weder die DSGVO noch § 26 BDSG für die Verarbeitung von Beschäftigtendaten im Konzern ein ausdrückliches „Konzernprivileg“ vor. Der Transfer von Beschäftigtendaten innerhalb eines Konzerns dürfte aber in den meisten Fällen aufgrund von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DSGVO zulässig sein.[15] Erwägungsgrund 48 zur DSGVO sieht hierzu vor: *„Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse ha-*

[11] Kühling/Buchner-*Maschmann*, DS-GVO/BDSG, Kommentar, 3. Auflage 2020, § 26 BDSG Rn. 14.
[12] Wolff/Brink-*Riesenhuber*, Beck'scher Online-Kommentar Datenschutzrecht, § 26 BDSG Rn. 20; Kiel/Lunk/Oetker-*Wybitul*, in: Münchener Handbuch zum Arbeitsrecht, Band 1: Individualarbeitsrecht I, 5. Aufl. Auflage 2021, § 96 Beschäftigtendatenschutz Rn. 127.
[13] Taeger/Gabel-*Zöll*, DSGVO/BDSG-, Kommentar, § 26 BDSG Rn. 11; Kühling/Buchner-*Maschmann*, DS-GVO/BDSG-, Kommentar, § 26 BDSG Rn. 5; Auernhammer-*Forst*, DSGVO - BDSG, Kommentar, 7. Auflage 2020, § 26 Rn. 17; Paal/Pauly-*Gräber/Nolden,* DS-GVO/BDSG, Kommentar, § 26 BDSG Rn. 16 f.; ErfK/Franzen, BDSG, § 26 Rn. 4.
[14] Siehe hierzu Kühling/Buchner-*Maschmann*, DS-GVO/BDSG, Kommentar, 3. Auflage 2020, Artikel 88 DSGVO Rn. 52.
[15] Siehe nur Simitis/Hornung/Spiecker-*Seifert*, Datenschutzrecht, Kommentar, 1. Auflage 2019, Artikel 88 DSGVO Rn. 177.

ben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln.“

5.4.2.2. Rückmeldungen und Bewertung zu § 27 BDSG

Rechtsgrundlagen der Verarbeitung

Nach § 27 Absatz 1 Satz 1 BDSG ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 DSGVO auch ohne Einwilligung zulässig, wenn die Verarbeitung zu Forschungs- oder Statistikzwecken erforderlich ist und die Interessen des Verantwortlichen die Interessen der betroffenen Person erheblich überwiegen. Es wird zum einen eine Klarstellung angeregt, dass § 27 Absatz 1 BDSG eine eigenständige Rechtsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 9 DSGVO) ist. Zum anderen wird vorgeschlagen, die Norm auf genetische, biometrische und Gesundheitsdaten i.S.v. Artikel 9 Absatz 4 DSGVO zu beschränken, da die Öffnungsklausel in Artikel 9 Absatz 4 DSGVO ausschließlich die Verarbeitung dieser Daten erfasse. Gleiches wird für § 27 Absatz 3 BDSG vorgeschlagen.

Keinem der beiden Ansätze vermag das BMI zu folgen. Aus der Gesetzesbegründung[16] ergibt sich, dass § 27 Absatz 1 Satz 1 BDSG als Ausnahmetatbestand zu verstehen ist.[17] Eine Beschränkung auf genetische, biometrische und Gesundheitsdaten im Sinne des Artikels 9 Absatz 4 DSGVO ist nicht angezeigt, da § 27 Absatz 1 und3 BDSG auf die Öffnungsklausel des Artikels 9 Absatz 2 Buchstabe j DSGVO gestützt sind[18] und es daher auf Artikel 9 Absatz 4 DSGVO nicht ankommt.

Beschränkung der Betroffenenrechte

Zu § 27 Absatz 2 BDSG wird bemängelt, dass Rechtsunsicherheit bestehe, wann Betroffenenrechte die Verwirklichung von Forschungszwecken „unmöglich machen oder ernsthaft beeinträchtigen“. § 27 Absatz 2 BDSG greift insoweit den Wortlaut der Öffnungsklausel des Artikels 89 Absatz 2 DSGVO auf, demgemäß Beschränkungen der Betroffenenrechte nur normiert werden können, wenn die Rechte die Verwirklichung der Verarbeitungszwecke „unmöglich machen oder ernsthaft beeinträchtigen“. Für die Auslegung ist die Entscheidungspraxis der Aufsichtsbehörden und des EuGH maßgeblich.

[16] BT-Drs. 18/11325, S. 99.
[17] In der Gesetzesbegründung wird auf das Vorliegen einer Rechtsgrundlage nach Artikel 6 Absatz 1 Unterabsatz 1 Satz 1 DSGVO abgestellt und beispielhaft auf den Fall eines berechtigten Interesses des Verantwortlichen gemäß Buchstabe f verwiesen (BT-Drs. 18/11325, S. 99).
[18] BT-Drs. 18/11325, S. 99; Gola/Heckmann-*Krohm*, Bundesdatenschutzgesetz, Kommentar, 13. Auflage 2019, § 27 Rn. 4.

Kritisiert wird des Weiteren, dass in § 27 Absatz 2 BDSG das Recht auf Datenübertragbarkeit (Artikel 20 DSGVO) nicht beschränkt wird. Hierzu ist anzumerken, dass eine Beschränkung des Artikels 20 DSGVO von der Öffnungsklausel des Artikels 89 Absatz 2 DSGVO nicht gedeckt wäre.[19]

Vorgeschlagen wird auch eine Beschränkung des Auskunftsrechts der betroffenen Person nach Artikel 15 DSGVO hinsichtlich von Daten zu Forschungszwecken analog § 630g Absatz 1 BGB. Nach § 630g BGB ist einem Patienten auf Verlangen Einsicht in seine Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen.

Artikel 27 Absatz 2 BDSG enthält bereits eine Einschränkung des Auskunftsrechts aus Artikel 15 DSGVO wenn die Auskunft voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Eine Ausweitung dieser bereits sehr weitgehenden Einschränkung von Betroffenenrechten in Bezug auf Daten zu Forschungszwecken hält das BMI nicht für interessengerecht.

Schließlich wird § 27 Absatz 2 BDSG dahingehend kritisiert, dass die Anforderungen, die Artikel 23 Absatz 2 DSGVO an beschränkende Gesetzgebungsmaßnahmen stellt, nicht erfüllt seien. § 27 Absatz 2 BDSG stützt sich indes nicht auf die Öffnungsklausel des Artikels 23 DSGVO, sondern auf Artikel 89 Absatz 2 DSGVO.[20]

Veröffentlichung personenbezogener Daten

Angeregt wird eine Regelung, nach der Daten auch veröffentlicht werden dürfen, wenn sie bereits allgemein zugänglich sind.

Eine solche Regelung scheint entbehrlich. Der Gesetzgeber geht davon aus, dass dem Veröffentlichungsinteresse grundsätzlich ausreichend dadurch Rechnung getragen werden kann, dass Forschungsdaten in anonymisierter Form (d.h. in einer nicht unter die DSGVO fallenden Form) veröffentlicht werden und daher eine Veröffentlichung personenbezogener Daten nur unter engen Voraussetzungen erforderlich sein kann.[21]

[19] Siehe nur Kühling/Buchner-*Buchner/Tinnefeld,* DS-GVO/BDSG, Kommentar 3. Auflage 2020, § 27 BDSG, Rn. 18.

[20] BT-Drs. 18/11325, S. 99; Kühling/Buchner-*Buchner/Tinnefeld,* DS-GVO/BDSG, Kommentar 3. Auflage 2020, § 27 BDSG Rn. 19.

[21] Siehe hierzu Kühling/Buchner-*Buchner/Tinnefeld*, 3. Auflage 2020, BDSG, § 27 Rn. 25; Buchner/Kipker, Datenschutz und Forschungsfreiheit, in: Lenk/Duttge/Fangerau, Handbuch Ethik und Recht der Forschung am Menschen, 2014, S. 507 (512).

Zweckbindungsklausel

Gewünscht wird, § 27 BDSG analog § 7 Absatz 1 Satz 3 Bundesfernstraßenmautgesetz (BFStrMG) dahingehend zu ändern, dass eine vertrauliche Behandlung von Forschungsdaten dadurch gesichert wird, dass Forschungsdaten nur zu Forschungszwecken verarbeitet (nicht aber z. B. beschlagnahmt) werden dürfen.

In § 7 Absatz 2 Satz 3 BFStrMG heißt es: „*Eine Übermittlung, Verwendung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig.*“ Dieses absolute Zweckänderungsverbot ist sehr umstritten. Das BMI lehnt entsprechende Weiterverarbeitungsverbote aus grundsätzlichen Erwägungen ab. Sie sind rechtlich nicht geboten, weil eine zweckändernde Weiterverarbeitung schon nach allgemeinen Vorschriften an strenge Voraussetzungen geknüpft ist, die die Möglichkeiten einer Zweckänderung abschließend regeln und damit hinreichend begrenzen (vgl. § 25 i. V. m. § 23 BDSG). Ein rechtliches Bedürfnis für eine weitergehende Regelung in Bezug auf Forschungsdaten wird insoweit nicht gesehen. Eine kategorische Sperre der Weiterverarbeitung verhindert zudem eine angemessene Reaktion auf unvorhergesehene Bedarfslagen. Das Weiterverarbeitungsverbot müsste ad hoc und unter großem zeitlichen Druck beseitigt werden, wenn nachträglich ein übergeordnetes öffentliches Interesse an der Datennutzung für andere Zwecke erkannt wird.

5.4.2.3. Rückmeldungen und Bewertung zu § 28 BDSG

In § 28 Absatz 1 Satz 1 BDSG heißt es (ähnlich wie in § 27 Absatz 1 Satz 1 BDSG), dass abweichend von Artikel 9 Absatz 1 DSGVO die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 DSGVO zulässig ist, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Wie für § 27 Absatz 1 und 3 BDSG (s.o.) wird auch für § 28 Absatz 1 BDSG vorgeschlagen, die Norm auf genetische, biometrische und Gesundheitsdaten i.S.v. Artikel 9 Absatz 4 DSGVO zu beschränken, da die Öffnungsklausel in Artikel 9 Absatz 4 DSGVO ausschließlich die Verarbeitung dieser Daten erfasse.

Eine solche Beschränkung ist nach Ansicht des BMI nicht angezeigt, da § 28 Absatz 1 BDSG auf die Öffnungsklausel des Artikels 9 Absatz 2 Buchstabe j DSGVO gestützt ist[22] und es daher auf Artikel 9 Absatz 4 DSGVO nicht ankommt.

5.4.2.4. Rückmeldungen und Bewertung zu § 29 BDSG

Beschränkung der Betroffenenrechte

§ 29 Absatz 1 BDSG beschränkt die Betroffenenrechte der Artikel 14 DSGVO („Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben

[22] BT-Drs. 18/11325, S. 100; Gola/Heckmann-*Krohm*, Bundesdatenschutzgesetz, Kommentar, 13. Auflage 2019, § 28 Rn. 5.

wurden“), Artikel 15 DSGVO („Auskunftsrecht der betroffenen Person“) und Artikel 34 DSGVO („Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person“), soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen einer anderen Person, geheim gehalten werden müssen. Hierzu wird vorgebracht, dass diese Beschränkungen weder durch Artikel 23 Absatz 1 noch Artikel 34 DSGVO gedeckt seien.

Art. 23 Absatz 1 Buchstabe i DSGVO eröffnet jedoch ausdrücklich die Möglichkeit, die Betroffenenrechte zum Schutz der Rechte und Freiheiten anderer Personen (als der betroffenen Person) einzuschränken. § 29 Absatz 1 BDSG ist daher von dieser Öffnungsklausel gedeckt.[23] Auch Artikel 34 DSGVO ist in Artikel 23 Absatz 1 DSGVO als eine der Normen genannt, die durch den nationalen Gesetzgeber beschränkt werden können.

Untersuchungsbefugnisse der Aufsichtsbehörden

Zu § 29 Absatz 3 BDSG wird vorgeschlagen, erstens die Norm zu streichen, zweitens die Untersuchungsbefugnisse der Aufsichtsbehörden noch weiter einzuschränken und drittens Rechtsunsicherheit zu beseitigen, die bezüglich des Anwendungsbereichs und Beschränkungsumfangs der Norm bestehe.

§ 29 Absatz 3 BDSG sollte aus Sicht des BMI nicht gestrichen werden. Die Norm sorgt für einen sachgerechten Ausgleich zwischen den Geheimhaltungspflichten einerseits und den Aufgaben und Befugnissen der Aufsichtsbehörden andererseits. Sie ist von Artikel 90 Absatz 1 DSGVO gedeckt.[24] Die Gesetzesbegründung[25] führt zu dieser Regelung zutreffend aus: *„... ihr entspricht Erwägungsgrund 164 der Verordnung. Nach Artikel 58 Absatz 1 Buchstaben e und f der Verordnung (EU) 2016/679 haben die Aufsichtsbehörden die Befugnis, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu erhalten zu allen für die Erfüllung ihrer Aufgaben notwendigen personenbezogenen Daten und Informationen sowie zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte. Artikel 90 Absatz 1 Verordnung (EU) 2016/679 eröffnet den Mitgliedstaaten die Möglichkeit, die Befugnisse der Aufsichtsbehörden im Sinne des Artikels 58 Absatz 1 Buchstaben e und f gegenüber Geheimnisträgern zu regeln.“*

Konträr zu dem Vorschlag, § 29 Absatz 3 BDSG zu streichen, wird vom BMI erbeten, sich auf unionsrechtlicher Ebene dafür einzusetzen, dass die Öffnungsklausel des Artikels 90 Absatz 1 DSGVO auf alle Untersuchungsbefugnisse des Artikels 58 Absatz 1 DSGVO erweitert und das BDSG entsprechend geändert wird. Hierbei wird jedoch nicht hinreichend

[23] Siehe BT-Drs. 18/11325, S. 100; Paal/Pauly-*Paal*, DS-GVO/BDSG, Kommentar, 3. Auflage 2021, Artikel 23 DSGVO Rn. 40 ff.; Paal/Pauly-*Gräber/Nolden*, DS-GVO/BDSG, Kommentar, 3. Auflage 2021, § 29 BDSG Rn. 1.
[24] Paal/Pauly/Gräber-*Nolden*, DS-GVO/BDSG, Kommentar, 3. Auflage 2021, § 29 BDSG Rn. 1.
[25] BT-Drs. 18/11325, S. 101.

berücksichtigt, dass die Aufgaben und Befugnisse der Aufsichtsbehörden durch den Anwendungsbereich der DSGVO und den Grundsatz der Erforderlichkeit beschränkt sind.[26] Die Untersuchungsbefugnisse des Artikels 58 Absatz 1 DSGVO sind schon nach ihrem Sinn und Zweck dahingehend auszulegen, dass sie zur Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sein müssen. In Artikel 58 Absatz 1 Buchstabe a und e DSGVO kommt dies zudem auch klar im Normtext zum Ausdruck. Des Weiteren wird den Interessen der Verantwortlichen auch durch die Vorgaben der Artikel 58 Absatz 4 sowie Artikel 83 Absatz 1 und Absatz 8 i. V. m. Artikel 78 Absatz 1 DSGVO Rechnung getragen: Danach darf eine Aufsichtsbehörde in jedem Einzelfall nur verhältnismäßige Bußgelder verhängen. All ihre Befugnisse unterliegen angemessenen Verfahrensgarantien, einschließlich wirksamer gerichtlicher Rechtsbehelfe.[27]

Soweit die Frage aufgeworfen wurde, ob § 29 Absatz 3 BDSG nur privatrechtlich organisierte Berufsgeheimnisträger außerhalb des Anwendungsbereichs landesrechtlicher Regelungen betrifft oder sich auch auf Personen erstreckt, die öffentliche Stellen im Sinne des § 2 BDSG sind, kann § 1 Absatz 1 Satz 1 Nummer 2 BDSG herangezogen werden: § 29 Absatz 3 BDSG – wie das gesamte BDSG – findet auch auf öffentliche Stellen des Bundes und auf öffentliche Stellen der Länder, „soweit der Datenschutz nicht durch Landesgesetz geregelt insoweit sie Bundesrecht ausführen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt". Dies kommt insbesondere bei Notaren zum Tragen, die nach Landesrecht teilweise öffentliche Stellen sind.

5.4.3. Schlussfolgerungen

Zu § 26 BDSG kann insgesamt festgehalten werden, dass sich aus den Rückmeldungen kein zwingender Bedarf für ein umfassendes eigenständiges Beschäftigtendatenschutzgesetz ergibt.

Unabweislicher Handlungsbedarf besteht im Hinblick auf §§ 27 und 29 BDSG: In § 27 Absatz 2 Satz 1 BDSG ist das Wort „beinträchtigen" durch das Wort „beeinträchtigen" zu ersetzen. § 29 Absatz 3 Satz 1 BDSG ist aufgrund von Änderungen des Strafgesetzbuchs (StGB) dahingehend anzupassen, dass auf § 203 Absatz 2 StGB verwiesen wird (und nicht auf den weggefallenen § 203 Absatz 2a StGB).

[26] Siehe hierzu Auernhammer-*Eßer*, DSGVO/BDSG, Kommentar, 7. Auflage 2020, § 29 BDSG Rn. 25; Gola-*Nguyen,* Datenschutz-Grundverordnung, Kommentar, 2. Auflage 2018, Artikel 58 DSGVO Rn. 14; Ehmann/Selmayr-*Selmayr*, Datenschutz-Grundverordnung, Kommentar, 2. Auflage 2018, Artikel 58 Rn. 6.
[27] Siehe zu den Möglichkeiten der Verantwortlichen auch Gola/Heckmann-*Lapp*, Bundesdatenschutzgesetz, Kommentar, 13. Auflage 2019, § 29 Rn. 33; Kühling/Buchner-*Herbst*, DS-GVO/BDSG, Kommentar, 3. Auflage 2020, § 29 BDSG Rn. 30.

5.5. Datenschutzbeauftragte öffentlicher und nichtöffentlicher Stellen – §§ 5 bis 7, § 38 BDSG

5.5.1. Zielsetzung und Gegenstand der Regelungen

Die Regelungen in den §§ 5 bis 7 und § 38 BDSG betreffen die Datenschutzbeauftragten öffentlicher und nichtöffentlicher Stellen. Mit den Bestimmungen werden die nach der DSGVO bestehenden nationalen Gestaltungs- bzw. Umsetzungsspielräume genutzt. Die §§ 5 bis 7 BDSG dienen außerdem der Umsetzung der Artikel 32 bis 34 der Richtlinie (EU) 2016/680.

5.5.1.1. §§ 5 bis 7 BDSG (Datenschutzbeauftragte öffentlicher Stellen)

Mit den §§ 5 bis 7 BDSG hat der Gesetzgeber einen einheitlichen gesetzlichen Rahmen für die Datenschutzbeauftragten öffentlicher Stellen des Bundes geschaffen, unabhängig davon, ob die jeweiligen Datenverarbeitungen in den Anwendungsbereich der DSGVO oder der Richtlinie (EU) 2016/680 fallen. Soweit die Regelungen der Umsetzung der Richtlinie (EU) 2016/680 dienen, ist der Gesetzgeber zum Teil auch über die Vorgaben der Richtlinie hinausgegangen.[28]

§ 5 BDSG wurde zur Umsetzung des Artikels 32 der Richtlinie (EU) 2016/680 geschaffen; er übernimmt gleichzeitig den Wortlaut von Artikel 37 Absatz 1 Buchstabe a, Absatz 3, 5 und 7 DSGVO. Mit § 5 Absatz 4 BDSG wurde – entsprechend Artikel 37 Absatz 6 DSGVO und über die Vorgaben der Richtlinie 2016/680 hinausgehend – klargestellt, dass Datenschutzbeauftragte sowohl aus internem als auch aus externem Personal bestellt werden dürfen.

Mit § 6 BDSG hat der Gesetzgeber konkrete Vorgaben zur Stellung eines Datenschutzbeauftragten normiert. Bezüglich des besonderen Abberufungs- und Kündigungsschutzes in Absatz 4 hat sich der Gesetzgeber insbesondere entschieden, § 4f Absatz 3 Satz 4 bis 6 BDSG a. F. beizubehalten. Hierbei handelt es sich um eine Regelung des materiellen Arbeitsrechts.[29] Ziel der Regelung ist ein umfassender Schutz der Unabhängigkeit von Datenschutzbeauftragten, den auch die DSGVO in Artikel 38 Absatz 3 Satz 2 verfolgt.[30]

---

[28] BT-Drs. 18/11325 vom 24. Februar 2017, S. 82.

[29] BT-Drs. 18/11325 vom 24. Februar 2017, S. 82; Simitis/Hornung/Spiecker gen. Döhmann-*Drewes*, Datenschutzrecht, Kommentar, 1. Auflage 2019, Artikel 38 DSGVO Rn. 36; Paal/Pauly-*Paal*, DS-GVO/BDSG, Kommentar, 3. Auflage 2021, Artikel 38 DSGVO Rn. 10; Kühling/Buchner-*Bergt*, DS-GVO/BDSG, Kommentar, 3. Auflage 2020, Artikel 38 DSGVO, Rn. 33.

[30] Die Regelung des § 38 Absatz 1 und 2 i. V. m. § 6 Absatz 4 BDSG ist derzeit Gegenstand zweier Vorabentscheidungsverfahren vor dem EuGH (EuGH-Rechtssachen C-534/20 –„Leistritz“, vgl. BAG, Beschluss vom 30. Juli 2020, 2 AZR 225/20, und C-453/21 –„X-FAB“, vgl. BAG, Beschluss vom 27. April 2021 – 9 AZR 383/19). Diese betreffen die Frage, ob Artikel 38 Absatz 3 Satz 1 DSGVO der Regelung, soweit sie die Abberufung einer oder eines Datenschutzbeauftragten an die weiteren Voraussetzungen des § 626 BGB knüpft, unabhängig davon, ob sie wegen der Erfüllung der Aufgaben einer oder eines Datenschutzbeauftragten erfolgt, entgegensteht.

§ 7 BDSG dient der Umsetzung des Artikels 34 der Richtlinie (EU) 2016/680 und entspricht im Wesentlichen Artikel 38 Absatz 6, Artikel 39 DSGVO.

5.5.1.2. § 38 BDSG (Datenschutzbeauftragte nichtöffentlicher Stellen)

§ 38 BDSG regelt die Benennungs- und Verschwiegenheitspflichten sowie ein Zeugnisverweigerungsrecht für Datenschutzbeauftragte in nichtöffentlichen Stellen. Der Gesetzgeber hat mit diesen die DSGVO ergänzenden Regelungen den Gestaltungsspielraum genutzt, den die DSGVO den Mitgliedstaaten in Artikel 37 Absatz 4 Satz 1 Halbsatz 2 DSGVO und Artikel 38 Absatz 5 DSGVO gewährt.

§ 38 Satz 1 BDSG ist inhaltlich an § 4f Absatz 1 Satz 4 BDSG a. F. angelehnt und regelt, dass nichtöffentliche Stellen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu bestellen haben, wenn sie eine bestimmte Zahl von Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen. Die Personenzahl wurde durch das DSAnpUG-EU ursprünglich auf zehn festgelegt. Durch das 2. DSAnpUG-EU wurde sie zur Entlastung kleiner und mittlerer Unternehmen[31] auf 20 Personen angehoben.

Satz 2 entspricht inhaltlich im Wesentlichen § 4f Absatz 1 Satz 6 BDSG a. F.; neu hinzugefügt hat der Gesetzgeber eine Benennungspflicht, soweit die Verarbeitungstätigkeiten des Verantwortlichen der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO unterliegen und somit ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen.

Mit Absatz 2 wird die Stellung der Datenschutzbeauftragten nichtöffentlicher Stellen in Hinblick auf Abberufungs- und Kündigungsschutz, Verschwiegenheitspflicht und Zeugnisverweigerungsrecht derjenigen der Datenschutzbeauftragten öffentlicher Stellen angeglichen. Absatz 2 verweist daher, sofern aufgrund der DSGVO oder Absatz 1 eine Pflicht zur Benennung besteht, auf den besonderen Kündigungsschutz des § 6 Absatz 4 BDSG, auf die Verschwiegenheitspflichten nach § 6 Absatz 5 Satz 2 BDSG und das Zeugnisverweigerungsrecht nach § 6 Absatz 6 BDSG.

5.5.2. Methodischer Hinweis

Aufgrund der Verweise in § 38 Absatz 2 auf § 6 Absatz 4, 5 und 6 BDSG erfolgte die Befragung bezüglich der Regelungen zu Datenschutzbeauftragten in den §§ 5 bis 7 und 38 BDSG in einem einheitlichen Fragenblock. Dementsprechend fasst auch die Auswertung zu § 6 BDSG Rückmeldungen bezüglich Datenschutzbeauftragter öffentlicher und nichtöffentlicher Stellen zusammen.

[31] BT-Drs. 19/11181, S. 19.

5.5.3. Empirische Ergebnisse und Bewertung

Im Rahmen der durchgeführten Befragung werden die §§ 5 bis 7 und § 38 BDSG überwiegend als sachgerecht, praktikabel und normenklar bewertet. Insbesondere das Ziel einer einheitlichen Regelung von Datenschutzbeauftragten aller öffentlichen und nichtöffentlichen Stellen kann dabei als erreicht betrachtet werden.

Kritikpunkte und Anmerkungen der Befragten beziehen sich schwerpunktmäßig auf Einzelheiten der (arbeits-)rechtlichen Stellung der oder des Datenschutzbeauftragten nach § 6 Absatz 4 BDSG (5.5.3.1) und auf die Voraussetzungen einer Benennungspflicht in §§ 5 und 38 BDSG (5.5.3.2).

5.5.3.1. Rückmeldungen zu § 6 Absatz 4 BDSG und Bewertung

Streichung § 6 Absatz 4 Satz 1 BDSG

Gewünscht wird vereinzelt eine erleichterte Möglichkeit zur Abberufung von *internen* Datenschutzbeauftragten; § 6 Absatz 4 Satz 1 BDSG solle gestrichen werden, der Kündigungsschutz nach § 6 Absatz 4 Satz 2 BDSG reiche aus. Es sei wichtig, dass interne Datenschutzbeauftragte, die sich als ungeeignet erwiesen, aus ihrer Position entfernt werden könnten, da dies eine Gefährdung des Datenschutzes bzw. des Betriebes insgesamt darstellte.

Im Hinblick auf diesen Vorschlag ist darauf hinzuweisen, dass § 6 Absatz 4 Satz 1 und 2 BDSG bewusst nicht nur das Arbeitsverhältnis der oder des Datenschutzbeauftragten schützen, sondern auch die Aufgabenwahrnehmung als Datenschutzbeauftragte oder Datenschutzbeauftragter im Rahmen dieses Arbeitsverhältnisses. Denn auch schon die Gefahr der jederzeitigen Abberufung kann die Unabhängigkeit einer oder eines Datenschutzbeauftragten und die effektive Erfüllung ihrer oder seiner Aufgabenerfüllung beeinträchtigen. Die DSGVO verlangt dementsprechend in Artikel 38 Absatz 3 Satz 2 DSGVO den Schutz von Datenschutzbeauftragten vor Abberufung oder Benachteiligung aufgrund der Erfüllung ihrer Aufgaben.

Gleichwohl besteht das praktische Bedürfnis, Datenschutzbeauftragte in bestimmten Fällen auch aus ihrer Position entfernen zu können. Dieses Bedürfnis ist mit dem Ziel der Unabhängigkeit von Datenschutzbeauftragten abzuwägen und in einen schonenden Ausgleich zu bringen. Der Gesetzgeber hat mit § 6 Absatz 4 Satz 1 BDSG einen solchen Ausgleich beabsichtigt, indem er eine Abberufung nicht gänzlich untersagt, aber auf Fälle schwerer Verfehlungen oder nachhaltiger Zerrüttung des Vertrauensverhältnisses begrenzt hat.

Das BMI ist daher der Auffassung, dass § 6 Absatz 4 Satz 1 BDSG nicht nur die Anforderungen des Artikels 38 Absatz 3 Satz 2 DSGVO aufgreift, sondern auch ein notwendiger und sachgerechter Ausgleich zur Gewährleistung der Unabhängigkeit von Datenschutzbeauftragten ist.

Der Verantwortliche hat die Möglichkeit, die oder den Datenschutzbeauftragten sorgfältig auszuwählen. Gerade bei seinem internen Personal wird er sich regelmäßig einen Überblick darüber verschaffen können, wer neben den nötigen Qualifikationen auch Gewähr dafür bietet, die Position verantwortungsvoll auszufüllen. Demgegenüber erscheint es in Hinblick auf die hohe Bedeutung der Unabhängigkeit von Datenschutzbeauftragten angemessen, nicht nur eine Kündigung, sondern auch eine Abberufung entsprechend nur in schwerwiegenden Fällen zuzulassen.

Abschließen befristeter Dienstverträge mit externen Datenschutzbeauftragten

Vereinzelt wird eine Klarstellung erbeten, dass mit *externen* Datenschutzbeauftragten auch das Abschließen befristeter Dienstverträge zulässig ist, da dies der Praxis entspreche.

Es ist nachvollziehbar, dass in der Praxis bei der Bestellung externen Personals als Datenschutzbeauftragte das Bedürfnis nach der Möglichkeit zum Abschluss auch befristeter Dienstverträge besteht, da für den Verantwortlichen nicht in derselben Weise wie bei eigenem Personal ersichtlich ist, ob sich der oder die Bestellte bewährt und mit hinreichender Zuverlässigkeit ihren Aufgaben nachkommt. Gegen diese Praxis bestehen keine Bedenken. Das BMI sieht jedoch keine Notwendigkeit einer gesetzlichen Klarstellung: Weder das BDSG noch die DSGVO verpflichten zur unbefristeten Beschäftigung einer oder eines Datenschutzbeauftragten. Auch aus der Befragung haben sich keine Fälle ergeben, in denen die Zulässigkeit eines solchen Vorgehens zwischen Rechtsanwendern strittig gewesen wäre und daher einer Klarstellung bedürfte.

Rücktritt der oder des Datenschutzbeauftragten

Eine weitere Klarstellungsbitte bezieht sich auf das Recht der oder des Datenschutzbeauftragten, von seiner oder ihrer Position jederzeit zurücktreten zu können.

Allerdings beschränkt § 6 Absatz 4 BDSG bereits nach seinem Wortlaut ersichtlich nur Abberufungs- und Kündigungsmöglichkeiten eines Dienstherrn bzw. des Auftrag- oder Arbeitgebers und damit einen speziellen Abberufungs- und Kündigungsschutz zugunsten der oder des Datenschutzbeauftragten. Das Recht von Datenschutzbeauftragten, von ihrer Aufgabe zurückzutreten oder zu kündigen, wird durch die §§ 5 bis 7 BDSG nicht berührt. Für eine rein klarstellende Regelung besteht aus Sicht des BMI vor diesem Hintergrund kein Bedarf.

5.5.3.2. Rückmeldungen zu § 38 Absatz 1 BDSG und Bewertung

Der große Schwerpunkt der Rückmeldungen liegt auf den in § 38 Absatz 1 BDSG geregelten Bestellungspflichttatbeständen, insbesondere auf der personenzahlabhängigen Bestellungspflicht-Grenze.

Bestellungspflicht-Grenze

Es wird vereinzelt vorgeschlagen, die Bestellungspflicht-Grenze in § 38 Absatz 1 Satz 1 BDSG – etwa auf 250 Personen – anzuheben. Die Zahl 250 wird dabei zum Teil mit Artikel 30 Absatz 5 DSGVO begründet, der bei Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern grundsätzlich von der Pflicht ausnimmt, ein Verzeichnis von Verarbeitungstätigkeiten zu führen.

Zugleich weisen Aufsichtsbehörden und mehrere Unternehmensverbände auf die aus ihrer Sicht bestehenden Folgen der letzten Anhebung der Bestellungspflicht-Grenze hin: Die letzte Anhebung habe dazu geführt, dass kleine und mittelständische Unternehmen sowie Vereine sich nicht mehr an die Vorgaben des Datenschutzrechts gebunden fühlten. Die Abberufung der Datenschutzbeauftragten infolge des Entfallens der Bestellungspflicht habe bei den Verantwortlichen zu einem spürbaren Kompetenz- und Kontrollverlust geführt; kleinere Unternehmen und Vereine, die nicht mehr der Bestellungspflicht unterfielen, würden sich nun nicht oder kaum mit der Erfüllung datenschutzrechtlicher Vorgaben befassen.

Mehrere Unternehmen und Verbände geben zudem an, die Anhebung der Bestellungspflicht-Grenze von zehn auf 20 Personen habe nicht zu einer Entlastung von kleinen und mittelständischen Unternehmen und Vereinen geführt, da die datenschutzrechtlichen Pflichten weiterhin auch durch diese zu erfüllen seien und dies durch den Wegfall der Datenschutzbeauftragten mangels Fachkunde schwieriger geworden sei.

Einzelne Unternehmen führten demgegenüber eine Entlastung durch Anhebung der Bestellungspflicht-Grenze an, die zum Teil auch damit beschrieben wird, dass die Verfügbarkeit externer Datenschutzbeauftragter sich verbessert und ihre marktübliche Vergütung gesunken sei.

In ihrer Gesamtschau sprechen die dargestellten Rückmeldungen, die sich zur Erhöhung der Bestellungspflicht-Grenze geäußert haben, aus Sicht des BMI allerdings dafür, dass eine weitere Anhebung der Bestellungspflicht-Grenze in § 38 Absatz 1 BDSG nicht zielführend ist:

Zunächst ist festzuhalten, dass die in Artikel 30 Absatz 5 DSGVO genannte Zahl schon wegen des anderen Regelungsziels des Artikels 30 DSGVO nicht auf die Frage der Bestellungspflicht-Grenze übertragen werden kann. Anknüpfungspunkt für die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten ist in erster Linie die Herstellung einer Übersicht über alle Verarbeitungstätigkeiten eines Unternehmens oder einer Einrichtung. Das Bedürfnis nach einer solchen Übersicht besteht gerade dann, wenn das Unternehmen oder die Einrichtung eine bestimmte Größe hat, da damit die Komplexität und Vielfältigkeit von Verarbeitungen wächst und das Erfordernis von Transparenz und Übersichtlichkeit zur effektiven Kontrolle durch Datenschutzbeauftragte und Aufsichtsbehörden zunimmt. Dementsprechend nimmt die DSGVO kleinere Einrichtungen von den Pflichten

des Artikels 30 Absatz 1 und 2 DSGVO aus, wenn es sich nicht um eine Verarbeitung mit hohem Risiko handelt. Damit unterscheiden sich die Erwägungen, die hinter Artikel 30 Absatz 5 DSGVO stehen, von denjenigen, die für die Bestellung von Datenschutzbeauftragten vorzunehmen sind; eine Vergleichbarkeit besteht nicht.

Darüber hinaus weisen die von den Aufsichtsbehörden und mehreren Unternehmensverbänden vorgetragenen Erfahrungen mit der Anhebung der Bestellungspflicht-Grenze durch das 2. DSAnpUG-EU darauf hin, dass eine Pflicht zur Bestellung von Datenschutzbeauftragten nicht nur eine konsequente und nachhaltige Umsetzung des Datenschutzrechts fördert, sondern für viele – gerade kleine und mittelständische – Unternehmen notwendig und hilfreich ist. In vielen Fällen kann nur so sichergestellt werden, dass das Eingreifen und die Reichweite des Datenschutzrechts nicht aufgrund mangelnder Fachexpertise beim Verantwortlichen schon von vorneherein verkannt werden. Datenschutzbeauftragte beraten und unterstützen bei der Umsetzung der datenschutzrechtlichen Pflichten und entlasten damit letztlich auch die Aufsichtsbehörden.

Bemerkenswert ist dabei, dass mehrere Unternehmen und Verbände darauf hinweisen, dass die Anhebung der Bestellungspflicht-Grenze nicht als Entlastung empfunden wurde, da die datenschutzrechtlichen Pflichten weiterhin einzuhalten seien. Dies deutet darauf hin, dass das Ziel der Entlastung von kleinen und mittelständischen Unternehmen und Vereinen durch eine schlichte Anhebung der Bestellungspflicht-Grenze nicht zwingend erreicht wird. Stattdessen erscheint es zielführender, eine Stärkung niedrigschwellig zugänglicher, qualifizierter datenschutzrechtlicher Beratungsmöglichkeiten für kleine und mittelständische Unternehmen und Vereine, insbesondere durch oder in Abstimmung mit den Aufsichtsbehörden anzustreben.

Ausnahme für gemeinnützige Vereine und Unternehmen von der Bestellungspflicht

Außerdem wird angeregt, gemeinnützige Vereine und Unternehmen von einer Bestellungspflicht für Datenschutzbeauftragte auszunehmen, um sie so zu entlasten. Datenverarbeitungen spielten bei solchen Einrichtungen nur eine untergeordnete Rolle.

Eine pauschale Ausnahme für gemeinnützige Vereine und Unternehmen ist indes sachlich nicht begründbar. Es kann nicht von der aufgrund steuerrechtlicher Kriterien zu beurteilenden Gemeinnützigkeit darauf geschlossen werden, dass Datenverarbeitungen in diesen Einrichtungen keine zentrale Rolle spielen. So ist etwa davon auszugehen, dass zunehmend gemeinnützige Datentreuhänder oder datenaltruistische Organisationen entstehen werden, deren Kerntätigkeit die Datenverarbeitung sein wird. Entsprechende Regularien werden auf nationaler und auf EU-Ebene derzeit beraten.[32]

[32] Vgl. etwa Vorschlag für eine Verordnung des Europäischen Parlamentes und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) vom 25. November 2020 (COM (2020) 767 final).

Rein risikobasierter Ansatz für die Bestellungspflicht

Teilweise wird die Entscheidung des Gesetzgebers für eine Personenzahlgrenze in § 38 Absatz 1 Satz 1 BDSG kritisiert. Diese stelle keinen geeigneten Parameter zur Beurteilung des Risikos für die Rechte und Freiheiten natürlicher Personen dar. Stattdessen sollte das Risiko der Verarbeitung zum zentralen Maßstab für die Pflicht zur Bestellung einer oder eines Datenschutzbeauftragten herangezogen werden. Auch die DSGVO habe einen risikobasierten Ansatz gewählt.

Ein ähnlicher Vorschlag lautet dahingehend, eine Bestellungspflicht für Datenschutzbeauftragte nur dann vorzusehen, wenn der Verantwortliche im Kern, d.h. nicht nur gelegentlich, eine umfangreiche regelmäßige und systematische Überwachung von Personen oder die Verarbeitung besonderer Kategorien von Daten gemäß der Artikel 9 und 10 DSGVO durchführe. Auch dies liefe auf eine stärker risikoorientierte Bestellungspflicht und eine Abschaffung der personenzahlbezogenen Benennungspflicht hinaus.

Der Kritik sollte aus Sicht des BMI jedoch nicht gefolgt werden. § 38 Absatz 1 BDSG normiert eine Benennungspflicht aus mehreren Gründen, die diejenigen der DSGVO ergänzen. Die personenzahlbezogene Benennungspflicht ist dabei nur ein Tatbestand, der zur Pflichtbestellung eines Datenschutzbeauftragten führen kann. Er orientiert sich nicht unmittelbar am Verarbeitungsrisiko, ihm liegt aber die gesetzgeberische Wertung zugrunde, dass die Komplexität und die Risiken des Datenschutzes erhöht sind, wenn mindestens 20 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind.

Ein stark risikobasierter Ansatz findet sich bereits jetzt in § 38 Absatz 1 Satz 2 Variante 1 BDSG: Danach haben der Verantwortliche oder der Auftragsverarbeiter Datenschutzbeauftragte zu bestellen, wenn sie Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO unterliegen. Artikel 35 DSGVO knüpft an ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen an, sodass die Risikoeinschätzung unmittelbar auch in die Bestellungspflicht nach § 38 Absatz 1 Satz 2 BDSG einfließt.

Im BDSG einen *rein* risikobasierten Ansatz zu verankern, der es den Verantwortlichen und Auftragsverarbeitern selbst überlässt, das Risiko zu beurteilen und einen Datenschutzbeauftragten zu bestellen, erweist sich aus Sicht des BMI dagegen nicht als gleich effektiv. Denn zum einen zeigen die Ergebnisse der Befragung, dass nicht alle Verantwortlichen und Auftragsverarbeiter, die Beratungsbedarf durch eine oder einen Datenschutzbeauftragten hätten, diesen auch bestellen; zum anderen erschwert ein rein risikobasierter Ansatz die Kontrollierbarkeit für die Aufsichtsbehörden, insbesondere in Fällen, in denen die Risikohöhe streitig ist.

Auch die ebenfalls vorgeschlagene Beschränkung der Bestellungspflicht für Datenschutzbeauftragte auf Fälle, in denen der Verantwortliche im Kern eine umfangreiche regelmäßige und systematische Überwachung von Personen oder die Verarbeitung besonderer

Kategorien von Daten gemäß der Artikel 9 und 10 DSGVO durchführt, erscheint nicht zielführend:

Zum einen dürften solche Verarbeitungen bereits regelmäßig Artikel 37 Absatz 1 Buchstabe c DSGVO unterfallen. Zum anderen kann eine Verarbeitung aber auch ohne Daten nach Artikel 9 und 10 DSGVO hoch risikobehaftet sein. Das gilt etwa für Verarbeitungstätigkeiten von erheblichem Umfang (Big Data).

Aus Sicht des BMI hat sich daher die Personenzahlgrenze als Parameter insgesamt weiterhin bewährt und sollte beibehalten werden.

Bestellungspflicht bei Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung

Ebenfalls kritisiert wird aber auch die Bestellungspflicht bei der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung. Die wenigsten Unternehmen und Vereine seien ohne qualifizierten Datenschutzbeauftragten in der Lage, das Bedürfnis einer Datenschutz-Folgenabschätzung zu erkennen und die erforderlichen Schritte einzuleiten. Die Benennungsvoraussetzung eines Datenschutzbeauftragten aufgrund der Durchführungsanforderung einer Datenschutz-Folgenabschätzung könne entfallen, weil sie inhaltlich in der Praxis ins Leere liefe.

Die Vorschrift knüpft indes an den risikobasierten Ansatz der DSGVO an und erfasst Fälle, in denen wenige Beschäftigte Verarbeitungstätigkeiten ausführen, die hoch riskant sind (Beispiel: Startup mit wenigen Mitarbeitern, dass eine KI-Anwendung entwickelt und vermarktet). Gerade in solchen Fällen ist eine datenschutzrechtliche Begleitung sinnvoll und angebracht. Die Vorschrift ist daher aus Sicht des BMI notwendig.

Generell ist darauf hinzuweisen, dass Verantwortliche, die selbst nicht in der Lage sind, die datenschutz- und sonstigen rechtlichen Auswirkungen ihrer Tätigkeiten mit eigener Expertise zu überblicken, insoweit (Rechts-)Beratung hinzuziehen können und sollten. Eine solche Beratung kann auch im Vorfeld abklären, ob eine Pflicht zur Bestellung einer oder eines Datenschutzbeauftragten nach § 38 Absatz 1 Satz 2 BDSG besteht.

Kopfzahlbasierte Berechnung der Personenzahl

Vereinzelt vorgetragen wird der Wunsch nach einer anderen Berechnung der Personenzahl nach § 38 Absatz 1 Satz 1 BDSG, die nicht von der Kopfzahl der Beschäftigten ausgeht, sondern Teilzeitkräfte auch nur anteilig berücksichtigt (wohl vergleichbar dem § 23 Absatz 1 Satz 5 Kündigungsschutzgesetz - KSchG).

Eine solche Berechnung würde zwar einerseits den "realen" Verarbeitungsumfang ggf. besser abbilden. Umgekehrt ist aber davon auszugehen, dass eine anteilige Berechnung auch den Prüfungsaufwand für die Verantwortlichen und damit auch die Rechtsunsicherheiten und Streitanfälligkeit erhöht.

Eine anteilige Berechnungsvorgabe wie die des § 23 KSchG ist auch aus sachlichen Gründen nicht für das BDSG geeignet. Denn der Gesetzgeber ging im BDSG ersichtlich davon aus, dass das Risiko für den Schutz personenbezogener Daten schon durch das „Mehr" der an der Verarbeitung beteiligten Personen (im Sinne von Köpfen) erhöht ist, während es keine Rolle spielt, wie groß der Anteil der jeweiligen Person an der Verarbeitung ist. Demgegenüber steht hinter § 23 Absatz 1 Satz 5 KSchG die Erwägung, dass die Struktur und die Eigenarten eines Kleinbetriebs im Vergleich zum Großbetrieb die erleichterte Möglichkeit erfordern, Arbeitsverhältnisse zu beenden.[33] Für diesen Zweck ist eine anteilige Berechnung zweck- und sachgerecht. Eine entsprechende Differenzierung ist für das Datenschutzrecht jedoch nicht angezeigt.

5.5.4. Schlussfolgerungen

Die Rückmeldungen zu den §§ 5 bis 7, 38 BDSG lassen darauf schließen, dass die Zielsetzungen des Gesetzgebers grundsätzlich erreicht werden konnten. Die Bestimmungen für Datenschutzbeauftragte öffentlicher und nichtöffentlicher Stellen schaffen einheitliche Rahmenbedingungen, die Datenschutzbeauftragte in ihrer Unabhängigkeit schützt und stärkt.

Es hat sich gezeigt, dass Datenschutzbeauftragte eine wichtige Rolle als Ansprechpartner für Aufsichtsbehörden und bei der wirksamen operativen Umsetzung des Datenschutzrechts übernehmen. Eine weitere Anhebung der Bestellungspflicht-Grenze des § 38 Absatz 1 BDSG kann nach den Rückmeldungen zu Problemen und Umsetzungsdefiziten bei Vereinen und kleineren und mittleren Unternehmen führen, während nach den Rückmeldungen ein Entlastungseffekt vielfach nicht wahrgenommen wird. Im Ergebnis erscheint eine weitere Änderung der Tatbestände für eine Bestellungspflicht derzeit nicht sachgerecht.

[33] Rolfs/Giesen/Kreikebohm/Meßling/Udsching-*Volkening*, Beck'scher Online-Kommentar zum Arbeitsrecht, 59. Edition, KSchG § 23 Rn. 1.

5.6. Rechte der betroffenen Person - §§ 32 bis 37 BDSG

5.6.1. Zielsetzung und Gegenstand der Regelungen

Die §§ 32 bis 37 BDSG sehen für bestimmte Sachverhalte Einschränkungen der Rechte betroffener Personen und der damit korrespondierenden Pflichten des Verantwortlichen vor. Sie beruhen auf Artikel 23 DSGVO, der vorsieht, dass durch Rechtsvorschriften der Mitgliedstaaten die Rechte und Pflichten gemäß den Artikeln 12 bis 22 DSGVO und Artikel 34 DSGVO sowie die in Artikel 5 DSGVO geregelten Grundsätze für die Verarbeitung personenbezogener Daten – sofern dessen Bestimmungen den in den Artikeln 12 bis 22 DSGVO vorgesehenen Rechten und Pflichten entsprechen – beschränkt werden können.

Die in den §§ 32 bis 37 BDSG vorgenommenen Einschränkungen der Rechte betroffener Personen ergänzen die in der DSGVO unmittelbar vorgesehenen Ausnahmen.

§ 32 BDSG beschränkt die Informationspflichten nach Artikel 13 Absatz 3 DSGVO für die Fälle, in denen personenbezogene Daten zu einem anderen Zweck weiterverarbeitet werden sollen, als für den sie ursprünglich bei der betroffenen Person erhoben wurden.

§ 33 BDSG sieht Einschränkungen der Pflichten nach Artikel 14 Absatz 1, 2 und 4 DSGVO vor, nach dem die betroffene Person dann, wenn die Daten nicht bei ihr erhoben wurden, im Fall einer beabsichtigten Weiterverarbeitung über den Zweck der Weiterverarbeitung sowie die weiteren Umstände nach Artikel 14 Absatz 3 DSGVO zu informieren ist. Sie ergänzen die Ausnahmen von der Informationspflicht aus Artikel 14 Absatz 5 DSGVO, wonach die betroffene Person nicht informiert werden muss, wenn sie etwa bereits über die Informationen verfügt oder die Information unmöglich oder nur mit einem unverhältnismäßigen Aufwand möglich ist.

§ 34 BDSG regelt ergänzend zu den in den §§ 27 bis 29 BDSG enthaltenen Ausnahmen weitere Einschränkungen des Auskunftsrechts der betroffenen Person nach Artikel 15 Absatz 1 DSGVO.

§ 35 BDSG ordnet für bestimmte Fälle anstelle einer Pflicht des Verantwortlichen zur Löschung personenbezogener Daten nach Artikel 17 DSGVO eine Einschränkung der Verarbeitung gemäß Artikel 18 DSGVO an.

§ 36 BDSG schränkt das Recht auf Widerspruch der betroffenen Person gegen die Verarbeitung ihrer personenbezogenen Daten aus Artikel 21 DSGVO gegenüber einer öffentlichen Stelle ein, wenn an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

§ 37 BDSG schränkt das Recht gemäß Artikel 22 Absatz 1 DSGVO, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu wer-

den, dahingehend ein, dass dieses nicht besteht, wenn damit dem Begehren der betroffenen Person stattgegeben wurde oder die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht.

5.6.2. Empirische Ergebnisse und Bewertung

Die Einschränkungen der Betroffenenrechte durch die §§ 32 bis 37 BDSG wurden in den dem BMI übermittelten Stellungnahmen in konträrer Weise bewertet: Während insbesondere von Wirtschaftsverbänden wegen von dort wahrgenommenen erheblichen bürokratischen Belastungen Anregungen zu weiteren Einschränkungen der Betroffenenrechte gegeben werden, wird auf der anderen Seite – insbesondere von den Datenschutzaufsichtsbehörden – die Einschränkung der Betroffenenrechte als zu weitgehend bemängelt und teilweise bezweifelt, dass für die Normen eine Öffnungsklausel in der DSGVO bestehe. Die Wirtschaftsverbände monieren insgesamt eine starke bürokratische Belastung insbesondere kleinerer und mittlerer Unternehmen durch die bestehenden Rechte betroffener Personen und nur eine geringe Erleichterung durch die Einschränkung der Betroffenenrechte durch das BDSG. Weitere Einschränkungen der Betroffenenrechte werden zum einen für bestimmte Verarbeitungssituationen vorgeschlagen, zum anderen aber auch generell für bestimmte Verarbeitungskontexte, wie etwa Verarbeitungen personenbezogener Daten in Arztpraxen.

Die folgende Darstellung thematisiert zunächst die in den Stellungnahmen gegebenen Anregungen zu weiteren Einschränkungen der Betroffenenrechte und sodann die Vorschläge für eine teilweise Rücknahme der Einschränkungen.

5.6.2.1. Vorschläge zu weiteren Einschränkungen der Betroffenenrechte

Vorschläge zu den Betroffenenrechten insgesamt

Verhältnismäßigkeitsvorbehalt für die Informationspflichten der DSGVO

Im Hinblick auf die generell als aufwändig empfundene Erfüllung von Informationspflichten bei der Verarbeitung personenbezogener Daten, die mit den Rechten der betroffenen Person korrespondieren, wird von Seiten der Verbände moniert, deren Ziele müssten in einem angemessenen Verhältnis zu dem erforderlichen Aufwand stehen. Hierin ist der Vorschlag einer generellen Einschränkung der Betroffenenrechte durch einen Verhältnismäßigkeitsvorbehalt zu sehen. In die gleiche Richtung geht der Vorschlag, die Missbrauchseinrede aus Artikel 12 Absatz 5 DSGVO zu erweitern.

Ein genereller Verhältnismäßigkeitsvorbehalt im BDSG, der nicht nur punktuelle Einschränkungen der Informationspflichten vorsieht, würde voraussichtlich zu einer erheblichen Beschneidung der Betroffenenrechte führen. Er wäre nach Ansicht des BMI nicht mehr von der Öffnungsklausel des Artikels 23 Absatz 1 Buchstabe i DSGVO gedeckt. Zwar ermöglicht Artikel 23 Absatz 1 Buchstabe i DSGVO eine Beschränkung der Betroffenenrechte auch zum Schutz der Rechte und Freiheiten anderer Personen und damit auch zum

Schutz der Rechte des Verantwortlichen[34]; eine solche Beschränkung muss allerdings den Wesensgehalt der Grundrechte und Grundfreiheiten achten und eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellen (Artikel 23 Absatz 1 DSGVO). Die Betroffenenrechte einem generellen Verhältnismäßigkeitsvorbehalt zu unterstellen, würde zudem den Wesensgehalt der Betroffenenrechte als Ausprägung des Grundrechts aus Artikel 8 der Charta der Grundrechte der Europäischen Union (EU-GRCh) auf den Schutz der eigenen personenbezogenen Daten unterminieren. Gleiches gilt hinsichtlich des Vorschlages einer Erweiterung der Missbrauchseinrede aus Artikel 12 Absatz 5 DSGVO durch eine Regelung im BDSG. Hier ist auch zu bedenken, dass Artikel 12 Absatz 5 DSGVO schon jetzt die Pflicht des Verantwortlichen ausschließt, bei offenkundig unbegründeten oder exzessiven Anträgen tätig zu werden.

Orientierung der Informationspflicht am Kontext der Verarbeitung

Aus dem Kreis der Verbände wird darüber hinaus vorgeschlagen, dass sich die Erforderlichkeit, die Art und Weise, der Umfang und der Zeitpunkt der Information der betroffenen Personen nach dem Kontext der Datenverarbeitung richten sollen. Zudem solle die Information nicht aktiv, sondern nur auf Anforderung zu erteilen sein, wenn vernünftigerweise nicht mit einer Information zu rechnen sei. Der von einigen Aufsichtsbehörden akzeptierte „layered approach", nach dem zunächst nur wenige grundlegende Informationen sowie ein Hinweis darauf erteilt werden, wo ausführliche Informationen abgerufen werden können, solle – insbesondere bei telefonischen Erstkontakten – explizit normiert werden.

Die Informationspflicht nach Artikel 13 Absatz 1 DSGVO ist grundsätzlich unmittelbar und vollumfänglich zu erfüllen. Sie entsteht zum Zeitpunkt der Erhebung der Daten.[35] Der Zeitpunkt der Information nach Artikel 14 Absatz 1 und 2 DSGVO ist in Artikel 14 Absatz 3 DSGVO geregelt und damit ebenfalls unionsrechtlich vorgegeben: Hiernach ist die betroffene Person spätestens einen Monat nach Erlangung der personenbezogenen Daten zu informieren.[36] Eine Informationserteilung nur auf Anforderung würde das Wesen der Informationspflicht konterkarieren und wäre in dieser allgemeinen Form mit Unionsrecht nicht vereinbar. Die Informationspflicht soll die betroffene Person gerade vollumfänglich in die Lage versetzen, den Umfang der Verarbeitung ihrer personenbezogenen Daten zu überschauen und ihre Rechte wahrzunehmen, auch und gerade in Situationen, in denen sie nicht mit der Verarbeitung ihrer Daten rechnet und keine Nachfragen stellen würde. Hinsichtlich des Vorschlages einer kontextbezogenen Informationspflicht würden Abgrenzungsschwierigkeiten eine Normierung jedenfalls schwierig machen.

---

[34] Kühling/Buchner-*Bäcker*, DS-GVO/BDSG, Kommentar, 3. Auflage 2020, Artikel 23 DSGVO Rn. 32; Paal/Pauly-*Paal*, DS-GVO/BDSG, Kommentar, 3. Auflage 2021, Artikel 23 DSGVO Rn. 42.

[35] Paal/Pauly-*Paal/Hennemann*, DS-GVO/BDSG, Kommentar, 3. Auflage 2021, Artikel 13 Rn. 4.

[36] Die Höchstfrist von einem Monat nach Artikel 14 Absatz 3 Buchstabe a DSGVO gilt dabei auch für die Fälle des Artikel 14 Absatz 3 Buchstabe b und c DSGVO. So auch Kühling/Buchner-*Bäcker*, DS-GVO/BDSG, Kommentar, 3. Auflage 2020, Artikel 14 DSGVO Rn. 33, 37.

In Fällen, in denen eine unmittelbare Information nicht praktikabel ist, wie etwa im Kontext von telefonischen Datenerhebungen, wird auch ein mündlicher Hinweis auf die in anderer Form vorliegenden Informationen nach überzeugender Auffassung bereits nach geltender Rechtslage für ausreichend gehalten, wenn die Informationen für die betroffene Person tatsächlich leicht zugänglich sind.[37] Die Artikel 29-Gruppe[38] hat in ihrem Arbeitspapier „Leitlinien für Transparenz gemäß der Verordnung 2016/679" zudem ausdrücklich Mehrebenen-Datenschutzerklärungen und –hinweise empfohlen, um Informationsermüdung zu vermeiden.[39] Einer gesetzlichen Änderung bedarf es deshalb aus Sicht des BMI nicht.

Nachholbarkeit der Information

Von Seiten der Verbände, insbesondere aus der Ärzteschaft, wird darüber hinaus angeregt, dass die Information der betroffenen Person nachholbar sein solle, weil die Informationspflicht bei Terminvereinbarungen am Telefon oder bei der Notfallversorgung schwerlich zu erfüllen sei.

In Fällen, in denen – wie etwa in der Notfallversorgung – die Pflicht zur Information mit anderen Pflichten, hier etwa der medizinischen Hilfeleistung, kollidiert, wird die Informationspflicht auch ohne gesetzliche Regelung aus Gründen der Pflichtenkollision so lange zurücktreten müssen, bis eine Information der betroffenen Person wieder möglich ist. Bei telefonischen Erstkontakten kann wie oben beschrieben verfahren werden.

Ausnahmen von Informationspflichten bei Gefährdung einer Heilbehandlung

Von Seiten der Ärzteschaft wird vorgeschlagen, die datenschutzrechtlichen Informationspflichten gemäß den Artikeln 13 ff. DSGVO für Ärzte praxisgerechter auszugestalten. So sollten sowohl von den Informationspflichten nach Artikel 13 Absatz 1 und 14 Absatz 1 DSGVO, aber auch von der Auskunftspflicht nach Artikel 15 DSGVO Ausnahmen im BDSG geschaffen werden, wenn die Information oder Auskunft eine ärztliche Heilbehandlung gefährden würde. Hier wird die Schaffung einer § 630g BGB entsprechenden Vorschrift angeregt, nach dem einem Patienten (nur) dann Einsicht in die ihn betreffende Patientenakte zu gewähren ist, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte anderer Personen entgegenstehen.

§ 630g BGB stellt eine (spezialgesetzliche) Einschränkung des Auskunftsrechts der betroffenen Person nach Artikel 15 DSGVO zum Schutz der Rechte der betroffenen Person

[37] Kühling/Buchner-*Bäcker*, DS-GVO/BDSG, Kommentar, 3. Auflage 2020, Artikel 13 DSGVO Rn. 58; Ehmann/Selmayr-*Knyrim*, Datenschutz-Grundverordnung, Kommentar, 2. Auflage 2018, Artikel 13 Rn. 22.
[38] In der Artikel-29-Gruppe haben die europäischen Datenschutzbehörden bis zum 24. Mai 2018 zusammengearbeitet und einige Leitlinien und Positionspapiere zur DSGVO veröffentlicht. Diese wurde von ihrem Nachfolgegremium, dem Europäischen Datenschutzausschuss (EDSA), bestätigt.
[39] „Leitlinien für Transparenz gemäß der Verordnung 2016/679", Arbeitspapier der Artikel 29-Gruppe; hierzu auch: Ehmann/Selmayr-*Knyrim*, Datenschutz-Grundverordnung, Kommentar, 2. Auflage 2018, Artikel 13 Rn. 23 f.

nach Artikel 23 Absatz 1 Buchstabe i DSGVO dar. Obwohl die Vorschrift bereits vor dem Geltungsbeginn der DSGVO in Kraft war, lässt sie sich auf diese Öffnungsklausel stützen.[40] Auch für weitere Einschränkungen der Rechte der betroffenen Person im Zusammenhang mit Heilbehandlungen wäre daher nicht das BDSG, sondern das BGB der richtige Regelungsstandort.

Rückmeldungen zu § 32 BDSG und Bewertung

Erweiterung der Ausnahme von der Informationspflicht in § 32 Absatz 1 Nummer 1 BDSG auf nicht analog gespeicherte Daten

Es wird vorgeschlagen, die Ausnahme von der Informationspflicht in § 32 Absatz 1 Nummer 1 BDSG, auch auf nicht analog, also digital gespeicherte Daten zu erweitern.

Dann wäre auch bei der Weiterverarbeitung digital gespeicherter, bei der betroffenen Person erhobener Daten diese unter den Voraussetzungen des § 32 Absatz 1 Nummer 1 BDSG nicht zu informieren.

Mit der Ausnahme von der Informationspflicht in den Fällen des § 32 Absatz 1 Nummer 1 BDSG bei analog gespeicherten Daten sollte einer alltäglichen Verarbeitungssituation Rechnung getragen werden, die mit einem geringen Risiko für die betroffene Person verbunden ist. Durch die Einschränkung der Informationspflicht sollten insbesondere kleine und mittlere Unternehmen der analogen Wirtschaft von der Informationspflicht ausgenommen werden, deren Kommunikationswege ausschließlich oder überwiegend in nicht digitaler Form erfolgen.[41] Die Begrenzung der Einschränkung auf analog gespeicherte Daten trägt damit dem Umstand Rechnung, dass auch eine Information bei der Weiterverarbeitung analog gespeicherter Daten mit besonderem Aufwand verbunden ist, da die Information nicht technisch automatisiert, sondern regelmäßig händisch erfolgt, während die Information bei der Weiterverarbeitung digital gespeicherter Daten technikgestützt zu bewerkstelligen ist. Eine Ausweitung der Ausnahmen von der Informationspflicht in § 32 Absatz 1 Nummer 1 BDSG auf digitale gespeicherte Daten hält das BMI daher nicht für angezeigt.

Rückmeldungen zu § 33 BDSG und Bewertung

Ausnahme bei der Verarbeitung öffentlicher Daten

In mehreren Stellungnahmen wird angeregt, die Pflicht zur Information des Betroffenen entfallen zu lassen, wenn Daten verarbeitet werden, die öffentlich verfügbar sind. Der Be-

[40] Dies gilt indes nur, soweit er sich in den Grenzen der Öffnungsklausel hält. Die Kostenpflichtigkeit der Information aus der Patientenakte ist nach teilweise vertretener Ansicht in der Literatur nicht mehr von der Öffnungsklausel gedeckt. So etwa Säcker/Rixecker/Oetker/Limperg- *Wagner*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 5, 8. Auflage 2020, § 630g Rn. 6; Westermann/Grunewald/Maier-Riemer- *Rehborn/Gescher*, Erman - BGB-, Kommentar, 16. Auflage 2020, § 630g Rn. 1.

[41] BT-Drs. 18/12144, S. 4 f.

troffene habe hier in einigen Konstellationen die Daten gerade deshalb öffentlich zur Verfügung gestellt, damit diese vom Rechtsverkehr zur Kenntnis genommen werden können. Da es sich hierbei um Daten handelt, die nicht beim Betroffenen erhoben wurden, wäre eine solche Ausnahme von der Informationspflicht im § 33 BDSG zu verorten.

In diesem Zusammenhang ist darauf hinzuweisen, dass die Informationspflicht aus Artikel 14 DSGVO die Transparenz von Datenverarbeitungsvorgängen für die betroffene Person gewährleisten soll.[42] Auch dann, wenn Daten veröffentlicht werden, besteht ein Interesse der betroffenen Person, über jede neue Datenverarbeitung informiert zu werden, weil aus dieser neue Risiken entstehen können, etwa durch die Verknüpfung mit anderen personenbezogenen Daten.

Übernahme von Ausnahmen aus § 33 Absatz 1 BDSG in den § 32 Absatz 1 BDSG

Es wird als Widerspruch erachtet, dass die Informationspflicht nach Artikel 14 DSGVO entfällt, wenn die Information die Durchsetzung zivilrechtlicher Ansprüche beeinträchtigen würde, die Informationspflicht nach Artikel 13 Absatz 3 DSGVO gemäß § 32 Absatz 1 Nummer 4 BDSG aber auch dann entfällt, wenn durch die Information die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche jedweder Art beeinträchtigt würden.

Auch wird eine Übertragung der Ausnahme des § 32 Absatz 2 Satz 3 BDSG auf § 33 BDSG vorgeschlagen. Hiernach ist der Verantwortliche dann nicht dazu verpflichtet, anstelle der Information der betroffenen Person geeignete Maßnahmen zum Schutz ihrer berechtigten Interessen zu ergreifen, wenn die Information unterbleibt, weil sie die Durchsetzung zivilrechtlicher Ansprüche beeinträchtigen oder die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

Die eingeschränkteren Ausnahmetbestände von der Informationspflicht nach Artikel 14 DSGVO in § 33 BDSG begründen sich insbesondere aus der Situation, bei der die Daten erhoben worden sind – nämlich im Gegensatz zu den Ausnahmen von der Informationspflicht nach Artikel 13 DSGVO in § 32 BDSG nicht bei der betroffenen Person selbst. Aus diesem Grund besteht in den Fällen des § 33 BDSG ein erhöhtes Interesse der betroffenen Person an der Information. Diese Wertung des Gesetzgebers sollte aus Sicht des BMI beibehalten werden.

[42] Kühling/Buchner-*Bäcker,* DS-GVO/BDSG, Kommentar, 3. Auflage 2020, Artikel 14 DSGVO Rn. 6.

Rückmeldungen zu § 34 BDSG und Bewertung

Konkretisierung des Auskunftsanspruchs und Ausschluss von Missbrauch

Vielfach wird in den Rückmeldungen vorgeschlagen, das Auskunftsrecht in § 34 BDSG zu konkretisieren, etwa indem Gegenstand und Art der Auskunft ausdrücklich geregelt werden. Auch wird angeregt, dass die betroffene Person selbst ihr Auskunftsersuchen konkretisieren solle.

Das Anliegen, als Verantwortlicher nur mit konkreten und nicht mit pauschalen Auskunftsbegehren in Anspruch genommen zu werden, ist nachvollziehbar. Es besteht indes bereits jetzt die Möglichkeit, zunächst von der betroffenen Person eine Konkretisierung des Anspruchs zu erbitten, wenn der Verantwortliche eine große Menge von Daten über die betroffene Person verarbeitet.[43]

Durch den Auskunftsanspruch soll die betroffene Personen zudem gerade in die Lage versetzt werden, einen Überblick über die zu ihrer Person gespeicherten personenbezogenen Daten zu gewinnen, um dann gegebenenfalls weitere Rechte auszuüben. Deswegen dürfte regelmäßig ein berechtigtes Interesse daran bestehen, über alle Verarbeitungsvorgänge der eigenen personenbezogenen Daten vollumfänglich Auskunft zu erhalten. Die Ausübung des Rechts von einer Konkretisierung des Auskunftsbegehrens abhängig zu machen, widerspräche dem Grundgedanken des Artikels 15 DSGVO.

Zudem ist darauf hinzuweisen, dass zur Verhinderung unverhältnismäßigen Aufwandes aufgrund missbräuchlicher Auskunftsbegehren nach Artikel 12 Absatz 5 DSGVO der Verantwortliche bei exzessiven Anträgen einer betroffenen Person entweder ein Entgelt verlangen oder sich weigern kann, aufgrund des Antrages tätig zu werden.

Der Gegenstand und die Art der Auskunft hingegen ergeben sich aus Artikel 15 DSGVO und können vom nationalen Gesetzgeber mangels Öffnungsklausel nicht konkretisiert werden.

Ausnahme vom Auskunftsausspruch nach Artikel 14 DSGVO wegen Gefährdung zivilrechtlicher Ansprüche

Ebenfalls wird vielfach vorgeschlagen, eine Ausnahme vom Auskunftsanspruch zu normieren, wenn die Auskunft die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde, und so einen Gleichlauf mit der Ausnahme von der Informationspflicht nach Artikel 14 DSGVO gemäß § 33 Absatz 1 Nummer 2 Buchstabe a BDSG herzustellen. Dies sei auch erforderlich, um die missbräuchliche oder sachfremde Geltendmachung des Anspruches auszuschließen, durch die etwa die Ausforschung im Zivilprozess aktuell möglich sei. Hierzu wird auch vorgeschlagen, die Unverhältnismäßigkeitseinrede zu erweitern.

[43] Erwägungsgrund 63 der DSGVO.

Die vom Gesetzgeber vorgesehenen Ausnahmen von der Auskunftspflicht in § 34 Absatz 1 Nummer 1 BDSG, der auf bestimmte Ausnahmen von der Informationspflicht in § 33 BDSG verweist, enthalten die Wertung, dass die Erteilung der Auskunft nur in Fällen unterbleiben kann, in denen öffentliche Interessen durch die Information berührt sind. Dies stellt aus Sicht des BMI eine sachgerechte Beschränkung der Ausnahmemöglichkeit dar und sollte nicht auf rein private Interessen übertragen werden.

Geheimhaltungsinteressen der Unternehmen

Außerdem wird angemerkt, dass Geheimhaltungsinteressen der Unternehmen im Rahmen der Auskunftspflicht nach Artikel 15 DSGVO zu berücksichtigen seien.

Soweit durch die Geheimhaltung Rechte des Unternehmens geschützt werden sollen, handelt es sich hierbei um Rechte des Verantwortlichen als anderer Personen, zu deren Sicherstellung eine Einschränkung der Rechte der betroffenen Person nach Artikel 23 Absatz 1 Buchstabe i DSGVO grundsätzlich zulässig ist.

Ob und inwieweit eine Einschränkung der Auskunftspflicht im Hinblick auf Geheimhaltungsinteressen tatsächlich geregelt werden sollte, wird das BMI prüfen.

Rückmeldungen zu § 35 BDSG und Bewertung

Zu § 35 BDSG werden erhebliche Probleme beim Erfüllen der Pflicht auf Löschung vorgetragen. Es sei aufgrund der Einstellungen einiger Programme nicht möglich, Daten zu löschen, ohne dass dies erhebliche Probleme im Gesamtsystem auslöse.

Im Einzelnen werden folgende Vorschläge gemacht:

Konkretisierung des Anspruchs auf Löschung

Mehrfach wird angeregt, die Reichweite der Pflicht auf Löschung zu konkretisieren. Die Regelung der DSGVO zur Löschung (Artikel 17 DSGVO) könne auch so verstanden werden, dass eine Anonymisierung die Löschpflicht erfüllen könne.

Es handelt sich um eine ausschließlich unionsrechtlich zu lösende Frage, die dem nationalen Gesetzgeber entzogen ist.

Regelmäßige Löschung als Erfüllung der Löschpflicht

Vielfach wird vorgeschlagen, dass die Pflicht, personenbezogene Daten zu löschen, durch eine in regelmäßigen zeitlichen Abständen durchgeführte, systematische Löschung erfüllt werden kann; auch eine Sperrung der Daten bis dahin sei denkbar.

Die Löschung ist gemäß Artikel 17 Absatz 1 DSGVO grundsätzlich unverzüglich durchzuführen. Dies bedeutet, dass der Verantwortliche die Daten nach Prüfung der Ausschlusstatbestände zu löschen hat. Die zeitliche Obergrenze für die Prüfung ergibt sich aus Artikel 12 Absatz 4 DSGVO, nach dem ein einmonatiges Prüfen die Ausnahme ist.

Verhältnismäßigkeitseinrede in § 35 Absatz 1 BDSG auch bei automatisierter Datenverarbeitung

Zudem wird mehrfach angeregt, die Verhältnismäßigkeitseinrede des § 35 Absatz 1 BDSG, nach der bei nichtautomatisierten Datenverarbeitungen eine Löschung der Daten unter bestimmten Umständen durch die Einschränkung der Bearbeitung ersetzt werden kann, auch auf Fälle automatisierter Datenverarbeitung zu erstrecken oder eine Sperrung der Daten anstelle einer Löschung zuzulassen.

Den Ausschluss der Löschpflicht einem generellen Verhältnismäßigkeitsvorbehalt zu unterstellen, dürfte den Kern des Rechts auf Löschung aushöhlen. Generell liegt in einer Einschränkung der Verarbeitung ein höheres datenschutzrechtliches Risiko als in einer Löschung. Mit der Vorschrift soll die Löschpflicht vor allem bei Archivierungen in Papierform oder bei der Nutzung früher gebräuchlicher analoger Speichermedien, bei denen es nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, einzelne Informationen selektiv zu entfernen, eingeschränkt werden.[44] Im Hinblick auf diese Daten besteht aufgrund ihrer analogen Speicherung zum einem ein geringeres datenschutzrechtliches Risiko, zum anderen bedeutet ihre Löschung aufgrund der Art der Speicherung einen besonderen Aufwand, der bei Löschung automatisch gespeicherter Daten durch geeignete technische Maßnahmen vermieden werden kann.

Zudem ist zu beachten, dass nach den Artikeln 24 ff. und 32 DSGVO bei automatisierten Datenverarbeitungen die eingesetzte Technik die Anforderungen der DSGVO berücksichtigen muss. Das bedeutet auch, dass der Verantwortliche dafür Sorge zu tragen hat, dass die Technik eine rechtskonforme Löschung ermöglicht.

Eine Gleichstellung der automatisierten Datenverarbeitung mit der nichtautomatisierten Datenverarbeitung in § 35 Absatz 1 BDSG sollte daher aus Sicht des BMI unterbleiben.

Rückmeldungen zu § 37 BDSG und Bewertung

Es wird eine Ausnahme von dem Verbot einer automatisierten Entscheidung neben den in § 37 BDSG genannten Fällen auch für Fälle gewünscht, in denen Versicherungsleistungen an Dritte erfolgen, die nicht Vertragspartner des Versicherers sind. Außerdem wird eine Ausdehnung auch auf die Kreditwirtschaft angeregt. Daneben wird aber auch die komplette Streichung des § 37 BDSG angeregt, weil die Norm entgegen der Regelung in der DSGVO impliziere, dass der Artikel 22 Absatz 1 DSGVO auch positive Entscheidungen gegenüber der betroffenen Person erfasse.

Aus Sicht des BMI wären eine entsprechende Erweiterung der Ausnahme auf die Kreditwirtschaft oder eine Erweiterung der Norm auf Dritte mit Artikel 22 DSGVO vereinbar. Das BMI wird eine Überarbeitung des § 37 BDSG prüfen.

[44] BT-Drs. 18/12144, S. 5.

5.6.2.2. Vorschläge zur Rücknahme der Einschränkung der Rechte der betroffenen Person

Rückmeldungen zu den §§ 32 und 33 BDSG

Streichung des § 32 Absatz 1 Nummer 1 BDSG

Von den Aufsichtsbehörden wird angeregt, den § 32 Absatz 1 Nummer 1 BDSG zu streichen, weil es für eine solche Regelung keine Öffnungsklausel in der DSGVO gebe. Zudem sei die Norm unbestimmt, weil unklar bliebe, wann „das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalles, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist". Auch von behördlicher Seite und aus dem Kreis der Verbände wird die Unionsrechtskonformität der Vorschrift angezweifelt.

Die Vorschrift beruht auf der Öffnungsklausel des Artikels 23 Absatz 1 Buchstabe i DSGVO zugunsten der Rechte und Freiheiten anderer Personen. Der Wortlaut der Regelung zeigt, dass es hier um Fälle geht, in denen die betroffene Person bereits mit einer Weiterverarbeitung rechnet und diese so unerheblich ist, dass ihr Interesse an der Information gering ist. Es handelt sich um eine Abwägungsklausel, die eine sachgerechte Einzelfallentscheidung ermöglicht. Aus Sicht des BMI ist hier keine Änderung angezeigt.

Kein Ausschluss der Informationspflicht nach Artikel 13 und 14 DSGVO bei nur unerheblicher Beeinträchtigung der Aufgaben öffentlicher Stellen oder der Durchsetzung zivilrechtlicher Ansprüche

Aus dem Kreis der Datenschutzreferate der Länder und der Aufsichtsbehörden wird vorgeschlagen, in § 32 Absatz 1 Nummer 2 BDSG und § 33 Absatz 1 Nummer 1 Buchstabe a BDSG eine Klarstellung aufzunehmen, dass nur unerhebliche Beeinträchtigungen der ordnungsgemäßen Erfüllung der Aufgabe einer öffentlichen Stelle durch die Information, etwa zeitliche Verzögerungen, eine Ausnahme von der Informationspflicht nicht begründen. Gleiches wird bezüglich § 32 Absatz 1 Nummer 4 BDSG und § 33 Absatz 1 Nummer 2 Buchstabe a BDSG angeregt, die jeweils eine Ausnahme von der Informationspflicht in Fällen vorsehen, in denen die Information die Durchsetzung (zivil-)rechtlicher Ansprüche gefährdet.

Im Falle einer nur geringfügigen Beeinträchtigung der ordnungsgemäßen Erfüllung der Aufgabe einer öffentlichen Stelle oder der Durchsetzung zivilrechtlicher Ansprüche vermag bereits das Interesse des Verantwortlichen an der Nichterteilung der Information das Interesse der betroffenen Person an der Information nicht zu überwiegen. Die in beiden Normen vorgesehene Interessenabwägung käme deshalb wohl in der überwiegenden Zahl der Fälle schon zu dem Ergebnis, dass eine Information zu erteilen ist. Aus diesem Grund hält das BMI eine Klarstellung im Gesetzestext, dass nur unerhebliche Beeinträchtigungen eine Ausnahme von der Informationspflicht nicht begründen, nicht für erforderlich.

Gefährdungsbeurteilung durch die öffentliche Stelle

Von den Aufsichtsbehörden wird zudem angeregt, dass § 32 Absatz 1 Nummer 3 BDSG dahingehend geändert werden solle, dass die zuständige öffentliche Stelle beurteilt, ob eine Gefährdung der öffentlichen Sicherheit vorliegt und diese Beurteilung nicht der verantwortlichen, gegebenenfalls also auch nichtöffentlichen Stelle zugemutet wird. Gleiches wird für § 33 Absatz 1 Nummer 1 Buchstabe b BDSG vorgeschlagen.

Für eine Einschränkung der Informationspflicht aufgrund von § 32 Absatz 1 Nummer 3 BDSG ist erforderlich, dass die Information tatsächlich die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde. Ist dies nur aus Sicht des Verantwortlichen, nicht aber tatsächlich der Fall, greift die Ausnahme nicht. Es ist dem Verantwortlichen deshalb anzuraten, – sofern die Sachlage nicht eindeutig ist – zunächst die Bestätigung der zuständigen Behörde einzuholen, dass ein solcher Fall vorliegt, bevor entsprechende Daten ohne Information der betroffenen Person übermittelt werden. Einer gesetzlichen Regelung bedarf es dafür aus Sicht des BMI nicht.

Ausschluss der Einschränkung der Informationspflicht zugunsten der öffentlichen Ordnung

Zudem wird vorgeschlagen, dass der Ausschluss der Informationspflicht zugunsten der öffentlichen Ordnung in § 32 Absatz 1 Nummer 3 BDSG und § 33 Absatz 1 Nummer 1 Buchstabe b BDSG gestrichen werden solle.

Diese Einschränkung der Informationspflicht beruht auf der Öffnungsklausel des Artikels 23 Absatz 1 Buchstabe e DSGVO, der die Einschränkung der Rechte der betroffenen Person zulässt, um den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses sicherzustellen. Auch der allgemein anerkannte Schutz der öffentlichen Ordnung liegt im allgemeinen öffentlichen Interesse. Die öffentliche Ordnung ist ein durch die Rechtsprechung hinreichend konturierter Begriff; er umfasst die Gesamtheit aller ungeschriebenen Regeln für das Verhalten des Einzelnen in der Öffentlichkeit, deren Beachtung nach den jeweils herrschenden Anschauungen als unerlässliche Voraussetzung eines geordneten staatsbürgerlichen Gemeinschaftslebens betrachtet wird.[45] Die Einschränkung sollte deshalb aus Sicht des BMI beibehalten werden.

Ersetzung des Wortes „rechtlicher“ durch „zivilrechtlicher“ in § 32 Absatz 1 Nummer 4 BDSG

Von behördlicher Seite wird vorgeschlagen, in § 32 Absatz 1 Nummer 4 BDSG, der eine Einschränkung der Informationspflicht vorsieht, um die Durchsetzung eines zivilrechtlichen Anspruchs zu gewährleisten, das Wort „rechtlicher“ durch das Wort „zivilrechtli-

[45] Vgl. BVerfGE 69, 315 (352); BVerfGE 2, 1 (6); 13, 82 (91).

cher“ zu ersetzen, da nur eine Einschränkung der Rechte der betroffenen Person zugunsten der Durchsetzung zivilrechtlicher Ansprüche von der Öffnungsklausel des Artikels 23 Absatz 1 Buchstabe j DSGVO gedeckt wäre.

Zwar trifft es zu, dass Artikel 23 Absatz 1 Buchstabe j DSGVO eine Einschränkung der Rechte der betroffenen Person nur zur Sicherstellung der Durchsetzung *zivil*rechtlicher Ansprüche vorsieht, die Regelung des § 32 Absatz 1 Nummer 4 BDSG wird hier aber zum Schutz der Rechte und Freiheiten anderer Personen auf Artikel 23 Absatz 1 Buchstabe i DSGVO gestützt.[46]

Vorrangiges Interesse an einer geheimen Behördenkommunikation

Von den Aufsichtsbehörden wird kritisiert, dass § 32 Absatz 1 Nummer 5 BDSG von einem allgemein vorrangigen Interesse an einer Kommunikation mit Behörden ausgehe, die gegenüber der betroffenen Person geheim zu halten wäre. Es müsse zudem eine Beschränkung dieser Ausnahme für den Fall vorgesehen werden, dass der Verantwortliche wissentlich falsche Anschuldigungen gegen die betroffene Person erhebt. Aus dem Kreis der Länder wird zudem für unklar gehalten, was unter „vertraulicher Kommunikation“ zu verstehen sei.

Eine vertrauliche, also nur für bestimmte Empfänger vorgesehene, Kommunikation mit Behörden ist in verschiedenen Konstellationen eine unverzichtbare Grundlage für die erfolgreiche Erfüllung rechtmäßiger behördlicher Verarbeitungszwecke. Praktische Anwendungsfälle sind etwa die Information der zuständigen Strafverfolgungsbehörde über den Verdacht einer Straftat oder Hinweise durch sogenannte Whistleblower an Behörden. Da die Ausnahme von der Informationspflicht in diesen Fällen eine vertrauliche Kommunikation mit den Behörden überhaupt erst ermöglicht, besteht aus Sicht des BMI auch weiterhin ein erhebliches öffentliches Interesse am Fortbestand dieser Regelung. Die Norm stützt sich daher auf Artikel 23 Absatz 1 Buchstabe e DSGVO.

Zielrichtung der Vorschrift ist es dabei nicht, wissentlich falsche Anschuldigungen gegen die betroffene Person von der Informationspflicht auszunehmen. In solchen Fällen dürfte bereits kein schützenswertes Interesse an der Vertraulichkeit der Kommunikation mit Behörden bestehen und die Vorschrift vor dem Hintergrund der inhaltlichen Anforderungen des Artikels 23 DSGVO im Rahmen der Missbrauchskontrolle nicht greifen.

Streichung von § 32 Absatz 2 Satz 3 BDSG

§ 32 Absatz 2 BDSG regelt die Verpflichtung des Verantwortlichen, in Fällen, in denen eine Information der betroffenen Person gemäß § 32 Absatz 1 BDSG unterbleibt, geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person zu ergreifen – u. a die Bereitstellung der Informationen für die Öffentlichkeit – sowie die Gründe zu dokumentieren. In § 32 Absatz 2 Satz 3 BDSG sind Ausnahmen hiervon für Fälle des § 32

[46] Siehe hierzu auch schon oben unter 5.3.2.4.

Absatz 1 Nummer 4 und 5 BDSG normiert, in denen die Information die Durchsetzung zivilrechtlicher Ansprüche oder die vertrauliche Übermittlung an eine öffentliche Stelle gefährden würde. Aus Sicht der Aufsichtsbehörden setzt die Einschränkung der Pflicht zum Ergreifen von Kompensationsmaßnahmen die Prinzipien des Artikels 23 Absatz 1 DSGVO nicht ausreichend um. Nach diesen müssen Einschränkungen der Rechte der betroffenen Person den Wesensgehalt der Grundrechte in einer demokratischen Gesellschaft achten und eine notwendige und eine verhältnismäßige Maßnahme darstellen.

Die Ausnahmen wurden eingeführt, um eine Vereitelung oder ernsthafte Beeinträchtigung des – legitimen – Verarbeitungszwecks durch die in Satz 1 und 2 vorgesehenen Maßnahmen zu vermeiden,[47] die durch die Bereitstellung der Informationen für die Öffentlichkeit zu befürchten wären. Diese Wertung des Gesetzgebers hält das BMI weiterhin für sachgerecht.

Rückmeldungen zu § 34 BDSG

Auskunftsverweigerung aufgrund satzungsmäßiger Aufbewahrungspflichten

Von Seiten der Aufsichtsbehörden wird angeregt, § 34 Absatz 1 Nummer 2 BDSG zu streichen. Nach dieser Vorschrift ist eine Auskunft nicht zu erteilen, wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen. Zum einen fehle es hier an einer Öffnungsklausel zum anderen würden Unternehmen in der Praxis der Pflicht zur Sicherung der Zweckbindung bzw. Einschränkung der Verarbeitung nicht nachkommen, die Voraussetzung für die Einschränkung des Auskunftsrechts ist. Dies könne zudem von den Betroffenen nicht überprüft werden.

Von Seiten der Länder wird vorgeschlagen, jedenfalls klarzustellen, dass die Vorschrift eine Auskunftspflicht nur aufgrund öffentlich-rechtlicher Satzungen, nicht aber aufgrund privater Satzungen ausschließe.

Die Anforderungen an den Ausschluss der Auskunftspflicht sind sehr hoch. So ist die Auskunftspflicht nur dann ausgeschlossen, wenn einer der Ausschlussgründe nach § 34 Absatz 1, 1. Halbsatz BDSG vorliegt und zudem die Auskunftserteilung einen unverhältnismäßigen Aufwand verursachen würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Darüber hinaus ist nach § 34 Absatz 2 BDSG die Ablehnung der Auskunftserteilung gegenüber der betroffenen Person vollumfänglich zu begründen. Ausweislich der Gesetzesbegründung hat der Verantwortliche bei der Ermittlung des Aufwands die bestehenden technischen Möglichkeiten zu berücksichtigen, gesperrte und archivierte Daten der betroffenen Person im Rahmen der Auskunftserteilung verfügbar zu machen.[48] Sofern die betroffene Person mit

[47] BT-Drs. 18/11325, S. 103.
[48] BT-Drs. 18/11325, S. 105.

dem Auskunftsverhalten des Verantwortlichen nicht einverstanden ist oder Zweifel an der Rechtmäßigkeit seines Vorgehens hat, hat sie zudem die Möglichkeit, sich an die zuständige Aufsichtsbehörde zu wenden.

Eine Klarstellung, dass die Vorschrift eine Auskunftspflicht nur aufgrund öffentlich-rechtlicher Satzungen, nicht aber aufgrund privater Satzungen ausschließt, erscheint erwägenswert. Der erhobenen Kritik, dass es dem Verantwortlichen sonst möglich wäre, durch die Schaffung von Satzungen Rechte der betroffenen Person einzuschränken, könnte so begegnet werden.

Verpflichtung von Bundesbehörden zur Information

§ 34 Absatz 3 BDSG trifft eine Regelung für den Fall, dass der betroffenen Person durch eine öffentliche Stelle des Bundes keine Auskunft erteilt wird. In dem Fall ist die Auskunft auf Verlangen der betroffenen Person dem oder der BfDI zu erteilen. Aus dem Kreis der Datenschutzreferate der Länder wird darauf hingewiesen, dass die Vorschrift eine Pflicht der Bundesbehörde nicht enthalte, die betroffene Person über die Möglichkeit, eine Auskunftserteilung an den oder die BfDI zu verlangen, zu informieren. Dies wird in der Literatur teilweise für eine planwidrige Regelungslücke gehalten, da der Gesetzgeber mit § 34 Absatz 3 BDSG an die bisherige Regelung in § 19 Absatz 6 BDSG a. F. anknüpfen wollte.

Das BMI wird die Einführung einer weiteren Hinweispflicht prüfen.

Rückmeldungen zu § 35 BDSG

Beschränkung des Löschungsanspruchs

Zu § 35 Absatz 1 BDSG ist von den Aufsichtsbehörden vorgetragen worden, die Beschränkung des Löschungsanspruchs sei nicht durch eine Öffnungsklausel des Artikels 23 Absatz 1 DSGVO gedeckt, da dort kein Ausnahmetatbestand der Vermeidung eines unverhältnismäßig hohen Aufwandes normiert sei.

Die Vorschrift beruht auf der Öffnungsklausel des Artikels 23 Absatz 1 Buchstabe i DSGVO. Die Vermeidung eines übermäßigen Aufwands dient der Sicherstellung der Rechte des Verantwortlichen als anderer Person. Sie ist bewusst auf Fälle nichtautomatisierter Datenverarbeitung beschränkt, in denen wegen der besonderen Art der Speicherung die Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Die Verhältnismäßigkeit wird zudem gewahrt, indem die Ausnahme nur in Fällen greift, in denen das Interesse der betroffenen Person an der Löschung als gering anzusehen ist.

Unterrichtung der betroffenen Person bei Vermutung der Verletzung schutzwürdiger Interessen durch Löschung

Von den Aufsichtsbehörden wird eine Änderung des § 35 Absatz 2 BDSG dahingehend vorgeschlagen, dass der Verantwortliche die betroffene Person unterrichten müsse, wenn

er vermute, dass durch die Löschung ihrer personenbezogenen Daten ihre schutzwürdigen Interessen beeinträchtigt würden. Denn nur die betroffene Person wisse, ob die Vermutung des Verantwortlichen, dass eine Löschung ihre schutzwürdigen Belange beeinträchtige, tatsächlich zutreffend sei; sie müsse daher davon erfahren. Es sei zudem keine Öffnungsklausel ersichtlich.

Die Beschränkung der Löschpflicht in § 35 Absatz 2 BDSG erfolgt zur Wahrung schutzwürdiger Interessen der betroffenen Person (Artikel 23 Absatz 1 Buchstabe i DSGVO). Dass die Daten nicht gelöscht werden müssen, sondern nur ihre Verarbeitung eingeschränkt werden muss, soll die betroffene Person gerade in die Lage versetzen, sich zu entscheiden, ob sie eine Einschränkung der Verarbeitung oder eine Löschung der Daten wünscht, und dies gegenüber dem Verantwortlichen zu äußern. Aus diesem Grund ist die betroffene Person auch schon nach der geltenden Rechtslage zu unterrichten und deshalb wird es sich in der Regel um eine vorübergehende Beschränkung der Löschpflicht des Verantwortlichen handeln.[49] Die Regelung dient allein der Verbesserung der Rechtsposition der betroffen Person.

Keine Öffnungsklausel für § 35 Absatz 3 BDSG

Auch hinsichtlich § 35 Absatz 3 BDSG wird sowohl aus dem Kreis der Länder als auch aus dem Kreis der Aufsichtsbehörden moniert, dass diese Regelung nicht auf einer Öffnungsklausel in Artikel 23 Absatz 1 DSGVO beruhe.

Die Regelung in § 35 Absatz 3 BDSG stützt sich auf die Öffnungsklausel des Artikels 23 Absatz 1 Buchstabe i DSGVO und soll verhindern, dass dem Verantwortlichen zivilrechtliche Sanktionen wegen der Verletzung von Aufbewahrungsfristen drohen.[50]

5.6.3. Schlussfolgerung

Die Rückmeldungen zu den §§ 32 bis 37 BDSG haben gezeigt, dass diesbezüglich eine große Uneinigkeit besteht: Während die Wirtschaft weitere Einschränkungen der Rechte der betroffenen Person wünscht, plädieren insbesondere die Aufsichtsbehörden für eine Rücknahme der Einschränkungen der Rechte der betroffenen Person. Mitunter werden Unklarheiten bei und Inkonsistenzen zwischen einzelnen Normen gesehen. Viele der insbesondere von den Wirtschaftsverbänden vorgetragenen Probleme lassen sich aus Sicht des BMI bereits mit der geltenden Rechtslage lösen. Die von den Aufsichtsbehörden teilweise vorgetragene Einschätzung, dass für einzelne Regelungen keine Öffnungsklausel bestehe, teilt das BMI nicht.

Lediglich hinsichtlich einzelner Normen sieht das BMI Prüfbedarf. Dieser bezieht sich auf

[49] BT-Drs. 18/11325, S. 103.
[50] Kühling/Buchner-*Herbst*, DS-GVO/BDSG, Kommentar, 3. Auflage 2020, § 35 BDSG Rn. 29.

- eine mögliche Einschränkung der Auskunftspflicht nach Artikel 15 DSGVO im Hinblick auf Geheimhaltungspflichten,
- eine mögliche Klarstellung, dass § 34 Absatz 1 Nummer 2 BDSG die Auskunftspflicht nach Artikel 15 DSGVO nur aufgrund öffentlich-rechtlicher Satzungen, nicht aber aufgrund privater Satzungen ausschließt,
- § 37 BDSG,
- sowie die mögliche Einführung einer Hinweispflicht auf die Pflicht jeder Bundesbehörde, die betroffene Person über die Möglichkeit, eine Auskunftserteilung an den oder die BfDI zu verlangen, wenn ihr keine Auskunft erteilt wird.

5.7. Haftung und Sanktionen - §§ 41 bis 43 BDSG

5.7.1. Zielsetzung und Gegenstand der Regelungen

Mit den §§ 41 bis 43 BDSG hat der Gesetzgeber den rechtlichen Rahmen für Bußgeld- und Strafverfahren bei Verstößen gegen die DSGVO geschaffen. Der Gesetzgeber beabsichtigte dabei, die verpflichtenden Regelungsaufträge der DSGVO in den Artikeln 83 Absatz 8 und 84 Absatz 1 DSGVO umzusetzen und in dem von der DSGVO geschaffenen Rahmen insgesamt an den bis dahin geltenden Grundzügen des datenschutzrechtlichen Bußgeld- und Strafverfahrens festzuhalten.[51]

§ 41 Absatz 1 Satz 1 und 2 BDSG bringen für Verstöße gegen Artikel 83 Absatz 4 bis 6 DSGVO mit einigen Ausnahmen das Gesetz über Ordnungswidrigkeiten (OWiG) zur Anwendung.

Mit § 41 Absatz 1 Satz 3 BDSG wird die gerichtliche Zuständigkeit ab einer Bußgeldhöhe von mehr als 100.000 Euro den Landgerichten zugewiesen. Damit ist der Gesetzgeber von § 68 OWiG abgewichen, der eine ausschließliche Zuständigkeit der Amtsgerichte vorsieht. Durch diese Abweichung sollte einer zu erwartenden höheren Komplexität von Sachverhalt und Verfahren bei höheren Bußgeldtatbeständen Rechnung getragen werden.

Durch § 41 Absatz 2 Satz 1 und 2 BDSG wird der Regelungsauftrag in Artikel 83 Absatz 8 DSGVO ausgeführt. Dazu werden für Bußgeldverfahren wegen Verstößen nach Artikel 83 Absatz 4 bis 6 DSGVO mit wenigen Ausnahmen die Vorschriften des OWiG und der allgemeinen Gesetze über das Strafverfahren entsprechend zur Anwendung gebracht. Um die primärrechtlich vorgeschriebene Unabhängigkeit der Datenschutzaufsichtsbehörden sicherzustellen, hat der Gesetzgeber mit § 41 Absatz 2 Satz 3 BDSG die Einstellung eines Verfahrens durch die Staatsanwaltschaft abweichend von § 69 Absatz 4 Satz 2 OWiG von der Zustimmung der zuständigen Datenschutzaufsichtsbehörde abhängig gemacht.

§ 42 BDSG setzt die Verpflichtung in Artikel 84 Absatz 1 DSGVO um, im nationalen Recht „andere Sanktionen“ – insbesondere strafrechtlicher Natur – für Verstöße gegen die Verordnung vorzusehen.

§ 43 Absatz 1 und 2 BDSG gibt die Bußgeldtatbestände des § 43 Absatz 1 Nummer 7 a und b BDSG a. F. wieder und behält den bis dahin geltenden Bußgeldrahmen bei; mit diesen Tatbeständen wird Artikel 9 der Verbraucherkreditrichtlinie 2008/48/EG umgesetzt.

Der Gesetzgeber hat sich in Absatz 3 dazu entschieden, von der Öffnungsklausel des Artikels 83 Absatz 7 DSGVO Gebrauch zu machen und die Verhängung von Geldbußen gegenüber Behörden und öffentlichen Stellen des Bundes (§ 2 Absatz 1 BDSG) auszuschließen.

[51] Vgl. BT-Drs. 18/11325, S. 108.

5.7.2. Empirische Ergebnisse und Bewertung

Rückmeldungen zu den §§ 41 bis 43 BDSG kamen vonseiten einiger Wirtschaftsverbände, einzelner Unternehmen und Bundesländer, im großen Schwerpunkt aber von der DSK.

5.7.2.1. Methodischer Hinweis

§ 41 BDSG hat den Charakter einer „Verweisungsnorm". Rückmeldungen zu der Vorschrift deckten dementsprechend eine große Bandbreite an Themen im Kontext des Bußgeldverfahrens und der gerichtlichen Zuständigkeit ab. Im Folgenden wird daher bezüglich der Rückmeldungen zu § 41 BDSG eine thematische Untergliederung vorgenommen.

Zu § 42 BDSG werden keine wesentlichen Bedenken geäußert, weshalb auf die Vorschrift im Folgenden nicht weiter eingegangen wird.

5.7.2.2. Allgemeine Rückmeldungen zur Regelungstechnik

Teilweise wird kritisiert, dass die Formulierung in § 41 Absatz 1 Satz 1 BDSG, nach der die Vorschriften des OWiG „sinngemäß" gälten, zu Rechtsunsicherheiten führe, da nicht klar sei, welche Vorschriften des OWiG Anwendung fänden.

Der Verweis in § 41 Absatz 1 Satz 1 BDSG auf das OWiG stellt eine übliche und den Anforderungen der Rechtsförmlichkeit[52] entsprechende Analogieverweisung dar. Damit wird ausgesagt, dass die Bezugsnormen des OWiG nicht wörtlich, sondern sinngemäß anzuwenden sind.

5.7.2.3. Rückmeldungen zu § 41 Absatz 1 Satz 1 und 2, Absatz 2 BDSG

Anwendbarkeit von §§ 30, 130 OWiG

Mehrfach wird angemerkt, dass der Verweis auf §§ 30, 130 des OWiG zur Verantwortlichkeit juristischer Personen und Personenvereinigungen den Vorgaben der DSGVO widerspreche. Die DSGVO lege einen funktionalen Unternehmensbegriff im Sinne der Artikel 101 und 102 AEUV zugrunde. Mit der Rechtsprechung des EuGH[53] genüge es für die Verantwortlichkeit eines Unternehmens, wenn eine berechtigte natürliche Person für das Unternehmen handle. Anders als in § 30 Absatz 1 OWiG vorgesehen, umfasse dies nicht nur gesetzliche Vertreter und andere Leitungspersonen, sondern alle Beschäftigten oder Beauftragten des Unternehmens. Für die Feststellung einer Verantwortlichkeit des Unternehmens sei es dementsprechend nicht erforderlich, die Begehung eines datenschutzrechtlichen Verstoßes oder einer darauf bezogenen Aufsichtspflichtverletzung gemäß § 130 OWiG durch Leitungspersonen nachzuweisen; lediglich Exzesse der handelnden Personen würden keine Verantwortlichkeit des Unternehmers begründen.

[52] Vgl. Handbuch der Rechtsförmlichkeit, BAnz. Nummer 160a vom 22. September 2008, Rn. 219, 232.
[53] EuGH, Urteil vom 7. Juni 1983, Rs. 100-103/80, Slg. 1983, 1825, Rn. 97; EuGH, Urteil vom 29. April 2004, Rs. T-236/01, Slg. 2004, 1181, Rn. 278; EuGH, Urteil vom 7. Februar 2013, Rs. C-68/12, Rn. 25-28.

Dass der Unionsgesetzgeber bei der Schaffung der DSGVO den funktionalen Unternehmensbegriff vor Augen hatte, ergebe sich insbesondere aus deren Erwägungsgrund 150 (*„Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen" im Sinne der Artikel 101 und 102 AEUV verstanden werden."*) Diese Rechtsauffassung habe auch das Landgericht Bonn in seiner Entscheidung vom 11. November 2020[54] vertreten.

Dazu ist zunächst darauf hinzuweisen, dass sich der Gesetzgeber seinerzeit bewusst – und in Kenntnis der Rechtsauffassung der Datenschutzaufsichtsbehörden[55] zu dieser Thematik – dafür entschieden hat, die §§ 30, 130 OWiG nicht aus den nach § 41 Absatz 1 Satz 1 BDSG anwendbaren Vorschriften des OWiG auszunehmen.

Diese Entscheidung basiert dabei auf der Erwägung, dass Artikel 83 Absatz 8 DSGVO es gerade den Mitgliedstaaten überlässt, die Einzelheiten des Bußgeldverfahrens zu regeln. Etwas anderes ergibt sich im Übrigen auch nicht aus Erwägungsgrund 150 zur DSGVO; dieser ist insgesamt und in seinem systematischen Kontext zu lesen. Er bezieht sich auf Artikel 83 DSGVO und konkret auf die dortigen Regelungen der Bußgeldhöhe, enthält aber keine Vorgaben zu den Voraussetzungen, unter denen Verstöße von natürlichen Personen eine bußgeldrechtliche Verantwortlichkeit von juristischer Person und Personenvereinigung auslösen.

Auch das Landgericht Berlin hat am 18. Februar 2021 entschieden[56], dass die DSGVO für den Bereich der Zurechnung schuldhaften Verhaltens keine abschließende Regelung getroffen habe. Die Regelung der Zurechnung der durch natürliche Personen begangenen Verstöße sei erforderlich, da die juristische Person selbst nicht handele, sondern ihre Organe und andere Vertreter dies für sie täten. Insoweit sei die Feststellung eines vorwerfbaren Verhaltens einer natürlichen Person die notwendige Grundvoraussetzung für die Begründung einer Verantwortlichkeit des möglicherweise pflichtigen Rechtsträgers. Dafür sprächen, so das Gericht, auch verfassungsrechtliche Gründe: Hintergrund des Erfordernisses der Anknüpfung an die Handlung einer natürlichen Person sei das aus dem Rechtsstaatsprinzip folgende Schuldprinzip. Ohne eine Anknüpfung an eine schuldhafte Handlung sei ein staatlicher Straf- und auch Bußgeldausspruch nicht begründbar. Die schuldhafte Handlung setze eine an die eigene Verantwortung und Willensfreiheit anknüpfende Entscheidung für oder gegen das Recht voraus, die eine juristische Person oder Personenvereinigung ihrem Wesen nach nicht treffen könne.[57]

[54] LG Bonn, Urteil vom 11. November 2020 – Az. 29 OWi 1/20 LG.
[55] Vgl. Entschließung der 97. Konferenz der DSK vom 3. April 2019.
[56] LG Berlin, Beschluss vom 18. Februar 2021 – 526 OWi LG 212 Js-OWi 1/20 (1/20).
[57] LG Berlin, ebenda, Rn. 20.

Aufnahme weiterer Befugnisse der Aufsichtsbehörden entsprechend dem GWB

Seitens der DSK wird die Aufnahme von Verweisen auf mehrere Vorschriften des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) in § 41 Absatz 1 BDSG angeregt, um die Befugnisse der Datenschutzaufsichtsbehörden in Bußgeldverfahren zu stärken.

So solle insbesondere eine Auskunftspflicht von Unternehmen hinsichtlich ihrer wirtschaftlichen Verhältnisse entsprechend § 59 GWB bzw. § 82b i. V. m. § 59 GWB ergänzt werden. Die Kenntnis der Umsätze eines Unternehmens sei erforderlich, um entsprechend Artikel 83 Absatz 4 bis 6 DSGVO die Bußgeldhöhe bestimmen zu können. Die praktischen Erfahrungen hätten gezeigt, dass Unternehmen ihre Umsätze oft nicht offenlegten und es für Aufsichtsbehörden regelmäßig schwierig bis unmöglich sei, die Umsätze anderweitig zu ermitteln. Zusätzlich solle mit Verweisen auf § 81c Absatz 5 Satz 2 GWB eine klare Befugnis zur Schätzung von Umsätzen aufgenommen werden.

Weitere Befugnisse sollten durch Verweis auf entsprechende GWB-Vorschriften geschaffen werden in Bezug auf:

- Durchsuchungsbefugnisse und Duldungs-/Mitwirkungspflichten natürlicher Personen (§ 59b Absatz 3 GWB),
- die Bebußbarkeit von Verstößen gegen Auskunfts- und Mitwirkungspflichten (§ 81 Absatz 2 Nummer 6–11 GWB),
- eine wirtschaftliche Nachfolge, auf gesamtschuldnerische Haftung mehrerer Adressaten eines Bußgeldbescheids und Verjährung (§§ 81a Absatz 2–5, 81g Absatz 2 GWB),
- die Möglichkeit der Verhängung auch gegenüber Unternehmensvereinigungen, insbesondere im Falle der Zahlungsunfähigkeit (§ 81b GWB),
- eine Ausfallhaftung bei Erlöschen eines Unternehmens (§ 81e GWB) und
- die Verzinsbarkeit von Geldbußen (§ 81f GWB).

Die Übernahme von Befugnissen aus dem GWB wäre nach Auffassung der DSK sachgerecht, da der Unionsgesetzgeber sich in Bezug auf die Sanktionsregelungen der DSGVO am Kartellrecht orientiert habe.

Die DSK führt insgesamt einen Bedarf nach mehr bzw. passgenaueren Befugnissen im Bußgeldverfahren an.

Klarstellend sei zunächst darauf hingewiesen, dass sich die Befugnisse der Aufsichtsbehörden nach Artikel 58 Absatz 1 DSGVO nur auf Maßnahmen im Rahmen von Verwaltungsverfahren vor Einleitung eines Bußgeldverfahrens beziehen. Die Befugnisse im Rahmen von Bußgeldverfahren sind im deutschen Recht mit § 41 BDSG abschließend geregelt.

Eine Ergänzung des § 41 BDSG um weitere Befugnisse der Datenschutzaufsichtsbehörden im Bußgeldverfahren bedarf einer umfassenden Prüfung, die auf Grundlage der Rückmeldungen im Rahmen der Evaluierung allein noch nicht abschließend vorgenommen werden kann. Zu berücksichtigen sein wird dabei insbesondere, dass das GWB in den §§ 59 ff. (soweit diese gemäß § 82b GWB in Bußgeldverfahren nach dem GWB entsprechend gelten) Verpflichtungen der von einem Verwaltungs- oder Bußgeldverfahren Betroffenen zur Mitwirkung an den Ermittlungen regelt. Das Kartellrecht stellt insoweit eine Sondermaterie gegenüber dem sonstigen Ordnungswidrigkeitenrecht dar. Insofern wird zu klären sein, ob und an welchen Stellen sich ein gesetzgeberischer Handlungsbedarf ergibt und ob und inwieweit sich GWB-Regelungen hierfür als Vorbild eignen.

Das BMI ist zu diesem Themenkomplex mit den Datenschutzaufsichtsbehörden bereits in einen weiteren Austausch eingetreten, um zunächst die Bedarfe aus Sicht der Verfolgungspraxis weiter aufzuklären, und wird einen gesetzgeberischen Handlungsbedarf unter Einbeziehung des Bundesministeriums für Justiz und Verbraucherschutz (BMJV) prüfen. Dabei sind auch die Belange der von Ordnungswidrigkeitenverfahren Betroffenen einzubeziehen.

Anwendbarkeit des Opportunitätsprinzips

§ 41 Absatz 2 Satz 1 BDSG verweist hinsichtlich des Bußgeldverfahrens auch auf § 47 OWiG und damit auf das im Bußgeldverfahren geltende Opportunitätsprinzip. In Bezug darauf wird vereinzelt vorgetragen, dass der Verweis auch auf § 47 OWiG mit der DSGVO nicht vereinbar und § 41 BDSG insoweit unionsrechtswidrig sei, beziehungsweise die Anwendbarkeit des Opportunitätsprinzips in datenschutzrechtlichen Bußgeldverfahren durch den Gesetzgeber ausdrücklich klargestellt werden sollte.

Die Bedenken hinsichtlich einer Unionsrechtswidrigkeit des § 41 BDSG, soweit er auch auf § 47 OWiG verweist, werden nicht geteilt. Die DSGVO selbst enthält Formulierungen, die Offenheit für Ermessen erkennen lassen (vgl. Artikel 58 Absatz 2: „…Abhilfebefugnisse, die es ihr gestatten… “; engl.: „…shall have the following corrective powers…“; frz.: „…dispose du pouvoir d'adopter toutes les mesures correctrices suivantes…“; sowie Artikel 83 Absatz 2 Satz 2: „Bei der Entscheidung über die Verhängung einer Geldbuße…“; engl.: „When deciding whether to impose an administrative fine…“; frz.: „Pour décider s'il y a lieu d'imposer une amende administrative…“). Anhaltspunkte dafür, dass der Verordnungsgeber die Datenschutzaufsichtsbehörden zur Verfolgung und Ahndung jedes einzelnen Verstoßes zwingen wollte, sind der DSGVO nicht zu entnehmen. Dies wäre in der Praxis auch mit gravierenden Konsequenzen für die Handlungsfähigkeit der Aufsichtsbehörden verbunden.

Der Gesetzgeber hat dementsprechend § 47 OWiG nicht aus dem Verweis in § 41 Absatz 2 Satz 1 BDSG ausgenommen. Eine explizite Klarstellung der entsprechenden Geltung von § 47 OWiG ist darüber hinaus nicht erforderlich; eine solche würde im Übrigen das Risiko

bergen, Folgefragen hinsichtlich der Geltung weiterer, aber nicht explizit benannter Normen des OWiG hervorzurufen.

5.7.2.4. Rückmeldungen zu § 41 Absatz 1 Satz 3 BDSG

Zu § 41 Absatz 1 Satz 3 BDSG wird die Aufteilung der gerichtlichen Zuständigkeit von Amts- und Landgerichten kritisiert und vorgeschlagen, die Zuständigkeit nur den Amts- bzw. nur den Landgerichten zu übertragen.

Mit Beschluss vom 15. November 2018 hat die 89. Konferenz der Justizministerinnen und Justizminister die Bundesregierung aufgefordert, zeitnah einen Gesetzentwurf vorzulegen, der die erstinstanzliche Zuständigkeit der Landgerichte in datenschutzrechtlichen Bußgeldsachen durch Streichung der Regelung des § 41 Absatz 1 Satz 3 BDSG wieder abschafft, und damit eine vollständige Zuweisung aller datenschutzrechtlichen Bußgeldverfahren an die Amtsgerichte vorgeschlagen. Diese wären in Bußgeldverfahren ausreichend erfahren. Die singuläre Zuständigkeitsbestimmung der Landgerichte in Bußgeldsachen in § 41 Absatz 1 Satz 3 BDSG werfe bisher ungelöste Fragen auf, insbesondere hinsichtlich der Besetzung, des Verfahrens und des Rechtswegs. Zudem bestehen nach Auffassung der Justizministerinnen und Justizminister keine Besonderheiten des Datenschutzrechts, die es geboten erscheinen lassen, in diesem Bereich ab einer bestimmten Bußgeldhöhe die ansonsten nicht mit erstinstanzlichen Bußgeldsachen befassten Landgerichte über einen Einspruch gegen den Bußgeldbescheid entscheiden zu lassen.

Die DSK spricht sich demgegenüber für eine Herabsetzung des Schwellenwertes in § 41 Absatz 1 Satz 3 BDSG für die Zuständigkeit der Landgerichte aus. Dies ermögliche eine Spezialisierung der Richterinnen und Richter und trage der Komplexität der Materie Rechnung. So gäbe es auch in Kartell- und Wirtschaftsstrafsachen eigene spezialisierte Kammern und speziell in Kartellrechtssachen eine Sonderzuweisung an die Oberlandesgerichte in erster Instanz. Zwar werde anerkannt, dass die Amtsgerichte den Großteil der Bußgeldverfahren bearbeiteten, hier ginge es aber nicht um Straßenverkehrsverstöße, sondern um unionsweit höchst relevante Verfahren zum Schutz des freien Datenverkehrs und der Privatsphäre der Bürgerinnen und Bürger.

Praktische Probleme bei der Bearbeitung von datenschutzrechtlichen Bußgeldverfahren durch die Amtsgerichte wurden nicht zurückgemeldet und sind dem BMI nicht bekannt.

Ein Bedarf für eine Änderung des § 41 Absatz 1 Satz 3 BDSG dahingehend, dass eine Zuweisung datenschutzrechtlicher Bußgeldverfahren auch unterhalb einer festgesetzten Geldbuße von einhunderttausend Euro an die Landgerichte erfolgt, ergibt sich insgesamt nicht. Eine erweiterte Zuweisung an die Landgerichte erscheint nicht angebracht, da datenschutzrechtliche Bußgeldverfahren – anders als etwa Kartell- oder Wirtschaftsstrafsachen – nicht zwangsläufig komplex sind, sondern auch einen überschaubaren Rahmen haben können und damit nicht bei den Landgerichten bearbeitet werden müssen. Nach

Auskunft der Aufsichtsbehörden ist davon auszugehen, dass die Mehrheit der Bußgeldsachen derzeit wegen einer relativ geringen Bußgeldhöhe in die Zuständigkeit der Amtsgerichte fällt. Dies entspricht der gesetzgeberischen Intention, die bußgeldrechtliche Erfahrung der Amtsgerichte grundsätzlich zu nutzen.

5.7.2.5. Rückmeldungen zu § 42 BDSG

Reichweite des Beweisverwendungsverbots

Vereinzelt wird angemerkt, dass unklar sei, ob es der betroffenen Person durch § 42 Absatz 4 BDSG verwehrt sei, die Benachrichtigung oder Einzelheiten aus der Benachrichtigung als Beweismittel in einem Schadensersatzprozess gegen den Verantwortlichen einzubringen.

Diesen Bedenken kann bereits der Wortlaut der Vorschrift entgegengehalten werden. Danach bezieht sich § 42 Absatz 4 BDSG nur auf Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden. Allein im Strafverfahren steht die Verwendung als Beweismittel unter einem Einwilligungsvorbehalt. Der Einführung der Information als Beweismittel in einem Schadensersatzprozess steht die Vorschrift daher nicht entgegen.

Aus dem Kreis der Bundesbehörden wird angemerkt, dass die Meldepflicht im Hinblick auf den Nemo-tenetur-Grundsatz problematisch sei. Zwar trüge § 42 Absatz 4 BDSG diesem Umstand im Bereich des Strafverfahrens Rechnung, allerdings sei eine Ausweitung auf Disziplinarverfahren und interne arbeitsrechtliche Ermittlungen erforderlich.

Unabhängig davon, ob die Regelung eines entsprechenden Beweisverwendungsverbots in dienst- und arbeitsrechtlichen Verfahren umsetzbar wäre, besteht aus Sicht des BMI für eine solche Regelung im BDSG kein Raum. Im BDSG sind in Umsetzung der DSGVO und der Richtlinie (EU) 2016/680 strafrechtliche Sanktionen für bestimmte Datenschutzverstöße vorgesehen. Das Beweisverwendungsverbot in § 42 Absatz 4 BDSG steht daher im Zusammenhang mit dem Strafverfahren. Dienst- oder arbeitsrechtliche Bestimmungen enthält das BDSG nicht. Ein etwaiges Beweisverwendungsverbot für dienst- oder arbeitsrechtliche Verfahren wäre daher im jeweiligen Fachrecht zu regeln.

5.7.2.6. Rückmeldungen zu § 43 BDSG

Seitens der DSK wird der Wunsch geäußert, § 43 Absatz 3 BDSG dahingehend zu ändern, dass die Verhängung von Geldbußen auch gegenüber öffentlichen Stellen des Bundes möglich wird. Dies habe eine abschreckende Wirkung gegenüber diesen Stellen, ermögliche es, die Schwere eines Verstoßes besser zum Ausdruck zu bringen, und diene damit der Sicherstellung der Einhaltung der DSGVO sowie der Gleichbehandlung öffentlicher und nichtöffentlicher Stellen.

Das BMI hat das Anliegen geprüft und ist zu dem Ergebnis gekommen, dass eine solche Anpassung des § 43 Absatz 3 BDSG nicht sachgerecht erscheint und der Argumentation der DSK insoweit nicht gefolgt werden kann:

Der oder die BfDI kann Datenschutzverstöße durch öffentliche Stellen des Bundes nicht nur durch Bußgelder ahnden. Vielmehr stehen ihr oder ihm nach Artikel 58 Absatz 2 DSGVO und § 16 BDSG grundsätzlich hinreichende Abhilfebefugnisse zur Verfügung, etwa die Möglichkeit der Verwarnung, Beanstandung oder Anweisung des Verantwortlichen oder Auftragsverarbeiters sowie der Beschränkung oder des Verbots der Verarbeitung. Diese Befugnisse ermöglichen nach Auffassung des BMI die effektive Durchsetzung der Einhaltung der datenschutzrechtlichen Vorgaben. Die Schwere eines Verstoßes kann durch die Reichweite der ergriffenen Maßnahme – von der Beanstandung oder Verwarnung bis zum Verbot – hinreichend abgebildet werden.

Die Verhängung von Bußgeldern gegenüber öffentlichen Stellen des Bundes hätte ferner letztlich lediglich eine Verschiebung von Haushaltsmitteln des Bundes zwischen öffentlichen Stellen des Bundes zur Folge. Insofern besteht auch bereits keine sachliche Vergleichbarkeit zu nichtöffentlichen Stellen, die eine Gleichbehandlung rechtfertigen könnte.

5.7.3. Schlussfolgerungen

Aus den Rückmeldungen zu § 41 BDSG ist noch eine gewisse Unsicherheit hinsichtlich der Geltung bestimmter Vorschriften des OWiG im Verhältnis zur DSGVO erkennbar. Dies kann zum einen als eine übliche und typische Folge einer gesetzlichen Neuregelung eingeordnet werden. Zum anderen ist zu berücksichtigen, dass in Hinblick darauf, dass BDSG und DSGVO noch relativ „neuen Datums“ sind, Bußgeldverfahren erst in den letzten Monaten zunehmend Gegenstand von behördlichen und gerichtlichen Entscheidungen werden.

Insbesondere in Bezug auf die von der DSK vorgetragenen Bedarfe nach weiteren Befugnissen im Bußgeldverfahren wird nun eine weitere Prüfung im Austausch mit den Datenschutzaufsichtsbehörden erfolgen müssen, um mögliche Bedarfe und etwaige gesetzgeberische Handlungsoptionen ermitteln zu können.

5.8. Aufgaben und Befugnisse der oder des BfDI, Zusammenarbeit in europäischen Angelegenheiten, Rechtsbehelfe sowie Bestimmung der zuständigen Aufsichtsbehörde – §§ 14, 16 bis 20, 40 Absatz 2 BDSG

5.8.1. Zielsetzung und Gegenstand der Regelungen

Mit den §§ 14, 16 bis 20 BDSG werden die Aufgaben und Befugnisse der oder des BfDI sowie die Vertretung im Europäischen Datenschutzausschuss (EDSA), die zentrale Anlaufstelle und die Zusammenarbeit der Aufsichtsbehörden auch in Angelegenheiten der Europäischen Union sowie der Rechtsschutz gegen Entscheidungen der Aufsichtsbehörden geregelt. § 40 Absatz 2 BDSG dient der Bestimmung der zuständigen Aufsichtsbehörde.

§ 14 BDSG bestimmt in seinem Absatz 1 neben den in der DSGVO genannten Aufgaben die Aufgaben der oder des BfDI zum Zwecke der Umsetzung des Artikels 46 der Richtlinie (EU) 2016/680. Absatz 2 regelt in Umsetzung des Artikels 47 Absatz 3 der Richtlinie (EU) 2016/680 sowie beruhend auf Artikel 58 Absatz 4 und 6 DSGVO und in Konkretisierung des Artikels 58 Absatz 3 Buchstabe b DSGVO das Recht der oder des BfDI zur Abgabe von Stellungnahmen sowie die Pflicht der oder des BfDI, auf Ersuchen des Bundestages oder einer seiner Ausschüsse oder der Bundesregierung Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nachzugehen. Absatz 3 und 4 setzen Artikel 46 Absatz 2 bis 4 der Richtlinie (EU) 2016/680 in Übereinstimmung mit den Vorgaben von Artikel 57 DSGVO um.

§ 16 Absatz 1 BDSG verweist für die Befugnisse der oder des BfDI und deren Ausübung im Anwendungsbereich der DSGVO auf Artikel 58 DSGVO („Befugnisse"). § 16 Absatz 2 BDSG regelt die Befugnisse der oder des BfDI bei Datenverarbeitungen außerhalb des Anwendungsbereichs der DSGVO. Dies betrifft sowohl Datenverarbeitungen öffentlicher Stellen, für die gemäß § 1 Absatz 8 BDSG die DSGVO entsprechend anzuwenden ist, als auch Datenverarbeitungen im Anwendungsbereich der Richtlinie (EU) 2016/680. § 16 Absatz 3 bis 5 BDSG gilt sowohl für den Anwendungsbereich der DSGVO und der Richtlinie (EU) 2016/680 als auch für Datenverarbeitungen außerhalb des Geltungsbereichs des Unionsrechts.

In Umsetzung des Regelungsauftrags der Artikel 51 und 68 DSGVO sowie des Erwägungsgrunds 119 zur DSGVO bestimmt § 17 Absatz 1 BDSG den oder die BfDI zum gemeinsamen Vertreter der Aufsichtsbehörden der Bundesrepublik Deutschland im EDSA und regelt zugleich das Verfahren der Wahl eines Vertreters aus dem Kreis der Leiter der Landesaufsichtsbehörden als dessen Stellvertreter; zugleich wird die Einrichtung einer zentralen Anlaufstelle bei dem oder der BfDI bestimmt.

§ 17 Absatz 2 BDSG überträgt dem oder der BfDI als gemeinsamen Vertreter die Verhandlungsführung und das Stimmrecht im EDSA. In Angelegenheiten, für die den Ländern das alleinige Gesetzgebungsrecht zusteht oder die Einrichtung oder das Verfahren von Landesbehörden betroffen ist, stehen diese Rechte hingegen dem Länder-Stellvertreter zu.

§ 18 BDSG setzt den Regelungsauftrag des Artikels 51 Absatz 3 DSGVO um: In Angelegenheiten der EU ist die wirksame Beteiligung aller nationalen Aufsichtsbehörden und die Einhaltung der Regeln für das Kohärenzverfahren durch alle nationalen Aufsichtsbehörden mit entsprechenden Vorschriften innerstaatlich sicherzustellen. Er verpflichtet die Aufsichtsbehörden von Bund und Ländern zur Zusammenarbeit und regelt das Verfahren der Zusammenarbeit der Aufsichtsbehörden. Dabei geht die Gesetzesbegründung zu § 18 BDSG erkennbar davon aus, dass Artikel 51 Absatz 3 DSGVO ebenso wie die darauf beruhenden Regelungen des § 18 BDSG sowohl das Kooperationsverfahren (Artikel 60 ff. DSGVO) als auch das Kohärenzverfahren (Artikel 63 ff. DSGVO) umfassen.[58]

Nach den Verfahrensregelungen in § 18 Absatz 1 und 2 BDSG zur Findung eines gemeinsamen Standpunkts sollen die Aufsichtsbehörden von Bund und Ländern möglichst Einvernehmen erzielen. Gelingt dies nicht, legen die federführende Behörde und in Ermangelung einer solchen der gemeinsame Vertreter und sein Länder-Stellvertreter einen Vorschlag vor. Vermögen diese sich nicht auf einen Vorschlag zu einigen, obliegt das Vorschlagsrecht – mit Ausnahme der Angelegenheiten, für die den Ländern die alleinige Gesetzgebungskompetenz zusteht oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen – dem gemeinsamen Vertreter. Die Aufsichtsbehörden von Bund und Ländern können sich dann aber mit einfacher Mehrheit auf einen anderen Standpunkt verständigen. § 18 Absatz 3 BDSG zufolge ist der Verhandlungsführer im EDSA an den gemeinsamen Standpunkt gebunden.

Ebenfalls beruhend auf dem Regelungsauftrag des Artikels 51 Absatz 3 DSGVO, ein ordnungsgemäßes Kohärenzverfahren sicherzustellen, und anknüpfend an den Begriff der zuständigen federführenden Aufsichtsbehörde in Artikel 56 Absatz 1 DSGVO trifft § 19 BDSG – ergänzend zu den Verfahrensregelungen des § 18 BDSG – Regelungen dazu, welche nationale Aufsichtsbehörde federführende Aufsichtsbehörde im Rahmen der Verfahren nach Artikel 60 ff. DSGVO und Artikel 63 ff. DSGVO ist. § 19 Absatz 1 BDSG knüpft dabei zunächst in Übereinstimmung mit Artikel 56 Absatz 1 DSGVO an den Begriff der Hauptniederlassung im Sinne des Artikels 4 Nummer 16 DSGVO bzw. der einzigen Niederlassung an. § 19 Absatz 1 BDSG bestimmt zudem, dass bei Meinungsverschiedenheiten über die federführende Zuständigkeit das in § 18 Absatz 2 BDSG zur Erlangung eines gemeinsamen Standpunkts geregelte Verfahren entsprechende Anwendung findet. § 19 Absatz 2 BDSG regelt schließlich, wie im Falle einer Beschwerde einer betroffenen Person zu verfahren ist.

§ 20 BDSG dient sowohl der Durchführung des Artikels 78 Absatz 1 DSGVO als auch der Umsetzung des Artikels 53 Absatz 1 der Richtlinie (EU) 2016/680. Danach hat jede natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

[58] BT-Drs. 18/11325, S. 91.

§ 40 BDSG trifft Regelungen zur Zuständigkeit und zu den Befugnissen der Landesaufsichtsbehörden und orientiert sich hierbei an § 38 BDSG a. F. § 40 Absatz 2 BDSG bestimmt zunächst unter Inbezugnahme auf Artikel 4 Nummer 16 DSGVO, dass im Falle mehrerer inländischer Niederlassungen die Aufsichtsbehörde am Ort der Hauptniederlassung (federführend) zuständig ist und zudem, dass im Streitfall über die Zuständigkeit das in § 18 Absatz 2 BDSG zur Erlangung eines gemeinsamen Standpunkts geregelte Verfahren entsprechende Anwendung findet.

5.8.2. Empirische Ergebnisse und Bewertungen

5.8.2.1. Rückmeldungen und Bewertung zu § 14 BDSG

Aus der Wirtschaft wird vereinzelt der Wunsch vorgetragen, die Beratungs- und Unterstützungsfunktion der Datenschutzaufsichtsbehörden im Vergleich zu ihrer Sanktionsbefugnis im BDSG zu stärken.

Die umfangreichen Aufgaben der Datenschutzaufsichtsbehörden sind in Artikel 57 DSGVO und dazu ergänzend für die Landesdatenschutzaufsichtsbehörden in § 40 BDSG sowie für den oder den BfDI in § 14 BDSG geregelt. Danach obliegen den Aufsichtsbehörden bereits nach geltendem Recht bestimmte Aufklärungs-, Sensibilisierungs-, Unterstützungs- und Beratungspflichten. Zwar sind die Datenschutzaufsichtsbehörden nicht zu einer umfassenden Beratung verpflichtet. Es liegt aber in ihrem Ermessen, über die Erfüllung ihrer Pflichtaufgaben hinaus im Rahmen der vorhandenen Kapazitäten datenschutzrechtliche Beratung etwa für Private, Vereine und Wirtschaftsunternehmen anzubieten. Die Beratung ist nach Kenntnis des BMI bereits derzeit ein fester Bestandteil der aufsichtsbehördlichen Praxis vieler Aufsichtsbehörden. Eine über die jetzigen gesetzlichen Regelungen hinausgehende allgemeine Beratungspflicht der Aufsichtsbehörden könnte nach Auffassung des BMI jedoch im Hinblick auf die vorhandenen personellen Kapazitäten zu einer Überforderung einzelner Aufsichtsbehörden führen.

Nach der Konzeption der DSGVO und des BDSG obliegt die Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters hinsichtlich aller datenschutzrechtlichen Fragen zudem in erster Linie dem betrieblichen bzw. behördlichen Datenschutzbeauftragten. Die Hauptaufgabe der Aufsichtsbehörden ist es nach DSGVO und BDSG hingegen, die Anwendung der datenschutzrechtlichen Vorschriften zu überwachen.

5.8.2.2. Rückmeldungen und Bewertung zu § 16 BDSG

Zu § 16 BDSG sind vornehmlich Rückmeldungen der Datenschutzaufsichtsbehörden eingegangen. Sie zielen im Wesentlichen – wie auch schon die Rückmeldungen zu § 41 Absatz 1 BDSG – auf eine Erweiterung der Befugnisse der Aufsichtsbehörden ab.

Zwangsmittel

Die DSK schlägt vor, in § 16 BDSG eine z. B. an § 17 Absatz 1 Satz 3 des Finanzdienstleistungsaufsichtsgesetzes (FinDAG) orientierte Regelung zu treffen, die es dem oder der BfDI ermöglicht, seine Maßnahmen auch gegenüber öffentlichen Stellen des Bundes mit Zwangsmitteln durchzusetzen.

Aus § 17 des Verwaltungsvollstreckungsgesetzes (VwVG) ergibt sich, dass Zwangsmittel gegenüber öffentlichen Stellen grundsätzlich unzulässig sind und von diesem Grundsatz nur durch anderweitige gesetzliche Regelung abgewichen werden kann. Diesem Grundsatz liegt die Erwartung zugrunde, dass Behörden ihren aus dem öffentlichen Recht folgenden Verpflichtungen auch ohne Anwendung von Zwangsmitteln nachkommen werden,[59] zumal sie im Weigerungsfalle hierzu von ihrer Aufsichtsbehörde angehalten werden können[60]. Bei der Frage, ob im BDSG eine gesetzliche Ausnahme von § 17 VwVG geschaffen werden sollte, ist die datenschutzrechtliche Besonderheit zu berücksichtigen, dass der oder die BfDI (wie auch alle anderen Datenschutzaufsichtsbehörden) im Vergleich zur Rechtslage vor Geltung der DSGVO und vor Inkrafttreten des neuen BDSG nunmehr über erheblich mehr Durchsetzungskraft verfügt: Die umfangreichen Untersuchungs- und Abhilfebefugnisse nach Artikel 58 Absatz 1 und 2 DSGVO gelten auch gegenüber öffentlichen Stellen. Sie gehen weit über das bloße Beanstandungsrecht des § 25 BDSG a. F. hinaus. Angesichts der nunmehr verfügbaren weitreichenden Abhilfebefugnisse der oder des BfDI wird kein zwingender Bedarf gesehen, im BDSG zusätzlich eine Ausnahmevorschrift vom Zwangsmittelverbot gegenüber öffentlichen Stellen zu schaffen.

Beschlagnahme

Es wird der Wunsch geäußert, für die Aufsichtsbehörden im BDSG ein Beschlagnahmerecht bereits im verwaltungsrechtlichen Aufsichts- und Kontrollverfahren vorzusehen, damit diese ebenso wie die Kartellbehörden (vgl. §§ 57, 58 GWB) Beweismittel bereits während der Kontrolle sicherstellen können.

Beschlagnahmen sind nach geltender Rechtslage schon nach dem Strafprozess- und Polizeirecht möglich. Ob darüber hinaus auch eine datenschutzrechtliche Regelung erforderlich ist, bedürfte sehr eingehender Prüfung. Bei dieser wäre insbesondere zu berücksichti-

[59] Vgl. *Ziemske*, Aufsichtsmaßnahmen gegen renitente Behörden, DÖV 1996, 45 (49).

[60] Fehling/Kastner/Stürmer-*Lemke*, Verwaltungsrecht, Kommentar, 5. Auflage 2021, § 17 VwVG Rn. 2; Koenig-*Fritsch*, Abgabenordnung, Kommentar, 3. Auflage 2014, § 255 Rn. 1; siehe auch BT-Drs. 1/3981, S. 9 zu § 17 VwVG: „*Der Vollzug gegen Behörden soll ausgeschlossen sein, weil es widersinnig und mit dem Ansehen der Behörden nicht vereinbar erscheint, wenn eine Behörde gegen eine andere vollstreckt.*“ sowie BT-Drs. 13/4854, S. 4 zu § 22 Absatz 3 Satz 4 ArbSchG: „*Satz 4 enthält eine Sonderregelung für den öffentlichen Dienst, die der Aufrechterhaltung seiner Funktionsfähigkeit dient und berücksichtigt, daß ein Konflikt zwischen verschiedenen Aufgabenträgern der Verwaltung aus verfassungsrechtlichen Gründen nicht mit hoheitlichen Maßnahmen gelöst werden kann.*“

gen, dass den Aufsichtsbehörden schon sehr weitreichende Untersuchungs- und Abhilfebefugnisse zustehen, die gegenüber nichtöffentlichen Stellen zudem durch die Möglichkeit empfindlicher Bußgelder flankiert werden.

Unterrichtung der Öffentlichkeit

Die DSK regt an, eine ausdrückliche Bestimmung im BDSG zu schaffen, nach der die Aufsichtsbehörden berechtigt sein sollen, Entscheidungen über Abhilfemaßnahmen und Sanktionen, die wegen Datenschutzverstößen getroffen wurden, zu veröffentlichen (vgl. § 53 Absatz 5 GWB, § 124 Wertpapierhandelsgesetz).

Die Befugnis der Datenschutzaufsichtsbehörden, zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, Stellungnahmen an die Öffentlichkeit zu richten, ergibt sich unmittelbar aus Artikel 58 Absatz 3 Buchstabe b DSGVO. Eine Öffnungsklausel zur weiteren Ausgestaltung der Voraussetzungen der Öffentlichkeitsarbeit im nationalen Recht enthält Artikel 58 Absatz 3 Buchstabe b DSGVO nicht. Daher vermag das BMI der Anregung der DSK nicht zu folgen.

Zudem veröffentlichen die Aufsichtsbehörden auf der Grundlage des Artikels 59 DSGVO ihre Tätigkeitsberichte, in denen die gemeldeten Verstöße und die Arten der getroffenen Maßnahmen dargestellt werden können.

Abbau von Videoüberwachungsanlagen

Es wird vorgeschlagen, für die Aufsichtsbehörden eine Befugnis einzuführen, den Abbau von Videoüberwachungsanlagen anzuordnen.

Hintergrund ist die Frage, wie weit die nach Artikel 58 Absatz 2 DSGVO bestehenden Abhilfebefugnisse reichen. Sie ist damit genereller Natur und nicht auf Videoüberwachungsanlagen beschränkt. Die Frage ist nicht durch den nationalen Gesetzgeber, sondern durch Auslegung des Artikels 58 Absatz 2 DSGVO und nötigenfalls abschließend durch gerichtliche Entscheidung zu beantworten.

Abhilfebefugnisse außerhalb des Geltungsbereichs der DSGVO

Die DSK weist darauf hin, dass die Aufsichtsbehörden generell die Möglichkeit haben sollten, verbindliche Anordnungen zu treffen. Im Bereich der Richtlinie (EU) 2016/680 sowie außerhalb des Geltungsbereichs des EU-Rechts bleibe der BfDI nach § 16 Absatz 2 BDSG auf die Instrumente der Warnung und der Beanstandung beschränkt. Artikel 47 Absatz 2 der Richtlinie (EU) 2016/680 enthalte die Verpflichtung, wirksame Abhilfebefugnisse zu gewähren. Ohne ergänzende fachgesetzliche Regelung seien diese Vorgaben unzureichend umgesetzt, weshalb eine einheitliche Regelung im BDSG vorzugswürdig sei.

Nach Auffassung des BMI stehen der oder dem BfDI grundsätzlich ausreichende Abhilfebefugnisse im Bereich der Richtlinie (EU) 2016/680 und außerhalb des Geltungsbereichs

des EU-Rechts zur Verfügung. Nach § 16 Absatz 2 BDSG kann die oder der BfDI die zuständigen Behörden vor drohenden Datenschutzverstößen warnen oder festgestellte Datenschutzverstöße beanstanden. Abgesehen davon kann die oder der BfDI gemäß § 15 BDSG in seinen Tätigkeitsberichten über Datenschutzverstöße öffentlicher Stellen des Bundes informieren und verfügt über sonstige nicht regelungsbedürftige Möglichkeiten, die an Recht und Gesetz gebundenen Verantwortlichen auf möglicherweise rechtswidrige Verarbeitungen aufmerksam zu machen. Im Übrigen stehen die allgemeinen Vorschriften des BDSG einer Konkretisierung oder weiteren Ausgestaltung der aufsichtsbehördlichen Abhilfebefugnisse in den jeweiligen Fachgesetzen nicht entgegen.[61] Vielmehr hat der Gesetzgeber sich in bestimmten Bereichen für weiterreichende Regelungen entschieden und diese spezialgesetzlich verankert. So sieht etwa § 69 Absatz 2 des Bundeskriminalamtgesetzes (BKAG) die Befugnis der oder des BfDI vor, verbindliche Anordnungen gegenüber dem Bundeskriminalamt bei erheblichen Datenschutzverstößen zu erlassen.[62]

Für das BMI ist nicht erkennbar, dass die Richtlinie (EU) 2016/680 insoweit unzureichend umgesetzt worden wäre. Der EU-Gesetzgeber hat die Abhilfebefugnisse in der Richtlinie (EU) 2016/680 im Hinblick auf die im Bereich der Polizei und der Strafverfolgung bestehenden besonderen fachlichen Bedürfnisse im Vergleich zur DSGVO unterschiedlich ausgestaltet und dem nationalen Gesetzgeber insoweit größere Flexibilität bei der Umsetzung eingeräumt.[63] Der Bundesgesetzgeber hat als aufsichtsbehördliches Mittel in § 16 Absatz 2 Satz 4 BDSG die Warnung vorgesehen, die in Artikel 47 Absatz 2 Buchstabe a der Richtlinie (EU) 2016/680 als eine Möglichkeit für wirksame Abhilfebefugnisse benannt ist. Abgesehen davon hat der Gesetzgeber in § 16 Absatz 2 Satz 1 BDSG mit dem aus § 25 BDSG a. F. bekannten Instrument der Beanstandung eine weitere wirksame Abhilfebefugnis im Sinne des Artikels 47 Absatz 2 der Richtlinie (EU) 2016/680 geschaffen.[64] Die weiteren in Artikel 47 Absatz 2 Buchstabe b und c der Richtlinie (EU) 2016/680 beispielhaft aufgezählten Befugnisse, d.h. das Anordnungsrecht und die Möglichkeit, eine Datenverarbeitung vorübergehend oder endgültig zu untersagen, können – wie bereits dargestellt- erforderlichenfalls im Fachrecht vorgesehen werden.[65] Aus Sicht des BMI ist das Fachrecht hierfür der geeignetere Regelungsstandort, weil durch eine fachgesetzliche Regelung besser gewährleistet werden kann, dass ggf. weitergehende Abhilfebefugnisse der oder des BfDI mit der Sensibilität und Komplexität der Verarbeitung sowie dem Bedürfnis nach der Verfügbarkeit rechtmäßig erhobener Daten und Datenverarbeitungsanlagen im Bereich der Polizei und Strafverfolgung im Einklang stehen.[66] Dies gilt entsprechend für den nicht EU-rechtlich erfassten Bereich von Verarbeitungen zu Zwecken außerhalb der DSGVO

[61] Vgl. BT-Drs. 18/11325, S. 88.
[62] Vgl. auch BT-Drs. 18/11163, S. 130.
[63] BT-Drs. 18/11325, S. 88.
[64] Vgl. BT-Drs. 18/11325, S. 88.
[65] Siehe auch BT-Drs. 18/11325, S. 88.
[66] Vgl. BT-Drs. 18/11325, S. 88.

und der Richtlinie (EU) 2016/680.[67] Ein Bedürfnis zur Regelung weitergehender Abhilfebefugnisse der oder des BfDI im BDSG besteht aus Sicht des BMI daher nicht.

Untersuchungsbefugnisse außerhalb des Geltungsbereichs der DSGVO

Die DSK regt eine Klarstellung der nach Artikel 47 Absatz 1 der Richtlinie (EU) 2016/680 erforderlichen Untersuchungsbefugnisse des BfDI an. Auch fehle es an einer ausdrücklichen Befugnis des BfDI, Zugang zu Gebäuden, Anlagen und Daten oder Auskünfte zu verlangen.

Nach Artikel 47 Absatz 1 der Richtlinie (EU 2016/680 ist durch Rechtsvorschriften vorzusehen, dass jede Aufsichtsbehörde über wirksame Untersuchungsbefugnisse verfügt, die es zumindest erlauben müssen, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten, die verarbeitet werden, und auf alle Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten. Der Gesetzgeber ist bei der Umsetzung der Richtlinie im BDSG über diese Vorgaben hinausgegangen. § 16 Absatz 4 BDSG gewährt der oder dem BfDI nicht nur ein umfassendes Informationsrecht, sondern ein Zugangsrecht zu den Grundstücken und Diensträumen einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die für die Erfüllung ihrer oder seiner Aufgaben erforderlich sind. Zu diesen Aufgaben gehören nach § 14 Absatz 1 Satz 1 Nummer 8 BDSG auch „*Untersuchungen über die Anwendung dieses Gesetzes oder sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften*“. Mit Blick auf die bestehenden Regelungen erscheinen weitere Klarstellungen in Bezug auf die Untersuchungs- und Zugangsbefugnisse der oder des BfDI in § 16 BDSG nicht geboten.

5.8.2.3. Rückmeldungen und Bewertung zu § 17 BDSG

Auffangregelung zur Bestellung des Stellvertreters im Europäischen Datenschutzausschuss

Sowohl aus dem behördlichen Bereich als auch aus der Wirtschaft wird vielfach angeregt, in § 17 BDSG eine Regelung für den Fall aufzunehmen, dass der Bundesrat keinen Stellvertreter des Gemeinsamen Vertreters im EDSA wählt.

Da die erstmalige Wahl des Stellvertreters durch den Bundesrat erst am 25. Juni 2021 und damit mehr als drei Jahre nach Inkrafttreten des BDSG erfolgt ist, erscheint eine Regelung, die eine Vakanz der Stellvertreterposition zukünftig verhindert, durchaus sinnvoll. Es wird daher zu überlegen sein, wie eine entsprechende Ergänzung des § 17 BDSG aussehen könnte. Denkbar wäre beispielsweise, für den Fall, dass die Wahl des Stellvertreters nicht

[67] BT-Drs. 18/11325, S. 88.

innerhalb einer bestimmten Zeit erfolgt, in der Vorschrift des § 17 BDSG einen Automatismus vorzusehen, durch den eine angemessene Vertretung der Länder sichergestellt wird. Diese könnte beispielsweise an den jeweiligen Bundesratsvorsitz geknüpft werden.

Anknüpfung der federführenden Zuständigkeit an die Verwaltungskompetenz

Teilweise wird aus dem behördlichen Bereich auch vorgeschlagen, die Regelung des § 17 Absatz 2 BDSG neu auszugestalten. Statt die federführende Zuständigkeit des Stellvertreters an die alleinige Gesetzgebungskompetenz der Länder bzw. an die Einrichtung oder das Verfahren von Landesbehörden zu knüpfen, solle der Länder-Stellvertreter immer dann Verhandlungsführung und Stimmrecht im EDSA innehaben, wenn die Länder nach Artikel 83 GG für den Vollzug einer gesetzlichen Regelung zuständig sind.

Die Außenvertretung der deutschen Aufsichtsbehörden ist in § 17 BDSG – gleiches gilt für § 18 Absatz 2 BDSG – in Anlehnung an die Vorschriften im Gesetz über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union (EUZBLG) entsprechend dem Grundsatz der Außenvertretung des Bundes, wie er Artikel 23 GG zugrunde liegt, normiert. Dieses Verfahren hat sich bewährt und sollte hinsichtlich der Vertretung Deutschlands im EDSA nicht anders ausgestaltet werden. Soweit es nicht nur um die Verhandlungsführung und die Ausübung des Stimmrechts im EDSA, sondern um die Herbeiführung eines gemeinsamen inhaltlichen Standpunkts nach § 18 Absatz 1 und 2 BDSG geht, haben Aufsichtsbehörden der Länder zudem die Möglichkeit, sich mit einfacher Mehrheit über den Vorschlag der oder des BfDI als gemeinsamen Vertreter hinwegzusetzen (siehe § 18 Absatz 2 Satz 4 BDSG). An den so gewonnenen gemeinsamen Standpunkt ist der deutsche Vertreter im EDSA zudem gem. § 18 Absatz 3 BDSG gebunden. Damit erscheint nicht nur die Vertretung Deutschlands im EDSA in § 17 Absatz 2 BDSG i. V. m. § 18 BDSG sachgerecht und praktikabel geregelt, sondern zudem auch das Spannungsverhältnis zwischen Bund und Ländern austariert und die Interessen der Länderaufsichtsbehörden angemessen berücksichtigt.

5.8.2.4. Rückmeldungen und Bewertung zu § 18 BDSG

Zwischen der Mehrheit der Landesdatenschutzbeauftragten einerseits und dem BfDI sowie einer Minderheit der Landesdatenschutzbeauftragten andererseits ist streitig, ob ein gemeinsamer Standpunkt im Sinne des § 18 BDSG bereits im Rahmen des Kooperationsverfahrens (Artikel 60 ff. DSGVO) oder erst im Rahmen des – diesem nachgeschalteten – Kohärenzverfahrens (Artikel 63 ff. DSGVO) herbeizuführen ist. Im Normtext des § 18 BDSG wird dies nicht explizit geregelt; die Begründung des § 18 BDSG geht jedoch von Ersterem aus.[68]

[68] BT-Drs. 18/11325, S. 90: *„§ 18 Absatz 1 erfasst alle Fallgestaltungen, in denen aufgrund der Wirkung für und gegen die übrigen deutschen Datenschutzbehörden und deren Vollzugsentscheidungen eine inhaltliche*

Nach Auffassung des BfDI sollte künftig vermieden werden, dass im Rahmen des Kooperationsverfahrens im Wege des Einspruchs gegen einen Beschlussentwurf einer Datenschutzaufsichtsbehörde eines anderen Mitgliedstaates zunächst von einzelnen deutschen Landesdatenschutzaufsichtsbehörden eine bestimmte Rechtsposition vertreten wird und im anschließenden Kohärenzverfahren – bedingt dadurch, dass diese Landesdatenschutzaufsichtsbehörde bei der Herbeiführung eines gemeinsamen Standpunkts im Sinne des § 18 BDSG unterlegen ist – Deutschland sodann eine andere Rechtsposition einnimmt. Dies sei für die anderen Mitgliedstaaten irritierend und für das Ansehen Deutschlands im EDSA abträglich. Es sei daher stets bereits im Kooperationsverfahren, also bereits vor Einlegung eines Einspruchs, ein gemeinsamer Standpunkt im Sinne des § 18 BDSG herbeizuführen.

Die Mehrheit der Landesdatenschutzbeauftragten möchte dagegen das bisherige Vorgehen beibehalten. Dies habe sich durchaus bewährt. Es sei nicht nur aufgrund der einzuhaltenden Fristen schwierig, sondern bedeute zudem einen unnötigen Bürokratieaufbau, wenn (bereits) im Kooperationsverfahren alle Landesaufsichtsbehörden eingebunden werden müssten. Es sei davon auszugehen, dass ohnehin nur ein Bruchteil der Verfahren in ein Kohärenzverfahren münden werden. Das Kooperationsverfahren sei ein auf Konsensfindung ausgerichtetes Verfahren, in welchem es darum gehe, im Wege des Einspruchs der betroffenen Behörden alle relevanten Aspekte in die Entscheidung einzubringen. Hier Behörden, die von der zu treffenden Entscheidung überhaupt nicht betroffen sind, mit einzubinden, sei daher auch systemwidrig.

Vor dem Hintergrund der auf beiden Seiten vorgetragenen Argumente erscheint es – auch im Sinne der Erprobung von Best Practices – angezeigt, zunächst abzuwarten, in welchem Umfang laufende Kooperationsverfahren tatsächlich in Kohärenzverfahren münden werden und ob vor diesem Hintergrund eine frühzeitigere Herbeiführung eines gemeinsamen deutschen Standpunkts tatsächlich geboten ist. Je nach tatsächlicher Entwicklung sollte sodann zur Beendigung der derzeit bestehenden Unsicherheit eine entsprechende Klarstellung im Normtext des § 18 BDSG erwogen werden. Denn die Vorschrift des § 18 BDSG erscheint insofern ambivalent, als einerseits die Begründung erkennen lässt, dass der Gesetzgeber von einem frühzeitigen gemeinsamen Standpunkt ausgegangen sein dürfte, die Frage, wann genau ein gemeinsamer Standpunkt herbeizuführen ist, aber andererseits im Normtext nicht explizit geregelt ist.

Vorabstimmung erforderlich ist, also unter anderem auch die Fälle gemäß Artikel 60 Absatz 6 der Verordnung (EU) 2016/679, in denen eine betroffene Aufsichtsbehörde Einspruch gegen den Vorschlag der federführend zuständigen Aufsichtsbehörde in einem Einzelfall einlegt."

5.8.2.5. Rückmeldungen und Bewertung zu § 19 BDSG

Unklare Zuständigkeitsregelung

In den Rückmeldungen aus dem behördlichen Bereich wird die Regelung des § 19 BDSG teilweise für nicht ganz vollständig und die Rechtslage im Hinblick auf bestimmte Sachverhalte für etwas unklar gehalten.

Einem Teil der Rückmeldungen zufolge bedürfe es einer Regelung zur Festlegung der zuständigen federführenden Datenschutzaufsichtsbehörde bezüglich international tätiger Unternehmen ohne Niederlassung in Deutschland. Weder aus § 19 BDSG – und damit im Kontext von Kooperations- und Kohärenzverfahren gemäß Artikel 60 bis 67 DSGVO – noch aus § 40 Absatz 2 BDSG lasse sich eine Zuständigkeitsregelung ableiten.

Ein Teil der Rückmeldungen sieht eine ähnliche Schwierigkeit bei international oder bundesweit tätigen Unternehmen mit mehreren Niederlassungen aber ohne (klare) Hauptniederlassung.

Das BMI versteht die Regelung des § 19 Absatz 1 BDSG so, dass Satz 1 die Fallgestaltung eines Unternehmens mit mehreren Niederlassungen (und einer Hauptniederlassung) sowie die Fallgestaltung nur einer Niederlassung betrifft, Satz 3 dagegen alle Fälle, bei denen Zweifel über die Zuständigkeit besteht, also neben den bereits in Satz 1 angesprochenen Fallgestaltungen beispielsweise auch die Fallgestaltung eines Unternehmens ohne Niederlassung sowie auch die Fallgestaltung eines Unternehmens mit mehreren Niederlassungen aber ohne eine (klare) Hauptniederlassung mit umfasst.

Vor dem Hintergrund der in den Rückmeldungen beschriebenen Unklarheiten erscheint es jedoch durchaus erwägenswert, die Vorschrift des § 19 Absatz 1 BDSG noch etwas deutlicher zu fassen, um Unsicherheiten darüber, wie mit den verschiedenen Fallgestaltungen umzugehen ist, zu vermeiden.

Zuständigkeit bei Mitarbeiterexzessen

Handelt ein Beschäftigter bewusst weisungswidrig, wird er zum Verantwortlichen gemäß Artikel 4 Nummer 7 DSGVO, soweit er dadurch selbst über Zweck und Mittel der Verarbeitung entscheidet. Neben seinem Arbeitgeber können den Beschäftigten damit Aufsichtsmaßnahmen und Bußgelder treffen. Dies kann z. B. zu einer parallelen Zuständigkeit der oder des BfDI einerseits (Zuständigkeit für öffentliche Stellen des Bundes und vereinzelte Unternehmen, §§ 9, 1 BDSG) und einer Landesaufsichtsbehörde andererseits (Zuständigkeit für den Beschäftigten als nichtöffentliche Stelle; §§ 40, 1 BDSG) im Hinblick auf das gleiche Unternehmen führen. Um ein solches Nebeneinander der Zuständigkeiten verschiedener Aufsichtsbehörden zu vermeiden, schlägt der BfDI vor, für die Fälle, in denen der Arbeitgeber der Zuständigkeit der oder des BfDI unterfällt, eine alleinige Zuständigkeit der oder des BfDI auch für Exzesse eines Beschäftigten zu schaffen.

Einen zwingenden regulatorischen Änderungsbedarf zugunsten der oder des BfDI sieht das BMI (derzeit) nicht: Nach den Rückmeldungen aus der Wirtschaft und den betroffenen Unternehmen und der überwiegenden Zahl der Landesaufsichtsbehörden ist nicht zu erkennen, dass es sich hierbei um ein relevantes praktisches Problem handelt. Ähnliche Konstellationen treten zudem auch zwischen einzelnen Landesaufsichtsbehörden auf – nämlich dann, wenn der Wohnsitz des Beschäftigten und der Sitz seines Arbeitgebers in unterschiedlichen Ländern liegen.

Datenverarbeitung bei Telekommunikations- und Post-Dienstleistungen

Die Zuständigkeit für die Aufsicht über die Datenverarbeitung bei Unternehmen, die Dienstleistungen der Telekommunikation und Post erbringen, ist zweigeteilt: Soweit Daten für die Erbringung der Dienstleistungen verarbeitet werden, unterliegt die Aufsicht über die Datenverarbeitung der Zuständigkeit der oder des BfDI (§ 9 BDSG, § 115 Telekommunikationsgesetz, § 42 Postgesetz), in allen anderen Fällen (wie z. B. der Verarbeitung von Beschäftigtendaten, Videoüberwachung) den Landesaufsichtsbehörden (§ 40 BDSG). Der BfDI schlägt vor, diese Zweiteilung aufzuheben und allein seiner Zuständigkeit zuzuweisen, um Telekommunikations- und Postdienstleistungsanbieter einer einheitlichen Datenschutzaufsicht zu unterstellen.

Für eine Zuständigkeitskonzentration bei dem oder dem BfDI bezüglich der Aufsicht über Telekommunikations- und Postdienstleistungsanbieter könnten Abgrenzungsschwierigkeiten und Zuständigkeitskonflikte sprechen.

Indes ist die zweigeteilte Zuständigkeit der oder des BfDI einerseits und der Landesaufsichtsbehörden andererseits nicht neu. Diese Zuständigkeitsverteilung bestand bereits vor der Neufassung des BDSG. In den Rückmeldungen zur Evaluierung des BDSG ist sie seitens der Wirtschaft mehrheitlich moniert worden. Auch die Landesdatenschutzaufsichtsbehörden haben nicht auf Probleme hingewiesen, die durch das Auseinanderfallen der Zuständigkeiten verursacht werden. Würde für Unternehmen der Telekommunikation und Post die Zuständigkeit für sämtliche datenschutzrechtliche Fallgestaltung bei dem oder der BfDI zusammengeführt, bewirkte dies zudem ebenfalls ein Auseinanderfallen von Zuständigkeiten zwar nicht im Hinblick auf die gleichen Unternehmen, aber im Hinblick auf die gleichen Themenfelder: So wäre z. B. für die Verarbeitung von Beschäftigtendaten und die Videoüberwachung bei Unternehmen der Telekommunikation und Post der oder die BfDI zuständig, bei allen anderen Unternehmen bestände aber (weiterhin) eine Zuständigkeit der Landesdatenschutzaufsichtsbehörden.

Von einer Änderung der Zuständigkeitsverteilung bei der Aufsicht über Telekommunikations- und Postdienstleistungsanbieter sollte deshalb abgesehen werden.

5.8.2.6. Rückmeldungen und Bewertung zu § 20 BDSG

Anordnung sofortiger Vollziehung

Es wird eine Streichung des § 20 Absatz 7 BDSG vorgeschlagen. Dieser bestimmt, dass Aufsichtsbehörden gegenüber einer Behörde nicht die sofortige Vollziehung gemäß § 80 Absatz 2 Satz 1 Nummer 4 Verwaltungsgerichtsordnung (VwGO) anordnen dürfen.

§ 20 Absatz 7 BDSG stellt keine datenschutzrechtliche Besonderheit dar. Regelungen, die die Anordnung der sofortigen Vollziehung gemäß § 80 Absatz 2 Satz 1 Nummer 4 der VwGO gegenüber einer Behörde ausschließen, finden sich z. B. auch in § 81a Absatz 7 SGB X und § 32i Absatz 10 Abgabenordnung. Insbesondere im Vergleich zur Rechtslage vor Geltung der DSGVO und vor Inkrafttreten des neuen BDSG haben die Aufsichtsbehörden gegenüber öffentlichen Stellen zudem bereits erheblich mehr Durchsetzungskraft: Die umfangreichen Untersuchungs- und Abhilfebefugnisse des Artikels 58 Absatz 1 und 2 DSGVO gelten auch gegenüber öffentlichen Stellen. Sie gehen weit über das bloße Beanstandungsrecht des § 25 BDSG a. F. hinaus. Im Übrigen ist denkbar, dass Aufsichtsbehörden einstweilige Anordnungen nach § 123 VwGO erwirken könnten. Ein Bedarf, den Aufsichtsbehörden über ihre bereits bestehenden umfangreichen Befugnisse hinaus, die Möglichkeit einzuräumen, auch gegenüber Behörden die sofortige Vollziehbarkeit ihrer Maßnahmen anzuordnen, wird deshalb nicht gesehen.

Klagebefugnis der Aufsichtsbehörden

Die DSK regt die Einführung eines Verfahrens im BDSG an, mit dem die Aufsichtsbehörden eigene Entscheidungen und damit inzident auch die ihnen zugrundeliegenden Rechtsnormen überprüfen lassen könnten. Dies soll den Datenschutzaufsichtsbehörden die Möglichkeit geben, Rechtsnormen an, die sie für europarechtswidrig oder – außerhalb des Anwendungsbereichs der DSGVO und der Richtlinie (EU) 2016/680 – für verfassungswidrig erachten, gerichtlich überprüfen zu lassen.

Ein solches Verfahren widerspräche dem Grundgedanken des deutschen Rechtsschutzsystems. Hiernach ist es nicht die Exekutive, die die eigenen Entscheidungen – und damit inzident auch die den Entscheidungen zugrundeliegenden Rechtsnormen – gerichtlich überprüfen lassen kann. Es obliegt vielmehr den Adressaten von Verwaltungsakten, gegen diese vorzugehen, wenn sie diese für rechtswidrig halten. Nach Auffassung des BMI ist es nicht angezeigt, im Rahmen des BDSG davon abzuweichen.

5.8.2.7. Rückmeldungen und Bewertung zu § 40 Absatz 2 BDSG

Änderung bezüglich des Vorschlagsrechts

Einem Teil der Rückmeldungen aus dem behördlichen Bereich zufolge bedarf der Verweis in § 40 Absatz 2 BDSG auf das Verfahren nach § 18 Absatz 2 BDSG insoweit einer Überar-

beitung, als er zu dem fragwürdigen Ergebnis führen würde, dass das Vorschlagsrecht, welche der Landesaufsichtbehörden als federführende Behörde zuständig ist, in der Mehrzahl der Streitfälle bei dem oder dem BfDI liegt.

Das in § 17 BDSG und § 18 Absatz 2 BDSG geregelte Verfahren ist in Anlehnung an das EUZBLG normiert worden und hat sich bewährt. Hiervon sollte – soweit es die Vertretung der Bundesrepublik Deutschland im Ausschuss betrifft – nicht abgewichen werden.

Auch soweit über § 40 Absatz 2 BDSG die Vorschrift des § 18 Absatz 2 BDSG im innerstaatlichen Bereich in Bezug genommen wird, bedarf es keiner gesetzlichen Änderung. Zwar liegt das Vorschlagsrecht dafür, welche der Landesaufsichtbehörden als federführende Behörde zuständig ist, hier in der Regel bei dem oder dem BfDI. Es steht den Landesaufsichtbehörden jedoch frei, sich mit einfacher Mehrheit über den Vorschlag der oder des BfDI als gemeinsamen Vertreter hinwegzusetzen.

Damit erscheint die Regelung des § 18 Absatz 2 BDSG auch insoweit durchaus ausgewogen.

Regelung der zuständigen Aufsichtsbehörden bei internationalen Unternehmen ohne Niederlassung in Deutschland

In einem Teil der Rückmeldungen aus dem behördlichen Bereich wird der Wunsch nach einer Neuregelung in § 40 Absatz 2 BDSG geäußert, mit der die zuständige federführende Datenschutzaufsichtsbehörde insbesondere bei internationalen Unternehmen ohne Niederlassung in Deutschland festgelegt wird.

Der BfDI plädiert in solchen Fällen für eine generelle Zuständigkeit der oder des BfDI. Die große Mehrheit der Landesaufsichtsbehörden spricht sich dagegen dafür aus, solche Fallgestaltungen – ebenso wie die Fälle, in denen ein (internationales oder bundesweit tätiges) Unternehmen mehrere Niederlassungen im Bundesgebiet hat – unter Heranziehung des § 40 Absatz 2 BDSG i. V. m. § 18 Absatz 2 BDSG zu handhaben.

Eine Zuständigkeit der oder des BfDI im privatwirtschaftlichen Bereich stellt bislang eine – auf bestimmte Sektoren begrenzte und spezialgesetzlich geregelte – Ausnahme dar, so insbesondere im Bereich der Telekommunikations- und Postunternehmen. Es würde einen Systembruch darstellen, den oder der BfDI branchenübergreifend für alle Unternehmen ohne Niederlassung im Bundesgebiet für zuständig zu erklären. Für eine solch weitreichende Änderung sind keine überzeugenden Gründe ersichtlich, zumal die Landesaufsichtsbehörden hier über langjährige Expertise verfügen. Nach alledem erscheint es sachgerecht, dass auch Unternehmen ohne Niederlassung in Deutschland den Regelungen der §§ 40 Absatz 2, 18 Absatz 2 BDSG unterworfen sind.

Das BMI versteht die Regelung des § 40 Absatz 2 BDSG so, dass Satz 1 die Fallgestaltung von Unternehmen mit mehreren Niederlassungen betrifft, Satz 2 dagegen alle Fälle, bei

denen Zweifel über die Zuständigkeit besteht, also neben der bereits in Satz 1 angesprochenen Fallgestaltung beispielsweise auch die Fallgestaltung von Unternehmen ohne Niederlassung. Damit wird im Übrigen auch die teilweise im behördlichen Bereich als ebenfalls schwierig empfundene Fallgestaltung von Unternehmen mit mehreren Niederlassungen aber ohne eine (klare) Hauptniederlassung mit umfasst. Dies alles soll nach Auffassung des BMI mit der Formulierung „aus anderen Gründen“ zum Ausdruck gebracht werden. Für all diese Fallgestaltungen wird mithin nach Auffassung des BMI letztlich auf die Regelungen des § 18 Absatz 2 BDSG verwiesen.

Vor dem Hintergrund der in den Rückmeldungen geäußerten Unsicherheiten wird das BMI jedoch prüfen, ob die Regelung des § 40 Absatz 2 BDSG noch etwas deutlicher gefasst werden sollte, um Unklarheiten darüber, wie mit den verschiedenen Fallgestaltungen umzugehen ist, zu vermeiden.

Zuständigkeitskonzentration für bundesweit tätige Unternehmen - insbesondere bei Vorliegen mehrerer datenschutzrechtlicher Verantwortlicher

Einem Teil der Rückmeldungen aus der Wirtschaft zufolge bedürfe es zudem für bundesweit tätige Unternehmen generell einer Zuständigkeitskonzentration auf eine federführend zuständige Datenschutzaufsichtsbehörde.

Es fehle insbesondere an einer Regelung zur Festlegung der zuständigen Datenschutzaufsichtsbehörde in § 40 Absatz 2 BDSG für den Fall, dass jede Niederlassung als *eigener* datenschutzrechtlicher Verantwortlicher zu qualifizieren ist. Dies sei insbesondere bei Unternehmen mit mehreren Gesellschaften und bei genossenschaftlichen Organisationsformen der Fall. Da nach bisheriger Praxis jede Datenschutzaufsichtsbehörde bezüglich dem in ihrem Bundesland niedergelassenen Verantwortlichen tätig werde, seien im Falle bundesweit tätiger Unternehmen oft die Datenschutzaufsichtsbehörden mehrerer Bundesländer zuständig. Dies könne beispielsweise bei der Einführung gemeinsamer bundesländerübergreifender IT-Lösungen oder bei einer bundesländerübergreifenden Datenverarbeitung ein Problem darstellen, da sich bundesweit tätige Unternehmen hier mit mehreren Datenschutzaufsichtsbehörden abstimmen müssten, welche zudem im Einzelfall unterschiedliche Rechtsauffassungen vertreten könnten.

Auch diese Fallgestaltung fällt dem Verständnis des BMI zufolge unter die Vorschrift des § 40 Absatz 2 Satz 2 BDSG und unterfällt mithin letztlich ebenfalls der Regelung des § 18 Absatz 2 BDSG.

Diese Rückmeldung gibt jedoch ebenfalls Anlass zu der Überlegung, die Regelung des § 40 Absatz 2 BDSG eventuell noch etwas deutlicher zu fassen, um Unklarheiten darüber, wie mit den verschiedenen Fallgestaltungen umzugehen ist, zu vermeiden.

Rückmeldungen und Bewertung zu sonstigen Aspekten von Zuständigkeiten und Befugnissen der Aufsichtsbehörden

In vielen Rückmeldungen wird der Wunsch nach einer möglichst einheitlichen Rechtsauslegung und Rechtsanwendung durch die Datenschutzaufsichtsbehörden in Bund und Ländern geäußert. Zum Teil wird angeregt, eine Regelung zur einheitlichen Meinungsbildung der Datenschutzaufsichtsbehörden in das BDSG aufzunehmen.

So wird insbesondere von den Datenschutzaufsichtsbehörden selbst vorgeschlagen, die DSK zu institutionalisieren und deren (Mehrheits-)Beschlüsse für verbindlich zu erklären – sei es mittels einer entsprechenden Bestimmung im BDSG oder sei es per Bund-Länder-Staatsvertrag.

In eine ganz ähnliche Richtung zielt der teilweise aus der Wirtschaft geäußerte Vorschlag das Kohärenzverfahren der Artikel 63 ff. DSGVO in § 40 BDSG abzubilden.

Aus Sicht des BMI ist es sehr zu begrüßen, dass sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zum Ziel gesetzt hat, mittels Entschließungen und Beschlüssen im Wege der freiwilligen Selbstbindung auch zu einer Vereinheitlichung der Rechtsanwendung im Datenschutzbereich beizutragen und hierzu in ihrer Geschäftsordnung auch Mehrheitsbeschlüsse vorgesehen hat. Eine weitergehende Institutionalisierung der DSK – sei es per Gesetz oder per Staatsvertrag – stößt jedoch an verfassungsrechtliche Grenzen. Zu beachten ist insoweit insbesondere das Verbot der Mischverwaltung. Ohne eine entsprechende Ergänzung des GG (z. B. im Abschnitt VIIIa. Verwaltungszusammenarbeit) kann in das BDSG daher keine entsprechende Regelung zur stärkeren Institutionalisierung der DSK aufgenommen werden.

5.8.3. Schlussfolgerungen

Im Ergebnis haben sich die Regelungen des BDSG zu Aufgaben und Befugnissen der oder des BfDI, zur Zusammenarbeit in europäischen Angelegenheiten, zu Rechtsbehelfen sowie zur Bestimmung der zuständigen Aufsichtsbehörde (§§ 14, 16 bis 20, 40 Absatz 2 BDSG) ganz überwiegend bewährt. Aus den Rückmeldungen ergibt sich kein zwingender normativer Änderungsbedarf. Insbesondere hält das BMI eine Klarstellung in § 18 BDSG hinsichtlich der Frage, ob ein gemeinsamer Standpunkt bereits im Kohärenzverfahren oder erst im Kooperationsverfahren herbeizuführen jedenfalls vorerst nicht für angezeigt, hier sollten zunächst Best Practices erprobt werden. Die Notwendigkeit einer Klarstellung in § 19 Absatz 1 und § 40 Absatz 2 BDSG wird das BMI weiter prüfen. Die vorgeschlagene Institutionalisierung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder schließlich würde eine Grundgesetzänderung voraussetzen.

5.9. Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten (Teil 3 BDSG) – §§ 45 bis 47 BDSG

5.9.1. Zielsetzung und Gegenstand der Regelungen

Mit § 45 BDSG hat der Gesetzgeber den Anwendungsbereich der Vorschriften von Teil 3 BDSG geregelt. Teil 3 BDSG dient im Wesentlichen der Umsetzung der Richtlinie (EU) 2016/680.

§ 45 BDSG stellt in Satz 1 klar, dass Teil 3 BDSG ausschließlich für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentliche Stellen und als öffentliche Stellen geltende Beliehene gilt, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Gemäß Satz 3 umfasst die Verhütung von Straftaten den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit. Satz 4 erweitert den Anwendungsbereich von Teil 3 BDSG auf die Verarbeitung durch öffentliche Stellen, die für die Vollstreckung von Strafen, Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 StGB, Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und Geldbußen zuständig sind, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten.

§ 46 BDSG dient der Umsetzung der Richtlinie (EU) 2016/680. Die Begriffsbestimmungen schließen an die Definitionen in Artikel 3 der genannten Richtlinie an. Außerdem wurde in die Vorschrift die in Artikel 10 der Richtlinie (EU) 2016/680 enthaltene Definition besonderer personenbezogener Daten aufgenommen. Zudem wird in § 46 BDSG der Begriff der Einwilligung unter Übernahme der Definition aus Artikel 4 Nummer 11 der DSGVO bestimmt.

Die Regelung des § 47 BDSG setzt Artikel 4 der Richtlinie (EU) 2016/680 um und führt die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten auf.

5.9.2. Empirische Ergebnisse und Bewertung

5.9.2.1. Rückmeldungen und Bewertung zu § 45 BDSG

Rückmeldungen zu § 45 BDSG kamen vonseiten der DSK, der Verbände, der Bundesbehörden und einiger Länder.

Abgrenzung zur DSGVO und Verhältnis zu Fachgesetzen

Vereinzelt wird auf Abgrenzungsschwierigkeiten zwischen dem Anwendungsbereich der DSGVO bzw. Teil 2 BDSG und der Richtlinie (EU) 2016/680 bzw. Teil 3 BDSG hingewiesen. Ein Rechtsanwender, der mit dem BDSG nicht vertraut sei, könne nicht erkennen, dass eine in Teil 3 BDSG enthaltene Vorschrift nur dann zur Anwendung komme, wenn die

Eingangsvoraussetzungen des § 45 BDSG gegeben seien. Im Hinblick darauf wird vereinzelt angeregt, die Regelungen für den Polizei- und Strafverfolgungsbereich in ein eigenständiges Gesetz auszugliedern, um Anwendungsklarheit zu schaffen.

Ein Bedarf für die Auslagerung der Regelungen von Teil 3 BDSG in ein eigenes Gesetz besteht nach Auffassung des BMI nicht. Leitgedanke bei der Neufassung des BDSG war es, entsprechend der Regelungssystematik des früheren BDSG ein datenschutzrechtliches Vollregime zu schaffen.[69] Die Regelungssystematik des BDSG trägt den voneinander abzugrenzenden Regelungsgegenständen durch eine Vierteilung des BDSG Rechnung. Dabei weisen bereits die amtlichen Überschriften der vier Teile darauf hin, für welche Bereiche und für welche Normadressaten die jeweiligen Vorschriften gelten. Soweit Teil 3 BDSG betroffen ist, ist § 45 BDSG den übrigen Vorschriften vorangestellt und beschreibt den personellen und sachlichen Anwendungsbereich der nachfolgenden Regelungen. Vor diesem Hintergrund wird auch nicht die Notwendigkeit einer Spezifizierung der Begrifflichkeiten der Vorschriften gesehen, um klarzustellen, dass Teil 3 BDSG nur für den Bereich der Polizei und Strafverfolgung gilt. Die Vorschriften von Teil 3 BDSG dienen der Umsetzung der Richtlinie (EU) 2016/680, die einheitliche Begrifflichkeiten zugrunde legt. Einer Änderung der rechtlichen Terminologien wären daher jedenfalls enge Grenzen gesetzt.

Teilweise wird angemerkt, dass das Zusammenspiel des BDSG mit den jeweiligen Prozessordnungen unübersichtlich sei. Hierbei wird insbesondere kritisiert, dass der Anwendungsbereich von Teil 3 BDSG in Bezug auf den Strafverfahrensbereich nicht klar genug sei, da zwar die Strafprozessordnung (StPO) auf das BDSG, nicht aber das BDSG auf die StPO verweise.

Das BMI teilt diese Kritik nicht. Der Gesetzgeber hat mit § 1 Absatz 2 Satz 1 BDSG klargestellt, dass das BDSG den Charakter eines Auffanggesetzes hat.[70] Danach gehen spezifische Rechtsvorschriften des Bundes den allgemeinen Vorschriften des BDSG grundsätzlich vor. Diese gesetzgeberische Grundentscheidung für eine gestufte Regelungstechnik mit allgemeinen Vorschriften im BDSG und bereichsspezifischen Sonderregelungen im Fachrecht gilt – wie auch durch die amtliche Überschrift zu Teil 1 des BDSG klargestellt wird („Gemeinsame Bestimmungen") – für den gesamten Anwendungsbereich des BDSG und damit auch für den Bereich der Polizei und der Strafverfolgung. Die Frage des anwendbaren Rechts ist nach allgemeinen Rechtsgrundsätzen zu bestimmen. Insoweit stellt § 1 Absatz 2 Satz 2 BDSG klar, dass die jeweilige bereichsspezifische Spezialregelung vorrangig gegenüber der allgemeinen Vorschrift ist, wenn eine Tatbestandskongruenz vorliegt.[71] Vor diesem Hintergrund erscheint dem BMI eine weitergehende Regelung des Anwendungsverhältnisses in Bezug auf einzelne Fachgesetze im BDSG nicht veranlasst und im Sinne der Übersichtlichkeit und Handhabbarkeit der Regelungen auch nicht sinnvoll. Der Gesetzge-

[69] BT-Drs. 18/11325, S. 69.
[70] BT-Drs. 18/11325, S. 79.
[71] BT-Drs. 18/11325, S. 79.

ber hat die Möglichkeit, das Verhältnis zum BDSG in den jeweiligen Fachgesetzen klarzustellen. Hiervon hat der Bundesgesetzgeber u. a. im Bereich des Strafverfahrensrechts Gebrauch gemacht.

Bestimmung des Anwendungsbereichs nach dem Zweck der Datenverarbeitung

Die DSK merkt an, dass in § 45 BDSG im Unterschied zur Richtlinie (EU) 2016/680 nicht in erster Linie auf den konkreten Zweck der Verarbeitungstätigkeit abgestellt werde, sondern auch auf die allgemeine Zuständigkeit der Behörde. Dies führe zu unterschiedlichen Ergebnissen bei Behörden, die selbst keine polizeilichen Aufgaben oder Aufgaben im Bereich der Strafverfolgung wahrnähmen, aber einzelne Verarbeitungstätigkeiten durchführten, die der Strafverfolgung dienten. Als Beispiel führt die DSK die Tätigkeit des BfJ als Registerbehörde für das Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV) an.

Aus Sicht des BMI liegen taugliche Kriterien vor, um den personellen und sachlichen Anwendungsbereich von Teil 3 BDSG rechtssicher zu bestimmen. Die Richtlinie (EU) 2016/680 verweist für die Bestimmung des Anwendungsbereichs ausdrücklich auf die „zuständigen Behörden“[72]. Unter „zuständige Behörden“ sind danach staatliche Stellen zu verstehen, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständig sind, sowie andere Stellen oder Einrichtungen, denen die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Erfüllung der genannten Aufgaben übertragen wurde.[73] Diese Vorgaben setzt § 45 BDSG um, indem die Vorschrift neben den Zwecken der Verarbeitungstätigkeit auch auf die allgemeine Zuständigkeit der öffentlichen Stellen abstellt. Ergänzend dazu ist auf die bereichsspezifischen Regelungen des jeweiligen Fachrechts zurückzugreifen, um das maßgebliche Datenschutzregime zu ermitteln. In Bezug auf Datenverarbeitungen im ZStV stellen etwa die §§ 493 und 494 StPO durch entsprechende Verweise klar, dass der Anwendungsbereich von Teil 3 BDSG eröffnet ist.

Anknüpfung an den Straftatenbegriff des EU-Rechts

Vereinzelt wird angeregt, in § 45 Satz 1 BDSG ausschließlich auf den unionsrechtlichen Begriff der Straftat abzustellen und diesen näher zu definieren. Die aktuelle Verwendung des Begriffspaares „Straftaten und Ordnungswidrigkeiten“ knüpfe dem Wortlaut nach an die Kategorien des nationalen Sanktionenrechts an, was der Richtlinie (EU) 2016/680 entgegenstünde.

[72] Artikel 2 Absatz 1 der Richtlinie (EU) 2016/680.
[73] Artikel 3 Nr. 7 der Richtlinie (EU) 2016/680.

Die Kritik übersieht, dass es sich bei dem Begriff der Straftat im Sinne der Richtlinie (EU) 2016/680 um einen eigenständigen Begriff des Unionsrechts handelt[74], der unter Berücksichtigung der unterschiedlichen Rechtstraditionen der Mitgliedstaaten zu bestimmen ist. Die Bezugnahme auf den Begriff der Straftat in der Richtlinie als einen eigenständigen Begriff des Unionsrechts unterstützt die Einbeziehung der Ordnungswidrigkeiten in den Anwendungsbereich von Teil 3 BDSG.[75] Der Gesetzgeber hat mit dem Verweis auf Straftaten und Ordnungswidrigkeiten den Anwendungsbereich von Teil 3 BDSG insoweit abschließend geregelt. Bei Straftaten und Ordnungswidrigkeiten handelt es sich um feststehende Rechtsbegriffe, die bereits legaldefiniert sind.[76] Bedarf für eine (wiederholende) Definition im BDSG besteht nach Auffassung des BMI nicht.

Klarstellung in Bezug auf die Gefahrenabwehr und Ordnungswidrigkeiten

Aus den Ländern wird angemerkt, dass in § 45 Satz 3 BDSG im Interesse der Normenklarheit das Wort „straftatbezogenen" vor den Wörtern „Gefahren für die öffentliche Sicherheit" eingefügt werden sollte, da die nicht straftatenbezogene Gefahrenabwehr in den Anwendungsbereich der DSGVO fiele. In eine ähnliche Richtung geht der Hinweis aus dem Kreis der Bundesbehörden, dass nicht ersichtlich sei, ob Teil 3 des BDSG auch bei der Datenverarbeitung zur Gefahrenabwehr durch die Ordnungsbehörden einschlägig sei.

Nach Ansicht des BMI unterliegen Datenverarbeitungen im Rahmen der allgemeinen Gefahrenabwehr nicht der Richtlinie (EU) 2016/680. Im Bereich der Gefahrenabwehr sind nur solche Vorgänge erfasst, die einen Straftatenbezug aufweisen.[77] Dabei ist bei polizeilichen Gefahrenabwehrmaßnahmen aufgrund der spezifischen Zuständigkeit der Polizeibehörden für die Kriminalitätsbekämpfung regelmäßig von einem Straftatenbezug auszugehen.[78] Dies gilt auch bei Sachverhalten, bei denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht. Die Verarbeitung personenbezogener Daten durch die Ordnungsbehörden im Rahmen der nicht straftatenbezogenen Gefahrenabwehr unterliegt dagegen regelmäßig dem Anwendungsbereich der DSGVO.[79]

Dieses Verständnis liegt auch Teil 3 BDSG zugrunde. Der in Bezug auf die Gefahrenabwehr erforderliche Straftatenbezug kommt in § 45 Satz 3 BDSG zum Ausdruck, wenn der Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit in einen Zusammenhang mit der Verhütung von Straftaten gestellt wird. Damit ist insbesondere die Gefahrenabwehrtätigkeit der Polizeibehörden, jedoch grundsätzlich nicht die der Verwaltungsbehörden erfasst.[80] § 45 Satz 3 BDSG macht durch die Bezugnahme auf die Verhütung von Straftaten hinreichend deutlich, dass nur die straftatbezogene Gefahrenabwehr dem Teil 3

[74] Vgl. Erwägungsgrund 13 zur Richtlinie (EU) 2016/680.
[75] BT-Drs. 18/11325, S. 110.
[76] Vgl. §§ 11 Absatz 1 Nr. 5, 12 Absatz 1 und 2 StGB, § 1 OWiG.
[77] Vgl. Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680 und Artikel 2 Absatz 2 Buchstabe d DSGVO.
[78] Vgl. Erwägungsgrund 12 zur Richtlinie (EU) 2016/680.
[79] Vgl. Erwägungsgrund 11 zur Richtlinie (EU) 2016/680.
[80] Vgl. auch BT-Drs. 18/11325, S. 110.

BDSG unterliegt. Eine zusätzliche Klarstellung im Gesetzeswortlaut ist nach Ansicht des BMI insoweit nicht erforderlich.

Die DSK merkt an, dass durch den aktuellen Wortlaut des § 45 Satz 1 BDSG nicht zum Ausdruck komme, dass der Gesetzgeber ausschließlich die Verfolgung und Ahndung von Ordnungswidrigkeiten, nicht aber deren Verhütung erfasst sehen wollte.

Das BMI wird diese Anregung weiter prüfen. Zwar wird in der Gesetzesbegründung erläutert, dass Datenverarbeitungen bei Verwaltungsbehörden grundsätzlich solange und soweit nicht in den Anwendungsbereich von Teil 3 BDSG fallen, wie die von ihnen geführten Verfahren nicht in ein konkretes Ordnungswidrigkeitenverfahren übergehen.[81] § 45 Satz 1 BDSG bezieht sich jedoch insgesamt auf „die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten". Es könnte daher sinnvoll sein, in der gesetzlichen Regelung deutlicher zum Ausdruck zu bringen, dass die Verhütung von Ordnungswidrigkeiten grundsätzlich nicht erfasst sein soll.

Anwendbarkeit von Teil 3 BDSG auf Auftragsverarbeiter

Aus dem behördlichen Bereich wird angemerkt, das unklar sei, inwieweit Teil 3 BDSG auch für Auftragsverarbeiter gelte, die im Übrigen nicht Teil 3 BDSG unterworfen seien.

Aus § 45 Satz 5 BDSG folgt indes, dass Teil 3 BDSG auch für Auftragsverarbeiter gilt, soweit dieser Vorschriften über die Auftragsverarbeitung enthält. Öffentliche oder nichtöffentliche Stellen, die Daten zur Erfüllung einer Auftragsverarbeitungsvereinbarung und nicht aufgrund eigener Aufgabenzuschreibung verarbeiten, unterliegen Teil 3 BDSG danach nur, soweit sie darin konkret angesprochen sind.[82] Die von ihnen durchgeführten Verarbeitungen richten sich im Übrigen nach den Regelungen der DSGVO sowie nach denen von Teil 1 und 2 BDSG.

Anwendbarkeit von Teil 3 BDSG auf die Dokumentation polizeilichen Handelns

Seitens der DSK wird kritisiert, dass aus dem Wortlaut des § 45 BDSG nicht hervorgehe, ob die Dokumentation des betreffenden polizeilichen Handelns auch vom Anwendungsbereich von Teil 3 BDSG erfasst sei. Abgesehen davon müssten die Vorgaben von Teil 3 BDSG auch für die elektronischen Akten der Polizeibehörden gelten, soweit diese der Dokumentation der polizeilichen Aufgabenerfüllung dienten.

Die Dokumentation polizeilichen Handelns unterliegt Teil 3 BDSG in dem Umfang, in dem die Polizeibehörden personenbezogene Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten und Ordnungswidrigkeiten sowie zur straftatbezogenen Gefahrenabwehr verarbeiten. Die Dokumentation dient vorrangig der Gewährleistung eines effektiven Rechtsschutzes für die Betroffenen und der

[81] Vgl. BT-Drs. 18/11325, S. 110 f.
[82] BT-Drs. 18/11325, S. 111.

Polizeibeamten vor unberechtigten Anschuldigungen. Sie steht in einem engen Sachzusammenhang mit der Aufgabenerfüllung. Dieser Sachzusammenhang wird grundsätzlich auch nicht aufgelöst, wenn die Dokumentation in den elektronischen Akten der Polizeibehörden erfolgt. Bedarf für eine Klarstellung im Wortlaut des § 45 BDSG sieht das BMI insoweit nicht.

5.9.2.2. Rückmeldungen und Bewertungen zu § 46 BDSG

Anmerkungen zu § 46 BDSG kamen vonseiten der Länder. In den Rückmeldungen wird vereinzelt angeregt, den Katalog der Begriffsbestimmungen um „Anonymisierung"; „Verschlüsselung"; „Akte" und „Dritter" zu ergänzen. In eine ähnliche Richtung geht der Hinweis der DSK zu § 76 BDSG, dass „Protokollierung" bislang nicht legaldefiniert und eine gesetzliche Klarstellung des Begriffs erforderlich sei.

Im Gegensatz zu einer entsprechenden Definition des Begriffs „Anonymisierung" in § 2 BDSG für das gesamte BDSG erscheint eine Ergänzung von § 46 BDSG um eine entsprechende Definition für Teil 3BDSG aus Sicht des BMI prüfenswert. Denn anders als die unmittelbar anwendbare DSGVO, bedarf es für die Richtlinie einer Umsetzung im nationalen Recht.

In Bezug auf eine aus Sicht des BMI aus diesen Erwägungen heraus ebenfalls grundsätzlich denkbare Ergänzung des Katalogs des § 46 BDSG um die Begriffe „Verschlüsselung" und „Protokollierung" wäre unter Berücksichtigung des Regelungsansatzes des EU-Datenschutzrechts auf eine technikneutrale Definition zu achten.[83] Außerdem müsste sich die Begriffsbestimmung in das bestehende Regelungsgefüge, insbesondere die in § 64 und 76 BDSG aufgestellten Anforderungen, einpassen.

Eine Definition der Begriffe „Akte" und „Dritter" sieht das BMI dagegen nicht als zielführend an. Abgesehen davon, dass Teil 3 BDSG keine besonderen Vorschriften zur Datenverarbeitung in Akten enthält, ist die Akte keine spezifisch datenschutzrechtliche Kategorie. Es handelt sich vielmehr um einen allgemeinen verwaltungsrechtlichen Begriff, der in einer Vielzahl von Gesetzen behandelt wird. Im Hinblick darauf erscheint das BDSG nicht als der geeignete Regelungsort. Entsprechendes gilt für den Begriff „Dritter". Auch dieser Begriff kann aus Sicht des BMI unter Anwendung der allgemeinen Auslegungsmethoden hinreichend sicher bestimmt werden.

5.9.2.3. Rückmeldungen und Bewertung zu § 47 BDSG

In den Rückmeldungen der Länder wird teilweise angemerkt, dass es sinnvoll erscheine, den § 47 BDSG um eine dem Artikel 4 Absatz 4 der Richtlinie (EU) 2016/680 entsprechende Regelung zu ergänzen. Es solle insoweit geregelt werden, dass der Verantwortliche für die

[83] Vgl. Erwägungsgrund 18 zur Richtlinie (EU) 2016/680: *„Um ein ernsthaftes Risiko einer Umgehung der Vorschriften zu vermeiden, sollte der Schutz natürlicher Personen technologieneutral sein und nicht von den verwendeten Techniken abhängen."*

Einhaltung der in der Vorschrift niedergelegten Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich sei und die Einhaltung dieser Grundsätze nachweisen können müsse.

Für eine Ergänzung des § 47 BDSG um den genannten Inhalt besteht aus Sicht des BMI keine Notwendigkeit. Es ergibt sich aus höherrangigen Grundsätzen, dass sich die handelnden Behörden rechtskonform zu verhalten haben. Die in Artikel 4 Absatz 4 der Richtlinie (EU) 2016/680 vorgesehene allgemeine Nachweispflicht ist im BDSG und in den Fachgesetzen jeweils in konkreten Bestimmungen geregelt. Zwingende Gründe, das sehr allgemeine Prinzip der Rechenschaftspflicht als allgemeinen Grundsatz in § 47 BDSG gesetzlich abzubilden, sind für das BMI nicht ersichtlich.

5.9.3. Schlussfolgerungen

Grundsätzlichen Änderungsbedarf in Bezug auf § 45 BDSG sieht das BMI nicht. Hinsichtlich § 45 Satz 1 BDSG wird das BMI eine weitere Differenzierung in Bezug auf die Verhütung von Ordnungswidrigkeiten prüfen.

Das BMI wird eine Aufnahme von Definitionen für die Begriffe „Anonymisierung“, „Verschlüsselung“ und „Protokollierung“ in die Begriffsbestimmungen des § 46 BDSG für Teil 3 BDSG weiter prüfen.

Die Regelung zu den allgemeinen Grundsätzen für die Verarbeitung personenbezogener Daten in § 47 BDSG hat sich insgesamt bewährt. Eine Ergänzung der Vorschrift um eine dem Artikel 4 Absatz 4 der Richtlinie (EU) 2016/680 entsprechenden Regelung erscheint nicht geboten.

5.10. Rechtsgrundlagen für die Datenverarbeitung – §§ 48 bis 51 BDSG

5.10.1. Zielsetzung und Gegenstand der Regelungen

Mit den §§ 48 bis 51 BDSG hat der Gesetzgeber den rechtlichen Rahmen für die Verarbeitung von besonderen Kategorien von personenbezogenen Daten, für die Änderung des Verarbeitungszwecks, die Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken sowie die Voraussetzungen für eine wirksame Einwilligung festgelegt.

§ 48 BDSG dient der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680. Absatz 1 legt fest, dass die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist. In Absatz 2 Satz 1 wird klargestellt, dass bei der Verarbeitung geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen werden müssen. In Satz 2 werden Beispielsfälle wiedergegeben, wie geeignete Garantien aussehen können.

Mit § 49 Satz 1 BDSG wird Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680 umgesetzt. Es wird klargestellt, dass Verantwortliche Daten zu anderen Zwecken, als zu denen sie ursprünglich erhoben wurden, verarbeiten dürfen, wenn es sich bei diesen anderen Zwecken um einen der in § 45 BDSG genannten Zwecke handelt und die Verarbeitung hierfür erforderlich und verhältnismäßig ist. § 49 Satz 2 BDSG betrifft die Weiterverarbeitung von zu Zwecken des § 45 BDSG erhobenen Daten zu anderen als den dort genannten Zwecken.

§ 50 BDSG greift Artikel 4 Absatz 3 der Richtlinie (EU) 2016/680 auf. Danach können Verantwortliche Daten auch zu wissenschaftlichen, statistischen und historischen Zwecken im Rahmen der in § 45 BDSG genannten Zwecke verarbeiten, wenn geeignete Garantien zugunsten der Rechtsgüter der betroffenen Person bestehen.

In § 51 BDSG sind die Voraussetzungen für eine Einwilligung im Anwendungsbereich von Teil 3 BDSG geregelt. Nach § 51 Absatz 1 muss die Möglichkeit der Einwilligung bei Datenverarbeitungen zum Zweck der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahnung von Straftaten oder Ordnungswidrigkeiten durch eine spezielle Rechtsvorschrift vorgesehen sein.

5.10.2. Empirische Ergebnisse und Bewertung

Rückmeldungen zu den §§ 48 bis 51 BDSG kamen vonseiten der DSK, den Bundesbehörden und aus den Ländern.

5.10.2.1. Rückmeldung und Bewertung zu § 48 BDSG

Anpassung der Kapitelüberschrift

Von der DSK wird angemerkt, dass es sich bei den §§ 48 bis 51 BDSG nicht um eigenständige Rechtsgrundlagen handele. Dies sei in der Kapitelüberschrift deutlich zu machen, die

aus Klarstellungsgründen entsprechend anzupassen sei. Ähnliche Anmerkungen kamen vereinzelt von den Ländern in Bezug auf den die Voraussetzungen der Einwilligung regelnden § 51 BDSG.

Die Kapitelüberschrift „Rechtsgrundlagen der Verarbeitung personenbezogener Daten" ist aus Sicht des BMI sachgerecht. Bei § 48 Absatz 1 BDSG handelt es sich um eine eigene Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten. Auf die Rechtsnatur dieser Vorschrift als allgemeine Rechtsgrundlage weist auch die Gesetzesbegründung hin.[84] Das Gleiche gilt für § 50 Satz 1 BDSG, der ebenfalls eine allgemeine Rechtsgrundlage enthält. §§ 49 und 51 BDSG nehmen auf Rechtsgrundlagen Bezug, die im Fachrecht geregelt bzw. weiter auszudifferenzieren sind. Das BMI sieht hier keinen Änderungsbedarf.

Begriff der unbedingten Erforderlichkeit

In den Rückmeldungen wird mehrfach angemerkt, dass unter Zugrundelegung des üblichen Verständnisses des Begriffs der Erforderlichkeit die Bedeutung des Begriffs „unbedingt" unklar sei. Die DSK steht auf dem Standpunkt, dass intensive Grundrechtseingriffe aufgrund der Unbestimmtheit der Formulierung nicht auf § 48 Absatz 1 BDSG gestützt werden könnten.

Den Begriff der unbedingten Erforderlichkeit hat der Gesetzgeber aus dem umzusetzenden Artikel 10 der Richtlinie (EU) 2016/680 übernommen. Ob eine Datenverarbeitung erforderlich für die Aufgabenerfüllung ist, bestimmt sich nach allgemeinen Rechtsgrundsätzen und ist im konkreten Einzelfall zu beurteilen. Der Zusatz „unbedingt" weist in Anbetracht der besonderen Schutzbedürftigkeit von besonderen Kategorien personenbezogener Daten dabei auf einen besonders strengen Maßstab für die Verhältnismäßigkeitsprüfung hin. Bei der Verhältnismäßigkeitsprüfung können die in Artikel 10 Buchstaben b und c der Richtlinie (EU) 2016/680 genannten Zusammenhänge zu berücksichtigen sein.[85]. Daneben kann es weitere Gesichtspunkte geben, die im jeweiligen Einzelfall in die Interessenabwägung einzustellen sein können und die für den Gesetzgeber nicht vorhersehbar sind. Dem trägt § 48 Absatz 1 BDSG durch eine offene Formulierung Rechnung.

Verhältnis von § 48 Absatz 1 BDSG zu bereichsspezifischen Regelungen

Des Weiteren wird mehrfach angemerkt, dass das Verhältnis von § 48 Absatz 1 BDSG zu den bereichsspezifischen Vorschriften unklar sei. Hierdurch bestehe in der Praxis ein erhöhtes Risiko unsachgemäßer Ergebnisse.

Aus der Funktion des BDSG als Auffanggesetz folgt, dass die §§ 45 ff. BDSG im Verhältnis zu den bereichsspezifischen Vorschriften im Zusammenspiel mit den Fachgesetzen und

[84] BT-Drs. 18/11325, S. 111.
[85] Vgl. BT-Drs. 18/11325, S. 111.

umgekehrt die Fachgesetze im Zusammenspiel mit den §§ 45 ff. BDSG zu lesen sind.[86] Im Ergebnis ist im konkreten Einzelfall zu prüfen, ob und in welchem Umfang spezialgesetzliche Vorschriften anwendbar sind. Dies ist nach Ansicht des BMI sachgerecht. Abgesehen davon erscheint eine weitergehende Regelung des Stufenverhältnisses im BDSG in Bezug auf alle Fachgesetze auch nicht umsetzbar. Es ist dem Gesetzgeber aber unbenommen, entsprechende Klarstellungen in den jeweiligen Fachgesetzen vorzunehmen.

Maßstab für geeignete Garantien

Ein Teil der Rückmeldungen kritisiert die Regelung des § 48 Absatz 2 BDSG dahingehend, dass durch die Ausgestaltung der Vorschrift kein ausreichender Schutz der besonderen Kategorien personenbezogener Daten gewährleistet sei. Dies ergebe sich aus dem Umstand, dass der in Satz 2 der Vorschrift enthaltene Katalog alternative Garantien beispielhaft aufzähle, die aber keinen gleichrangigen Schutzstandard böten.

Bei den in § 48 Absatz 2 BDSG aufgezählten Garantien handelt es sich um Beispielsfälle.[87] Durch die Aufzählung ist noch nicht ausgesagt, dass eine dieser Maßnahmen allein geeignet ist, den Schutz für die Rechtsgüter der betroffenen Personen zu gewährleisten, was durch die Formulierung „können insbesondere sein“ deutlich wird. Dass aber insgesamt geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen sind, ergibt sich aus § 48 Absatz 1 BDSG, der Artikel 10 der Richtlinie (EU) 2016/680 umsetzt. Der Schutz der besonderen Kategorien personenbezogener Daten ist aus Sicht des BMI damit gewährleistet.

Sonstige Anmerkungen

Teilweise wird angeregt den Begriff „Rechtsgüter“ in § 48 Absatz 2 Satz 1 BDSG durch die in der Richtlinie (EU) 2016/680 gebrauchte Formulierung „Rechte und Freiheiten“ zu ersetzen. Hierdurch könne klargestellt werden, dass die Vorschrift auch die Grundfreiheiten der Europäischen Union erfasse.

Die Formulierung im Gesetzestext ist bewusst gewählt und sollte daher beibehalten werden. Der Begriff „Rechtsgut“ stellt klar, dass es sich bei den Interessen und Güter der betroffenen Person, die in Teil 3 BDSG in Bezug genommen werden, um rechtlich geschützte Interessen und Güter handeln muss. Dieser Gedanke käme in der Formulierung „Rechte und Freiheiten“ nicht hinreichend zum Ausdruck.

[86] Vgl. BT-Drs. 18/11325, S. 79.
[87] BT-Drs. 18/11325, S. 111.

5.10.2.2. Rückmeldungen und Bewertung zu § 49 BDG

Umsetzung der verfassungsrechtlichen Vorgaben an die zweckändernde Verarbeitung

Die DSK kritisiert, dass § 49 BDSG mit zentralen Vorgaben des Urteils des Bundesverfassungsgerichts (BVerfG) zum früheren BKAG[88] nicht vereinbar sei, und regt an, die Voraussetzungen für zulässige Zweckänderungen im Fachrecht zu regeln.

Die zusätzlichen verfassungsrechtlichen Anforderungen an die zweckändernde Weiterverarbeitung personenbezogener Daten, die durch eingriffsintensive Maßnahmen erhoben worden sind, sind im Fachrecht bereits umgesetzt. So regelt etwa § 12 Absatz 2 und 3 BKAG für den Bereich des Bundeskriminalamts den Grundsatz der hypothetischen Datenneuerhebung und setzt damit die Vorgaben des BVerfG um. Vergleichbare Regelungen finden sich auch in anderen Fachgesetzen.

Verarbeitung nicht rechtsstaatlich erhobener oder zu löschender Daten

Zum Teil wird angemerkt, dass § 49 BDSG nicht das Problem der Weiterverarbeitung von nicht rechtsstaatlich erhobenen Daten für andere Zwecke regele. Außerdem fehle es an einer Regelung, ob Daten, die noch vorhanden sind, aber schon hätten gelöscht werden müssen, bei entsprechendem Anlass weiterverwendet werden könnten.

Die aufgeworfenen Fragen beziehen sich nach dem Verständnis des BMI weniger auf die zweckändernde Weiterverarbeitung als auf die Anforderungen an die Erhebung und Aufbewahrung personenbezogener Daten. Insoweit bestimmt § 47 BDSG, dass personenbezogene Daten für rechtmäßige Zwecke erhoben (Nummer 2) und sachlich richtig sein müssen (Nummer 4) und nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, gespeichert werden dürfen (Nummer 5). Darüber hinaus regelt § 75 Absatz 2 BDSG die Bedingungen, unter denen der Verantwortliche personenbezogene Daten zu löschen hat. Nach § 75 Absatz 3 Satz 1 i. V. m. § 58 Absatz 3 Nummer 2 BDSG kann die Verarbeitung von Daten, die gelöscht werden müssten, eingeschränkt werden, wenn die Daten zu Beweiszwecken in Verfahren, die Zwecken des § 45 BDSG dienen, weiter aufbewahrt werden müssen. Die Fachgesetze sehen teilweise ergänzende Bestimmungen vor (vgl. etwa § 78 Absatz 2 BKAG). Weitergehende Vorgaben im BDSG sind aus Sicht des BMI insoweit nicht erforderlich.

Verarbeitung von Daten zu Ausbildungszwecken

Einem Teil der Rückmeldungen aus dem behördlichen Bereich zufolge sei es nicht sachgerecht, dass § 49 BDSG keine zweckändernde Nutzung von Daten zu Ausbildungszwecken erlaube. Für eine wirklichkeitsgetreue Aus- und Weiterbildung an den Gerichten und Staatsanwaltschaften sei es notwendig, authentische Beispiele aus der Praxis zu nutzen. Dabei sei eine Anonymisierung häufig mit einem großen Aufwand verbunden oder sogar

[88] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 und 1 BvR 1140/06.

unmöglich, zumal auch vollständige Akten mit einer Vielzahl an personenbezogenen Daten genutzt werden müssten.

Nach Auffassung des BMI tragen die Vorschriften der §§ 49 und 50 BDSG dem Bedürfnis einer zweckändernden Verarbeitung von Daten, die zu einem der in § 45 BDSG genannten Zwecke erhoben worden sind, bzw. einer Verarbeitung der Daten zu bestimmten im öffentlichen Interesse liegenden Zwecken hinreichend Rechnung. Soweit die Verarbeitung personenbezogener Daten zu einem anderen, in § 45 BDSG nicht genannten Zweck in Rede steht, stellt § 49 Satz 2 BDSG klar, dass eine solche zweckändernde Datenverarbeitung zulässig ist, wenn sie in einer Rechtsvorschrift vorgesehen ist. Die Gesetzesbegründung führt als typischen Fall einer solchen Weiterverarbeitung die Datenübermittlung an nicht für die Zwecke der Richtlinie zuständige Behörden in § 25 BDSG an.[89] In diesem Zusammenhang dürfte aber insbesondere auch § 23 Absatz 1 BDSG von Bedeutung sein. Soweit eine der dort genannten tatbestandlichen Voraussetzungen erfüllt ist, kann die Weiterverarbeitung personenbezogener Daten durch öffentliche Stellen im Anwendungsbereich der DSGVO auf diese Vorschrift gestützt werden.[90] Nach § 23 Absatz 1 Nummer 6 BDSG können öffentliche Stellen personenbezogene Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, im Rahmen ihrer Aufgabenerfüllung insbesondere auch zu Ausbildungs- und Prüfungszwecken verarbeiten, soweit schutzwürdige Interessen der betroffenen Personen dem nicht entgegenstehen.

5.10.2.3. Rückmeldungen und Bewertung zu § 50 BDSG

Von der DSK wird angemerkt, dass diese Vorschrift nicht über die Vorgaben des Artikels 4 Absatz 3 der Richtlinie (EU) 2016/680 hinausgehe, und damit keine Konkretisierung darstelle.

Mit § 50 BDSG ist der nationale Gesetzgeber seiner Verpflichtung nachgekommen, die genannte Richtlinienvorschrift umzusetzen. Der nationale Gesetzgeber hat bei der Umsetzung einen Gestaltungsspielraum, insbesondere kann er strengere Datenschutzbestimmungen vorsehen.[91] Der Bundesgesetzgeber hat von seinem Umsetzungsspielraum Gebrauch gemacht, soweit er die Vorkehrungen, die bei einer Verarbeitung von Daten zu archivarischen, wissenschaftlichen oder statistischen Zwecken zum Schutz der Rechtsgüter der betroffenen Personen getroffen werden müssen, in § 50 Satz 2 BDSG beispielhaft beschrieben hat. Für eine weitergehende Regelung im BDSG besteht aus Sicht des BMI keine rechtliche Notwendigkeit. Dem Gesetzgeber steht es jedoch frei, die zum Schutz der Rechtsgüter der betroffenen Personen zu treffenden Vorkehrungen im Fachrecht weiter auszudifferenzieren, wie dies etwa für entsprechende Datenverarbeitungen des Bundeskriminalamts in § 21 BKAG erfolgt ist.[92]

[89] BT-Drs. 18/11325, S. 111.
[90] BT-Drs. 18/11325, S. 95.
[91] Artikel 1 Absatz 3 der Richtlinie (EU) 2016/680.
[92] Vgl. BT-Drs. 18/11325, S. 112.

5.10.2.4. Rückmeldungen und Bewertung zu § 51 BDSG

Anwendung der Vorschrift im Bereich des Strafverfahrensrechts

Wiederholt wird angemerkt, dass das Verhältnis der in § 51 BDSG getroffenen Regelungen zum Strafverfahrensrecht unklar sei. Insbesondere sei in Bezug auf § 51 BDSG nicht klar geregelt, ob und in welchem Umfang die Vorschrift nach § 500 Absatz 1 StPO auch für die Gewinnung von Beweismitteln im Strafverfahren gelte. In diesem Zusammenhang wird auch darauf hingewiesen, dass die Möglichkeit von Einwilligungen in strafprozessuale Zwangsmaßnahmen in der Rechtsprechung ohne Einschränkungen anerkannt und es daher nicht denkbar sei, dass der Gesetzgeber diese geübte Praxis grundlegend haben ändern wollen. Aus diesem Grund wird eine Streichung der Formulierung „nach einer Rechtsvorschrift“ in § 51 Absatz 1 BDSG angeregt.

Darüber hinaus wird die Sachgerechtigkeit der Widerrufsmöglichkeit nach § 51 Absatz 3 BDSG mehrfach in Frage gestellt. Wären Einwilligungen in strafprozessualen Maßnahmen frei widerruflich, so könnten die so erlangten Beweise nach dem Widerruf nicht mehr genutzt werden, sodass die Aufklärung von Straftaten erheblich erschwert werden würde.

In Teilen der Rückmeldungen wird außerdem angemerkt, dass unklar sei, ob eine Einwilligung im Strafverfahren gemäß § 51 Absatz 4 BDSG freiwillig erteilt werden könne, da die konkrete Maßnahme auch jederzeit durch die Strafverfolgungsbehörden unter Einbeziehung des zuständigen Ermittlungsrichters angeordnet werden könne. In den Rückmeldungen wird außerdem mehrfach vorgetragen, dass nicht deutlich sei, ob und inwieweit die in § 51 Absatz 4 BDSG geregelten Belehrungs- und Dokumentationspflichten im Kontext strafrechtlicher Einwilligungen anzuwenden seien.

§ 1 Absatz 2 Satz 2 BDSG stellt klar, dass die jeweilige bereichsspezifische Spezialregelung vorrangig gegenüber der allgemeinen Vorschrift ist, wenn eine Tatbestandskongruenz vorliegt. Liegt allerdings keine bereichsspezifische Datenschutzregelung für einen vergleichbaren Sachverhalt vor, so übernimmt das BDSG seine lückenfüllende Auffangfunktion. Diesen Leitgedanken greift § 500 StPO in Bezug auf die Anwendung von Teil 3 BDSG auf die Datenverarbeitung durch die öffentlichen Stellen der Länder im Anwendungsbereich des Strafverfahrensrechts nochmals auf, indem er bestimmt, dass Teil 3 BDSG entsprechend anzuwenden ist (Absatz 1), was jedoch nur gilt, soweit nicht im Strafverfahrensrecht etwas anderes bestimmt ist (Absatz 2 Nummer 1). Ausgangspunkt für die Bestimmung der datenschutzrechtlichen Pflichten im Bereich des Strafverfahrens ist daher immer Teil 3 BDSG; ergänzend ist zu prüfen, ob bereichsspezifische Sonderregelungen bestehen.[93] Soweit die StPO eigene, nicht abschließende datenschutzrechtliche Vorschriften enthält, treten sie ergänzend neben die allgemeinen Regelungen des BDSG. Danach gelten die allgemeinen Vorgaben für die Anforderungen an die datenschutzrechtliche Einwilli-

[93] BT-Drs. 19/4671, S. 44.

gung einer betroffenen Person nach § 51 BDSG auch im Strafverfahren. Vor diesem Hintergrund erscheint eine weitergehende Regelung des Anwendungsverhältnisses in Bezug auf das Strafverfahrensrecht im BDSG selbst aus Sicht des BMI nicht veranlasst.

Für eine Streichung der Formulierung „nach einer Rechtsvorschrift" in § 51 Absatz 1 BDSG besteht dabei aus rechtlichen Gründen kein Raum. Die Vorschrift stellt keine eigenständige Ermächtigung für eine Datenverarbeitung auf Grundlage einer Einwilligung dar. Vielmehr schreibt § 51 BDSG vor, dass die Einwilligung gesetzlich geregelt sein muss. Unter welchen Umständen die Einwilligung der betroffenen Person im Strafverfahren für die Verarbeitung personenbezogener Daten maßgeblich sein kann, ergibt sich aus dem Fachrecht selbst, etwa aus § 161 Absatz 3 StPO.[94]

Form der Einwilligung

Vereinzelt wird in Bezug auf § 51 Absatz 2 BDSG eine Klarstellung dahingehend angeregt, dass eine Einwilligung in schriftlicher Form nicht erforderlich sei.

Aus Sicht des BMI besteht kein Bedarf für eine klarstellende Regelung. Dass die Schriftform für die Einwilligung nicht erforderlich ist, folgt bereits aus dem (offenen) Wortlaut von § 51 Absatz 1 BDSG, der lediglich von einer „Einwilligung" spricht. Abgesehen davon stellt § 51 Absatz 2 BDSG spezifische Anforderungen für den Fall auf, dass die Einwilligung durch schriftliche Erklärung erfolgt. Daraus folgt im Umkehrschluss, dass die Einwilligung grundsätzlich keiner Schriftform bedarf.

5.10.3. Schlussfolgerungen

Die Rückmeldungen zu den §§ 48 bis 51 BDSG lassen darauf schließen, dass die Zielsetzungen des Gesetzgebers grundsätzlich erreicht worden sind. Die in den Rückmeldungen kommentierten Anwendungsschwierigkeiten betreffen in erster Linie das Zusammenspiel zwischen BDSG und dem Strafverfahrensrecht. Etwaige Klarstellungen wären in den jeweiligen Fachgesetzen vorzunehmen. Änderungsbedarf in Bezug auf das BDSG sieht das BMI insoweit nicht.

[94] BT-Drs. 19/4671, S. 44.

5.11. Rechte der betroffenen Person – §§ 55 bis 61 BDSG

5.11.1. Zielsetzung und Gegenstand der Regelungen

Mit den §§ 55 bis 61 BDSG hat der Gesetzgeber die Rechte der von der Datenverarbeitung betroffenen Personen festgelegt.

§ 55 BDSG dient der Umsetzung von Artikel 13 Absatz 1 der Richtlinie (EU) 2016/680. Die Vorschrift regelt aktive Informationspflichten des Verantwortlichen gegenüber betroffenen Personen unabhängig von der Geltendmachung von Rechten der betroffenen Person.

§ 56 BDSG betrifft Fälle, in denen in fachgesetzlichen Regelungen eine aktive Benachrichtigung betroffener Personen vorgesehen ist. Absatz 1 regelt, welche Informationen betroffenen Personen von dem Verantwortlichen bei entsprechender fachgesetzlicher Anordnung aktiv übermittelt werden müssen. Absatz 2 ermöglicht es, zu den dort genannten Zwecken von der Bereitstellung der Informationen abzusehen, sie einzuschränken oder sie aufzuschieben. Absatz 3 statuiert ein Zustimmungserfordernis der dort genannten Stellen, wenn sich die Benachrichtigung auf die Übermittlung an diese Stellen bezieht.

§ 57 BDSG normiert das Auskunftsrecht und dessen Einschränkungen. Das Auskunftsrecht setzt – im Gegensatz zu den in den §§ 55 und 56 BDSG angesprochenen Informations- und Benachrichtigungspflichten – einen entsprechenden Antrag der betroffenen Person voraus. Absatz 1 legt den Umfang des der betroffenen Person zustehenden Auskunftsrechts fest. Nach Absatz 2 gilt das Auskunftsrecht nicht für Daten, die nur aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen. Absatz 3 sieht vor, dass von der Auskunftserteilung abzusehen ist, wenn der Antrag der betroffenen Person nicht konkret genug und der Aufwand für die Auskunft daher unverhältnismäßig ist. Absatz 4 normiert, dass unter den Voraussetzungen des § 56 Absatz 2 BDSG von einer Auskunft abgesehen oder die Auskunftserteilung ausgeschlossen oder vollständig oder teilweise eingeschränkt werden kann. Absatz 5 statuiert ein Zustimmungserfordernis der dort genannten Stellen, wenn sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an diese Stellen bezieht. Absatz 6 regelt, dass der Verantwortliche die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft grundsätzlich zu unterrichten hat. Absatz 7 dient der Umsetzung von Artikel 17 der Richtlinie (EU) 2016/680. Satz 2 sieht eine Unterrichtung der betroffenen Person durch den Verantwortlichen über die Möglichkeit der Anrufung der oder von gerichtlichem Rechtsschutz vor. Diese Unterrichtungspflicht gilt allerdings nicht in Fällen, in denen der Verantwortliche berechtigt ist, von einer Information über das Absehen von oder die Einschränkung der Auskunft an den Antragsteller ganz abzusehen.

§ 58 BDSG regelt die Rechte der betroffenen Personen auf Berichtigung und Löschung der sie betreffenden personenbezogenen Daten sowie auf Einschränkung der Verarbeitung.

Absatz 1 betrifft das Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten. Während Absatz 2 das Recht der betroffenen Person auf Löschung der sie betreffenden Daten regelt, betrifft Absatz 3 die Voraussetzungen, unter denen an die Stelle der Löschung eine Einschränkung der Verarbeitung treten kann.

In § 59 BDSG, der das Verfahren für die Ausübung der Rechte der betroffenen Personen betrifft, werden Elemente von Artikel 12 der Richtlinie (EU) 2016/680 umgesetzt. Absatz 1 regelt insoweit, dass der Verantwortliche mit der betroffenen Person unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren hat.

§ 60 BDSG stellt klar, dass sich betroffene Personen mit Beschwerden über die bei Verantwortlichen durchgeführte Verarbeitung an die oder den BfDI wenden können.

§ 61 BDSG setzt Artikel 53 der Richtlinie (EU) 2016/680 um und bestimmt, dass Adressaten von verbindlichen Entscheidungen der oder des BfDI und betroffene Personen in Fällen der Untätigkeit der oder des BfDI unbeschadet anderer Rechtsbehelfe gerichtlichen Rechtsschutz gegen den oder die BfDI suchen können.

5.11.2. Empirische Ergebnisse und Bewertung

Rückmeldungen zu den §§ 55 bis 59 BDSG kamen vonseiten der DSK, aus dem Kreis der Bundesbehörden und aus den Ländern. Zu den §§ 60 und 61 BDSG wurden keine Anmerkungen übermittelt.

5.11.3. Rückmeldungen und Bewertung zu § 55 BDSG

Die Vorschrift wird als sachgerecht und praktikabel bewertet. Beanstandungen hinsichtlich der Normenklarheit liegen ebenfalls nicht vor.

5.11.4. Rückmeldungen und Bewertung zu § 56 BDSG

Verhältnis zum Fachrecht

Einem Teil der Rückmeldungen zufolge sei das Verhältnis der Benachrichtigungspflicht in § 56 BDSG zu den jeweiligen fachrechtlichen Regelungen unklar. So stelle sich etwa die Frage, ob § 101 StPO als bereichsspezifische Sonderregelung dem § 56 BDSG vorgehe oder die Regelungen kombiniert werden müssten. Außerdem wird angemerkt, dass das BDSG strenger als das Strafverfahrensrecht sei, soweit in § 56 Absatz 2 BDSG ein Abwägungserfordernis in Bezug auf die Interessen der betroffenen Person auch für die Fälle statuiert werde, in denen eine Verfahrensgefährdung vorliege (vgl. § 406e Absatz 2 Satz 2 und 3 StPO). Vereinzelt wird – auch im Zusammenhang mit § 57 Absatz 4 BDSG – angeregt, die Regelung in § 56 Absatz 2 BDSG mit dem Fachrecht (etwa § 21 EGGVG) und den landesrechtlichen Bestimmungen zu synchronisieren.

Soweit die Frage nach dem Verhältnis zum Fachrecht aufgeworfen wird, ist aus Sicht des BMI darauf hinzuweisen, dass § 56 BDSG nach seinem Absatz 1 Anwendung findet, wenn die Benachrichtigung betroffener Personen in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet ist. Für diesen Fall sieht die Vorschrift bestimmte Angaben vor, die in der Benachrichtigung mindestens enthalten sein müssen. Da es sich um Mindestangaben handelt, ist es dem Gesetzgeber unbenommen, mit einer entsprechenden Pflicht zur Benachrichtigung auch weitere Inhalte der Benachrichtigung im jeweiligen Fachrecht zu regeln. So ordnet etwa § 101 Absatz 4 StPO in Satz 1 eine Benachrichtigung an und trifft in Satz 2 zusätzliche Regelungen über die Hinweise, die bei der Benachrichtigung zu erteilen sind. Es handelt sich daher um eine spezielle Rechtsvorschrift im Sinne des § 56 Absatz 1 BDSG.

Im Hinblick auf die in § 56 Absatz 2 BDSG geregelten Voraussetzungen, unter denen von einer Benachrichtigung abgesehen oder eine eingeschränkte Benachrichtigung erteilt werden kann, und etwaige davon abweichende bereichsspezifische Vorgaben in den Fachgesetzen ist erneut darauf hinzuweisen, dass bereichsspezifische Sonderregelungen bei Tatbestandskongruenz dem BDSG vorgehen.[95] In Bezug auf die Rechte betroffener Personen ist insoweit z. B. nach den Sachverhalten „Informationspflicht", „Auskunftsrecht" oder „Widerspruchsrecht" zu unterscheiden.

Regelung der Voraussetzungen für die Versagung der Zustimmung zur Benachrichtigung durch die zu beteiligenden Stellen

Vereinzelt wird angemerkt, dass in § 56 Absatz 3 BDSG die Voraussetzungen geregelt werden sollten, nach denen die dort genannten Behörden ihre Zustimmung zur Benachrichtigung an betroffene Personen versagen dürfen. Andernfalls könne die Rechtmäßigkeit einer Verweigerung nicht geprüft werden. Entsprechende Vorschläge werden auch in Bezug auf § 57 Absatz 5 BDSG im Hinblick auf die Verweigerung der Auskunftserteilung gegenüber betroffenen Personen vorgetragen.

Das BMI sieht keine Notwendigkeit dafür, in § 56 Absatz 3 BDSG die Voraussetzungen zu regeln, unter denen die betreffenden Behörden ihre Zustimmung zu einer Benachrichtigung der betroffenen Person verweigern können. Der Vorschrift liegt der Gedanke zugrunde, dass im Fachrecht eine Benachrichtigungspflicht vorgesehen oder angeordnet ist, wenn Daten vom Verantwortlichen an Behörden der nationalen Sicherheit und Verteidigung übermittelt werden.[96] Daher bleibt auch eine Regelung der Voraussetzungen, unter denen die betreffenden Behörden ihre Zustimmung zu der Benachrichtigung versagen können, dem jeweiligen Fachrecht vorbehalten. Die Nutzung der Möglichkeit, von der Bereitstellung der in § 56 Absatz 1 BDSG genannten Informationen abzusehen, sie einzuschränken oder aufzuschieben, wird dabei den allgemeinen Verhältnismäßigkeitsanforderungen genügen müssen. So wird der Verantwortliche im Einzelfall zu prüfen haben, ob

[95] BT-Drs. 18/11325, S. 79.
[96] Sydow, Bundesdatenschutzgesetz, Kommentar, 1. Auflage 2020, § 56 Rn. 27.

die Auskunft etwa nur teilweise eingeschränkt oder zu einem späteren Zeitpunkt erteilt werden kann.[97] Aber auch diese auf allgemeinen Rechtsgrundsätzen beruhenden Anforderungen müssen nicht ausdrücklich im BDSG geregelt werden.

5.11.4.1. Rückmeldungen und Bewertung zu § 57 BDSG

Verhältnis zum Fachrecht

Einem Teil der Rückmeldungen zufolge stellt § 57 Absatz 6 Satz 1 BDSG die Strafverfolgung vor Probleme. Durch gezielt gestellte Anträge könnten Strafverteidiger aufgrund der Ablehnung der Auskunftserteilung oder einer Nichtbeantwortung des Auskunftsersuchens Rückschlüsse auf nicht konkret benannte Ermittlungsverfahren ziehen. Vor diesem Hintergrund wird angeregt, den datenschutzrechtlichen Auskunftsanspruch für laufende Ermittlungsverfahren insgesamt auszuschließen.

Nach § 57 Absatz 6 Satz 2 BDSG kann eine Unterrichtung der betroffenen Person über das Absehen von oder die Einschränkung einer Auskunft unterbleiben, wenn bereits die Erteilung dieser Informationen die Erfüllung der in § 45 BDSG genannten Aufgaben, die öffentliche Sicherheit oder Rechtsgüter Dritter gefährden würde. Für eine weitergehende Ausnahmeregelung für den Bereich des Strafverfahrens im BDSG besteht aus Sicht des BMI aufgrund der Gesetzessystematik kein Raum. Soweit Bedarf für eine entsprechende strafverfahrensrechtliche Ausnahmeregelung bestehen sollte, wäre dies im Fachrecht zu regeln.

Gegenstand des Auskunftsrechts

Einem Teil der Rückmeldungen zufolge sei unklar, ob von dem Auskunftsanspruch des § 57 Absatz 1 BDSG auch Protokolldaten erfasst seien.

Vonseiten der DSK wird angemerkt, dass § 57 Absatz 2 BDSG den Vorgaben der Richtlinie (EU) 2016/680 widerspreche. Artikel 15 Absatz 1 der genannten Richtlinie bestimme abschließend, unter welchen Voraussetzungen das Auskunftsrecht eingeschränkt werden könne, und sehe eine Begrenzung des Auskunftsrechts auf bestimmte personenbezogene Daten nicht vor. Die Vorschrift sei daher zu streichen.

Nach § 57 Absatz 2 BDSG gilt das Auskunftsrecht nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. § 76 Absatz 3 BDSG bestimmt, dass Protokolldaten für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die oder den behördlichen Daten-

[97] BT-Drs. 18/11325, S. 113.

schutzbeauftragten und die oder den BfDI sowie die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten sowie für Strafverfahren verwendet werden dürfen. Damit fallen Protokolldaten grundsätzlich in den Anwendungsbereich der Bereichsausnahme.

Dabei teilt das BMI die Kritik an der fehlenden Richtlinienkonformität der Bereichsausnahme in § 57 Absatz 2 BDSG nicht. Aus Artikel 25 Absatz 2 der Richtlinie (EU) 2016/680 folgt, dass Protokolle ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung, der Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für Strafverfahren verwendet werden dürfen. Darüber hinaus stellt § 57 Absatz 3 BDSG klar, dass der Verantwortliche sowie der Auftragsverarbeiter die Protokolle der Aufsichtsbehörde auf Anforderung zur Verfügung stellen. Im Hinblick darauf ist die Regelung in § 57 Absatz 2 BDSG aus Sicht des BMI nicht zu beanstanden.

Absehen von der Auskunftserteilung wegen unverhältnismäßigen Aufwands

Vereinzelt wird angemerkt, dass unklar sei, wann ein unverhältnismäßiger Aufwand im Sinne des § 57 Absatz 3 BDSG vorliege, um ein nicht hinreichend konkretisiertes Auskunftsersuchen ablehnen zu können. Außerdem sei offen, in welchem Umfang die Behörde hierfür darlegungspflichtig sei. Darüber hinaus wird vereinzelt angeregt, § 57 Absatz 3 BDSG in eine Ermessensnorm umzuwandeln, da betroffene Personen in bestimmten Fällen gar nicht in der Lage wären, die erforderlichen Angaben zu machen.

Aus Sicht des BMI stellt § 57 Absatz 3 BDSG grundsätzlich hinreichend klar, unter welchen Voraussetzungen von einer Auskunftserteilung abzusehen ist. Dies ist der Fall, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und sich deshalb der für die Erteilung der Auskunft erforderliche Aufwand als unverhältnismäßig in Bezug auf das Interesse der betroffenen Person an der Auskunftserteilung darstellt. Daraus folgt, dass die fehlende Mitwirkung auf Seiten der betroffenen Person ursächlich für den unverhältnismäßigen Aufwand sein muss. Der mit der Auskunftserteilung verbundene Verwaltungsaufwand hängt dabei vom konkreten Einzelfall ab. Nach den konkreten Umständen bestimmt sich auch, ob eine Auskunftserteilung unverhältnismäßig wäre. Der Aufwand ist vom Verantwortlichen zu bewerten und die Bewertung zu dokumentieren. Für die Bewertung dürfte insbesondere maßgeblich sein, ob und in welchem Umfang der mit der Auskunftserteilung verbundene Aufwand dazu führt, dass behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren behindert werden. Darauf weist auch die Richtlinie (EU) 2016/680 hin.[98] Nach dem Verständnis des BMI hat sich der Gesetzgeber bewusst für die Verwendung eines unbestimmten Rechtsbegriffs entschieden, damit den Umständen des jeweiligen Einzelfalls in der Praxis Rech-

[98] Vgl. Artikel 15 Absatz 1 Buchstabe a sowie Erwägungsgrund 44 zur der Richtlinie (EU) 2016/680.

nung getragen werden kann. Das BMI wird jedoch weiter prüfen, ob eine klarstellende Regelung, die etwa den Regelungsgedanken aus der Richtlinie (EU) 2016/680 stärker zum Ausdruck bringen könnte, umgesetzt werden kann.

Eine Umwandlung des § 57 Absatz 3 BDSG in eine Ermessensvorschrift erscheint jedoch nicht angezeigt. Der Umstand, dass betroffene Personen eventuell nicht in der Lage sind, bestimmte Angaben zu machen, ist im Rahmen der tatbestandlichen Voraussetzungen zu würdigen. Danach ist die Bewertung, ob der mit der Auskunftserteilung verbundene Aufwand unverhältnismäßig ist, unter Berücksichtigung des Informationsinteresses der betroffenen Person vorzunehmen. Einer erneuten Berücksichtigung der genannten Umstände im Rahmen eines behördlichen Ermessens ist aus Sicht des BMI nicht angezeigt.

Möglichkeit von neutralen Auskünften oder Negativ-Auskünften zum Schutz des Ermittlungsverfahrens

Aus dem Kreis der Bundesbehörden wird vorgetragen, dass die Regelung in § 57 Absatz 4 BDSG, wonach unter den Voraussetzungen des § 56 Absatz 2 BDSG von der Auskunftserteilung abgesehen oder die Auskunft teilweise oder vollständig eingeschränkt werden kann, im Rahmen von verdeckt geführten Ermittlungsverfahren nicht praxistauglich sei. Zwar könne zum Schutz des Ermittlungsverfahrens nach § 57 Absatz 6 Satz 2 und 3 BDSG sowohl von der Unterrichtung der betroffenen Person als auch von der Begründung, weshalb von der Unterrichtung abgesehen wurde, abgesehen werden. Dennoch könne die betroffene Person nach Ablauf von drei Monaten eine Untätigkeitsklage nach § 75 VwGO erheben. Es wird daher eine Regelung vorgeschlagen, nach der in den beschriebenen Fällen eine neutrale Auskunft, mit dem Inhalt, dass keine Daten vorliegen, über die Auskunft erteilt werden könne, oder eine Negativ-Auskunft zulässig wäre.

Aus Sicht des BMI bestehen Zweifel daran, dass eine Regelung, nach der eine neutrale Auskunft, mit dem Inhalt, dass keine Daten vorliegen, über die Auskunft erteilt werden könnte, oder eine Negativ-Auskunft zulässig wären, richtlinienkonform umsetzbar wäre. Die Richtlinie (EU) 2016/680 sieht in Artikel 15 Absatz 1 Ausnahmen in Form der vollständigen oder teilweisen Einschränkung der Auskunftspflicht bzw. des Absehens von der Auskunft vor. Diese Ausnahmen unterliegen den Grundsätzen der Erforderlichkeit und der Verhältnismäßigkeit und müssen den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung tragen. Die Möglichkeit einer neutralen Auskunft oder einer Negativ-Auskunft regelt die Richtlinie (EU) 2016/680 insoweit nicht.

Unterrichtung über das Recht zur Anrufung der oder des BfDI und auf gerichtlichen Rechtsschutz

Die DSK bemängelt, dass § 57 Absatz 7 Satz 2 BDSG insofern der Richtlinie (EU) 2016/680 widerspreche, als der Verantwortliche die betroffene Person nicht nur im Falle einer Unterrichtung über das Absehen von oder die Einschränkung der Auskunft, sondern stets –

ggf. mit der Eingangs- oder einer Zwischennachricht – über das Recht zur Anrufung der oder des BfDI und den gerichtlichen Rechtsbehelf informieren müsse.

Aus Sicht des BMI kann diesem Einwand nicht gefolgt werden. Mit § 57 Absatz 7 Satz 2 BDSG hat der Gesetzgeber die Vorgaben aus Artikel 15 Absatz 3 der Richtlinie (EU) 2016/680 umgesetzt. Danach hat der Verantwortliche die betroffene Person über die Möglichkeit, eine Beschwerde bei der Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen, in den Fällen zu informieren, in denen die Person über das Absehen von oder die Einschränkung der Auskunftserteilung unterrichtet wird. Besteht jedoch keine Pflicht, den Antragsteller über das Absehen von der Auskunft oder ihre Einschränkung zu unterrichten, weil bereits die Erteilung dieser Information die Erfüllung der in § 45 BDSG genannten Aufgaben, die öffentliche Sicherheit oder Rechtsgüter Dritter gefährden würde, kann der Verantwortliche auch von einer Information des Antragstellers über das Beschwerderecht und den gerichtlichen Rechtsschutz absehen.[99] Sinn und Zweck der Regelung ist es, zu verhindern, dass der Antragsteller auf eine Verarbeitung von ihn betreffenden personenbezogenen Daten durch den Verantwortlichen schließt und dadurch die genannten Schutzgüter gefährdet werden. Dieser Regelungsgedanke liegt auch Artikel 15 Absatz 3 Satz 2 der Richtlinie (EU) 2016/680 zugrunde. Eine Vorgabe, nach der der Verantwortliche in jedem Fall den Antragsteller über das Recht zur Anrufung der oder des BfDI und den gerichtlichen Rechtsbehelf informieren müsste, würde diesem gesetzgeberischen Ziel zuwiderlaufen. Außerdem ist zu berücksichtigen, dass der Verantwortliche bereits nach § 55 Nummer 4 BDSG verpflichtet ist, in allgemeiner und für jedermann zugänglichen Form über das Recht zur Anrufung der oder des BfDI zu informieren. Eine entsprechende allgemeine Information kann etwa über die Website des Verantwortlichen erfolgen. Abgesehen davon haben betroffene Personen nach § 75 VwGO das Recht, nach Ablauf von drei Monaten Untätigkeitsklage vor dem Verwaltungsgericht zu erheben. Auch vor diesem Hintergrund erscheint die Regelung, wonach auf die individuelle Unterrichtung des Antragstellers zum Schutz der Ermittlungen, der öffentlichen Sicherheit oder der Rechtsgüter Dritter verzichtet werden kann, interessengerecht.

Vereinzelt wird die Normenklarheit von § 57 Absatz 7 Satz 2 BDSG in Frage gestellt, da sich daraus nicht ergebe, welcher Rechtsweg einschlägig sei, und eine Regelung der gerichtlichen Zuständigkeit angeregt.

Der einschlägige Rechtsweg und das zuständige Gericht bestimmt sich nach den allgemeinen verfahrensrechtlichen Vorschriften. Das BMI sieht insoweit keinen Bedarf für eine klarstellende Regelung im BDSG.

[99] BT-Drs. 18/11325, S. 114.

Ausübung des Auskunftsrechts mittels der oder des BfDI

Die DSK kritisiert die Regelung in § 57 Absatz 7 Satz 3 BDSG, wonach die Auskunft auf Verlangen der betroffenen Person dem oder der BfDI zu erteilen ist, „soweit nicht die zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde“, und regt eine Streichung des betreffenden Halbsatzes an. Zur Begründung führt die DSK an, dass Artikel 17 der Richtlinie (EU) 2016/680 eine solche Einschränkung nicht vorsehe. Zudem sei durch die verpflichtende Sicherheitsüberprüfung der Mitarbeiterinnen und Mitarbeiter der oder des BfDI den Aspekten der Sicherheit des Bundes und der Länder hinreichend Rechnung getragen.

Das BMI teilt diese Sichtweise nicht. § 57 Absatz 7 Satz 3 BDSG nimmt den Regelungsgedanken des § 19 Absatz 6 Satz 1 BDSG a. F. auf, wonach die Auskunft auf Verlangen des Betroffenen dem oder dem BfDI zu erteilen war, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellte, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet wurde. Durch die Fortführung des Regelungsgedankens wird klargestellt, dass Rechte der betroffenen Person nicht indirekt über die Aufsichtsbehörde ausgeübt werden können, wenn ein Bezug zu Tätigkeiten besteht, die vom Anwendungsbereich der Richtlinie (EU) 2016/680 ausgenommen sind, weil sie Belange der nationalen Sicherheit betreffen.[100] In Anbetracht dessen überzeugt der Hinweis, dass die genannte Richtlinie eine entsprechende Einschränkung nicht vorsehe, aus Sicht des BMI nicht. Vielmehr hat der Bundesgesetzgeber mit § 57 Absatz 7 Satz 3 BDSG von dem ihm zustehenden Umsetzungsspielraum in zulässiger und sachgerechter Weise Gebrauch gemacht.

Sonstige Anmerkungen

Vonseiten der DSK wird eine Klarstellung gewünscht, wonach der Verantwortliche im Rahmen des § 57 Absatz 4 BDSG das Vorliegen der Voraussetzungen bei wiederholten Auskunftsersuchen der betroffenen Person stets neu zu prüfen habe. Schließlich merkt die DSK an, dass in § 57 Absatz 6 Satz 2 BDSG deutlich gemacht werden müsse, dass ein Absehen von der Unterrichtung nur Ultima Ratio sein könne.

Das BMI sieht insoweit keinen Anpassungsbedarf. Dass die tatbestandlichen Voraussetzungen für ein Absehen von oder der Einschränkung der Auskunftserteilung bei jedem Ersuchen erneut zu prüfen sind, ergibt sich bereits aus allgemeinen Rechtsgrundsätzen. Auch der Verzicht auf eine entsprechende Unterrichtung der betroffenen Person muss den Anforderungen an ein rechtmäßiges Verwaltungshandeln, insbesondere dem Verhältnismäßigkeitsgrundsatz, genügen. Die betreffenden Anforderungen gelten allgemein für die Teil 3 BDSG unterworfenen öffentlichen Stellen und bedürfen keiner spezialgesetzlichen Regelung.

[100] Diese Ausnahme vom Anwendungsbereich ergibt sich aus Artikel 2 Absatz 3 Buchstabe a der Richtlinie (EU) 2016/680.

5.11.4.2. Rückmeldungen und Bewertung zu § 58 BDSG

Streichung der Einschränkung „wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist“

Die DSK regt an, die Einschränkung des § 58 Absatz 1 Satz 5 BDSG „wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist“ zu streichen. Die Regelung berge die Gefahr, dass ein Antrag aus Gründen des Verwaltungsaufwands abgelehnt werde, obwohl dies kein Kriterium der Richtlinie (EU) 2016/680 sei.

Das BMI sieht insoweit keinen Anpassungsbedarf. Die Einschränkung in § 58 Absatz 1 Satz 5 BDSG setzt die Vorgaben von Artikel 16 Absatz 1 Satz 2 der Richtlinie (EU) 2016/680 um, wonach die Mitgliedstaaten vorsehen, dass die betroffene Person unter Berücksichtigung der Zwecke der Verarbeitung das Recht hat, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

Geringe Praktikabilität des § 58 Absatz 3 BDSG

Die DSK kritisiert, dass § 58 Absatz 3 Satz 1 Nummer 3 BDSG nicht praktikabel sei: Wenn der Verantwortliche seine Verarbeitung so gestalte, dass nur mit unverhältnismäßig hohem Aufwand gelöscht werden könne, gewährleiste er insbesondere die Intervernierbarkeit nicht und verarbeite damit die Daten rechtswidrig.

Das BMI teilt die Kritik an der Praktikabilität bzw. Sachgerechtigkeit von § 58 Absatz 3 Satz 1 Nummer 3 BDSG nicht. Die Möglichkeit, von der Löschung wegen unverhältnismäßigen Aufwands abzusehen, hat der Gesetzgeber als restriktiv auszulegende Ausnahmeregelung ausgestaltet. Hinzu kommt, dass der Verantwortliche schon nach den Grundsätzen der Datenverarbeitung verpflichtet ist, die zum Einsatz kommende IT-Infrastruktur darauf auszulegen, dass eine Löschung von unrichtigen Daten oder Daten, die nicht (mehr) verarbeitet werden dürfen, technisch umsetzbar ist.[101] Dies schließt es nicht aus, dass es Fälle geben kann, in denen eine Löschung der Daten wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

5.11.4.3. Rückmeldungen und Bewertung zu § 59 BDSG

Vereinzelt wird angemerkt, dass die in § 59 Absatz 1 Satz 1 BDSG enthaltene Verpflichtung, in klarer und einfacher Sprache in präziser verständlicher und leicht zugänglicher Form zu kommunizieren, nicht erfüllt werden könne, da die Regelungen zu den Rechten der betroffenen Person auf mehrere Gesetze – BDSG, bereichsspezifische Regelungen etwa in der StPO sowie landesrechtliche Regelungen – verteilt seien. Das Auffinden der Regelungen werde durch diese Komplexität erheblich beeinträchtigt.

[101] Vgl. BT-Drs. 18/11325, S. 114 f.

Aus Sicht des BMI steht die Kritik in keinem Zusammenhang mit § 59 Absatz 1 Satz 1 BDSG. Die Regelung bezieht sich auf die Form, in der der Verantwortliche mit der betroffenen Person zu kommunizieren hat, nicht jedoch auf die Inhalte der Kommunikation. Soweit die Systematik des Datenschutzrechts bemängelt wird, wird auf die bereits an anderer Stelle gemachten Ausführungen verwiesen.

5.11.5. Schlussfolgerungen

Die Regelungen zu den Rechten der betroffenen Personen werden durch die Rechtsanwender insgesamt als normenklar und sachgerecht bewertet. Die zahlreichen Anmerkungen insbesondere zu den §§ 57 und 58 BDSG zeigen jedoch, dass die Anwendung einzelner Vorschriften in der Praxis noch zahlreiche Fragen aufwirft. Grundsätzlichen Änderungsbedarf sieht das BMI aktuell nicht. Das BMI wird jedoch den Bedarf für gesetzliche Klarstellungen in § 57 Absatz 3 BDSG weiter prüfen.

5.12. Verantwortliche und Auftragsverarbeiter – §§ 62 und 63 BDSG

5.12.1. Zielsetzung und Gegenstand der Regelungen

§ 62 BDSG dient der Umsetzung von Artikel 22 der Richtlinie (EU) 2016/680 und regelt die Anforderungen an eine Auftragsverarbeitung. Absatz 1 regelt die Pflichten des Verantwortlichen im Rahmen von Auftragsverarbeitungsverhältnissen. Absatz 2 beschreibt an den Auftragsverarbeiter zu stellende Anforderungen. In Absatz 5 werden die erforderlichen Inhalte einer der Auftragsverarbeitung zugrundeliegenden Vereinbarung niedergelegt.

§ 63 BDSG regelt die Rahmenbedingungen für gemeinsam Verantwortliche sowie die Anforderungen an die zu treffende Vereinbarung zwischen den gemeinsam Verantwortlichen.

5.12.2. Empirische Ergebnisse und Bewertung

Zu den §§ 62 und 63 BDSG sind Rückmeldungen aus den Ländern eingegangen.

5.12.2.1. Rückmeldungen und Bewertung zu § 62 BDSG

Begriff der „Auftragsverarbeitung“

In den Rückmeldungen wird vereinzelt angemerkt, dass in der Vorschrift des § 62 BDSG eine Definition der „Auftragsverarbeitung“ fehle.

Eine solche Definition ist aus Sicht des BMI nicht erforderlich. Die die Auftragsverarbeitung prägenden Merkmale sind bereits hinreichend klar im BDSG geregelt. § 46 Nummer 8 BDSG enthält eine Bestimmung des Begriffs „Auftragsverarbeiter“. Danach ist ein Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Das die Auftragsverarbeitung prägende Unterordnungsverhältnis kommt in § 62 BDSG in vielfacher Weise zum Ausdruck. So unterliegt der Auftragsverarbeiter nach Absatz 5 den Weisungen des Verantwortlichen (Satz 2 Nummer 1), muss dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen (Satz 2 Nummer 5) und nach Überprüfungen durch den Verantwortlichen dulden (Satz 2 Nummer 6). Auch darf der Auftragsverarbeiter nach Absatz 3 ohne die vorherige Zustimmung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen. Aus der Definition des „Verantwortlichen“ in § 46 Nummer 7 BDSG folgt im Umkehrschluss, dass für die Auftragsverarbeitung die vom beauftragenden Verantwortlichen bestimmten Zwecke und Mittel der Verarbeitung prägend sind. Dies wird durch § 62 Absatz 7 BDSG bestätigt, der die Folgen für den Fall bestimmt, dass der Auftragsverarbeiter die vom Verantwortlichen festgelegten Zwecke und Mittel der Verarbeitung missachtet.

Rechtslage in Dreiecksverhältnissen

Einem Teil der Rückmeldungen zufolge sei unklar, wie die Rechtslage in Dreiecksverhältnissen zu bewerten sei, wenn ein IT-Dienstleister (Auftragsverarbeiter) zentral durch eine Behörde (Dritter) mit der Datenverarbeitung für mehrere andere Behörden (Verantwortliche) beauftragt werden solle. § 62 BDSG lasse offen, ob der Dritte zum Abschluss eines Auftragsverarbeitungsvertrages mit dem Dienstleister für die Verantwortlichen bevollmächtigt werden könne, oder ob der Auftragsverarbeitungsvertrag direkt zwischen den Verantwortlichen und dem Dienstleister zu schließen sei.

Das BMI sieht hier keine Notwendigkeit einer gesetzlichen Klarstellung. Bei der Auftragsverarbeitungsvereinbarung dürfte es sich im Regelfall um ein Vertragsverhältnis handeln, dessen Wirksamkeit sich nach vertragsrechtlichen Grundsätzen bestimmt. Insoweit gelten für die Auftragsverarbeitungsvereinbarung u. a. die allgemeinen Regelungen über die Stellvertretung beim Abschluss von Verträgen. Soweit eine Verwaltungsvereinbarung als Grundlage für die Auftragsverarbeitung dient, richten sich die Vertretungsverhältnisse nach den organisationsrechtlichen Regelungen der betroffenen öffentlichen Stellen. § 62 BDSG enthält keine Vorgaben in Bezug auf die geschilderten Dreiecksverhältnisse und schließt insoweit eine Beauftragung des Auftragsverarbeiters durch einen Dritten mit Wirkung für und gegen den Verantwortlichen nicht aus. Die Vorschrift gewährt dem Verantwortlichen damit weitgehende Flexibilität auch im Kontext entsprechender Dreiecksverhältnisse.

5.12.2.2. Rückmeldungen und Bewertung zu § 63 BDSG

Anwendung innerhalb der Behördenstrukturen

In den Rückmeldungen wird teilweise angemerkt, dass die Regelung in § 63 Satz 2 BDSG, wonach gemeinsam Verantwortliche ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in einer Vereinbarung festzulegen haben, nicht praxisgerecht sei. Zum einen gehe die Vorschrift ersichtlich nur von gleichgeordneten Stellen aus, obwohl im hierarchischen Behördenaufbau, wie etwa in der Justiz, eine der beteiligten Stellen regelmäßig das Recht habe, die Regelungen einseitig zu bestimmen. Zum anderen sei die gesetzliche Regelungsdichte so groß, dass die in der Vorschrift vorgesehene Ausnahmeregelung, wonach eine Vereinbarung nicht getroffen werden müsse, soweit die jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten bereits in Rechtsvorschriften festgelegt seien, letztlich regelmäßig einschlägig sein dürfte.

Im Hinblick darauf, dass Teil 3 BDSG keine bereichsspezifischen, sondern allgemeine Vorschriften für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen zum Zweck der Erfüllung dieser Aufgaben enthält, wirken sich die Regelungen je nach Anwendungsbereich unterschiedlich stark aus. Eine möglicherweise geringere Praxisrelevanz in einem Anwendungsbereich spricht aus Sicht

des BMI nicht gegen ein Regelungsbedürfnis und die Sachgerechtigkeit der Regelung in anderen Bereichen. Abgesehen davon ist der Bundesgesetzgeber mit der Schaffung der Vorschrift seinem unionsrechtlichen Auftrag zur Umsetzung des Artikel 21 der Richtlinie (EU) 2016/680 nachgekommen.

Vereinzelt wird angeregt, die besondere Konstellation der Behördenhierarchie durch die Zuweisung datenschutzrechtlicher Verantwortlichkeiten im Fachaufsichtsverhältnis vorzusehen. Für eine solche Regelung habe es bereits Ansatzpunkte in der Vorgängerfassung des BDSG (vgl. § 11 Absatz 2 Satz 3 sowie § 18 Absatz 1 BDSG a. F.) gegeben.

Eine entsprechende Regelung dürfte mit der Richtlinie (EU) 2016/680 grundsätzlich nicht in Einklang zu bringen sein. In Umsetzung der genannten Richtlinie regelt Teil 3 BDSG die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen zum Zweck der Erfüllung dieser Aufgaben. Diese Stellen entscheiden in Wahrnehmung der genannten Aufgaben über die Zwecke und Mittel der Verarbeitung. Vor diesem Hintergrund kommen im Anwendungsbereich der genannten Richtlinie grundsätzlich nur die genannten Stellen als datenschutzrechtlich Verantwortliche in Betracht. Für eine Regelung, durch die die datenschutzrechtliche Verantwortlichkeit auf die Fachaufsichtsbehörden übertragen würde, die mangels entsprechender Aufgabenzuweisung grundsätzlich selbst nicht zur Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten tätig werden können, besteht nach Auffassung des BMI kein Raum.

Sonstige Anmerkungen

Vereinzelt wird angemerkt, dass die Verteilung der datenschutzrechtlichen Verantwortlichkeit bei Entwicklungsverbünden der Länder problematisch sei, da nach der derzeitigen Regelung die einzelnen Behördenleiter eine datenschutzrechtliche Mitverantwortung für den Einsatz der Softwaregestaltung trügen, ungeachtet ihrer allenfalls in begrenztem Maße bestehenden Einflussmöglichkeiten auf eine solche Softwaregestaltung.

Unabhängig von der Frage, ob auf den geschilderten Sachverhalt das Datenschutzrecht des Bundes anwendbar wäre[102], teilt das BMI die Bewertung zur datenschutzrechtlichen Verantwortlichkeit nicht. Nach § 45 BDSG wird mit Teil 3 BDSG die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen zum Zweck der Erfüllung dieser Aufgaben geregelt. Unter „öffentlichen Stellen“ sind nach § 2 Absatz 1 und 2 BDSG die Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes oder eines Landes, einer Gemeinde,

[102] Nach § 2 Absatz 1 Nummer 2 BDSG gilt das BDSG für die Verarbeitung personenbezogener Daten durch öffentliche Stellen der Länder insbesondere nur, soweit der Datenschutz nicht durch Landesgesetz geregelt ist.

eines Gemeindeverbandes oder sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts, der bundesunmittelbaren Körperschaften, der Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform zu verstehen. Als datenschutzrechtlich Verantwortlicher ist daher im Einklang mit der Richtlinie (EU) 2016/680 grundsätzlich die zuständige öffentliche Stelle anzusehen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.[103] Die datenschutzrechtliche Verantwortlichkeit trifft insoweit die öffentlichen Stellen, nicht aber die jeweiligen Behördenleiter. Nur in Ausnahmefällen gilt ein Auftragsverarbeiter, der auch eine natürliche Person sein kann, als Verantwortlicher, wenn er die Zwecke und Mittel der Verarbeitung unter Verstoß gegen § 62 BDSG bestimmt.

5.12.3. Schlussfolgerungen

Aus den Rückmeldungen wird deutlich, dass die Regelung der Auftragsverarbeitungsverhältnisse in § 62 BDSG – trotz der punktuell geäußerten Kritik – als insgesamt gelungen anzusehen ist. Die Länder bewerten diese Vorschrift überwiegend als sachgerecht, praxistauglich und normenklar. Zu § 63 BDSG kann festgehalten werden, dass sich einige Länder für eine stärkere Berücksichtigung der Abläufe und Verantwortlichkeiten in der hierarchischen Behördenstruktur aussprechen.

[103] Artikel 3 Nummer 8 der Richtlinie (EU) 2016/680.

5.13. Anforderungen an die Sicherheit der Datenverarbeitung, Meldung von und Benachrichtigung bei Verletzungen des Schutzes personenbezogener Daten – §§ 64 bis 66 BDSG

5.13.1. Zielsetzung und Gegenstand der Regelungen

Die §§ 64 bis 66 BDSG betreffen die Anforderungen an die Datensicherheit, die Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den BfDI sowie die Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten.

§ 64 BDSG setzt Artikel 29 der Richtlinie (EU) 2016/680 um und regelt die technischen und organisatorischen Maßnahmen, die Verantwortliche und Auftragsverarbeiter zu ergreifen haben, um die Rechte und Freiheiten natürlicher Personen bei der Datenverarbeitung zu gewährleisten. In Absatz 1 wird geregelt, dass die Ausgestaltung der Maßnahmen Ergebnis eines Abwägungsprozesses sein soll, in den die mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen einzustellen sind. Außerdem wird klargestellt, dass bei der Festlegung der technisch-organisatorischen Maßnahmen die einschlägigen Standards und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu berücksichtigen sind. In Absatz 2 werden Inhalte aus Artikel 32 Absatz 1 Buchstaben a bis c DSGVO übernommen und die mit den technischen und organisatorischen Maßnahmen verfolgten Grundzwecke festgelegt. Absatz 3 benennt die Ziele, die im Hinblick auf automatisierte Verarbeitungen durch die Etablierung geeigneter technisch-organisatorischer Maßnahmen verfolgt und erreicht werden sollen.

§ 65 BDSG dient der Umsetzung von Artikel 30 der Richtlinie (EU) 2016/680 und legt den Umfang und die Modalitäten der Meldung von Verletzungen des Schutzes personenbezogener Daten nach § 46 Nummer 10 BDSG an die oder den BfDI fest. § 65 Absatz 7 BDSG stellt die Verwendung der gemeldeten Informationen in einem Strafverfahren durch Verweis auf § 42 Absatz 4 BDSG unter einen Einwilligungsvorbehalt. Dies beruht auf dem Gedanken, dass die Motivation zur Meldung einer Verletzung des Schutzes personenbezogener Daten nicht dadurch verringert werden soll, dass die Meldung zur Einleitung eines Strafverfahrens führen kann.[104]

§ 66 BDSG setzt Artikel 31 der Richtlinie (EU) 2016/680 um und regelt die Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten.

[104] BT-Drs. 18/11325, S. 116 f.

5.13.2. Empirische Ergebnisse und Bewertung

Rückmeldungen zu den §§ 64 bis 66 BDSG kamen vonseiten der DSK, aus dem Kreis der Bundesbehörden und aus den Ländern.

5.13.2.1. Rückmeldungen und Bewertung zu § 64 BDSG

Anpassung der Begrifflichkeiten an die Richtlinie (EU) 2016/680

Die DSK hält eine Anpassung des Wortlauts der Vorschrift an die Richtlinie (EU) 2016/680 für erforderlich. Konkret wird angeregt, in § 64 Absatz 1 Satz 1 BDSG anstelle des Begriffs „Gefahren" den Begriff „Risiken" zu verwenden. Ein weiterer Vorschlag bezieht sich auf den Begriff „Rechtsgüter der betroffenen Personen", der durch den europarechtlichen Begriff „Rechte und Freiheiten natürlicher Personen" zu ersetzen sei. Gleiches schlägt die DSK für die genannten Begriffe in den §§ 65 und 66 BDSG vor.

Aus Sicht des BMI besteht kein Bedarf für eine Änderung des Gesetzeswortlauts. Der Gesetzgeber hat mit den gewählten Formulierungen den ihm zustehenden Umsetzungsspielraum sachgerecht genutzt. Bei den Begriffen „Gefahr" und „Rechtsgüter" handelt es sich um rechtliche Kategorien, die im deutschen Recht fest etabliert und inhaltlich beschrieben sind. Im Hinblick darauf, dass dem Verantwortlichen durch § 64 Absatz 1 BDSG konkrete Handlungspflichten auferlegt werden, kommt es darauf an, dass die gesetzlichen Voraussetzungen für diese Pflichten hinreichend klar beschrieben sind. Dies ist nach Auffassung des BMI durch die gewählten Begrifflichkeiten „Gefahr" und „Rechtsgüter" eher gewährleistet als durch die wesentlich unbestimmteren und damit stärker auslegungsbedürftigen Formulierungen „Risiko" bzw. „Rechte und Freiheiten".

Ausdrücklicher Verweis auf die BSI-Standards

Die DSK regt außerdem Änderungen des Wortlauts des § 64 Absatz 1 Satz 2 BDSG an. Der Verantwortliche solle verpflichtet werden, die einschlägigen Standards, Technischen Richtlinien und Empfehlungen des BSI einzuhalten anstatt sie nur zu berücksichtigen. Zudem seien neben den bereits erwähnten Technischen Richtlinien und Empfehlungen auch die Standards des BSI in die Vorschrift aufzunehmen.

Das BMI sieht auch insoweit keinen Änderungs- bzw. Ergänzungsbedarf. Die Regelung in § 64 Absatz 1 Satz 2 BDSG hat lediglich klarstellende Funktion.[105] Daher ist es folgerichtig, dass die Vorschrift auf die Berücksichtigung der Standards des BSI zum IT-Grundschutz verweist und keine darüber hinausgehenden Verpflichtungen statuiert. Abgesehen davon ist zu beachten, dass § 64 BDSG die Sicherheit der Datenverarbeitung im Hinblick auf den Schutz personenbezogener Daten regelt. Der Datenschutz hat einen anderen Schutzzweck als die IT-Sicherheit. Im Hinblick darauf erscheint es sachgerecht, dass der Gesetzgeber in § 64 Absatz 1 Satz 2 BDSG nicht die Einhaltung der BSI-Standards anordnet, aber auf deren

[105] Vgl. BT-Drs. 18/11325, S. 116.

Berücksichtigung hinweist. Bei deren Einbeziehung ist der unterschiedliche Schutzzweck der IT-Sicherheit im Hinblick auf die Sicherheit von Organisationen, insbesondere bei der Auswahl der erforderlichen technischen und organisatorischen Maßnahmen, zu beachten. Soweit das Fehlen einer ausdrücklichen Bezugnahme in § 64 Absatz 1 Satz 2 BDSG auf die „Standards" des BSI bemängelt wird, ist die gesetzliche Regelung aus Sicht des BMI auch insoweit nicht zwingend anzupassen. Wie eingangs festgestellt, sind die BSI-Standards ohnehin zu berücksichtigen; die Vorschrift hat insoweit nur klarstellenden Charakter. Im Übrigen ist die Aufzählung nicht abschließend, wie sich auch aus der Gesetzesbegründung ergibt.[106]

Überprüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen

Die DSK regt die Aufnahme einer dem Artikel 32 Absatz 1 Buchstabe d DSGVO entsprechenden Regelung in § 64 BDSG an, wonach der Verantwortliche ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzurichten habe.

Unabhängig davon, dass die Regelung eines solchen Verfahrens in Artikel 29 der Richtlinie (EU) 2016/680 nicht vorgesehen ist, erscheint sie auch aus Klarstellungsgründen nicht notwendig. Nach § 64 Absatz 2 Satz 2 Nummer 1 BDSG sollen die technischen und organisatorischen Maßnahmen dazu führen, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden. Aus der Formulierung „auf Dauer" wird deutlich, dass die betreffenden Maßnahmen nicht nur bei ihrer Einführung oder für eine bestimmte Zeit, sondern dauerhaft wirksam sein sollen. Dies setzt eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen voraus.

Gewährleistungsziele technischer und organisatorischer Maßnahmen

Schließlich regt die DSK an, die in § 64 Absatz 2 Satz 2 BDSG genannten Gewährleistungsziele an das sog. Standard-Datenschutzmodell der deutschen Datenschutzaufsichtsbehörden anzupassen. Die bisher geregelten Gewährleistungsziele deckten nicht alle erforderlichen Aspekte der Datenverarbeitung ab. Im Gegensatz dazu beschrieben die sieben Gewährleistungsziele des Standard-Datenschutzmodells (Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Nicht-Verkettung von personenbezogenen Verfahren, Datenminimierung) die Schutzrichtung des Datenschutzes, seien in Artikel 4 der Richtlinie (EU) 2016/680 und der DSGVO vorgebildet und hätten ihre Praxistauglichkeit bewiesen. Bei einer entsprechenden Änderung könne § 64 Absatz 3 BDSG gestrichen werden.

[106] BT-Drs. 18/11325, S. 116.

Aus Sicht des BMI besteht auch insoweit aktuell kein Anpassungsbedarf. Aus den Rückmeldungen haben sich keine Hinweise ergeben, die an der Normenklarheit, Sachgerechtigkeit oder Praktikabilität der bestehenden Regelungen zweifeln ließen. Insbesondere enthält § 64 Absatz 3 BDSG einen ausdifferenzierten Katalog von Gewährleistungszielen bei automatisierten Datenverarbeitungen, der auf § 9 BDSG a.F. und der Anlage zu § 9 BDSG a.F. zurückgeht und daher bereits in der Praxis etabliert ist. Die Gewährleistungsziele stehen auch im Einklang mit den in Artikel 4 der Richtlinie (EU) 2016/680 normierten und in § 47 BDSG umgesetzten Datenverarbeitungsgrundsätzen.

5.13.2.2. Rückmeldungen und Bewertung zu §§ 65 und 66 BDSG

In den Rückmeldungen wird vereinzelt angemerkt, dass unklar sei, aus welchem Grund in § 65 Absatz 7 und § 66 Absatz 6 BDSG auf § 42 Absatz 4 BDSG verwiesen werde. Das Verwendungsverbot für durch die Meldung von Datenschutzverstößen verfügbar werdende Informationen im Strafverfahren folge bereits aus § 84 BDSG, der die entsprechende Anwendung von § 42 BDSG für Teil 3 des BDSG anordne. Im Übrigen ginge aus der Überschrift zu § 84 BDSG „Strafvorschrift“ hervor, dass sich das Verwendungsverbot nur auf das Strafverfahren beziehe.

Nach Auffassung des BMI ist der Verweis auf § 42 Absatz 4 BDSG in den §§ 65 und 66 BDSG aus Bestimmtheitsgründen erforderlich. § 42 Absatz 4 BDSG bezieht sich seinem Wortlaut nach nur auf Meldungen nach Artikel 33 DSGVO und auf Benachrichtigungen nach Artikel 34 Absatz 1 DSGVO. Allein die Anordnung der entsprechenden Anwendung von § 42 BDSG, dessen Absatz 4 – wie eingangs festgestellt – nur auf Meldungen und Benachrichtigungen nach der DSGVO Bezug nimmt, und die Überschrift „Strafvorschriften“ in § 84 BDSG bringen nicht hinreichend rechtssicher zum Ausdruck, dass die strafprozessuale Privilegierung auch für Meldepflichtige und Benachrichtigende im Anwendungsbereich von Teil 3 BDSG gilt.

5.13.3. Schlussfolgerungen

Im Ergebnis ist festzuhalten, dass die §§ 64 bis 66 BDSG insgesamt als sachgerecht, praktikabel und normenklar anzusehen sind. Im Hinblick auf § 64 BDSG ist darauf hinzuweisen, dass die Umsetzung von Artikel 29 der Richtlinie (EU) 2016/680 auf mehrfache Kritik vonseiten der DSK stößt. Zwingenden Änderungsbedarf sieht das BMI nicht.

5.14. Zusammenarbeit mit dem oder der Bundesbeauftragten – § 68 BDSG

5.14.1. Zielsetzung und Gegenstand der Regelungen

§ 68 BDSG dient der Umsetzung von Artikel 26 der Richtlinie (EU) 2016/68, der wiederum weitgehend Artikel 31 DSGVO entspricht. Nach § 68 BDSG hat der Verantwortliche mit dem oder dem BfDI bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten. Diese Pflicht zur Zusammenarbeit fasst die ohnehin sich aus anderen Vorschriften des BDSG ergebenden Kooperationspflichten und Kooperationsbeziehungen des Verantwortlichen mit dem oder dem BfDI zusammen.

5.14.2. Empirische Ergebnisse und Bewertung

Rückmeldungen zu § 68 BDSG kamen vonseiten der Länder.

In den Rückmeldungen wird vereinzelt angemerkt, dass unklar sei, ob aus § 68 BDSG über die reine Auskunftserteilung oder Zugangsgewährung hinausgehende Pflichten folgen würden. Dies gelte etwa in Bezug auf die Bereitstellung von Kopien und Dateien. Es solle geprüft werden, ob für solche Fälle von erweiterten Vorlagepflichten besondere Verfahrensvoraussetzungen geregelt werden sollten.

Das BMI sieht für eine weitergehende Regelung der Zusammenarbeit des Verantwortlichen mit dem oder der BfDI vorläufig keinen Bedarf. Aus Sicht des BMI sind die Voraussetzungen für die Bereitstellung von personenbezogenen Daten und Informationen an die oder den BfDI in § 16 Absatz 4 Satz 1 BDSG grundsätzlich sachgerecht geregelt. Danach sind die öffentlichen Stellen des Bundes verpflichtet, dem oder der BfDI jederzeit Zugang zu den Grundstücken und Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer oder seiner Aufgaben notwendig sind, zu gewähren und alle Informationen, die für die Erfüllung ihrer oder seiner Aufgaben erforderlich sind, bereitzustellen. Aus Sicht des BMI ist maßgeblich, dass die genannten Daten und Informationen für die Aufgabenerfüllung der oder des BfDI notwendig bzw. erforderlich sind. Die Aufgaben der oder des BfDI ergeben sich aus § 14 BDSG, der insoweit eine abschließende Regelung trifft. Fehlt es an der Erforderlichkeit zur Aufgabenerfüllung, ist der Verantwortliche datenschutzrechtlich nicht verpflichtet, die entsprechenden Daten oder Informationen zur Verfügung zu stellen.

5.14.3. Schlussfolgerungen

Aus den Rückmeldungen zu § 68 BDSG ist eine gewisse Unsicherheit hinsichtlich der Pflichten im Rahmen der Zusammenarbeit des Verantwortlichen mit dem oder der BfDI

zu entnehmen. Die bestehenden Regelungen bieten aus Sicht des BMI jedoch eine hinreichende Grundlage zur Ausgestaltung der Kooperationsbeziehung in der Praxis. Normativer Änderungs- oder Ergänzungsbedarf sieht das BMI insoweit nicht.

5.15. Unterscheidung bestimmter Personenkategorien sowie zwischen Tatsachen und persönlichen Einschätzungen – §§ 72 und 73 BDSG

5.15.1. Zielsetzung und Gegenstand der Regelungen

§ 72 BDSG dient der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680 und betrifft die Unterscheidung zwischen verschiedenen Kategorien personenbezogener Daten.

§ 73 BDSG setzt Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680 um und regelt ein Differenzierungsgebot für solche personenbezogenen Daten, die einerseits auf Tatsachen und andererseits auf persönlichen Einschätzungen beruhen. Insbesondere sind nach Satz 2Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich zu machen.

5.15.2. Empirische Ergebnisse und Bewertung

Rückmeldungen zu den §§ 72 und 73 BDSG kamen vonseiten der DSK, aus dem Kreis der Bundesbehörden und von einigen Ländern.

Die DSK kritisiert, dass die §§ 72 und 73 BDSG nur die Vorgaben der Richtlinie (EU) 2016/680 wiedergäben und keine Konkretisierung darstellten, weshalb der Mehrwert der Vorschriften gering sei. Aus den Ländern wird darauf hingewiesen, dass im Bereich des Strafrechts, insbesondere bei Zeugenaussagen und darauf beruhenden weiteren Folgerungen für das Ermittlungs- bzw. Strafverfahren, nicht immer trennscharf zwischen Tatsachen und persönlichen Einschätzungen unterschieden werden könne. Aus dem Kreis der Bundesbehörden wird angemerkt, dass nicht hinreichend deutlich werde, welche Rechtsfolgen an die in den Vorschriften vorgenommene Unterscheidung geknüpft seien.

Mit §§ 72 und 73 BDSG hat der Gesetzgeber Artikel 6 und Artikel 7 Absatz 1 der Richtlinie (EU) 2016/680 umgesetzt und seinen unionsrechtlichen Regelungsauftrag erfüllt. Soweit die Regelungen als zu wenig präzise kritisiert werden, ist darauf hinzuweisen, dass der nationale Gesetzgeber bei der Umsetzung von Richtlinien weitergehende Bestimmungen vorsehen kann, hierzu jedoch nicht verpflichtet ist.[107] Im Hinblick auf die Funktion des BDSG als Auffanggesetz wird auch in der Gesetzesbegründung erläutert, dass die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen der Datensicherheit, dem Fachrecht überlassen werden.[108] Von dieser Möglichkeit hat der Bundesgesetzgeber in unterschiedlichen Fachgesetzen, etwa dem BKAG und der StPO, Gebrauch gemacht.

[107] Artikel 1 Absatz 3 der Richtlinie (EU) 2016/680.
[108] Vgl. BT-Drs. 18/11325, S. 118 und 119.

5.15.3. Schlussfolgerungen

Die §§ 72 und 73 BDSG werden insgesamt als sachgerecht, praxistauglich und normenklar bewertet. Das BMI sieht aktuell keinen Änderungsbedarf in Bezug auf die Vorschriften.

5.16. Durchführung der Datenschutz-Folgenabschätzung, Anhörung der oder des Bundesbeauftragten, Verzeichnis von Verarbeitungstätigkeiten, Protokollierung – §§ 67, 69, 70 und 76 BDSG

5.16.1. Zielsetzung und Gegenstand der Regelungen

§ 67 BDSG dient der Umsetzung von Artikel 27 der Richtlinie (EU) 2016/680 und regelt die Durchführung der Datenschutz-Folgenabschätzung. Nach Absatz 1 hat eine Datenschutz-Folgenabschätzung zu erfolgen, wenn eine Form der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge hat. Absatz 2 nimmt Artikel 35 Absatz 1 Satz 2 DSGVO auf und behandelt gemeinsame Datenschutz-Folgenabschätzungen für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge. Absatz 4 legt den Inhalt der Datenschutz-Folgenabschätzung fest und konkretisiert die in Artikel 27 Absatz 2 der Richtlinie (EU) 2016/680 enthaltenen allgemeinen Angaben unter Übernahme der Angaben aus Artikel 35 Absatz 7 DSGVO.

§ 69 BDSG dient der Umsetzung von Artikel 28 der Richtlinie (EU) 2016/680 und thematisiert die – im BDSG als Anhörung bezeichnete – vorherige Konsultation der oder des BfDI. Die Anhörung dient der datenschutzrechtlichen Absicherung in Bezug auf beabsichtigte Verarbeitungen in neu anzulegenden Dateisystemen, die ein erhöhtes Gefährdungspotential für Rechtsgüter der betroffenen Personen in sich bergen.

§ 70 BDSG dient der Umsetzung von Artikel 24 der Richtlinie (EU) 2016/680 und verpflichtet den Verantwortlichen zur Führung eines Verzeichnisses über bei ihm durchgeführte Kategorien von Datenverarbeitungstätigkeiten. Das Verzeichnis ist von dem fachgesetzlich in einigen Bereichen vorgesehenen System der Errichtungsanordnungen für Dateien zur Vorbereitung, Planung und Vorprüfung vorgesehener Verarbeitungen zu unterscheiden. In Absatz 1 werden die in das Verzeichnis aufzunehmenden Angaben benannt. Die Begrifflichkeit „Kategorien von Verarbeitungstätigkeiten“ stellt hierbei klar, dass sich das Verzeichnis auf sinnvoll abgrenz- und kategorisierbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen bezieht.

§ 76 BDSG dient der Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680 und statuiert in Absatz 1 eine umfassende Pflicht des Verantwortlichen zur Protokollierung der unter seiner Verantwortung durchgeführten Datenverarbeitungen. Nach Absatz 2 müssen die Protokolle es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen. Absatz 3 enthält Verwendungsbeschränkungen, wobei von der durch die Richtlinie (EU) 2016/680 eröffneten Möglichkeit, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit hinaus auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten Gebrauch gemacht worden ist. Empirische Ergebnisse und Bewertung

5.16.2. Empirische Ergebnisse und Bewertung

Zu den Regelungen der §§ 67, 69, 70 und 76 BDSG gingen Rückmeldungen vonseiten der DSK, aus dem Kreis der Bundesbehörden und einiger Länder ein.

5.16.2.1. Rückmeldungen und Bewertung zu § 67 BDSG

Voraussetzungen für die Durchführung der Datenschutz-Folgenabschätzung

Die DSK kritisiert, dass § 67 BDSG im Gegensatz zu Artikel 35 Absatz 3 DSGVO nicht konkretisiere, in welchen Fällen eine Datenschutz-Folgenabschätzung durchzuführen sei. Die Regelung sei für Fehlinterpretationen anfällig und weise daher Mängel in der Praktikabilität auf. Zudem würde von § 67 BDSG in der Praxis kaum Gebrauch gemacht, da es an einer zwingenden Vorgabe, dass auch bereits bestehende Verfahren an den Vorgaben des neuen Datenschutzrechts zu messen seien, fehle.

Der Gesetzgeber hat bei der Ausgestaltung der Vorschrift die sehr allgemeinen Vorgaben von Artikel 27 der Richtlinie (EU) 2016/680 in beträchtlichem Maße konkretisiert. Soweit kritisiert wird, dass die Vorschrift mangels einer Artikel 35 Absatz 3 DSGVO entsprechenden Regelung nicht praktikabel sei, ist darauf hinzuweisen, dass die angeführte Regelung der DSGVO lediglich Beispielsfälle benennt und die dortige Aufzählung nicht abschließend ist („insbesondere“). Die genannte Bestimmung regelt daher nicht die Voraussetzungen, unter denen eine Datenschutz-Folgenabschätzung durchzuführen ist. Diese Voraussetzungen ergeben sich vielmehr aus Artikel 35 Absatz 1 DSGVO, der im Wesentlichen der Regelung in § 67 Absatz 1 BDSG entspricht. Die weitere Konkretisierung dieser Voraussetzungen, die nur unvollkommen gesetzlich ausgestaltet werden können, muss nach Auffassung des BMI der Praxis vorbehalten bleiben. Entscheidend ist aus Sicht des BMI, dass die entstehenden Aufwände angemessen und beherrschbar bleiben.[109] In diesem Zusammenhang ist nicht zuletzt darauf hinzuweisen, dass der oder die BfDI nach § 69 Absatz 1 Satz 2 BDSG die Befugnis hat, eine Liste der Verarbeitungsvorgänge zu erstellen, die der Pflicht zur Anhörung unterliegen. Die Anhörung nach § 69 BDSG dient der datenschutzrechtlichen Absicherung in Bezug auf beabsichtigte Verarbeitungen in neu anzulegenden Dateisystemen, die ein erhöhtes Gefährdungspotential für Rechtsgüter der betroffenen Personen in sich bergen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutz-Folgenabschätzung.[110]

In den Rückmeldungen wird vereinzelt angemerkt, dass § 67 BDSG nicht praxisgerecht sei, da die Anwendung einer Maßnahme, die nach dem Gesetz zur Aufklärung einer Straftat vorgesehen sei, nicht von der Durchführung einer Datenschutz-Folgeabschätzung abhängen könne. In diesem Zusammenhang wird auch vereinzelt die Frage aufgeworfen, ob mit

[109] So auch die Gesetzesbegründung: BT-Drs. 18/11325, S. 117.
[110] BT-Drs. 18/11325, S. 117.

der Einführung der elektronischen Akte im Bereich des Strafverfahrens stets eine Datenschutz-Folgenabschätzung zu erfolgen habe.

Dazu ist aus Sicht des BMI festzuhalten, dass sich die Datenschutz-Folgenabschätzung nach dem Wortlaut des § 67 Absatz 1 BDSG nicht auf einzelne (Ermittlungs-)Maßnahmen, sondern auf bestimmte Formen von Datenverarbeitungen bezieht. Dies wird auch in der Gesetzesbegründung nochmals klargestellt, die darauf hinweist, dass nicht die Einzelverarbeitung, sondern lediglich die Verwendung maßgeblicher Systeme und Verfahren zur Verarbeitung personenbezogener Daten mithilfe der Datenschutz-Folgenabschätzung in den Blick genommen werden müssen.[111] Abgesehen davon besteht für den Verantwortlichen nach § 67 Absatz 2 BDSG die Möglichkeit, für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotenzial eine gemeinsame Datenschutz-Folgenabschätzung vorzunehmen. Dabei kommt eine Datenschutz-Folgenabschätzung gemäß § 67 Absatz 1 BDSG insbesondere bei Verwendung neuer Technologien in Betracht. Nach dem Verständnis des BMI gilt das Erfordernis einer Datenschutz-Folgenabschätzung daher nur für neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden Systemen oder Verfahren.[112]

Vereinzelt wird darauf hingewiesen, dass die Datenschutz-Folgenabschätzung mit einem enormen personellen Aufwand verbunden sei, der für die Staatsanwaltschaften und Gerichte nicht zu leisten sei.

Wenngleich die erheblichen Aufwände für die Verantwortlichen anzuerkennen sind, die aus der Durchführung einer Datenschutz-Folgenabschätzung folgen, bestehen aus Sicht des BMI keine Regelungsspielräume für den Gesetzgeber hinsichtlich des grundsätzlichen Erfordernisses einer Folgenabschätzung. § 67 Absatz 1 BDSG setzt insoweit Artikel 27 Absatz 1 der Richtlinie (EU) 2016/680 um und dient der Erfüllung des unionsrechtlichen Regelungsauftrags des nationalen Gesetzgebers.

Datenschutz-Folgenabschätzung bei mehreren Verantwortlichen

Vereinzelt wird angemerkt, dass unklar sei, wie eine Datenschutz-Folgenabschätzung im Rahmen der Entwicklungsverbünde zu bewältigen sei und inwieweit Synergieeffekte genutzt werden könnten. In diesem Zusammenhang wird angeregt, eine ausdrückliche Regelung für einheitliche Datenschutz-Folgenabschätzungen für Verfahren, die im Rahmen der Verbünde entwickelt worden sind, auf Verbundebene in Zuständigkeit der Justizministerien zu schaffen.

Aus § 67 Absatz 1 BDSG folgt, dass die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung den jeweiligen Verantwortlichen trifft. Die Vorschrift setzt auch insoweit zwingende Vorgaben aus Artikel 27 Absatz 1 der Richtlinie (EU) 2016/680 um. Dies

[111] BT-Drs. 18/11325, S. 117.
[112] BT-Drs. 18/11325, S. 117.

schließt es nach Auffassung des BMI nicht aus, dass Teilnehmer an Entwicklungsverbünden bei der Erstellung von Datenschutz-Folgenabschätzungen zusammenarbeiten und sich daraus ergebende Synergieeffekte nutzen, soweit dies zweckmäßig ist, weil die betroffenen Stellen denselben rechtlichen Rahmen anzuwenden haben. Die datenschutzrechtliche Verantwortlichkeit für die Datenschutz-Folgenabschätzung würde aber auch in diesem Fall beim jeweiligen Verantwortlichen verbleiben. Eine Regelung dieser Konstellation im BDSG, die insoweit rein klarstellenden Charakter hätte, ist nach der Bewertung des BMI nicht geboten.

Begriff der erheblichen Gefahr

In mehreren Rückmeldungen wird kritisiert, dass der in § 67 Absatz 1 und Absatz 4 Nummer 3 BDSG verwendete Begriff „Gefahr" von dem Begriff „Risiko" in Artikel 27 der Richtlinie (EU) 2016/680 abweiche. Dies führe in fachlichen Datenschutzdokumenten zu einem zusätzlichen Begründungsaufwand, da wiederholt klargestellt werden müsse, dass der Gefahrenbegriff des BDSG nicht mit dem polizeilichen Gefahrenbegriff identisch sei. Daher wird angeregt, den Begriff „Gefahr" im BDSG durch den Begriff „Risiko" zu ersetzen. Darüber hinaus wird teilweise vorgetragen, dass unklar sei, unter welchen Voraussetzungen eine erhebliche Gefahr im Sinne des § 67 Absatz 1 BDSG anzunehmen sei. Dazu liege bislang noch keine Rechtsprechung vor.

Aus Sicht des BMI besteht kein Bedarf für eine Änderung des Gesetzeswortlauts. Der Gesetzgeber hat mit der gewählten Formulierung den ihm zustehenden Umsetzungsspielraum sachgerecht genutzt. Bei dem Begriff „Gefahr" handelt es sich um eine rechtliche Kategorie, die im deutschen Recht bereits etabliert ist. Im Hinblick darauf, dass dem Verantwortlichen durch § 67 Absatz 1 BDSG eine konkrete Handlungspflicht auferlegt wird, kommt es darauf an, dass die gesetzlichen Voraussetzungen für diese Pflicht hinreichend klar konturiert sind. Dies ist nach Auffassung des BMI durch den Begriff „erhebliche Gefahr" eher gewährleistet als durch den wesentlich unbestimmteren und damit stärker auslegungsbedürftigen Terminus „hohes Risiko". Die weitere Ausformung des Gefahrenbegriffs im spezifischen Kontext der Datenverarbeitung durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen muss letztlich der Praxis vorbehalten bleiben.[113]

Verhältnis der Datenschutz-Folgenabschätzung zur Errichtungsanordnung

Der DSK zufolge bestünden in der Praxis Unklarheiten dahingehend, ob eine Datenschutz-Folgenabschätzung erstellt werden müsse, wenn die Behörde eine fachgesetzliche Pflicht zum Erlass einer Errichtungsanordnung trifft. Es wird insoweit eine Klarstellung im Gesetzestext vorgeschlagen. Entsprechenden Klarstellungsbedarf sieht die DSK zudem

[113] Vgl. BT-Drs. 18/11325, S. 117.

im Verhältnis zwischen dem Verzeichnis von Verarbeitungstätigkeiten und der Errichtungsanordnung.

Das BMI sieht für das BDSG diesbezüglich keinen Regelungsbedarf. Das BDSG ordnet unter den in § 67 Absatz 1 BDSG bestimmten Voraussetzungen die Durchführung einer Datenschutz-Folgenabschätzung an. Außerdem folgt aus § 70 Absatz 1 BDSG, dass ein Verzeichnis von Verarbeitungstätigkeiten zu führen ist. Diese allgemeinen, von der Richtlinie vorgesehenen und europarechtlich hinreichenden datenschutzrechtlichen Pflichten werden in bestimmten Bereichen durch die fachrechtlich normierte Pflicht zum Erlass von Errichtungsanordnungen ergänzt. Während sich die Datenschutz-Folgenabschätzung auf bestimmte Verarbeitungsformen und das Verzeichnis von Verarbeitungstätigkeiten auf alle in die Zuständigkeit des Verantwortlichen fallenden Verarbeitungstätigkeiten bezieht, ist Bezugspunkt der Errichtungsanordnung die Datenverarbeitung in einer bestimmten Datei bzw. einem bestimmten Dateisystem. Die fachgesetzlichen Vorschriften über die Errichtungsanordnung regeln daher einen anderen Sachverhalt als das BDSG. Die allgemeinen Vorschriften über die Datenschutz-Folgenabschätzung und das Verzeichnis von Verarbeitungstätigkeiten finden daher gemäß § 1 Absatz 2 Satz 2 BDSG in vollem Umfang Anwendung. Darauf weist – in Bezug auf das Verzeichnis von Verarbeitungstätigkeiten – auch die Gesetzesbegründung nochmals ausdrücklich hin.[114] Selbst wenn eine klarstellende Regelung für erforderlich gehalten würde, wäre das BDSG aus Sicht des BMI nicht der geeignete Regelungsstandort. Das BDSG kennt das Instrument der Errichtungsanordnung selbst nicht. Eine etwaige Klarstellung käme daher allenfalls in den betreffenden Fachgesetzen in Betracht.

5.16.2.2. Rückmeldungen und Bewertung zu § 69 BDSG

Notwendigkeit der Anhörung

Aus dem Kreis der Bundesbehörden wird angemerkt, dass die Regelung des § 69 Absatz 1 Satz 1 BDSG in der Praxis Schwierigkeiten bereite, da die in den Nummern 1 und 2 geregelten Fallkonstellationen nicht klar voneinander abzugrenzen seien.

Im Hinblick darauf ist festzuhalten, dass der Gesetzgeber mit § 69 Absatz 1 BDSG die Vorgaben von Artikel 27 Absatz 1 der Richtlinie (EU) 2016/680 im Wesentlichen eins zu eins umgesetzt hat. Der Bundesgesetzgeber ist damit seinem unionsrechtlichen Regelungsauftrag nachgekommen. Aus Sicht des BMI wird kein Raum für eine gesetzgeberische Lösung auf nationaler Ebene zur Klärung der aufgeworfenen Abgrenzungsfrage gesehen.

Zeitpunkt der Anhörung

In den Rückmeldungen wird vereinzelt erwähnt, dass unklar sei, zu welchem Zeitpunkt die Anhörung nach § 69 BDSG zu erfolgen habe.

[114] BT-Drs. 18/11325, S. 118.

Nach der ausdrücklichen Regelung in § 69 Absatz 1 BDSG hat der Verantwortliche vor der Inbetriebnahme von neu anzulegenden Dateisystemen die oder den BfDI anzuhören. Die Vorschrift knüpft damit an die Einleitung des Anhörungsverfahrens durch den Verantwortlichen an, setzt aber nicht voraus, dass dieses zwingend abgeschlossen sein muss, bevor personenbezogene Daten entsprechend verarbeitet werden können.[115] Dieser Gedanke liegt auch der Eilfallregelung in § 69 Absatz 4 BDSG zugrunde, die entsprechenden operativen und fachlichen Erfordernissen in erweitertem Umfang Rechnung trägt.[116]

Anhörung bei mehreren Verantwortlichen

Im Kontext der Entwicklungsverbünde des Justizbereichs wird vereinzelt angemerkt, dass eine Regelung sinnvoll sei, die klarstelle, ob die Datenschutzaufsichtsbehörden aller beteiligten Länder vor Inbetriebnahme eines neuen Dateisystems angehört werden müssten oder ob bereits die Anhörung einer Aufsichtsbehörde genüge. In diesem Zusammenhang stelle sich auch die Frage, wie mit unterschiedlichen Bewertungen eines neu anzulegenden Dateisystems durch die jeweiligen Aufsichtsbehörden umzugehen sei.

Auch diesbezüglich stellt die gesetzliche Regelung klar, dass die datenschutzrechtliche Verantwortung beim jeweiligen Verantwortlichen liegt. Aus Sicht des BMI erscheint im Kontext von Entwicklungsverbünden eine entsprechende Abstimmung sowohl auf der Seite der Verantwortlichen als auch der Seite der Aufsichtsbehörden grundsätzlich sinnvoll.

5.16.2.3. Rückmeldungen und Bewertung zu § 70 BDSG

Erforderliche Angaben des Verzeichnisses von Verarbeitungstätigkeiten

In Teilen der Rückmeldungen wird die Frage aufgeworfen, ob nach § 70 Absatz 1 Satz 2 BDSG eine konkrete Beschreibung der einzelnen Verarbeitungstätigkeiten erforderlich sei. Weiterhin wird vereinzelt angemerkt, dass Unklarheiten hinsichtlich des Umfangs des Verzeichnisses von Verarbeitungstätigkeiten bestünden. Teilweise wird in den Rückmeldungen angemerkt, dass es unklar sei, ob in allen Fällen eine Beschreibung der technischen und organisatorischen Maßnahmen erfolgen müsse, da im Gegensatz zu Artikel 24 Absatz 1 Buchstabe i der Richtlinie (EU) 2016/680 der Zusatz „wenn möglich“ in § 70 Absatz 1 Satz 2 Nummer 9 BDSG fehle. Außerdem wird vereinzelt vorgetragen, dass sich – im Hinblick auf eine Bereitstellung des Verzeichnisses und eine etwaige Veröffentlichung durch die oder den BfDI und um mögliche Ansatzpunkte für Angriffe auf IT-Systeme auszuschließen – die Frage nach dem Detaillierungsgrad und einer Einstufung der Beschreibung der technischen und organisatorischen Maßnahmen stelle.

Aus Sicht des BMI enthält § 70 Absatz 1 Satz 2 BDSG grundsätzlich hinreichend bestimmte Regelungen zu den im Verzeichnis von Verarbeitungstätigkeiten zu machenden Angaben.

[115] BT-Drs. 18/11325, S. 118.
[116] BT-Drs. 18/11325, S. 118.

Insbesondere geht aus dem Wortlaut der Vorschrift hervor, dass der Verantwortliche – im Gegensatz zum Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 DSGVO, das eine Darstellung aller Verarbeitungstätigkeiten vorsieht – lediglich zur Führung eines Verzeichnisses über Kategorien von bei ihm durchgeführten Verarbeitungstätigkeiten verpflichtet ist. Die gewählte Begrifflichkeit stellt hierbei klar, dass sich das Verzeichnis nach § 70 BDSG nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenz- und kategorisierbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen bezieht.[117] Soweit technische und organisatorische Maßnahmen betroffen sind, folgt aus § 70 Absatz 1 Nummer 9 BDSG, dass diese Maßnahmen stets darzustellen sind, jedoch eine allgemeine Beschreibung ausreichend ist.

5.16.2.4. Rückmeldungen und Bewertung zu § 76 BDSG

Inhalt der Protokollierung

Die DSK regt an, zur Sicherstellung einer effizienten Datenschutzkontrolle die in § 76 Absatz 2 BDSG genannten Vorgaben für die Protokollinhalte über die Abfrage und die Offenlegung einschließlich der Übermittlung auf alle zu protokollierenden Verarbeitungsvorgänge zu erstrecken. Zudem solle die Einschränkung durch die Wörter „soweit wie möglich“ in Bezug auf die Identität der abfragenden oder offenlegenden Person gestrichen werden, da eine solche Einschränkung beim heutigen Stand der Technik nicht mehr nachvollziehbar sei.

Das BMI sieht aktuell keinen Änderungsbedarf. Mit der Regelung in § 76 Absatz 2 BDSG sind die Vorgaben von Artikel 25 Absatz 1 Satz 2 der Richtlinie (EU) 2016/680 eins zu eins umgesetzt worden. Aus der Rückmeldung der DSK ergeben sich keine Anhaltspunkte dafür, dass die bestehende Regelung nicht normenklar wäre, zu Anwendungsproblemen geführt hätte oder die mit ihr verfolgten Zwecke verfehlen würde. In Bereichen, in denen der Gesetzgeber über die allgemeinen Vorgaben in § 76 BDSG eine weitergehende Protokollierung für geboten und angemessen erachtet hat, sind fachgesetzliche Regelungen geschaffen worden. Dies betrifft etwa die Datenverarbeitung durch das Bundeskriminalamt, für die mit § 81 BKAG ergänzende Vorgaben für die Protokollierung normiert worden sind.

Teilweise wird angemerkt, dass die in § 76 Absatz 2 BDSG vorgesehene Begründung von Abfragen und Offenlegungen in der Praxis der Staatsanwaltschaften und Gerichte insbesondere angesichts des insofern anfallenden Massengeschäfts der Geschäftsstellen nicht umsetzbar sei. In diesem Zusammenhang wird vorgetragen, dass sich der Zugriffsgrund auch allein aus der Person des Zugreifenden ergeben könne. Es müsse daher ausreichend sein, dass sich aus der Protokollierung ein Zeitstempel und die Identität der die Abfrage

[117] BT-Drs. 18/11325, S. 118.

bzw. Offenlegung vornehmenden Person und gegebenenfalls die Identität des Empfängers ergäbe. Insoweit sei eine Anpassung der Vorschrift aus Klarstellungsgründen erforderlich.

Aus Sicht des BMI ist § 76 Absatz 2 BDSG auch insoweit hinreichend bestimmt. Nach dem Wortlaut der Vorschrift müssen die Protokolle es ermöglichen, die Begründung für die Abfrage oder Offenlegung festzustellen. Der Regelung, die der Bundesgesetzgeber aus Artikel 25 Absatz 1 Satz 2 der Richtlinie (EU) 2016/680 übernommen hat, sind diesbezüglich keine spezifischen Vorgaben in Bezug auf den Inhalt der Protokolle zu entnehmen. Nach dem Verständnis des BMI ist es erforderlich, aber auch ausreichend, dass sich die Begründung für die genannten Verarbeitungsvorgänge aus der Protokollierung ableiten lässt. Sofern der Zugriffsgrund bereits anhand der Person des Zugreifenden festgestellt werden kann, ist den Anforderungen des § 76 Absatz 2 BDSG Rechnung getragen.[118] Vor dem Hintergrund der aus der Praxis berichteten Unsicherheiten in Bezug auf die Auslegung der Vorschrift wird das BMI weiter prüfen, ob diesbezüglich eine gesetzliche Klarstellung vorgenommen werden sollte.

Verwendung der Protokolle für Strafverfahren

Vereinzelt wird angemerkt, dass fraglich sei, ob eine uneingeschränkte Verwendung der Protokolldaten für Strafverfahren nach § 76 Absatz 3 BDSG angemessen sei. Die DSK regt hierzu an, dass im Interesse der Normenklarheit im Gesetzestext klargestellt werden sollte, dass Protokolldaten für Strafverfahren nur dann verwendet werden dürfen, wenn das Strafverfahren im Zusammenhang mit der Kontrolle der Rechtmäßigkeit der Verarbeitung, Eigenüberwachung oder Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten stehe.

Nach dem Verständnis des BMI hat der Gesetzgeber bei der Umsetzung von Artikel 25 Absatz 2 der Richtlinie (EU) 2016/680 bewusst von der dort vorgesehenen Möglichkeit Gebrauch gemacht, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung und Datensicherheit hinaus auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten zu nutzen.[119] Zwingende Gründe für die von der DSK angeregte Begrenzung der Verwendungszwecke im Zusammenhang mit Strafverfahren sind für das BMI, insbesondere auch nicht aus der Richtlinie (EU) 2016/680, erkennbar.

Bereitstellung der Protokolle an die oder den BfDI

Die DSK wendet ein, dass § 76 Absatz 5 BDSG nicht den verfassungsrechtlichen Anforderungen entspreche. Nach der Rechtsprechung des BVerfG müsse durch technische und

[118] Vgl. Erwägungsgrund 57 der Richtlinie (EU) 2016/680: *„Die Identifizierung der Person, die personenbezogene Daten abgefragt oder offengelegt hat, sollte protokolliert werden und aus dieser Identifizierung sollte sich die Begründung für die Verarbeitungsvorgänge ableiten lassen."*
[119] Vgl. BT-Drs. 18/11325, S. 119.

organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzaufsichtsbehörden in praktikabel auswertbarer Weise zur Verfügung stünden und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Datenverarbeitungsvorgang enthielten. Hieraus seien in der Praxis folgende Anforderungen abzuleiten: Die Protokolldaten müssten in einem strukturierten, gängigen, maschinenlesbaren und maschinenauswertbaren Format vorliegen oder in ein entsprechendes Format exportierbar sein. Ferner müsste die verantwortliche Stelle die Daten in diesem Format der Datenschutzaufsichtsbehörde vorlegen können. Schließlich müssten die Protokolldaten zeitnah zur Verfügung gestellt werden können und es müsse möglich sein, die Protokolldaten für Zwecke der Datenschutzkontrolle auszuwerten.

Die Regelung in § 76 Absatz 5 BDSG, die sich auf Protokollierungen in automatisierten Datenverarbeitungssystemen für alle Teil 3 BDSG unterfallenden Verarbeitungen bezieht, genügt aus Sicht des BMI sowohl den unionsrechtlichen als auch den verfassungsrechtlichen Vorgaben. Dies schließt es nicht aus, dass für Verarbeitungskontexte, für die nach der Rechtsprechung des Bundesverfassungsgerichts weitergehende Anforderungen an die Form der bereitzustellenden Protokollierung zu stellen sind, ergänzende Regelungen in den jeweiligen Fachgesetzen getroffen werden können. Dies hat der Gesetzgeber etwa in § 81 Absatz 1 Nummer 1 BKAG für die Protokollierungen zu Verarbeitungsvorgängen im Informationssystem des Bundeskriminalamts umgesetzt. Danach müssen die Protokolle dem oder der BfDI in elektronisch auswertbarer Form zum Zwecke der Datenschutzkontrolle zur Verfügung stehen, um eine effiziente und IT-gestützte Datenschutzkontrolle zu ermöglichen.[120] Damit wird den Besonderheiten der Datenverarbeitung im Informationssystem des Bundeskriminalamts und den daraus resultierenden spezifischen Anforderungen an die Datenschutzkontrolle Rechnung getragen. Weitergehende Konkretisierungen in Bezug auf die Form der Protokollierung in § 76 BDSG sind aus Sicht des BMI nicht geboten, sondern sollten der Praxis vorbehalten bleiben. Maßgeblich ist insoweit, dass die Protokollierung eine wirksame Datenschutzkontrolle ermöglicht, gleichzeitig aber die entstehenden Aufwände für den Verantwortlichen angemessen und beherrschbar bleiben.[121]

5.16.3. Schlussfolgerungen

Im Ergebnis ist festzuhalten, dass die §§ 67, 69, 70 und 76 BDSG insgesamt als normenklar und sachgerecht anzusehen sind. In Bezug auf die Kritik an der Praktikabilität insbesondere des § 67 BDSG ist darauf hinzuweisen, dass eine weitere Konkretisierung der Anforderungen der Praxis vorbehalten bleiben sollte. In diesem Zusammenhang kommt insbe-

[120] BT-Drs. 18/11163, S. 133.
[121] Vgl. insoweit auch BT-Drs. 18/11325, S. 117.

sondere den Datenschutzaufsichtsbehörden eine zentrale Rolle zu. In Bezug auf § 76 Absatz 2 BDSG wird das BMI vor dem Hintergrund der aus der Praxis berichteten Unsicherheiten eine etwaige Anpassung der Vorschrift weiter prüfen.

5.17. Berichtigung und Löschung sowie Einschränkung der Verarbeitung personenbezogener Daten – § 75 BDSG

5.17.1. Zielsetzung und Gegenstand der Regelung

§ 75 BDSG dient der Umsetzung von Artikel 16 der Richtlinie (EU) 2016/680 in seiner Ausformung als Pflicht des Verantwortlichen. Systematisch werden in § 75 BDSG Pflichten des Verantwortlichen zur Berichtigung und Löschung personenbezogener Daten sowie zur Einschränkung ihrer Verarbeitung thematisiert, die unabhängig davon bestehen, ob eine betroffene Person darum nachsucht. Die spiegelbildlich bestehenden Rechte der betroffenen Person auf Berichtigung und Löschung personenbezogener Daten sowie auf Einschränkung der Verarbeitung durch den Verantwortlichen sind in § 58 BDSG geregelt.

5.17.2. Empirische Ergebnisse und Bewertung

Rückmeldungen zu § 75 BDSG kamen vonseiten der DSK und einiger Länder.

Ein Teil der Rückmeldungen kritisiert, dass § 75 Absatz 2 BDSG, der über § 500 StPO auch im Strafverfahren entsprechend Anwendung finde, nicht sachgerecht und überflüssig sei, weil die Rechtsgrundlagen für die Datenverarbeitung bereits im Strafverfahrensrecht zu finden seien.

Diese Kritik blendet aus, dass sich der Anwendungsbereich von Teil 3 BDSG nicht auf das Strafverfahren beschränkt, sondern sich insgesamt auf die Datenverarbeitung durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen zur Erfüllung der genannten Aufgaben erstreckt. Da das BDSG ein Auffanggesetz ist, gehen spezifische Rechtsvorschriften des Bundes den Vorschriften des BDSG grundsätzlich vor.[122] Es hängt damit vom jeweiligen Praxisbereich ab, ob und ggf. welche Bestimmungen des BDSG konkret zum Tragen kommen. Dass es in bestimmten Bereichen wegen spezieller datenschutzrechtlicher Vorschriften nicht des Rückgriffs auf die allgemeinen Vorschriften bedarf, vermag die Notwendigkeit und Sachgerechtigkeit der Regelungen des BDSG daher nicht generell in Frage zu stellen.

5.17.3. Schlussfolgerungen

Die Regelungen zur Berichtung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung in § 75 BDSG haben sich insgesamt bewährt. Aus den Rückmeldungen ergibt sich nach Auffassung des BMI kein Änderungsbedarf.

[122] BT-Drs. 18/11325, S. 79; BT-Drs. 19/4671, S. 44.

5.18. Schadensersatz und Entschädigung, Strafvorschriften – §§ 83 und 84 BDSG

5.18.1. Zielsetzung und Gegenstand der Regelungen

Mit den §§ 83 und 84 BDSG hat der Gesetzgeber Haftungsfragen und Sanktionen im Zusammenhang mit der Verarbeitung personenbezogener Daten im Anwendungsbereich von Teil 3 BDSG geregelt.

Die Schadensersatzvorschrift des § 83 BDSG dient der Umsetzung von Artikel 56 der Richtlinie (EU) 2016/680. Absatz 1 normiert einen eigenen außervertraglichen Schadensersatzanspruch für nach diesem Gesetz oder nach anderen Vorschriften rechtswidrige Verarbeitungen personenbezogener Daten. Die Ersatzpflicht entfällt, soweit bei einer nichtautomatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist. Absatz 2 statuiert, dass die betroffene Person bei immateriellen Schäden eine angemessene Entschädigung in Geld verlangen kann.

Die Strafvorschrift des § 84 BDSG setzt Artikel 57 der Richtlinie (EU) 2016/680 um. Danach wird § 42 BDSG in Bezug auf Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Anwendungsbereich von Teil 3 BDSG für entsprechend anwendbar erklärt. Dadurch soll der Gleichlauf der Sanktionsmöglichkeiten gegenüber öffentlichen Stellen bzw. deren Bediensteten und den bei diesen Stellen Beschäftigten unabhängig von dem mit der Verarbeitung verfolgten Zweck hergestellt werden.[123]

5.18.2. Empirische Ergebnisse und Bewertung

Zu den §§ 83 bis 84 BDSG sind vornehmlich Rückmeldungen der DSK und einiger Länder eingegangen.

5.18.2.1. Rückmeldungen und Bewertung zu § 83 BDSG

Verhältnis zur DSGVO

In der Rückmeldung der DSK wird bemängelt, dass die Verwendung der Formulierung „nach diesem Gesetz“ in § 83 Absatz 1 Satz 1 BDSG gegen das unionsrechtliche Wiederholungsverbot verstoße, da die unmittelbar anwendbare DSGVO in Artikel 82 selbst einen Schadensersatzanspruch regele. Zudem könnten sich unterschiedliche Ergebnisse gegenüber der Anwendung von Artikel 82 DSGVO ergeben, sodass eine unzulässige Einschränkung der DSGVO das Resultat sein könne. § 83 Absatz 1 Satz 1 BDSG dürfe sich richtigerweise nur auf Teil 3 BDSG beziehen.

[123] BT-Drs. 18/11325, S. 121.

§ 83 BDSG ist eine Vorschrift von Teil 3 BDSG, dessen Bestimmungen nach § 45 Satz 1 und 4 BDSG nur für die Datenverarbeitung durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten sowie die Vollstreckung von Strafen, Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 StGB, Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und Geldbußen zuständigen öffentlichen Stellen gelten, soweit die genannten Stellen Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Daher folgt bereits aus dem Standort der Regelung, dass § 83 BDSG nicht auf Datenverarbeitungen im Anwendungsbereich der DSGVO anwendbar ist. Abgesehen davon bezieht sich der Wortlaut der Vorschrift auf den Verantwortlichen. Unter Zugrundelegung systematischer und teleologischer Gesichtspunkte kann sich die Regelung insoweit nur auf Verantwortliche im Sinne des § 46 Nummer 7 BDSG, d. h. die in § 45 Satz 1 und 4 BDSG genannten öffentlichen Stellen beziehen. Ein Verstoß gegen das unionsrechtliche Wiederholungsverbot oder eine unzulässige Einschränkung der DSGVO, insbesondere von Artikel 82 DSGVO, ist für das BMI nicht ersichtlich.

Voraussetzungen des Schadensersatzanspruchs

Vereinzelt wird die Frage aufgeworfen, unter welchen Voraussetzungen eine „nicht automatisierte Verarbeitung“ im Sinne des § 83 Absatz 1 Satz 2 BDSG vorliege. Außerdem sei unklar, ob die verschuldensunabhängige Haftung lediglich für Schäden gelte, die durch die Automatisierung verursacht worden seien, oder ob die Vorschrift weitergehende Anwendung finden solle.

Mit der in § 83 Absatz 1 BDSG vorgenommenen Differenzierung hat der Gesetzgeber den unterschiedlichen Risiken automatisierter und nicht automatisierter Datenverarbeitung Rechnung getragen. Das Risiko einer Verletzung des Schutzes personenbezogener Daten steigt durch die Automatisierung der Verarbeitung. Hinzu kommt, dass die automatisierte Datenverarbeitung auf komplexen Vorgängen beruht oder solche beinhaltet, die für außenstehende Dritte in der Regel kaum nachvollziehbar sind. Im Hinblick darauf erscheint es nicht zumutbar, betroffenen Personen bei Schäden, die durch eine automatisierte Verarbeitung verursacht werden, den Verschuldensnachweis gegen den Verantwortlichen aufzuerlegen.[124] Diese Wertungen liegen der Gefährdungshaftung nach § 83 Absatz 1 Satz 1 BDSG zugrunde. Die Vorschrift setzt die automatisierte Verarbeitung dabei als Regelfall voraus. Eine Verschuldenshaftung besteht nur dann, wenn personenbezogene Daten nicht automatisiert verarbeitet werden. In diesem Fall hat der Verantwortliche nach § 83 Absatz 1 Satz 2 BDSG die Möglichkeit, sich vom Vorwurf des Verschuldens zu entlasten. Eine nicht automatisierte Verarbeitung liegt vor, wenn personenbezogene Daten ohne Einsatz von Datenverarbeitungssystemen verarbeitet werden.[125] Eine Haftung setzt

[124] Vgl. BT-Drs. 11/4306, S. 41 f. zur entsprechenden Regelung in § 7 Absatz 1 BDSG a. F.
[125] Vgl. die Definition in § 7 Absatz 2 Satz 2 BDSG a. F.: *„Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.“*

dabei nach allgemeinen Rechtsgrundsätzen voraus, dass die automatisierte Datenverarbeitung ursächlich für den Schaden gewesen ist und der Schaden in adäquatem Zusammenhang mit der Verarbeitung steht. Eine Gefährdungshaftung kommt daher nicht in Betracht, wenn die Unrichtigkeit der Daten bereits vor der Speicherung im Datenverarbeitungssystem vorlag. Ebenso wird die Vorschrift nicht eingreifen, wenn die Daten unrichtig manuell eingegeben worden sind. Es ist dann aber Sache des Verantwortlichen, nachzuweisen, dass der Schaden nicht auf der automatisierten Datenverarbeitung beruht, sondern der Fehler bereits vor der Speicherung oder bei der manuellen Eingabe vorgelegen hat.[126]

Umfang des Schadensersatzanspruchs

In den Rückmeldungen wird vereinzelt bemängelt, dass § 83 Absatz 1 und 2 BDSG einen Anspruch auf immateriellen Schadensersatz bei jeder rechtswidrigen Verarbeitung personenbezogener Daten als Regelfall ermögliche. Dies stelle eine Umkehr des bestehenden Schadensersatzsystems dar, bei dem der Ersatz immaterieller Schäden die Ausnahme sei.

Mit der Regelung eines Ersatzanspruchs für immaterielle Schäden ist der Gesetzgeber seinem Auftrag zur Umsetzung von Artikel 56 der Richtlinie (EU) 2016/680 nachgekommen. Nach der genannten Richtlinie sehen die Mitgliedstaaten vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder einer anderen Handlung, die gegen nach Maßgabe der Richtlinie erlassene nationale Vorschriften verstößt, ein materieller oder immaterieller Schaden entstanden ist, ein Recht auf Schadensersatz seitens des Verantwortlichen oder jeder sonst nach dem Recht der Mitgliedstaaten zuständigen Stelle zusteht. Im Gegensatz zur früheren Regelung in § 8 Absatz 2 BDSG a.F. handelt sich um einen umfassenden Ersatzanspruch für immaterielle Schäden, unabhängig davon, ob eine schwere Verletzung des Persönlichkeitsrechts vorliegt.

5.18.2.2. Rückmeldungen und Bewertung zu § 84 BDSG

In den Rückmeldungen wurde die Anordnung der entsprechenden Anwendung von § 42 BDSG als sachgerecht, praktikabel und normenklar bewertet. Weitergehende Anmerkungen zu § 84 BDSG sind nicht eingegangen.

5.18.3. Schlussfolgerungen

Die Evaluierung hat gezeigt, dass sich die Regelungen in den §§ 83 und 84 BDSG in der Praxis bewährt haben. Das BMI sieht hier keinen Anpassungsbedarf.

[126] Vgl. BT-Drs. 11/4306, S. 42, zur entsprechenden Regelung in § 7 Absatz 1 BDSG a. F.

5.19. Verfahren bei Datenübermittlungen, Datenübermittlungen an Drittstaaten und an internationale Organisationen – §§ 74 und 78 bis 81 BDSG

5.19.1. Zielsetzung und Gegenstand der Regelungen

§ 74 BDSG trifft Vorgaben für das Verfahren bei Übermittlungen personenbezogener Daten durch den Verantwortlichen. Absatz 1 dient der Umsetzung von Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680 und regelt die vom Verantwortlichen zu treffenden Maßnahmen zur Gewährleistung der Richtigkeit und Aktualität der zu übermittelnden Daten. Absatz 2 setzt Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680 um und regelt Hinweispflichten in Bezug auf etwaige im Fachrecht vorgesehene besondere Bedingungen für die Weiterverarbeitung der Daten. Absatz 3 setzt Artikel 9 Absatz 4 der Richtlinie (EU) 2016/680 um und statuiert die Pflicht zur Gleichbehandlung von Empfängern in anderen Mitgliedstaaten und Einrichtungen der Union hinsichtlich der Übermittlung von Daten mit Empfängern im Inland.

§ 78 BDSG dient der Umsetzung von Artikel 35 der Richtlinie (EU) 2016/680 und legt Voraussetzungen fest, die bei jeder Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen vorliegen müssen. Darüber hinaus enthält die Vorschrift zusätzliche Anforderungen an die Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen aufgrund der Rechtsprechung des Bundesverfassungsgerichts.[127]

§ 79 BDSG dient der Umsetzung von Artikel 37 der Richtlinie (EU) 2016/680. In der Vorschrift werden § 78 BDSG ergänzende Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten, zu denen die Europäische Kommission keinen Angemessenheitsbeschluss gemäß Artikel 36 der Richtlinie (EU) 2016/680 gefasst hat, formuliert. Unter diesen Bedingungen kommt dem Verantwortlichen nach Absatz 1 – insbesondere nach dessen Nummer 2 – die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. Absatz 2 regelt die Pflicht des Verantwortlichen zur Dokumentation der nach Absatz 1 Nummer 1 vorgenommenen Übermittlungen. Absatz 3 BDSG sieht die Unterrichtung der oder des BfDI über Kategorien von Übermittlungen vor, die ohne Vorliegen eines Angemessenheitsbeschlusses der Kommission, aber wegen Bestehens geeigneter Garantien für den Schutz personenbezogener Daten im Drittstaat nach entsprechender Beurteilung durch den übermittelnden Verantwortlichen erfolgen.

§ 80 BDSG dient der Umsetzung von Artikel 38 der Richtlinie (EU) 2016/680 und regelt Sachverhalte, in denen weder ein Angemessenheitsbeschluss der Europäischen Kommis-

[127] So etwa BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 und 1 BvR 1140/06.

sion vorliegt noch die in § 79 BDSG erwähnten Garantien in Form eines rechtsverbindlichen Instruments oder nach Beurteilung durch den übermittelnden Verantwortlichen bestehen. Insbesondere ist gemäß Absatz 1 Nummer 4 eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 78 BDSG zulässig, wenn die Übermittlung im Einzelfall für die in § 45 BDSG genannten Zwecke erforderlich ist.

§ 81 BDSG dient der Umsetzung von Artikel 39 der Richtlinie (EU) 2016/680 und weitet den Kreis der möglichen Empfänger über öffentliche Stellen hinaus auf sonstige öffentliche Stellen und Private aus.

5.19.2. Empirische Ergebnisse und Bewertung

Rückmeldungen zu den §§ 74 und 78 bis 80 BDSG kamen vonseiten der DSK, aus dem Kreis der Bundesbehörden und aus den Ländern. Zu § 81 BDSG wurden keine Anmerkungen übermittelt.

5.19.2.1. Rückmeldungen und Bewertung zu § 74 BDSG

Die Vorschrift wird von den befragten Stellen grundsätzlich als sachgerecht, praktikabel und normenklar bewertet. In den Rückmeldungen wird teilweise vorgetragen, dass das Verhältnis zu den spezialgesetzlichen Regelungen der StPO sowie einzelnen strafrechtlichen Fachgesetzen, insbesondere zu den §§ 77c ff. IRG und § 49a OWiG, klärungsbedürftig sei.

Das BMI teilt diese Kritik nicht. Wie bereits an anderer Stelle festgestellt worden ist, hat das BDSG den Charakter eines Auffanggesetzes. Daraus folgt, dass die §§ 45 ff. BDSG im Verhältnis zu den bereichsspezifischen Vorschriften im Zusammenspiel mit den Fachgesetzen und umgekehrt die Fachgesetze im Zusammenspiel mit §§ 45 ff. BDSG zu lesen sind. Die spezifischen Rechtsvorschriften des Bundes gehen dabei den allgemeinen Vorschriften des BDSG grundsätzlich vor.[128] Dies gilt auch in Bezug auf spezialgesetzlich geregelte Übermittlungsvorschriften.

5.19.2.2. Rückmeldungen und Bewertung zu § 78 BDSG

Die Regelung wird insgesamt als normenklar, sachgerecht und praktikabel bewertet. Jedoch wird angemerkt, dass aufgrund des Fehlens von Angemessenheitsbeschlüssen der Europäischen Kommission der vom europäischen Gesetzgeber normierte und in § 78 BDSG umgesetzte Regelfall des Datenaustauschs nicht zu Anwendung kommen könne. Dies beeinträchtige die Praxis der drittstaatlichen polizeilichen Rechtshilfe.

[128] § 1 Absatz 2 Satz 1 und 2 BDSG.

Das BMI teilt diese Sichtweise und setzt sich im Rahmen seiner Zuständigkeiten für Angemessenheitsbeschlüsse der Europäischen Kommission im Anwendungsbereich der Richtlinie (EU) 2016/680 ein.

5.19.2.3. Rückmeldungen und Bewertung zu § 79 BDSG

Begriff der geeigneten Garantien

In den Rückmeldungen wird mehrfach angeregt, eine Definition für den Begriff „geeignete Garantien" vorzusehen. § 79 BDSG werde aktuell dem Grundsatz der Normenklarheit nicht gerecht, was Anwendungsschwierigkeiten in der Praxis zur Folge habe. Der Begriff der geeigneten Garantien sei weder im BDSG noch in der zugrundeliegenden Richtlinie (EU) 2016/680 näher bestimmt. Daher sei unklar, welche Voraussetzungen erfüllt sein müssten, damit von geeigneten Garantien ausgegangen werden könne. Der DSK zufolge führe das Fehlen von Legaldefinitionen zu erheblichen Unsicherheiten und Anwendungsschwierigkeiten. Aus der Praxis wird u. a. angemerkt, dass die in § 79 BDSG gestellten Anforderungen beim Umgang mit Auslieferungs- und Rechtshilfeersuchen von Drittstaaten und dem Austausch der damit verbundenen Daten einen erheblichen Arbeitsaufwand verursachen würden, da für die notwendige Einzelfallentscheidung zunächst eine ausreichende Tatsachengrundlage geschaffen sowie die getroffene Abwägung und Einzelfallentscheidung dokumentiert werden müssten.

Das BMI teilt die Sichtweise, dass der Begriff der geeigneten Garantien auslegungsbedürftig ist, und kann den Wunsch der Praxis nach einer Konkretisierung der gesetzlichen Vorgaben nachvollziehen. Die § 79 Absatz 1 BDSG zugrundeliegenden unionsrechtlichen Bestimmungen sind Gegenstand der laufenden Evaluierung der Richtlinie (EU) 2016/680 durch die Europäische Kommission. Diese hat bis zum 6. Mai 2022 einen Bericht über die Bewertung und Überprüfung der Richtlinie vorzulegen, in deren Rahmen insbesondere die Anwendung und Wirkungsweise der Bestimmungen über die Übermittlung personenbezogener Daten an Drittsaaten und internationale Organisationen zu prüfen sind.[129] Abgesehen davon hat der EDSA die Veröffentlichung von Anwendungshinweisen zu Übermittlungen personenbezogener Daten an Drittstaaten auf Grundlage geeigneter Garantien angekündigt.[130] An den diesbezüglichen Arbeiten des EDSA sind auch die deutschen Datenschutzaufsichtsbehörden beteiligt. Der Befassung der Europäischen Kommission und des EDSA mit den unionsrechtlichen Grundlagen für Datenübermittlungen in Drittstaaten kann mit der vorliegenden Evaluierung nicht vorgegriffen werden. Das BMI wird nach Vorlage der Ergebnisse dieser Befassung etwaige Rechtsänderungsbedarfe weiter prüfen.

[129] Artikel 62 Absatz 1 und 2 der Richtlinie (EU) 2016/680.
[130] https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf.

5.19.2.4. Rückmeldungen und Bewertung zu § 80 BDSG

Begriff des Einzelfalls

In einigen Rückmeldungen wird angemerkt, dass es hilfreich wäre, wenn der Begriff „Einzelfall“ in § 80 Absatz 1 Nummer 4 BDSG konkretisiert werden könnte, um ein einheitliches Verständnis der Norm zu erzielen.

Für eine Konkretisierung des Begriffs des Einzelfalls in § 80 BDSG sieht das BMI keinen Bedarf. Es handelt sich um einen gängigen Rechtsbegriff, dessen Bedeutung und Inhalt sich unter Heranziehung der allgemeinen Auslegungsmethoden bestimmen lässt.

Anforderungen an die Interessenabwägung

Weiterhin wird vereinzelt angemerkt, dass in Bezug auf die nach § 80 Absatz 2 BDSG vorzunehmende Interessenabwägung unklar sei, in welchen Fällen das Überwiegen der Grundrechte der betroffenen Person anzunehmen sei. Vor diesem Hintergrund wären weitergehende Festlegungen, etwa ein Kriterienkatalog, wünschenswert.

Auch insoweit hält das BMI eine gesetzliche Konkretisierung nicht für zielführend. Nach § 80 Absatz 2 BDSG hat eine Abwägung zwischen dem öffentlichen Interesse an der Übermittlung der Daten und den Grundrechten der betroffenen Person zu erfolgen. Diese Interessenabwägung ist abhängig von den konkreten Umständen des jeweiligen Einzelfalls und vom Verantwortlichen auf Grundlage der ihm zur Verfügung stehenden Erkenntnisse nach den gängigen Grundsätzen einer Verhältnismäßigkeitsprüfung vorzunehmen.

Berichtspflichten gegenüber dem oder dem BfDI

Aus der Sicht der DSK fehlt eine Berichtspflicht für Übermittlungen nach § 80 Absatz 1 BDSG an die Datenschutzaufsichtsbehörden. Dies führe zu Schwierigkeiten in der Praxis. Zwar habe die Datenschutzaufsichtsbehörde nach § 80 Absatz 3 BDSG das Recht, die Dokumentation entsprechender Übermittlungen anzufordern. Die Aufsichtsbehörden könnten ihre Aufgaben allerdings nur sinnvoll ausüben, wenn die Übermittlungen an den Empfängerstaat auch berichtet würden.

Der Gesetzgeber hat mit § 80 Absatz 3 BDSG die Vorgaben aus Artikel 38 Absatz 3 der Richtlinie (EU) 2016/680 umgesetzt, der – im Gegensatz zu Datenübermittlungen auf Grundlage geeigneter Garantien gemäß Artikel 37 Absatz 2 der Richtlinie – keine Berichtspflichten an die Aufsichtsbehördenvorsieht. Der Vorschlag einer § 79 Absatz 3 BDSG entsprechenden jährlichen Berichtspflicht auch im Fall von Datenübermittlungen ohne geeignete Garantien erscheint jedoch grundsätzlich nachvollziehbar. Das BMI wird eine Umsetzbarkeit, auch unter Berücksichtigung der mit einer Berichtspflicht für die Verantwortlichen verbundenen Aufwände, weiter prüfen.

5.19.3. Schlussfolgerungen

Die §§ 74 und 78 BDSG sind als sachgerecht, praktikabel und normenklar zu bewerten. In Bezug auf § 79 BDSG bestehen erhebliche Rechtsunsicherheiten im Zusammenhang mit der Auslegung des Begriffs der geeigneten Garantien. Bei § 80 BDSG stellt sich die Frage nach einer Berichtspflicht an die oder den BfDI in Bezug auf Datenübermittlungen ohne geeignete Garantien. Das BMI wird die etwaigen Regelungsbedarfe in Bezug auf den Begriff geeignete Garantien § 79 Absatz 1 BDSG und Berichtspflichten an die Datenschutzaufsichtsbehörden für Übermittlungen ohne geeignete Garantien nach § 80 Absatz 1 BDSG in § 80 Absatz 3 BDSG prüfen.

6. Kostennachmessung

Die Kostennachmessung wurde vom Statistischen Bundesamtes durchgeführt und bezog sich auf das gesamte DSAnpUG-EU.

Aufgrund des Charakters des DSAnpUG-EU als Umsetzungsgesetz haben viele Änderungen auf den Erfüllungsaufwand keine oder nur geringe Auswirkungen. Dies trifft auf alle Vorgaben für Bürgerinnen und Bürger zu.

Auf Seiten der Verwaltung entsteht die größte Belastung durch das Gesetz im Rahmen des Informationsaustausches und der gegenseitigen Stellungnahmen zwischen dem oder der BfDI und den Datenschutzaufsichtsbehörden der Länder zur Findung eines gemeinsamen Standpunktes nach § 18 BDSG. Sie beträgt knapp 1,3 Millionen Euro. Der Personaleinsatz liegt dabei jedoch unter einer Stelle pro Land, sodass der Erfüllungsaufwand hierfür tatsächlich unter der Ex-ante-Schätzung von 1,95 Millionen Euro liegt.

Der BfDI wird in seiner Tätigkeit als gemeinsamer Vertreter im EDSA und durch den Betrieb einer zentralen Anlaufstelle für die Zusammenarbeit mit anderen EU-Staaten und -Institutionen sowie mit den Ländern mit 781.000 Euro belastet. Die durch den Bundesrat zu wählende Stellvertretung war zum Zeitpunkt der Kostennachmessung noch nicht eingerichtet, sodass die Messung an dieser Stelle zurückgestellt worden ist. Insgesamt erhöht sich der Erfüllungsaufwand der Verwaltung somit um etwa 2,76 Millionen Euro. Der Erfüllungsaufwand der Verwaltung durch Datenschutzfolgeabschätzungen liegt wie zuvor geschätzt bei 555.000 Euro.

Der im Vorfeld erwartete Erfüllungsaufwand für die Wirtschaft von rund 20,2 Millionen Euro für die Dokumentationspflicht und die Pflicht zum Ergreifen von Maßnahmen zum Schutz der betroffenen Person nach §§ 32 Absatz 2, 33 Absatz 2 BDSG, die zu erfüllen sind, wenn die Informationspflichten nach Artikel 13 Absatz 3 und 14 Absatz 1, 2 und 4 DSGVO gemäß § 32 Absatz 1 oder § 33 Absatz 1 BDSG nicht bestehen, ist nicht entstanden. Vielmehr wurden hierfür von den befragten Unternehmen keine Kosten und keine Zeitaufwände angegeben.

Die Wirtschaft wird damit insgesamt um 949.000 Euro entlastet. Diese Entlastung basiert vornehmlich auf dem Wegfall der Verpflichtung zur Information der Öffentlichkeit nach § 42 Satz 5 BDSG a. F. Hiernach musste die Öffentlichkeit, bei unrechtmäßigen Übermittlungen personenbezogener Daten in bundesweit erscheinenden Tageszeitungen informiert werden, wenn die Information der betroffenen Personen einen unverhältnismäßigen Aufwand verursachen würden. Hierfür fallen Sachkosten in Höhe von 1 Millionen Euro weg.

7. Gesamtergebnis

Die durchgeführte Evaluierung hat gezeigt, dass die überwiegende Zahl der Regelungen des BDSG als sachgerecht, praktikabel und normenklar angesehen werden kann. Die meisten der eigegangenen Rückmeldungen beziehen sich jeweils nur auf wenige Vorschriften und äußern zu einem Großteil der Regelungen weder Verständnis- noch Anwendungsschwierigkeiten.

Soweit im Hinblick auf einzelne BDSG-Vorschriften berichtete Unklarheiten nicht überzeugend durch Auslegung zu klären sind, werden gesetzliche Änderungen geprüft werden.

Im Einzelnen wird das BMI zu folgenden Regelungen Klarstellungen prüfen:

- eine Klarstellung der Regelung in § 1 Absatz 4 Satz 2 Nummer 3 BDSG, um ggf. eindeutig zum Ausdruck zu bringen, dass das BDSG nur anwendbar ist, wenn ein Inlandsbezug der Datenverarbeitung besteht;
- eine Umformulierung des § 1 Absatz 4 Satz 3 BDSG, um ggf. deutlich zu machen, dass die Norm nur nichtöffentliche Stellen adressiert;
- eine mögliche Klarstellung, dass § 34 Absatz 1 Nummer 2 BDSG die Auskunftspflicht nach Artikel 15 DSGVO nur aufgrund öffentlich-rechtlicher Satzungen, nicht aber aufgrund privater Satzungen ausschließt;
- die Notwendigkeit einer Klarstellung in § 19 Absatz 1 BDSG und § 40 Absatz 2 BDSG bezüglich der zuständigen federführenden Datenschutzaufsichtsbehörde;
- eine weitere Differenzierung in § 45 Satz 1 BDSG, um zum Ausdruck zu bringen, dass die Verhütung von Ordnungswidrigkeiten grundsätzlich nicht vom Anwendungsbereich von Teil 3 BDSG erfasst ist;
- die Aufnahme von Definitionen für die Begriffe „Anonymisierung“, „Verschlüsselung“ und „Protokollierung“ in die Begriffsbestimmungen des § 46 BDSG für den Anwendungsbereich von Teil 3 BDSG;
- eine Klarstellung in § 57 Absatz 3 BDSG im Hinblick auf die Voraussetzungen für das Absehen von einer Auskunftserteilung;
- eine etwaige Anpassung des § 76 Absatz 2 BDSG im Hinblick auf die Protokollierung der Begründung von Abfragen und Offenlegungen in automatisierten Verarbeitungssystemen;
- eine etwaige Konkretisierung des Begriffs „geeignete Garantien“ in § 79 Absatz 1 BDSG.

Auch einige der inhaltlichen Änderungsvorschläge werden weiter geprüft werden. Dies betrifft im Einzelnen folgende Themen:

- die Frage, inwieweit für Betriebe, die in einem untergeordneten Teil ihrer Tätigkeit als Beliehene tätig werden, Erleichterungen geschaffen werden können;
- die Regelungen zur Videoüberwachung öffentlich zugänglicher Räume durch nichtöffentliche Stellen in § 4 BDSG;
- eine Ergänzung des § 17 BDSG, um Vakanzen in der Stellvertretung des Gemeinsamen Vertreters im Europäischen Datenschutzausschuss zu vermeiden;
- eine mögliche Einschränkung der Auskunftspflicht nach Artikel 15 DSGVO durch § 34 BDSG im Hinblick auf Geheimhaltungsinteressen;
- die Regelung zur automatisieren Entscheidung im Einzelfall in § 37 BDSG;
- die mögliche Einführung einer Pflicht jeder Bundesbehörde, die betroffene Person über die Möglichkeit nach § 34 Absatz 3 Satz 1 BDSG zu informieren, dass eine Auskunftserteilung an den oder den BfDI verlangt werden kann, wenn ihr von der Behörde nicht unmittelbar Auskunft erteilt wird;
- Bedarfe nach weiteren Befugnissen der Datenschutzaufsichtsbehörden im Bußgeldverfahren;
- Berichtspflichten an die Datenschutzaufsichtsbehörden für Übermittlungen personenbezogener Daten an Drittstaaten nach § 80 Absatz 1 BDSG.

Zudem werden folgende redaktionelle Änderungen im BDSG vorgenommen:

- In § 27 Absatz 2 Satz 1 BDSG ist das Wort „beinträchtigen“ durch das Wort „beeinträchtigen“ zu ersetzen;
- § 29 Absatz 3 Satz 1 BDSG ist aufgrund von Änderungen des Strafgesetzbuchs (StGB) dahingehend anzupassen, dass auf § 203 Absatz 2 StGB verwiesen wird (und nicht auf den weggefallenen § 203 Absatz 2a StGB).

Eine Regelung im BDSG zur weitergehenden Institutionalisierung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder stößt wegen des Verbots der Mischverwaltung an verfassungsrechtliche Grenzen. Es bedürfte daher einer Änderung des Grundgesetzes, um die DSK weiter zu institutionalisieren.

Anlage - Fragebogen

I. Anwendungsbereich und Begriffsbestimmungen

1. Ist der Anwendungsbereich in § 1 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?
2. Ist der Anwendungsbereich in § 45 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?
3. Sind die Begriffsbestimmungen in § 2 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

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?
2. Sind die Rechtsgrundlagen für die Datenübermittlung in § 25 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?
3. Sind die Regelungen in Bezug auf besondere Verarbeitungssituationen in den §§ 26 bis 31 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?
4. Sind die Rechtsgrundlagen für die Datenverarbeitung in den §§ 48 bis 51 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?

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?
2. Sind die Regelungen zu Datenschutzbeauftragten nichtöffentlicher Stellen in § 38 BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar?
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?
   b) Hat die Änderung der Norm nach Ihrer Kenntnis zu einer Erleichterung für Unternehmen und Vereine geführt?

IV. Zusammenarbeit, Zuständigkeiten und Befugnisse der Aufsichtsbehörden

1. Ist die Zusammenarbeit der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?
2. Sind die Zuständigkeiten der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?
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?
4. Sind die Befugnisse der Aufsichtsbehörden im BDSG aus Ihrer Sicht sachgerecht, praktikabel und normenklar geregelt?

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?

V. Betroffenenrechte

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

VI. Pflichten der Verantwortlichen und Auftragsverarbeiter

1. Sind die Regelungen über die Auftragsverarbeitung in § 62 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?
2. Sind die Regelungen über gemeinsam Verantwortliche in § 63 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?
3. Sind die Bestimmungen über die Datensicherheit und Meldungen von Verletzungen des Schutzes personenbezogener Daten in den §§ 64 bis 66 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?
4. Sind die Regelungen über die Datenschutz-Instrumente (Datenschutz-Folgenabschätzung, Anhörungsverfahren, Verzeichnis von Verarbeitungstätigkeiten, Protokollierung) in den §§ 67, 69, 70 und 76 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?
5. Sind die Regelungen über die Unterscheidung bestimmter Personenkategorien sowie zwischen Tatsachen und persönlichen Einschätzungen in den §§ 72 und 73 BDSG aus Ihrer Sicht normenklar?
6. Sind die Regelungen über das Verfahren bei Datenübermittlungen in § 74 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?
7. Sind die Regelungen über die Pflicht zur Berichtigung und Löschung sowie die Einschränkung der Verarbeitung in § 75 BDSG aus Ihrer Sicht normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?

VII. Datenübermittlungen an Drittstaaten und an internationale Organisationen

1. Sind die allgemeinen Bestimmungen über Datenübermittlungen an Drittstaaten und an internationale Organisationen in § 78 BDSG normenklar und, soweit sie über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinausgehen, sachgerecht und praktikabel?
2. Sind die weiteren Bestimmungen über Datenübermittlungen an Drittstaaten und an internationale Organisationen in den §§ 79 bis 81 BDSG normenklar?

VIII. Haftung und Sanktionen

1. Sind die Regelungen zu Sanktionen in den §§ 41 bis 43 BDSG aus Ihrer Sicht sachgerecht und normenklar?
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.)
3. Sind die Regelungen zu Haftung und Sanktionen in den §§ 83 und 84 BDSG aus Ihrer Sicht sachgerecht und normenklar?

IX. Allgemein zu den Regelungen des BDSG

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