Bundesversicherungsamt

Frequently Ask Questions

Oft gestellt Fragen zur Umsetzung der EU-Datenschutzgrundverordnung (DSGVO) in der gesetzlichen Sozialversicherung

- Version 5 -

DATUM: 22.05.2018
VERFASSER: Referat 116
AKTENZEICHEN 116-8240-2075/2017

Dokumentenhistorie

Datum	Version	Autor	Änderungen
	1-4		Vorversionen dienen der ersten, unstrukturierten Darstellung der an das Bundesversicherungsamt herangetragenen Fragen
22.05.2018	5		Neugestaltung und Neustrukturierung der FAQ-Liste, Einführung einer Dokumentenhistorie ab Version 5

Inhaltsverzeichnis

1 Allgemeines zur Rechtssystematik

1.1 In welchem Verhältnis steht die EU-Datenschutzgrundverordnung (im Folgenden kurz DSGVO) zum deutschen Recht?

Bei der DSGVO handelt es sich um eine EU-Verordnung. Das bedeutet, dass die im sachlichen (Artikel 2 DSGVO) und räumlichen (Artikel 3 DSGVO) Anwendungsbereich geregelten Konstellationen europaweit einheitlich behandelt werden sollen. Damit sind in erster Linie die in der DSGVO getroffenen Regelungen für den Datenschutz maßgeblich.

Der nationale Gesetzgeber kann dennoch abweichende Regelungen treffen. Denn diverse Normen der DSGVO enthalten sog. Öffnungsklauseln. Diese ermöglichen es dem deutschen Gesetzgeber, von den in der DSGVO enthaltenen Regelungen abzuweichen, indem er sie ergänzt, erweitert oder sogar beschränkt. Welche konkreten Abweichungen der Gesetzgeber vornehmen darf, hängt von der jeweiligen Ausgestaltung der Öffnungsklausel ab.

Vor diesem Hintergrund wurden durch den nationalen Gesetzgeber bislang das Bundesdatenschutzgesetz (BDSG) und das Sozialgesetzbuch (SGB) Erstes Buch (I) und Zehntes Buch (X) neu gefasst. Die Anpassungen von SGB V und XI sind in Vorbereitung.

1.2 Wann ist nun die DSGVO anzuwenden, wann die Vorschriften des SGB?

Als verkürzter Grundsatz kann gelten: DSGVO vor SGB vor BDSG. Grundsätzlich wird das Datenschutzrecht in der DSGVO geregelt. Lediglich bei Abweichungen oder Ergänzungen bestimmt sich das (Sozialdatenschutz-) Recht nach dem SGB. Das BDSG findet dann Anwendung, wenn im SGB explizit auf diese Vorschriften verwiesen werden.

Beispiele: Grundlegende Definitionen sind in Artikel 4 DSGVO geregelt (z. B. Was bedeutet „Verarbeitung“? Wer ist „Verantwortlicher“ und wer „Dritter“?). Deshalb sieht § 67 SGB X[1] dazu keine Vorschrift mehr vor. Auch die Meldepflicht bei Datenpannen regelt Artikel 33 DSGVO abschließend. Daher verweist § 83a SGB X für die Meldung von Datenpannen bei Sozialdaten auch auf diese Vorschrift.

[1] Wenn im Folgenden Normen nach dem SGB I und X zitiert werden, handelt es sich jeweils um die Fassung, die ab dem 25. Mai 2018 zur Anwendung kommt.

1.3 Die DSGVO verwendet den Begriff „Aufsichtsbehörde“. Welche Stelle ist damit konkret gemeint?

Wenn in der DSGVO der Begriff „Aufsichtsbehörde“ verwendet wird, sind damit die nationalen Datenschutzaufsichtsbehörden gemeint. Für die Anwendung des BDSG und der DSGVO ist in Deutschland u. a. die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig (§ 14 Absatz 1 BDSG[2]). Die BfDI vertritt die Bundesrepublik Deutschland auch im Europäischen Datenschutzausschuss (§ 17 Absatz 1 Satz 1 BDSG). Die Neufassung des SGB X enthält zur Unterscheidung davon das Begriffspaar „Rechts- und Fachaufsichtsbehörde“. Das Bundesversicherungsamt ist Rechtsaufsicht im Sinne der §§ 88 ff. SGB IV.

Beispiel: Die Verantwortlichen haben unter bestimmten Voraussetzungen einen Datenschutzbeauftragten zu benennen und dies der Aufsichtsbehörde mitzuteilen (Artikel 37 Absätze 1 und 7 DSGVO). Adressat der Mitteilungspflicht ist die jeweils zuständige Datenschutzaufsicht und nicht das Bundesversicherungsamt als Rechtsaufsichtsbehörde.

1.4 Welche Vorschriften des SGB X sind ab dem 25. Mai 2018 anwendbar?

Die Neufassung des SGB X wurde im Rahmen des Gesetzgebungsverfahrens zu Änderungen des Bundesversorgungsgesetzes veröffentlicht (Bundesgesetzblatt Teil 1, Nr. 49 vom 24. Juli 2017, S. 2541 ff., 2558). Die Gesetzesbegründung findet man als Bundestags-Drucksache (BT-Drs. 18/ 12611).

1.5 Wird diese FAQ-Liste regelmäßig überarbeitet? Woran ist dies erkennbar?

Ja, diese FAQ-Liste wird abhängig von den eingehenden Fragen aktualisiert. Dies ist erkennbar an den Versionsnummern und der Änderungshistorie. Dadurch können die inhaltlichen Veränderungen nachvollzogen werden.

[2] Wenn im Folgenden Normen nach dem BDSG zitiert werden, handelt es sich um die Fassung, die ab dem 25. Mai 2018 zur Anwendung kommt.

2 Informationspflichten gegenüber Betroffenen

Informationspflichten sollen zu einer fairen und transparenten Verarbeitung beitragen. In erster Linie sollen die betroffenen Personen über die Existenz des Verarbeitungsvorgangs sowie seine Zwecke informiert werden. So wird danach unterschieden, ob die Daten bei dem Betroffenen selbst erhoben werden (Artikel 13 DSGVO i. V. m. § 82 SGB X) oder ob die Daten bei einem Dritten erhoben werden (Artikel 14 DSGVO i. V. m. § 82a SGB X). Über beide Aspekte muss der Betroffene informiert werden.

2.1 Worüber muss der Betroffene informiert werden?

Der Betroffene muss darüber informiert werden, wenn bei ihm erstmalig Daten erhoben werden (Artikel 13 Absatz 1 und 2 DSGVO). Auch trifft den Verantwortlichen eine Informationspflicht, wenn die Daten zu einem anderen als dem ursprünglich erhobenen Zweck verwendet werden sollen (Artikel 13 Absatz 3 DSGVO). Hingegen besteht keine Informationspflicht, wenn der Betroffene seine Rechte bereits kennt (Artikel 13 Absatz 4 DSGVO). Auch sieht § 82 Absatz 1 SGB X weitere Ausnahmen von den Informationspflichten vor, beispielsweise muss nicht über die Kategorien von Empfängern informiert werden, wenn die betroffene Person an eine Übermittlung an diese Kategorien von Empfängern rechnen muss. Damit wird die bisherige Regelung des § 67 Absatz 3 Satz 3 SGB X ersetzt.

Ähnliche Informationspflichten ergeben sich, wenn die Daten nicht bei dem Betroffenen selbst erhoben wurden, sondern bei einem Dritten (Artikel 14 Absatz 1 und Absatz 2 DSGVO). Auch besteht eine Informationspflicht, wenn die so erhaltenen Daten zu anderen Zwecken verwendet werden (Artikel 14 Absatz 5 DSGVO).

2.2 Umfasst die Informationspflicht auch die Nennung der Rechtsaufsichtsbehörde?

Die Informationspflicht umfasst auch „das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde“ (Artikel 13 Absatz 2 Buchstabe d DSGVO). Damit wird auf das normierte Beschwerderecht in der DSGVO abgestellt (Artikel 77 DSGVO), das wiederum auf die zuständige Datenschutzaufsicht zielt.

Das allgemeine Petitionsrecht aus Artikel 17 Grundgesetz (kurz: GG) bleibt nach Auffassung des Bundesversicherungsamtes von dieser Beschwerdemöglichkeit unberührt, sodass eine Petition an die Rechtsaufsicht im Sinne von § 88 SGB IV weiterhin möglich ist. Vor dem Hintergrund des allgemeinen Beratungsauftrags (§ 14 SGB I) ist ein Hinweis der Sozialversicherungsträger auf dieses Petitionsrecht hilfreich.

2.3 Unter bestimmten Voraussetzungen besteht keine Informationspflicht. Welche Maßnahmen müssen die Verantwortlichen trotzdem treffen?

Auch wenn keine Informationspflicht besteht (§ 82 Absatz 2 SGB X), muss der Verantwortliche entsprechende Maßnahmen treffen (§ 82 Absatz 3 SGB X). Unter anderem soll die Öffentlichkeit die Gründe des Wegfalls der Informationspflicht erfahren.

Nach der Gesetzesbegründung (BT-Drs. 18/ 12611, S. 128) liegt eine „geeignete Maßnahme“ insbesondere in der Bereitstellung der Informationen für die Öffentlichkeit. Zum Beispiel können diese auf der Homepage oder in der Mitgliederzeitschrift veröffentlicht werden.

3 Informationspflichten gegenüber Empfängern

Die DSGVO sieht auch Informationspflichten vor, wenn der Betroffene die Berichtigung oder Löschung von Daten verlangt. Diese Information muss dann durch den Verantwortlichen an die Empfänger der Daten weitergeben werden, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßig großen Aufwand verbunden (Artikel 19 DSGVO). Diese sog. Nachberichtspflicht stellt eine Ergänzung der Betroffenenrechte dar. Sie dient einerseits dazu, dass die Datenempfängern ihren datenschutzrechtlichen Verpflichtungen nachkommen, andererseits werden die Betroffen vor einer Weiterverarbeitung mit unrichtigen oder unrechtmäßig verarbeiteten Daten durch die Datenempfänger geschützt.

3.1 Ist der maschinelle Datenaustausch eine Konstellation, bei der eine Information unmöglich bzw. unverhältnismäßig ist?

Grundsätzlich ist der Verantwortliche dazu verpflichtet, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der Daten oder eine Einschränkung der Verarbeitung mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden (Artikel 19 Satz 1 DSGVO).

Gemäß der Legaldefinition ist „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht (Artikel 4 Nr. 9 DSGVO). Mithin sind davon auch Dritte erfasst, denen die Daten übermittelt wurden.

Daher besteht auch im Rahmen eines maschinellen Datenaustauschs gegenüber Dritten gemäß gem. Artikel 19 Satz 1 DSGVO die Verpflichtung, diese über Berichtigungen und Löschungen zu informieren, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigem Aufwand verbunden. Insoweit könnte sich aus dem Umstand, dass Löschungen im Rahmen von maschinellen Datenaustauschverfahren sehr aufwändig sind, ein „unverhältnismäßig großer Aufwand“ ergeben. Dies muss jedoch im Einzelfall geprüft und abgewogen werden. Das Ergebnis ist nachvollziehbar zu dokumentieren.

3.2 Muss der Sozialversicherungsträger Empfänger auch dann informieren, wenn Daten berichtigt oder gelöscht werden, die der Sozialversicherungsträger selbst von einem anderen Dritten erhalten hat?

Der Verantwortliche kann Daten nicht nur bei der betroffenen Person, sondern auch bei einem Dritten erheben (Artikel 14 DSGVO).

Erhält der Sozialversicherungsträger Kenntnis darüber, dass Daten, die von einem Dritten erhoben wurden, berichtigt oder gelöscht wurden (Artikel 16 DSGVO), hat er diese Informationen auch an seine Empfänger weiterzugeben (Artikel 14 i. V. m. Artikel 19 DSGVO).

4 Die automatisierte Verarbeitung von Sozialdaten

Die DSGVO enthält für eine automatisierte Entscheidung im Einzelfall konkrete Regelungen (Artikel 22 DSGVO). Auch im Sozialgesetzbuch existieren Vorschriften hierzu (§ 31 a SGB X). Im Rahmen der Digitalisierung der Verwaltungsabläufe gewinnen diese Regelungen zunehmend an Bedeutung.

4.1 Wann kann man davon ausgehen, dass eine ausschließlich „automatisierte Entscheidung“ im Einzelfall vorliegt?

Damit der Anwendungsbereich von Artikel 22 Absatz 1 DSGVO eröffnet ist, ist zunächst die Frage zu klären, wann es sich überhaupt um ein automatisierte Entscheidung handelt. An dieser Stelle ist ein Verweis auf die Wirtschaftsinformatik hilfreich. Danach erfolgt eine differenzierte Betrachtung der Automatisierbarkeit von Aufgaben.

Von einer Vollautomatisierung wird gesprochen, wenn a) die Vorgangsauslösung, b) die eigentliche Aktion und c) die Steuerung von maschinellen Aufgabenträgern durchgeführt werden. Von einer Teilautomatisierung wird gesprochen, wenn mindestens ein Schritt aber nicht alle automatisiert ausgeführt werden (vgl. u. a. Ferstl/Sinz: Grundlagen der Wirtschaftsinformatik, Oldenbourg-Verlag, München 2013, S. 95 ff.). Nach dieser Definition wäre z. B. eine durch einen Sachbearbeiter ausgelöste Rentenberechnung mit automatisch erstelltem Rentenbescheid eine Ausprägungsform der Teilautomatisierung. Eine Vollautomatisierung läge vor, wenn eine elektronische Antragstellung über ein Online-Formular mit einem fest vorgegebenen Antwortbereich ermöglicht wird und eine Bearbeitung bis hin zum Bescheid vollautomatisiert erfolgt.

Nur im letztgenannten Fall würde der gesamte Verwaltungsvorgang in einer sog. Dunkelverarbeitung ablaufen, ohne dass hier eine Prüf- und Steuerungsmöglichkeit im Rahmen einer Einzelfallbearbeitung besteht. Nur in diesem Fall ist nach unserer Auffassung der Anwendungsbereich des Artikels 22 Absatz 1 DSGVO eröffnet.

4.2 Sind von der Regelung nur die Verarbeitungen erfasst, die eine negative Auswirkung für den Betroffenen haben?

Bei dieser Frage herrscht Rechtsunsicherheit. In Artikel 22 Absatz 1 DSGVO wird darauf abgestellt, dass die Entscheidung „rechtliche Wirkung entfalten“ oder eine „erhebliche Beeinträchtigung“ darstellen muss (so auch Martini in: Paal/Pauly DSGVO Artikel 22 Rn. 28: „Nicht eindeutig ist der Wortlaut in der Frage, ob er nur belastende (nachteilige) oder alle Entscheidungen erfasst“).

Für die Praxis bedeutet dies einen wesentlichen Unterschied: Im ersten Fall (rechtliche Wirkung genügt) wären von Artikel 22 DSGVO auch die Geschäftsprozesse erfasst, die in automatisierter Verarbeitung auch zu einer positiven rechtlichen Wirkung (z.B. automatisiert erstellter Genehmigungsbescheid) führen. Bei dem anderen Verständnis (nur belastende Entscheidungen) kommt die Vorschrift nur für automatisierte Verarbeitung, die rechtlich nachteilig ist (z.B. automatisiert erstellter Ablehnungsbescheid), zur Anwendung.

Nach kursorischer Durchsicht der dazu vertretenen Auffassungen tendiert die Literatur eher zur letzteren Auffassung, wonach bei dem Betroffenen eine erhebliche Beeinträchtigung hervorgerufen werden muss, ohne aber die andere Sichtweise kategorisch auszuschließen.

So führt SCHULZ aus: „Mit „rechtliche Wirkung“ sind nur Rechtsfolgen gemeint, die eine Rechtsposition begründen, ändern oder aufheben. Nach dem Wortlaut von Absatz 1 werden nur beeinträchtigende rechtliche Wirkungen, d.h. nur solche, die Rechtspositionen der betroffenen Person negativ beeinträchtigen, erfasst, was nur teilweise begünstigende Entscheidungen mit einbezieht. Dies entspreche auch dem Schutzzweck der Norm. Als Beispiel werden einseitig gestaltende Rechtsakte wie beispielsweise belastende Verwaltungsakte aufgeführt“ (Schulz in: Gola, DSGVO, 1. Aufl. 2017, Artikel 22, Rn. 22, 23).

Auch BUCHNER stellt auf dieses Erfordernis ab, wenn er ausführt: „Eine rechtliche Wirkung ist immer dann anzunehmen, wenn sich die Rechtsposition der betroffenen Person in irgendeiner Weise verändert, ein Recht oder ein Rechtsverhältnis begründet oder aufgehoben wird oder in ein Recht eingegriffen wird. Eine rechtliche Wirkung ist im öffentlichen Recht etwa bei der Entscheidung über den Erlass von leistungsgewährenden Verwaltungsakten. Fraglich ist, ob für das Verbot des Absatz 1 eine rechtliche Wirkung nur dann von Relevanz sein soll, wenn diese für die betroffene Person nachteilig ausfällt. Unter der Richtlinie geht man für die „rechtlichen Folgen“ i. S. d. Artikel 15 DSRL davon aus, dass es unerheblich ist, ob diese für den Einzelnen nachteilig oder günstig sind. Dies spricht zunächst einmal dafür, die „rechtlichen Wirkungen“ ebenso weit zu fassen. Allerdings verbindet Artikel 22 DSGVO im Folgenden mit der rechtlichen Wirkung offensichtlich doch eine nachteilige Komponente, wenn die erste Alternative mit einer anderen gleichgesetzt wird, die den Einzelnen „in ähnlicher Weise erheblich beeinträchtigt“. Ebenso spricht auch Erwägungsrund 71 von einer Entscheidung, die „rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise beeinträchtigt“. Aufgrund dieses eindeutigen Wortlauts ist daher davon auszugehen, dass zumindest solche Entscheidungen, die einem Begehren der betroffenen Person vollumfänglich stattgeben, nicht unter Artikel 22 fallen“ (Buchner in: Kühling/Buchner, DSGVO, 1. Aufl. 2017, Artikel 22 Rn. 24, 25).

Auf diesen Meinungsstreit kommt es indes nicht an, wenn eine Ausnahmevorschrift im Sinne von Artikel 22 Absatz 2 DSGVO greift, die eine automatisierte Verarbeitung ausdrücklich zulässt.

Soweit die Rechtsunsicherheit weder durch Änderung der Vorschriften noch durch richterliche Rechtsfortbildung geklärt ist, vertritt das Bundesversicherungsamt einen pragmatischen Ansatz. Zweck der Regelung von Artikel 22 Absatz 1 DSGVO ist es, einen Betroffenen im Einzelfall vor einer vollständig automatisierten Entscheidung zu schützen. Daher erscheint es sinnvoll, eine unter Artikel 22 Absatz 2 DSGVO fallende Ausnahme für eine automatisierte Verarbeitung zu nutzen. Im Bereich der Sozialversicherung eröffnet § 31a SGB X (i. V. m. Artikel 22 Absatz 2 Bst. b DSGVO) die Möglichkeit, unter bestimmten Voraussetzungen einen Verwaltungsakt vollständig automatisiert zu erlassen. Dafür gelten die bekannten Rechtsbehelfe. Soweit ein anderer Ausnahmetatbestand aus Artikel 22 Absatz 2 DSGVO zum Zuge kommt, sollten in jedem Fall geeignete Maßnahmen – allen voran die Möglichkeit des Betroffenen, die automatisierte Entscheidung durch einen Menschen überprüfen zu lassen – getroffen werden. Daher sollte für die automatisierte Verarbeitung ein Ausnahmetatbestand von Artikel 22 Absatz 2 DSGVO genutzt werden.

4.3 Kann die bisherige Regelung in § 67b Absatz 4 SGB X a. F., wonach auf die Bewertung einzelner Persönlichkeitsmerkmale abgestellt wird, auf die neue Regelung im Artikel 22 DSGVO übertragen werden oder gibt es Bedeutungsunterschiede?

Die bisherige Regelung des § 67b Absatz 4 SGB X a. F. hat darauf abgestellt, dass Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung von Sozialdaten gestützt werden dürfen, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Diese Vorschrift ist in der Neufassung des SGB X aufgrund der Regelung des Artikels 22 DSGVO entfallen. Der Wortlaut von Artikel 22 DSGVO stellt hingegen nicht auf das Merkmal „Bewertung einzelner Persönlichkeitsmerkmale“ ab.

Es wurde nunmehr die Frage gestellt, ob auch Artikel 22 Absatz 1 DSGVO – wie der bisherige § 67b Absatz 4 SGB X a. F. – darauf abstellt, dass die automatisierte Bearbeitung auf die Bewertung einzelner Aspekte einer Person abzielt. Wenn dieses Merkmal von Artikel 22 Absatz 1 DSGVO erfasst wird, würde dies den Tatbestand des Artikels 22 DSGVO – zusätzlich zu der unter Frage 4.2 getroffenen Wertung – einschränken. Daher kommt es darauf an, ob in Artikel 22 Absatz 1 DSGVO das Tatbestandsmerkmal „Bewertung von Persönlichkeitsmerkmalen“ hineinzulesen ist.

BUCHNER führt an, dass in der endgültigen Fassung des Artikels 22 DSGVO diese Einschränkung nicht mehr enthalten ist. Daraus könnte geschlossen werden, dass Artikel 22 DSGVO nunmehr für sämtliche automatisierte Datenverarbeitungsprozesse gelten soll, unabhängig davon, ob diese auf eine Bewertung von Persönlichkeitsmerkmalen abzielt oder nicht. Erfasst sein

soll nunmehr jede automatisierte Entscheidung, sofern sie nur der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (vgl. Buchner in: Kühling/Buchner, ebenda, Artikel 22 Rn. 17).

Schon vom Ergebnis her könne ein solch weites Verständnis des Artikels 22 DSGVO nicht überzeugen. Erfasst wären nach diesem Verständnis selbst einfache „wenn- dann-Entscheidungen“, wenn diese automatisiert voreingestellt sind. Mit dem eigentlichen Schutzzweck hätten diese Konstellationen aber nichts zu tun (vgl. Buchner in: Kühling/Buchner, ebenda, Artikel 22 Rn. 18).

BUCHNER kommt aus der Zusammenschau mit Erwägungsgrund 71 sowie der Definitionsnorm Artikel 4 Nr. 4 zu dem Ergebnis, dass Artikel 22 Absatz 1 nur solche automatisierten Verarbeitungen erfassen soll, die auf die Bewertung einzelner Persönlichkeitsziele abzielen (vgl. Buchner in: Kühling/Buchner, ebenda, Artikel 22 Rn. 19).

Genauso argumentiert VON LEWINSKI: Für die Auslegung des Artikel 22 ist deshalb von dem Verständnis der Vorgängervorschrift auszugehen. Eine ähnliche Aufzählung (wie in Artikel 15 Absatz 1 RL) findet sich in Erwägungsgrund 71 Satz 2. Anknüpfungspunkt der Regelung ist deshalb die Bewertung von persönlichen Merkmalen in ihrem Zusammenspiel. Die Formulierung „Bewertung von persönlichen Aspekten“ greift auch Erwägungsgrund 71 ausdrücklich auf (vgl. von Lewinski in: BeckOK Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Artikel 22 Rn. 9).

VON LEWINSKI kommt zu dem Schluss: „Wegen der Streichung der Aufzählung der Merkmale im Normtext wird teilweise sogar eine Erweiterung des Anwendungsbereiches auf jede automatisierte Entscheidung angenommen. Im Hinblick auf die Aufzählung in Erwägungsgrund 71 S. 2 kann dies jedoch nicht überzeugen. Vielmehr ist davon auszugehen, dass Verfahren der automatisierten Einzelentscheidung eine gewisse Komplexität implizieren.“ (von Lewinski in: BeckOK Datenschutzrecht, Wolff/Brink, 20. Edition, Stand: 01.05.2017, Artikel 22 Rn. 12, 13).

Legt man diese Bewertungen als überwiegende Auffassung der Auslegung von Artikel 22 Absatz 1 DSGVO zugrunde, so wird die „Bewertung von Persönlichkeitsmerkmalen“ in diese Norm hineingelesen.

Nach jetziger Einschätzung werden sich auch zukünftig die Anforderungen, die in der bisherigen Regelung des § 67b Absatz 4 SGB X getroffen wurden, auf die neue Rechtslage des Artikels 22 DSGVO übertragen lassen. Zumindest ist vorübergehend von einer Fortgeltung der Rechtslage auszugehen. Insoweit kann auf die bisherige Kommentierung zu § 67b Absatz 4 SGB X zurückgegriffen werden.

5 Die Auftragsverarbeitung

Auch nach der neuen Rechtslage wird es ermöglicht, bestimmte Tätigkeiten durch einen Auftragsverarbeiter durchführen zu lassen (Artikel 28 i. V. m. Erwägungsgrund 81 DSGVO). Maßgebliches Kriterium ist, dass der Verantwortliche die Zwecke und Mittel der Verarbeitung festlegt und der Auftragsverarbeiter sich an die ihm festgelegten Weisungen hält.

5.1 Welche Anforderungen muss der Vertrag zur Auftragsverarbeitung zukünftig erfüllen?

Die inhaltlichen Anforderungen an den Vertrag werden in Artikel 28 Absatz 3 DSGVO aufgeführt (bisher § 80 Absatz 2 SGB X a. F.). Damit müssen die Auftragsverarbeitungsverträge (im Folgenden kurz: AVV) alle in dieser Vorschrift aufgezählten Inhalte abdecken.

5.2 Das Erfordernis der Anzeige gegenüber dem Bundesversicherungsamt ergibt sich nicht aus der DSGVO, sondern aus dem SGB X. Damit wird eine Anforderung geschaffen, die über die Regelungen der DSGVO hinausgeht. Auf welcher Rechtsgrundlage erfolgt dies?

Die durch den Gesetzgeber auferlegte Pflicht zur Anzeige der Auftragsverarbeitung an das Bundesversicherungsamt basiert auf einer Öffnungsklausel der DSGVO. So wird von der Öffnungsklausel des Artikel 6 Absatz 1 Buchstabe e) i. V. m. Absätzen 2 und 3 DSGVO Gebrauch gemacht. Vor diesem Hintergrund wird im deutschen Recht eine Anzeigepflicht begründet. Insoweit stellt die Anzeigenpflicht im deutschen Recht auch keinen Verstoß gegen das europäische Recht dar. In diesem Zusammenhang ist auch zu berücksichtigen, dass die Anzeigepflicht gegenüber dem Bundesversicherungsamt keine Abweichung des in der DSGVO geregelten Datenschutzstandards darstellt. Insoweit stellt die Anzeige ein Spezifikum des deutschen Sozialrechts dar, das in der DSGVO keine Regelung erfährt.

5.3 Gibt es ein Muster für die Anzeigen gem. § 80 Absatz 1 SGB X?

Das Bundesversicherungsamt hat für neue Anzeigen ab dem 25. Mai 2018 ein Formular entwickelt. Dieses kann von den Sozialversicherungsträgern zukünftig für die neuen Anzeigen gemäß § 80 Absatz 1 SGB X verwendet werden.

5.4 Was ist der wesentliche Unterschied zwischen § 80 SGB X in der Neufassung und in der bis zum 24. Mai 2018 geltenden Fassung?

Durch die neue Rechtslage verändern sich rein formal nur wenige Aspekte. Ein wesentlicher Unterschied besteht darin, dass der bisherige § 80 Absatz 2 SGB X, in dem der Inhalt des Auftrags festgelegt wird, durch Artikel 28 Absatz 3 DSGVO ersetzt wird. Eine inhaltlich wesentliche Veränderung ergibt sich jedoch daraus, dass für die Einhaltung der technisch-organisatorischen Maßnahmen zukünftig nicht mehr auf den Kriterienkatalog des § 78a SGB X bzw. die dazugehörige Anlage verwiesen wird. Dieser stellte nach unserer Einschätzung auch nur einen Ausschnitt des jeweiligen Sicherheitskonzepts dar. Nunmehr ist die Sicherheit der Verarbeitung ganzheitlich zu betrachten (vgl. Artikel 32 DSGVO), was in Anbetracht der zu schützenden Daten auch angemessen ist.

5.5 Welche Änderungen ergeben sich für die Auftragsverarbeiter nach der neuen Rechtslage?

Die DSGVO verändert die rechtliche Lage der Auftragsverarbeiter. Dies ist jedoch nicht einheitlich in Artikel 28 DSGVO geregelt, sondern ergibt sich aus der Gesamtschau aller in der DSGVO aufgeführten Normen. So sieht Artikel 30 Absatz 2 DSGVO als Neuerung vor, dass auch die Auftragsverarbeiter – wie die Verantwortlichen – ein Verarbeitungsverzeichnis erstellen müssen. Jedoch ist das durch den Auftragsverarbeiter zu erstellende Verzeichnis von geringerem Umfang als das des Verantwortlichen. So muss der Auftragsverarbeiter nicht die Kategorien von Empfängern auflisten, gegenüber denen die Daten offengelegt werden. Sein Verzeichnis bemisst sich demgegenüber mehr an den im Auftrag genannten Kategorien der Verarbeitungstätigkeit. Zudem haften auch Auftragsverarbeiter gemäß Artikel 82 Absatz 1 DSGVO für materielle oder immaterielle Schäden, die bei einem Verstoß gegen die DSGVO entstehen. Für die Auftragsverarbeiter besteht auch die in Artikel 37 DSGVO aufgeführte Pflicht zur Benennung eines Datenschutzbeauftragten. Zusätzlich können die in Artikel 58 DSGVO aufgeführten Befugnisse auch gegenüber den Auftragsverarbeitern erlassen werden.

Zusammenfassend lässt sich damit festhalten, dass die DSGVO für Auftragsverarbeiter mehr Pflichten begründet, als es nach der bisherigen Rechtslage der Fall ist.

5.6 Die bisherige Regelung sieht ausdrücklich eine regelmäßige Prüfungspflicht vor. Eine solche Regelung enthält § 80 SGB X n. F. nicht. Entfällt damit die Pflicht zur Prüfung des Auftragsverarbeiters?

Nein, die Prüfpflichten bei dem Auftragsverarbeiter entfallen nicht. Die diesbezügliche Regelung ist nunmehr in Artikel 28 DSGVO enthalten. Das Prüfrecht ist so ausgestaltet, „dass der Auftragsverarbeiter dem Verantwortlichen (….) Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht oder dazu beiträgt“ (Artikel 28 Absatz 3 Bst. h DSGVO). Damit wird die Überprüfungspflicht bereits Bestandteil des konkreten Vertrags zur Auftragsverarbeitung. In welchen Abständen diese Prüfungen zu erfolgen haben, ist nicht in der DSGVO geregelt. Dies kann in den jeweiligen Verträgen variieren. Jedoch ist in diesem Zusammenhang Folgendes zu beachten: Gemäß Artikel 28 Absatz 1 DSGVO arbeitet der Verantwortliche nur mit Auftragsverarbeitern, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der Personen gewährleistet. Dies beinhaltet implizit die Verpflichtung, dass diese Garantien nicht nur zu Beginn des Auftragsverhältnisses vorliegen müssen, sondern darüber hinaus während des gesamten Zeitraumes fortgelten.

5.7 Die Notwendigkeit, eine AVV bei Prüfung oder Wartung durch andere Stellen abzuschließen, existiert nach neuer Rechtslage ausschließlich in § 80 Absatz 5 SGB X. Welche Folgen hat dies vor dem Hintergrund der Rechtehierarchie?

Bislang ordnet sowohl § 11 Absatz 5 BDSG a. F. für personenbezogene Daten als auch § 80 Absatz 7 SGB X a. F. für Sozialdaten an, dass bei Prüfungs- und Wartungsverträgen, bei denen ein Zugriff auf diese Daten nicht ausgeschlossen werden kann, ein Vertrag über eine Auftragsdatenverarbeitung abzuschließen ist.

Diese Rechtslage wird unter dem neuen Recht nicht beibehalten. Eine solche Regelung enthält zukünftig nur § 80 Absatz 5 SGB X für die Verarbeitung von Sozialdaten. In der Gesetzesbegründung (BT- Drs. 18/12611, S. 124) wird erörtert: „Bei Verträgen über die Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag, bei denen ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann, handelt es sich um Auftragsverarbeitung im Sinne des Artikels 28 der Verordnung. Somit sind auch die Absätze 1, 2 und 4 anzuwenden“. Weder die Neufassung des BDSG noch die DSGVO sehen eine explizite Einordung der Prüfungs- und Wartungsverträge vor.

In der Literatur zur Auftragsverarbeitung ist es umstritten, wie Prüfungs- und Wartungsverträge rechtlich einzuordnen sind. Vor diesem Hintergrund ist es fraglich, ob nach künftigem Recht für Prüfungs- und Wartungsverträge, bei denen eine Kenntnisnahme personenbezogener Daten möglich ist, ein Vertrag zur Auftragsverarbeitung nach Artikel 28 DSGVO abzuschließen ist.

So hält es das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) für möglich, dass bestimmte Tätigkeiten, wie bei einer rein technischen Wartung, unter Umständen nicht zu einer Qualifikation als Auftragsverarbeitung und einer Anwendung von Artikel 28 DSGVO führen. Anders sei es hingegen, wenn der Auftragsgegenstand gerade der Umgang mit Datensätzen mit personenbezogenen Daten ist. Dann würde es sich weiter um eine Auftragsverarbeitung handeln (Quelle: BayLDA, Informationspapier Nr. X: Auftragsverarbeitung nach der DSGVO, Stand: 26.10.2016).

Ähnlich differenziert der Branchenverband BITKOM: Danach stellen Aufträge über Wartung oder Prüfung von IT-Systemen keine Auftragsverarbeitung dar, sofern Gegenstand des Vertrages keine Datenverarbeitung ist, sondern der Vertrag allein auf die Support-Leistung abzielt. Nach der DSGVO müssen aber deswegen keine den ADV-Vorgaben entsprechenden Regelungen wie nach § 11 Abs. 5 BDSG abgeschlossen werden. Die Wartung und Prüfung müsse so organsiert werden, dass die Daten entsprechend den in Artikel 24 DSGVO festgelegten Pflichten des Verantwortlichen angemessen geschützt sind. Eine Verschwiegenheitsverpflichtung solle dazu genügen. Infolgedessen kämen bei vielen Dienstleistungen in der IT-Branche die gesetzlichen Anforderungen an eine Auftragsverarbeitung nicht zur Anwendung (Quelle: BITKOM, Begleitende Hinweise zu der Anlage Auftragsverarbeitung – Leitfaden; Stand: 2017, S. 22).

Auch nach SPOERR fällt die Auftragsverarbeitung nicht darunter: „Ebenso wenig dürfte die Wartung von IT-Hardware eine Auftragsverarbeitung sein. Bei solchen Unterstützungsprozessen sind aber sowohl Verantwortlicher als auch Auftragsverarbeiter verpflichtet, die IT-Sicherheit zu gewährleisten“ (Spoerr in: BeckOK Datenschutzrecht, Wolff/ Brink, 21. Edition, Stand: 01.08.2017, Artikel 28 Rn. 21).

Gleichlautend ist die Darstellung von INGOLD, wenn dargelegt wird, dass Verträge über Wartung oder Fernwartung durch externe von der Privilegierung ausgenommen sind, soweit in deren Rahmen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Insoweit werde eine analoge Anwendung der Vorschriften über die Auftragsverarbeitung angedacht (vgl. Ingold in: Sydow, Europäische Datenschutzgrundverordnung, 1. Aufl. 2017, Artikel 28 Rn. 20).

Andererseits vertreten SCHMIDT/FREUND die Auffassung, dass die Regelungen des Artikels 28 DSGVO auf die Systemwartung direkt anwendbar sind. Denn der Dienstleister erhalte die Möglichkeit, auf personenbezogene Daten zuzugreifen. Dabei handele es sich um eine Verarbeitung

im Sinne von Artikel 4 Nr. 2 DSGVO (Schmidt/Freund, Perspektiven der Auftragsverarbeitung, ZD 2017, 14).

Auch die o. a. Gesetzesbegründung zur Neufassung des § 80 SGB X lässt darauf schließen, dass der Gesetzgeber grundsätzlich von einer Auftragsverarbeitung und daher einer Vereinbarung gem. Artikel 28 DSGVO ausgeht.

Die jeweilige Bewertung hat – bezüglich der Verarbeitung personenbezogener Daten – unterschiedliche Auswirkungen. Je nach Ansicht sollte ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen werden oder nicht. Unstreitig ist jedenfalls, dass für Sozialdaten gem. § 80 SGB X derartige Verträge abgeschlossen werden müssen.

Schließlich ist die konkrete Einordnung, ob Wartungs- und Prüfungsverträge, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, unter Artikel 28 DSGVO zu fassen sind, noch nicht abschließend erfolgt. Daher sind die Sozialversicherungsträger grundsätzlich in ihrer Entscheidung frei, welcher Auffassung in der Literatur sie sich anschließen.

Aufgrund der bestehenden Rechtsunsicherheit empfehlen wir bis zur endgültigen Entscheidung den Abschluss einer solchen Vereinbarung auch für Wartungen, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

5.8 Das Muster des Bundesversicherungsamtes zur Anzeige gem. § 80 SGB X sieht vor, dass der Verantwortliche vor Beginn der Auftragsverarbeitung eine Prüfung durchgeführt oder veranlasst hat. Sind, was den Zeitpunkt der Prüfung anbelangt, Besonderheiten bei der Durchführung von Vergabeverfahren zu berücksichtigen?

Grundsätzlich ist eine Kontrolle vor Beginn der eigentlichen Auftragsverarbeitung erforderlich. In der Regel werden die technischen und organisatorischen Maßnahmen vor Vertragsschluss individuell vereinbart. Im Vergabeverfahren kommt der Vertrag aber durch den Zuschlag zustande. Eine Kontrolle aller am Vergabeverfahren beteiligten Bieter vor Vertragsabschluss ist kaum möglich und auch nicht sinnvoll. Insoweit haben wir, was den Zeitpunkt der Prüfung anbelangt, auf den Beginn der Auftragsverarbeitung abgestellt.

5.9 Das Muster des Bundesversicherungsamtes zur Anzeige gem. § 80 SGB X sieht die Frage vor, ob die bzw. der Datenschutzbeauftragte beteiligt wurde. Wie ist diese Beteiligung zu verstehen?

Die „Beteiligung“ der bzw. des Datenschutzbeauftragten bedeutet nicht, dass diese Stelle die gesamten Auftragsverarbeitungen im Einzelnen aushandeln bzw. prüfen muss. Die Aufgaben

einer bzw. eines Datenschutzbeauftragten ergeben sich aus Artikel 39 DSGVO. Danach steht insbesondere die Beratungs- und Überwachungsfunktion im Vordergrund. Diese Funktionen können nach unserer Einschätzung aber nur wahrgenommen werden, wenn auch zumindest eine Kenntnisnahme der Vorgänge organisationsintern sichergestellt werden kann. Wie die oder der Datenschutzbeauftragte diese Funktion letztlich ausübt, ist organisationsintern auszugestalten.

6 Das Verarbeitungsverzeichnis

Das nach geltendem Recht zu führende Verfahrensverzeichnis wird zukünftig durch ein Verarbeitungsverzeichnis ersetzt. Dieses beinhaltet nähere Informationen, die für die konkrete Verarbeitung von Bedeutung sind, wie z. B. die Zwecke der Verarbeitung, die Kategorien von Empfängern und – wenn dies möglich ist – Löschfristen sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (vgl. Artikel 30 DSGVO).

6.1 Stellt das Bundesversicherungsamt ein Muster für ein Verarbeitungsverzeichnis gemäß Artikel 30 DSGVO zur Verfügung?

Nein, das Bundesversicherungsamt stellt aktuell kein Muster für ein Verarbeitungsverzeichnis zur Verfügung. Zuständige datenschutzrechtliche Aufsichtsbehörde für die Auslegung der DSGVO ist die BfDI bzw. die Landesdatenschutzaufsichten.

Bei Unsicherheiten sollte insoweit zunächst die BfDI zu Rate gezogen werden. Soweit sich aus unserer Aufsichtspraxis jedoch konkrete Hinweise ergeben, die eine Erstellung und Ausgestaltung des Verarbeitungsverzeichnisses erleichtern, werden wir diese an dieser Stelle als Empfehlung formulieren.

7 Sicherheit der Verarbeitung

Vorgaben für die Sicherheit der Verarbeitung werden nunmehr direkt in der DSGVO gemacht. Anstatt – wie bisher die Anlage zu § 78a SGB X – nur einzelne Aspekte der Sicherheit zu betrachten, liegt der DSGVO ein risikoorientierter Gesamtansatz zugrunde.

7.1 Stellt das Bundesversicherungsamt den Sozialversicherungsträgern allgemeingültige IT-Sicherheitskonzepte zur Verfügung?

Die angemessene Ausgestaltung eines IT-Sicherheitskonzepts ist von den individuellen Gegebenheiten eines Sozialversicherungsträgers abhängig und unterliegt – auch aufgrund der technischen Weiterentwicklung – einem schnellen Wandel. Insofern können hier nach Auffassung des Bundesversicherungsamtes keine allgemeingültigen Vorgaben definiert werden, die über die allgemeinen Vorgaben z. B. des Bundesamts für Sicherheit in der IT-Sicherheit (BSI) hinausgehen. Bei der Erstellung eines IT-Sicherheitskonzepts bietet sich daher die Anlehnung an anerkannte Regelwerke (bspw. den BSI-Grundschutz oder die ISO 27000-Normenreihe) an.

7.2 Stellt das Bundesversicherungsamt eine Hilfe für die Auswahl der technischen und organisatorischen Maßnahmen zur Verfügung?

Die Vorschriften zur Sicherheit der Verarbeitung knüpfen künftig nicht mehr an die zu treffenden Maßnahmen, sondern an die Gewährleistung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit im Einzelfall an. Hierzu muss der Verantwortliche im Rahmen eines risikoorientierten Vergehens individuell angemessene technische und organisatorische Maßnahmen ermitteln, auswählen und umsetzen. Aus dem Ansatz der Risikoorientierung ergibt sich auch, dass eine regelmäßige Überprüfung und gegebenenfalls Anpassung der Maßnahmen erforderlich ist. Aufgrund der erforderlichen Berücksichtigung der individuellen – und üblicherweise im Zeitlauf veränderlichen – Gegebenheiten ist eine allgemeingültige Aussage darüber, welche Maßnahmen in welcher Ausprägung umzusetzen sind, nicht möglich. Aus diesem Grund kann das Bundesversicherungsamt auch hierzu keine Vorlage liefern.

8 Meldung von sog. Datenschutzpannen an die Aufsichtsbehörden

Verletzungen des Schutzes personenbezogener Daten (sog. Datenschutzpannen) müssen unverzüglich innerhalb einer bestimmten Frist an die Datenschutzaufsicht (BfDI/LfDI) gemeldet werden (Artikel 33 DSGVO). Als Sonderregelung für den Bereich des Sozialrechts sind die gleichen Meldungen ebenfalls an die Rechtsaufsichtsbehörde zu richten (§ 83a SGB X). Damit wird die bisherige Anzeigepflicht bei gleichzeitiger Ausweitung der meldepflichtigen Tatbestände und Straffung des Meldeverfahrens beibehalten.

8.1 Welche Mindestanforderungen muss eine Meldung von Datenpannen erfüllen?

Die Anforderungen an eine Meldung sind in Artikel 33 Absatz 3 DSGVO aufgeführt. Danach muss eine Meldung die Art der Verletzung des Schutzes personenbezogener Daten beschreiben, die Kontaktdaten des Datenschutzbeauftragten beinhalten, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung beschreiben.

8.2 Nach der neuen Rechtslage soll eine Meldung sowohl an das Bundesversicherungsamt als auch an die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) erfolgen. Ist eine doppelte Meldung notwendig?

Ja. Denn das Gesetz sieht ausdrücklich eine zweifache Meldung sowohl an das Bundesversicherungsamt als auch an die BfDI vor.

8.3 Gemäß Artikel 33 Absatz 1 2.Halbsatz DSGVO muss der Verantwortliche keine Meldung abgeben für den Fall, „dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“. Muss der Verantwortliche in dieser Konstellation keinerlei Maßnahmen durchführen?

Doch. Auch, wenn der Verantwortliche keine Meldung abgibt, trifft ihn dennoch eine Pflicht zur Dokumentation des Vorfalls. Diese ergibt sich aus Artikel 33 Absatz 5 DSGVO. Danach ist der Verantwortliche dazu verpflichtet, insbesondere solche Datenpannen zu dokumentieren, bei denen er von der Meldung absieht. Dabei sollte die Dokumentation auch die Gründe für das Absehen von der Meldung, also die konkrete fachliche Einschätzung des Verantwortlichen, enthalten.

9 Die Datenschutz-Folgenabschätzung

Wenn Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, sollten die Verantwortlichen die Folgen der Verarbeitung im Vorfeld genau analysieren (Artikel 35 i.V. m. Erwägungsgrund 84 DSGVO). Insbesondere sollen die Ursache, die Art, die Besonderheit und die Schwere des Risikos evaluiert werden.

9.1 Welche Kriterien sind bei einer Datenschutz-Folgeabschätzung gem. Artikel 35 DSGVO anzulegen?

Nach aktueller Einschätzung wird die Datenschutz-Folgenabschätzung gem. Artikel 35 DSGVO inhaltlich mit der bisherigen Vorabkontrolle gem. § 4d BDSG weitestgehend vergleichbar sein. Dies ist insbesondere für die Übergangszeit hilfreich.

9.2 Gibt das Bundesversicherungsamt weitere Hinweise, wie die Datenschutzfolgeabschätzung durchzuführen ist?

Wie unter Punkt 1.3 angeführt, ist die für die Auslegung der DSGVO zuständige Datenschutzaufsicht (BfDI, LfDI) zuvorderst für etwaige Hinweise zuständig. Insoweit verweisen wir zum einen auf das von der Datenschutzkonferenz (DSK) herausgegebene Arbeitspapier Nr.5 zur Datenschutzfolgeabschätzung und auf das Working Paper der Artikel 29-Gruppe [„WP 248 rev.01“], das sich mit dem Thema Datenschutz-Folgeabschätzung befasst und am 04.10.2017 in überarbeiteter Version veröffentlicht wurde.

9.3 Gibt es die in Artikel 35 Absatz 4 DSGVO erwähnte Positivliste?

Die in Artikel 35 Absatz 4 DSGVO genannte Positivliste, d.h. die Auflistung von Verarbeitungsvorgängen, in denen zwingend eine Datenschutz-Folgenabschätzung durchzuführen ist, wird von der Aufsichtsbehörde der DSGVO festgelegt. Dies ist jedoch nicht das Bundesversicherungsamt, sondern die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bzw. die Landesdatenschutzaufsichten. Ob und wann es eine solche Liste geben wird, ist dem Bundesversicherungsamt nicht bekannt.

9.4 Gibt es die in Artikel 35 Absatz 5 DSGVO erwähnte Negativliste?

Die in Artikel 35 Absatz 5 DSGVO genannte Negativliste, d.h. die Auflistung von Verarbeitungsvorgängen, in denen keine Datenschutz-Folgenabschätzung durchzuführen ist, wird von der Aufsichtsbehörde der DSGVO festgelegt. Dies ist jedoch nicht das Bundesversicherungsamt,

sondern die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bzw. die Landesdatenschutzaufsicht. Ob und wann es eine solche Liste geben wird, ist dem Bundesversicherungsamt nicht bekannt.

9.5 Ist bereits bekannt, ob gem. Artikel 35 Absatz 10 DSGVO eine Datenschutzfolgenabschätzung für nicht erforderlich erachtet wird?

Artikel 35 Absatz 10 DSGVO beschreibt die Konstellation, dass eine Datenschutz-Folgenabschätzung (DSFA) ausnahmsweise nicht durchzuführen ist, obwohl ein hohes Risiko vorliegt. Eine Voraussetzung dieser Ausnahme ist, dass die Rechtsgrundlage der Datenverarbeitung bereits die konkreten Datenverarbeitungsvorgänge regelt und für die bereits im Zusammenhang mit ihrem Erlass eine DSFA durchgeführt wurde. Das bedeutet, dass die DSFA bereits im Gesetzgebungsverfahren durchgeführt wird. Bislang ist ein solch umfassendes Gesetzgebungsverfahren noch nicht bekannt.

10 Der Datenschutzbeauftragte

Der vierte Abschnitt der DSGVO (Artikel 37-39 DSGVO) enthält Vorschriften zum Datenschutzbeauftragten und legt u. a. die Stellung und die Aufgaben des Datenschutzbeauftragten fest. Insoweit regelt Artikel 37 DSGVO, unter welchen Voraussetzungen ein Datenschutzbeauftragter zu benennen ist und welche Pflichten damit verbunden sind.

10.1 Ist die gemäß Artikel 37 Absatz 7 DSGVO zu erfolgende Mitteilung über den Datenschutzbeauftragten gegenüber dem Bundesversicherungsamt zu machen?

Gemäß Artikel 37 Absatz 7 DSGVO veröffentlicht der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten und teilt diese der Aufsichtsbehörde mit. Auch in diesem Kontext meint „Aufsichtsbehörde“ die Datenschutzaufsichtsbehörde. Nicht davon erfasst ist das Bundesversicherungsamt als zuständige Rechtsaufsichtsbehörde. Daher hat die gemäß Artikel 37 Absatz 7 DSGVO vorgeschriebene Meldung an die Datenschutzaufsichtsbehörde zu erfolgen. Über eine nachrichtliche Mitteilung an das Bundesversicherungsamt würden wir uns jedoch freuen.

11 Besondere Arten von Daten

Im Folgenden werden sowohl Betriebs- und Geschäftsgeheimnisse als auch personenbezogene Daten Verstorbener als besondere Arten behandelt, da diese eine Besonderheit des Sozialdatenschutzes sind.

11.1 Betriebs- und Geschäftsgeheimnisse

Die DSGVO bezieht sich auf personenbezogene Daten (Artikel 1 DSGVO). Betriebs- und Geschäftsgeheimnisse sind also von der DSGVO nicht umfasst (vgl. Freund/Shagdar: Sozialdatenschutz – europäisch? In: SGb 04.18, S. 199). Aus § 35 Absatz 4 SGB I ergibt sich jedoch weiterhin eine Gleichstellung von Betriebs- und Geschäftsgeheimnissen mit Sozialdaten, sodass dieses Rechtskonstrukt ausschließlich im Sozialdatenschutz Berücksichtigung findet.

11.1.1 Welche Vorschriften sind auf Betriebs- und Geschäftsgeheimnisse aufgrund dieser Gleichstellung zu Sozialdaten anwendbar?

Zunächst führt die beschriebene Gleichstellung von Betriebs- und Geschäftsgeheimnissen mit Sozialdaten dazu, dass die Vorschriften des Sozialgesetzesbuches auch auf Betriebs- und Geschäftsgeheimnisse Anwendungen finden.

Das bedeutet praktisch z. B., dass Meldungen von Datenschutzverletzungen (§ 83a SGB X) auch bei der Verletzung von Betriebs- und Geschäftsgeheimnissen erfolgen müssen. Dies hat aber ausschließlich gegenüber der Rechts- und Fachaufsichtsbehörde zu erfolgen. Auch sind gemäß § 80 SGB X Anzeigen gegenüber der Rechts- und Fachaufsichtsbehörde abzugeben, wenn im Rahmen von Auftragsverarbeitungen Betriebs- und Geschäftsgeheimnisse verarbeitet werden.

11.2 Personenbezogene Daten Verstorbener

Artikel 1 Absatz 1 DSGVO legt den Schutzbereich der Datenschutzgrundverordnung fest. Danach enthält die Verordnung Vorschriften zum Schutz natürlicher Personen bei der der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. Erwägungsgrund 27 regelt, dass diese Verordnung nicht für die personenbezogenen Daten Verstorbener gilt, Mitgliedstaaten aber Vorschriften für die Verarbeitung der personenbezogenen Daten vorsehen können.

Der deutsche Gesetzgeber hat von dieser Öffnungsklausel Gebrauch gemacht, indem er § 35 Absatz 5 SGB I normiert hat, dass die Sozialdaten Verstorbener nach der Maßgabe des Zweiten Kapitels des Zehnten Buches verarbeitet werden dürfen. Sie dürfen außerdem verarbeitet

werden, wenn schutzwürdige Interessen des Verstorbenen oder seiner Angehörigen dadurch nicht beeinträchtigt werden können.

11.2.1 Was ist die Folge dieser Beibehaltung der möglichen Datenverarbeitung personenbezogener Sozialdaten Verstorbener?

Dadurch, dass der Gesetzgeber von der Öffnungsklausel Gebrauch gemacht hat, legt er die Bedingungen fest, unter denen Sozialdaten Verstorbener verarbeitet werden dürfen. Insoweit wird explizit auf das 2. Kapitel des SGB X verwiesen, also auf die Vorschriften §§ 67- 85a SGB X. Daraus folgt, dass die in diesen Vorschriften normierten datenschutzrechtlichen Anforderungen eingehalten werden müssen. Damit sind beispielsweise auch Datenschutzpannen nach § 83a SGB X an die Rechtsaufsichtsbehörde zu melden, soweit ein hohes Risiko für die Rechte und Freiheiten der Betroffenen gesehen wird.

12 Die Aufsichtsbehörden

Die Datenschutzgrundverordnung verändert die Verhältnisse der Aufsichtsbehörden. So wird der Datenschutzaufsichtsbehörde aufgrund der neu gewonnenen Befugnisse aus Artikel 58 DSGVO bzw. § 16 BDSG eine neue Rolle zuteil. Das Verhältnis zwischen der Datenschutzaufsichtsbehörde und der Rechtsaufsichtsbehörde wird nunmehr in § 16 BDSG geregelt.

12.1 Welche Rolle spielt das Bundesversicherungsamt, wenn die Datenschutzaufsichtsbehörde Maßnahmen nach Art. 58 DSGVO gegenüber einem Verantwortlichen vornehmen möchte?

§ 16 Absatz 1 BDSG regelt den konkreten Ablauf, wenn die Datenschutzaufsichtsbehörde von ihren in Artikel 58 Absatz 2 Buchstabe b bis g, i und j DSGVO eingeräumten Befugnissen Gebrauch machen möchte. Kommt die Datenschutzaufsichtsbehörde zu dem Ergebnis, dass Verstöße gegen den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt sie dies der zuständigen Rechts- oder Fachaufsichtsbehörde mit und gibt dieser vor Ausübung der Befugnisse gegenüber dem Verantwortlichen Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. Es soll die Gefahr divergierender Entscheidungen zwischen Rechts- und Fachaufsichtsbehörde reduzieren.

Somit ist das Bundesversicherungsamt beteiligt, wenn die BfDI von ihren Befugnissen gemäß Artikel 58 Absatz 2 Buchstabe b bis g, i und j DSGVO gegenüber bundesunmittelbaren Sozialversicherungsträgern Gebrauch macht und entsprechende Maßnahmen einleiten möchte.