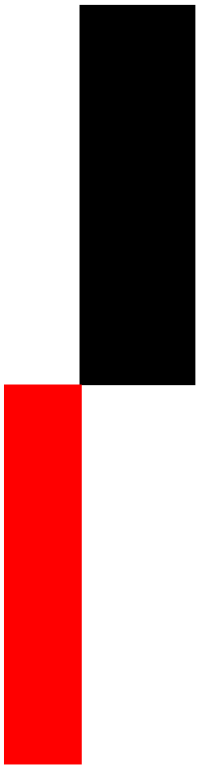
Aufsichtsbehörden der Sozialversicherungsträger des Bundes und der Länder

Frequently Asked Questions

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



VERSION: 6
DATUM: 08.05.2019
STAND: Finalversion

Dokumentenhistorie

Datum	Version	Autor	Änderungen
08.05.2019	6		Veröffentlichung einer gemeinsamen FAQ-Liste der Aufsichtsbehörden der Sozialversicherungsträger des Bundes und der Länder Neue Aspekte: - Aufnahme von Literaturverweisen zu den einzelnen Themen - Kapitel 4 (Betroffenenrechte) - Frage 2.5 (Informationspflichten) - Frage 7.2 (Verarbeitungsverzeichnis) - Fragen 8.4, 8.5 (Datenschutzverletzungen) - Fragen 9.3, 9.6,.9.7, 9.8 (Datenschutzfolgeabschätzung)
22.05.2018	5		Neugestaltung der FAQ-Liste, Einführung einer Dokumentenhistorie ab Version 5
Vorversionen	1-4		Vorversionen dienen der ersten, unstrukturierten Darstellung der an das Bundesversicherungsamt herangetragenen Fragen

Inhaltsverzeichnis

Vorbemerkungen

Zu den anwendbaren Gesetzen:
Wenn im Folgenden Normen nach dem SGB I und X zitiert werden, handelt es sich um die Fassungen, die seit dem 25. Mai 2018 zur Anwendung kommen.

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

Zu den Aufsichtsbehörden:
Wenn im Folgenden der Begriff „Aufsichtsbehörden“ verwendet wird, sind damit die Aufsichtsbehörden der Sozialversicherungsträger des Bundes und der Länder gemeint. Demgegenüber meint der Begriff „Aufsichtsbehörde“ in der DSGVO die jeweiligen Datenschutzaufsichtsbehörden des Bundes und der Länder. Diese werden im weiteren Verlauf als „Datenschutzaufsichtsbehörden“ bezeichnet.

1 Allgemeines

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

Bei der DSGVO handelt es sich um eine 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 in Deutschland das Bundesdatenschutzgesetz (BDSG) und – bislang (Stand: 01.12.2017) – das Sozialgesetzbuch (SGB) Erstes Buch (I) und Zehntes Buch (X) neu gefasst. Die Anpassungen der weiteren Sozialgesetzbücher stehen noch aus und werden im Rahmen des sog. „ 2. Datenschutz- Anpassungs- und Umsetzungsgesetzes“ (2. DSAnpUG) erwartet.

1.2 Wann ist nun die DSGVO anzuwenden, wann das 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 das SGB darauf verweist

Dazu einige Beispiele: Grundlegende Definitionen (z.B. Was bedeutet „Verarbeitung“? Wer ist „Verantwortlicher“, wer „Dritter“?) sind in Artikel 4 DSGVO geregelt. Deshalb sieht § 67 SGB X 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.

Auch legt nunmehr die DSGVO die Informationen fest, die der Verantwortliche dem Betroffenen zur Verfügung zu stellen hat. Soweit das nationale Recht davon Abweichungen vorsieht, werden diese neu geregelt.

1.3 Die DSGVO verwendet den Begriff „Aufsichtsbehörde“, die Neufassung des SGB X den Begriff „Rechts- und Fachaufsichtsbehörde“. Ist damit immer das Bundesversicherungsamt bzw. die jeweilige Aufsichtsbehörde des Landes gemeint?

Nein. Wenn in der DSGVO der Begriff „Aufsichtsbehörde“ verwendet wird, sind damit die nationalen Datenschutzaufsichtsbehörden – in Deutschland nach dem BDSG – gemeint. Gemäß § 17 Absatz1 Satz 1 BDSG wird die Bundesrepublik Deutschland im Europäischen Datenschutzausschuss durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) vertreten. Die Neufassung des SGB X enthält zur Unterscheidung davon den Begriff „Rechts- und Fachaufsichtsbehörde“. Das Bundesversicherungsamt und die entsprechenden Landesaufsichtsbehörden sind Rechts- und Fachaufsicht im Sinne der §§ 88 ff. SGB IV.

1.4 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.

1.5 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).

1.6 Stellen die Aufsichtsbehörden den Sozialversicherungsträgern für die Beschreibung der technischen und organisatorischen Maßnahmen ein Muster 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 können die Rechts- und Fachaufsichtsbehörden auch hierzu keine Vorlage liefern.

1.7 Stellen die Aufsichtsbehörden 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 der Aufsichtsbehörden der Sozialversicherungsträger 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.

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 (vgl. Artikel 13 DSGVO i.V.m. § 82 SGB X) oder ob die Daten bei einem Dritten erhoben werden (vgl. Artikel 14 DSGVO i.V.m. § 82a SGB X). Über beide Aspekte muss der Betroffene informiert werden.

Literaturhinweise: DSK-Kurzpapier Nr. 10: „Informationspflichten bei Dritt- und Direkterhebung“

2.1 Worüber muss der Betroffene informiert werden?

Der Betroffene muss darüber informiert werden, wenn bei ihm erstmalig Daten erhoben werden (vgl. 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 (vgl. Artikel 13 Absatz 3 DSGVO). Hingegen besteht keine Informationspflicht, wenn der Betroffene seine Rechte bereits kennt (vgl. 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 (vgl. 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 aus Artikel 13 Absatz 2 Buchstabe d) DSGVO i. V. m. § 82 SGB X auch die Nennung der jeweiligen Aufsichtsbehörden der Sozialversicherungsträger?

Die in Artikel 13 Absatz 2 Buchstabe d) DSGVO aufgeführte Informationspflicht über „das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde“ stellt auf das in Artikel 77 DSGVO

normierte Beschwerderecht ab. Damit ist also das Beschwerderecht bei der im Sinne der DSGVO zuständigen Datenschutzaufsicht gemeint.

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

2.3 Welche Pflichten treffen den Verantwortlichen, wenn keine Informationspflicht besteht?

Auch wenn keine Informationspflicht besteht, muss der Verantwortliche entsprechende Maßnahmen treffen. Gemäß § 82 Absatz 3 SGB X soll die Öffentlichkeit die Gründe des Wegfalls der Informationspflicht erfahren. Als erforderliche Maßnahme wird insoweit beispielsweise die Veröffentlichung auf der Homepage oder in der Mitgliederzeitschrift erachtet.

2.4 Meint das „Ergreifen geeigneter Maßnahmen“ in § 82 Absatz 3 SGB X die „Sperrung“ von Daten?

Nein, das „Ergreifen geeigneter Maßnahmen“ in Artikel 13 DSGVO zielt nicht auf die „Sperrung“ von Daten ab. Dies ergibt sich aus der Gesetzessystematik.

Nach der Gesetzesbegründung (BT-Drs. 18/ 12611, S. 128) liegt eine „geeignete Maßnahme“ insbesondere in der Bereitstellung der Information für die Öffentlichkeit. Sie soll über die Gründe des Wegfalls der Informationspflicht informiert werden. Diese Informationspflicht wird nicht durch die Sperrung von Daten erfüllt. Dabei handelt es sich vielmehr um ein Betroffenenrecht, das durch den Einzelnen ausgeübt wird.

2.5 In welcher Form kann den Informationspflichten nachgekommen werden? Abstrakt und generell oder konkret und individuell?

Artikel 13 DSGVO enthält keine Form- und Verfahrensvorgaben für die Informations- und Mitteilungspflichten. Als Richtschnur ist insoweit Artikel 12 DSGVO einschließlich der dazu gehörenden Erwägungsgründe (insb. ErwGr. 58 und 59) maßgeblich. Jedenfalls muss die Form der Informationen und Mitteilungen leicht zugänglich ausgestaltet sein. Leichte Zugänglichkeit setzt voraus, dass die betroffene Person mit den ihr zur Verfügung stehenden Mitteln die Informatio-

nen erreichen kann. Bei Mitteilungen in Schriftform muss diese dem Betroffenen physisch zugänglich sein, ohne dass es einer Aufforderung eines Betroffenen oder einer Mitwirkung des Verantwortlichen bedarf. Im Online-Kontext hat der Verantwortliche insb. sicherzustellen, dass die Information oder Mitteilung mit allen gängigen Softwareprogrammen visualisierbar ist. Informationen dürfen nicht innerhalb eines Angebots versteckt werden, sondern müssen für den Betroffenen sofort erkennbar sein. Grafisch müssen die Informationen so gestaltet sein, dass sie den Standards der Barrierefreiheit entsprechen. Zudem muss sich der Text optisch hinreichend vom Hintergrund abheben (vgl. Paal/Pauly, Artikel 12, Rn. 27-32a).

Zudem enthält das Rundschreiben des GKV-Spitzenverbandes (Nr. 2017/654) weitere Ausführungen zur Umsetzung der Transparenzpflichten. Insbesondere wurde hierzu vertreten, dass ein Medienbruch bei Artikel 13 Absatz 1 (Datenschutzhinweis) und Absatz 2 (Transparenzinformation) erlaubt ist. Diese Position unterstützten die Aufsichtsbehörden der Sozialversicherungsträger ausdrücklich.

In der Praxis wird es im Ergebnis – abhängig vom Sachverhalt – zu einem Mix aus verschiedenen Informationsformen kommen. In den allermeisten Fällen hat sich eine Kombination aus digitaler Information auf der Webseite bzw. in der Online-Geschäftsstelle sowie förmliche Informationen, die in den Geschäfts- und Servicestellen eingesehen und mitgenommen werden können. Eine Veröffentlichung in der Mitgliederzeitschrift ist in einigen Anwendungsfällen zudem eine gute Ergänzung.

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 (vgl. 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.

Literaturhinweise: DSK-Kurzpapier Nr. 10: „Informationspflichten bei Dritt- und Direkterhebung“

3.1 Gibt es Konstellationen, in denen die Informationspflicht gem. Artikel 19 DSGVO mit Schwierigkeiten verbunden ist? Sind auch Informationspflichten bei maschinellen Datenaustauschen erfasst?

Gemäß Artikel 19 Satz 1 DSGVO ist der Verantwortliche dazu verpflichtet, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Benachrichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

Gemäß der Legaldefinition Artikel 4 Nr. 9 DSGVO 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. 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. In diesem Fall ist die Abwägung nachvollziehbar zu dokumentieren.

3.2 Muss der Sozialversicherungsträger den Dritten auch dann informieren, wenn Drittdaten berichtigt werden, die nicht durch den Sozialversicherungsträger selbst erhoben wurden?

Aus Artikel 14 DSGVO ergibt sich, dass der Verantwortliche Daten nicht nur bei der betroffenen Person, sondern auch bei einem Dritten erheben kann.

Wenn sich der Berichtigungsanspruch der betroffenen Person aus Artikel 16 DSGVO auch auf derartige Daten (Drittdaten) bezieht, wird der Anwendungsbereich des Artikels 19 DSGVO auch in diesem Maße erweitert.

Daher muss der Sozialversicherungsträger auch bei einer Berichtigung der Drittdaten sämtliche Empfänger darüber informieren.

4 Betroffenenrechte

Die DSGVO enthält viele Betroffenenrechte. Zum Beispiel Auskunftsrechte, Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung. Diese Rechte bestanden zum Teil bereits nach der bisherigen Rechtslage, erfahren durch die Datenschutzgrundverordnung aber eine neue Ausprägung. Teilweise wird die Möglichkeit der Geltendmachung dieser Rechte durch Regelungen in der DSGVO und im SGB X modifiziert.

Literaturhinweise: DSK-Kurzpapier Nr. 11: „Recht auf Löschung/ Recht auf Vergessenwerden“

4.1 Inwieweit findet das Recht auf Löschung (Art. 17 Abs. 3 c) DSGVO) auf die Sozial- und Gesundheitsdaten Anwendung, die von Sozialversicherungsträgern verarbeitet werden?

In Artikel 17 Absatz 1 und 2 DSGVO ist geregelt, dass der Betroffene in bestimmten Konstellationen vom Verantwortlichen die Löschung seiner Daten verlangen kann und welche zusätzlichen Maßnahmen der Verantwortliche ergreifen muss. Dieser Grundsatz gilt auch für Sozial- und Gesundheitsdaten und findet in § 84 SGB X seine Entsprechung im Sozialrecht. Von der Möglichkeit, die Löschung der Daten zu verlangen, macht Artikel 17 Absatz 3 DSGVO Ausnahmen. Das heißt, der Betroffene kann sein Recht auf Löschung nicht geltend machen, wenn nach Artikel 17 Absatz 3 DSGVO die Verarbeitung der Daten weiterhin erforderlich ist. So sieht Artikel 17 Absatz 3 lit c) DSGVO eine Ausnahme vor, wenn die Verarbeitung erforderlich ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gem. Artikel 9 Absatz 2 lit.) h und i sowie Artikel 9 Absatz 3 DSGVO. Zusätzlich zu dieser Ausnahme sieht § 84 SGB X auch weitere Ausnahmen vor, in denen eine Löschung der Daten ausgenommen wird.

Es ist im jeweiligen Einzelfall zu prüfen, ob die Voraussetzungen für eine Löschung bzw. Ausnahmen von der Löschung bestehen. Maßgeblich ist, ob die Daten „für die Verarbeitung erforderlich“ sind. Weiterhin ist zu berücksichtigen, dass es im Sozialrecht bestimmte Aufbewahrungsfristen gibt, die ebenfalls einer Löschung entgegenstehen können. Daher kann keine allgemeingültige Aussage getroffen werden und die Voraussetzungen sind im jeweiligen Einzelfall zu prüfen.

5 Die automatisierte Verarbeitung von Sozialdaten

Nach der DSGVO wird es dem Verantwortlichen verboten, unter bestimmten Umständen eine automatisierte Verarbeitung ohne menschliche Einflussnahme zu treffen (vgl. Artikel 22 DSGVO). Doch auch von dieser Regelung kann gem. Artikel 22 Absatz 2 DSGVO abgewichen werden.

Literaturhinweise: Artikel-29-Datenschutzgruppe: WP251rev.01 („Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2019/679“)

5.1 Wann kann man davon ausgehen, dass eine ausschließlich „automatisierten 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 „(voll-) 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 i) die Vorgangsauslösung, ii) die eigentliche Aktion und iii) 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 2008, S. 108 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 vollautomatisch erfolgt. In diesem Fall würde dann aber der gesamte Verwaltungsvorgang in sog. Dunkelverarbeitung ablaufen, ohne dass hier eine Prüf- und Steuerungsmöglichkeit seitens der Verwaltung besteht. Nur im Fall dieser „vollautomatisierten Entscheidung“ ist nach Auffassung der Aufsichtsbehörden der Anwendungsbereich des Artikels 22 Absatz 1 DSGVO eröffnet.

5.2 Wie ist Artikel 22 DSGVO auszulegen: Ist davon nur die Verarbeitung erfasst, die eine negative Auswirkung für den Betroffenen hat oder fallen auch positive Auswirkungen für den Betroffenen darunter?

Es kommt darauf an, ob in Artikel 22 Absatz 1 DSGVO allein darauf abgestellt wird, dass die Entscheidung „rechtliche Wirkung entfaltet“ oder ob diese Entscheidung 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“). Demnach ist entscheidend, ob das Ergebnis des Verarbeitungsvorgangs ohne menschliche Einflussnahme eine Beeinträchtigung enthält oder nicht.

Für die Praxis bedeutet dies einen wesentlichen Unterschied: Im ersten Fall (rechtliche Wirkung genügt) wären von dem Verbot des 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 jedoch (nur belastende Entscheidungen) enthielte das Verbot lediglich automatisierte Verarbeitung, die rechtlich nachteilig sind (z.B. automatisiert erstellter Ablehnungsbescheid). Daher ist das Ergebnis der Auslegung für die Beurteilung des Anwendungsbereichs von Artikel 22 DSGVO wesentlich.

Nach kursorischer Durchsicht der dazu vertretenen Auffassungen im Schrifttum stellt die Literatur insbesondere auf die letztere Auffassung ab, wonach bei dem Betroffenen eine erhebliche Beeinträchtigung hervorgerufen werden muss.

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 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]

Nach einer ersten Einschätzung ist von diesem Verständnis der Vorschrift auszugehen. Dies führt dazu, dass Artikel 22 Absatz 1 DSGVO nur dann anzuwenden ist, wenn die automatisierte Verarbeitung zu einer negativen Folge führt. Das bedeutet, dass Artikel 22 Absatz 1 DSGVO das Verbot enthält, dass keine negativen Entscheidungen aufgrund automatisierter Verfahren ohne menschliches Zutun getroffen werden dürfen.

5.3 Gibt es bei Artikel 22 Absatz 1 DSGVO eine weitere Einschränkung oder sind alle automatisierten negativen Entscheidungen erfasst? Welche Bedeutung hat die bisherige Regelung in § 67b Absatz 4 SGB X, wonach eine automatisierte Verarbeitung von Sozialdaten erfasst ist, die „der Bewertung einzelner Persönlichkeitsmerkmale dient“?

Fraglich ist, ob auch in Artikel 22 Absatz 1 DSGVO – wie im bisherigen § 67b Absatz 4 SGB X – darauf abgestellt wird, ob 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 weiter 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 diese Einschränkung nicht mehr enthalten ist. Daraus würde geschlossen werden, dass Artikel 22 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 Wir-

kung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt [Buchner in: Kühling/Buchner, ebenda, Artikel 22 Rn. 17].

Schon vom Ergebnis her könne ein solch weites Verständnis des Artikels 22 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 [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 [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 S. 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 [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 DS-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 Artikel 22 DSGVO übertragen lassen. Zumindest ist insoweit vorübergehend von einer Fortgeltung der Rechtslage auszugehen. Insoweit kann auf die bisherige Kommentierung zu § 67b Absatz 4 SGB X zurückgegriffen werden.

5.4 Welchen Anwendungsbereich umfasst damit Artikel 22 DSGVO?

Nach der hier vertretenen Auffassung (s.o. die Antworten unter 4.2 sowie 4.3) verbietet Artikel 22 Absatz 1 DSGVO nicht alle Formen der automatisierten Entscheidung ohne menschliche Einflussnahme. Vielmehr wird verboten, dass ohne menschliche Einflussnahme für den Betroffenen rechtlich verbindliche Entscheidungen getroffen werden, die im Zusammenhang mit der Bewertung von persönlichen Aspekten des Betroffenen stehen.

Nach Auffassung der Aufsichtsbehörden ist die Kommentierung von ROMBACH zu § 67b Absatz 4 SGB X auch weiterhin zutreffend. Zitat „Absatz 4 bestimmt, dass Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht auf eine automatisierte Verarbeitung von Sozialdaten gestützt werden dürfen, die der Bewertung einzelner Persönlichkeitsmerkmale dient. Dies wäre der Fall, wenn Daten zum Zweck der Bewertung einzelner Aspekte einer Person, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens verarbeitet werden. Diese Einschränkung soll verhindern, dass Entscheidungen, aufgrund von Persönlichkeitsprofilen ergehen, ohne dass der Betroffene die Möglichkeit hat, die zugrunde liegenden Sachverhalte und Bewertungskriterien zu erfahren. Im Bereich des Sozialrechts mit seiner Massenverwaltung kommen zwar häufig Verwaltungsakte auf der Basis automatisierter Verarbeitung von Sozialdaten vor, wie z.B. die jährlichen Bescheide, mit denen laufende Geldleistungen an die wirtschaftliche Entwicklung angepasst werden. Insgesamt dürfte diese Regelung im Bereich des Sozialrechts aber kaum eine Rolle spielen, da in diesem Verfahren keine Persönlichkeitsmerkmale bewertet werden.“ (vgl. Rombach in: Hauck/Noftz § 67b SGB X, Rn. 83a).

Zudem sind automatisierte Entscheidungen nicht vom Verbot des Absatzes 1 betroffen, wenn sie auf einer nationalen Regelung beruhen, vgl. die Ausnahmeregelung in Artikel 22 Absatz 2 Buchstabe b) DSGVO. Im SGB ist insbesondere § 31a SGB X zu erwähnen.

Dies hat beispielsweise zur Folge, dass trotz dieses Verbots gem. § 31a SGB X ein vollständig automatisierter Verwaltungsakt ergehen kann, wenn dieser für den Betroffenen einen rechtlichen Vorteil begründet oder nachteilig ist, sich aber nicht auf die Bewertung von Persönlichkeitsmerkmalen bezieht.

5.5 Welchen Einfluss hat es auf die Anwendbarkeit von Artikel 22 Absatz 1 DSGVO, wenn zwar in einem ersten Schritt („Erstprüfung“) eine „automatisierte Entscheidung ohne menschliches Zutun“ erfolgt, aber in einem zweiten Schritt („Nachprüfung“) im Rahmen eines Widerspruchsverfah-

rens ein Mensch diese Entscheidung überprüft? Führt diese Überprüfungsmöglichkeit dazu, dass Artikel 22 Abs. 1 DSGVO anwendbar ist?

Für die Beurteilung, ob eine „automatisierte Entscheidung ohne menschliches Zutun“ getroffen wird, kommt es nach Artikel 22 Absatz 1 DSGVO ausschließlich auf das Ergebnis der automatisierten Entscheidung (Schritt 1: „Erstprüfung“) an. Eine nach der Entscheidung eröffnete Überprüfungsmöglichkeit (Schritt 2: „Nachprüfung“) durch einen Menschen (auch) für automatisiert erlassene Verwaltungsakte spielt nach Auffassung der Aufsichtsbehörden für die Beurteilung von der Anwendbarkeit von Artikel 22 Absatz 1 DSGVO keine Rolle.

Das bedeutet, dass die Anwendbarkeit des Artikels 22 Absatz 1 DSVO auf die oben genannten Konstellationen beschränkt ist. Soweit in diesem Zusammenhang auf ein „menschliches Zutun“ abgestellt wird, kann dieses nicht dadurch ersetzt werden, dass in einem Widerspruchsverfahren – d. h. nach einer getroffenen Entscheidung – eine menschliche Überprüfung stattfinden kann.

6 Die Auftragsverarbeitung

Auch nach der neuen Rechtslage wird es ermöglicht, bestimmte Tätigkeiten durch einen Auftragsverarbeiter durchführen zu lassen, vgl. Art 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.

Literaturhinweise: DSK-Kurzpapier Nr. 13: „Auftragsverarbeitung, Artikel 28"; BfDI: Muster Auftragsverarbeitung nach DSGVO

6.1 Welche Anforderungen muss der Vertrag zur Auftragsverarbeitung zukünftig erfüllen?

Die inhaltlichen Anforderungen an den Vertrag werden in Artikel 28 Absatz 3 DSGVO aufgeführt. Damit müssen die Auftragsverarbeitungsverträge alle in dieser Vorschrift aufgezählten Inhalte abdecken.

6.2 Das Erfordernis der Anzeige gegenüber der Rechts- und Fachaufsichtsbehörde 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 (Rechts-) Grundlage erfolgt dies?

Die durch den Gesetzgeber auferlegte Pflicht zur Anzeige der Auftragsverarbeitung an die Rechts- und Fachaufsichtsbehörde basiert auf einer Öffnungsklausel der DSGVO. So wird von der Öffnungsklausel des Artikel 6 Absatz 1 Buchstabe e) i. V. m. Absatz 2 und Absatz 3 Satz 3 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 der Rechts- und Fachaufsichtsbehörde 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.

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

Die Aufsichtsbehörden der Sozialversicherungsträger haben für Anzeigen ein gemeinsames Formular entwickelt. Dieses kann von den Sozialversicherungsträgern für die Anzeigen gemäß § 80 Absatz 1 SGB X verwendet werden.

6.4 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 Einschätzung der Aufsichtsbehörden 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.

6.5 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.

6.6 Die bisherige Regelung sah ausdrücklich eine regelmäßige Prüfungspflicht vor. Eine solche Regelung enthält § 80 SGB X 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 (….) und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht oder dazu beiträgt“ (vgl. Artikel 28 Absatz 3 DSGVO lit. h). 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.

6.7 Sind nach der neuen Rechtslage Auftragsverarbeitungsverträge (AVV) zur Prüfung und Wartung nur bei Sozialdaten oder auch bei personenbezogenen Daten abzuschließen?

Nach bisherigem Recht ordnete sowohl § 11 Absatz 5 BDSG (a. F.) für personenbezogene Daten als auch § 80 Absatz 7 SGB X 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, da für personenbezogene Daten weder die DSGVO noch das BDSG eine Regelung enthalten. 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 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 DS-GVO, 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 DS-GVO 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 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 DS-GVO (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 personenbezogene Daten.

6.8 Sind hinsichtlich der Überprüfung der Auftragsverabeitung durch den Verantwortlichen 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 zustan-

de. Eine Kontrolle aller am Vergabeverfahren beteiligten Bieter vor Vertragsabschluss ist kaum möglich und auch nicht sinnvoll. Insoweit haben die Aufsichtsbehörden, was den Zeitpunkt der Prüfung anbelangt, auf den Beginn der Auftragsverarbeitung abgestellt.

6.9 Das Muster der Aufsichtsbehörden der Sozialversicherungsträger zur Anzeige gem. § 80 SGB X sieht die Frage vor, ob die bzw. der Datenschutzbeauftragte beteiligt wurde (vgl. Muster, Ziffer 14). 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 Einschätzung der Aufsichtsbehörden 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.

7 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).

Literaturhinweise: DSK-Kurzpapier Nr. 1: „ Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DSGVO“; BfDI: Hinweise zum Verzeichnis von Verarbeitungstätigkeiten; BfDI: Muster zum Verarbeitungsverzeichnis Verantwortlicher; BfDI: Muster zum Verarbeitungsverzeichnis Auftragsverarbeiter

7.1 Stellen die Aufsichtsbehörden der Sozialversicherungsträger ein Muster für ein Verarbeitungsverzeichnis gemäß Artikel 30 DSGVO zur Verfügung?

Nein, die Aufsichtsbehörden der Sozialversicherungsträger stellen aktuell kein Muster für ein Verarbeitungsverzeichnis zur Verfügung. Zuständige datenschutzrechtliche Aufsichtsbehörde für die Auslegung der DSGVO ist die BfDI bzw. LfDI.

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

7.2 Wie umfangreich sollte das Verarbeitungsverzeichnis sein?

Was den Umfang des Verarbeitungsverzeichnisses anbelangt, wurde u. a. die Frage aufgeworfen, ob jedes einzelne Verfahren angegeben werden muss oder eine Unterteilung in Teilsysteme (z. B. Leistungsmanagement, Meldungen, Pflege, etc.) genügt.
Artikel 30 DSGVO schreibt das Führen eines Verarbeitungsverzeichnisses durch den Verantwortlichen vor. Dieses löst das bisherige Verfahrensverzeichnis ab.
Der Mindestinhalt des Verarbeitungsverzeichnisses ergibt sich aus Artikel 30 Absatz 1 lit. a) bis g). Das bedeutet, es muss die wesentlichen Angaben zur Verarbeitung beinhalten, wie z. B. die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Da-

ten, der betroffenen Personen und der Empfänger. Die BfDI-Homepage enthält Arbeitshilfen zu diesem Themenkomplex.

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.

Literaturhinweise: DSK-Kurzpapier Nr. 18: „Risiko für die Rechte und Freiheiten natürlicher Personen"; Infoblatt der BfDI „Meldung von Datenschutzverstößen"; Arbeitspapier der Artikel 29-Gruppe: WP250rev.01 („Leitlinien für die Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679")

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 die Aufsichtsbehörden als auch an die Datenschutzaufsichtsbehörden erfolgen. Ist eine doppelte Meldung notwendig?

Ja. Denn das Gesetz sieht ausdrücklich eine zweifache Meldung sowohl an die Aufsichtsbehörden der Sozialversicherungsträger des Bundes und der Länder als auch an die Datenschutzaufsichtsbehörden vor. Dabei beruht die Meldung an die Datenschutzaufsichtsbehörden auf der Regelung in Artikel 33 DSGVO, die Meldung an die Aufsichtsbehörden der Sozialversicherungsträger erfolgt aufgrund von § 83a SGB X.

8.3 Welche Maßnahmen hat der Verantwortliche durchzuführen, wenn zwar eine Datenschutzverletzung stattgefunden hat, aber keine Meldepflicht gegenüber den Aufsichtsbehörden besteht?

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." 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.

8.4 Wann liegt nach Auffassung der Aufsicht ein „Risiko für die Rechte und Freiheiten natürlicher Personen" vor (Definition)?

Eine genaue Definition fehlt in der DSGVO. Sie müsste durch die Datenschutzaufsichtsbehörden erfolgen und werden von diesen veröffentlicht. Hinweise ergeben sich aus dem DSK-Kurzpapier Nr. 18 „ Risiko für die Rechte und Freiheiten natürlicher Personen".

8.5 Was ist, wenn Auftragsverarbeiter eine Datenpanne –verspätet – melden? Liegt die Verantwortlichkeit bei dem Sozialversicherungsträger?

Artikel 33 Absatz 2 DSGVO verpflichtet den Auftragsverarbeiter dazu, den Verantwortlichen zu informieren, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird. Die Verletzung muss nicht aus seinem eigenen Verantwortungsbereich resultieren: Entscheidend ist nicht die Verantwortlichkeit für eine Verletzung, sondern deren Kenntnis (vgl. dazu auch Sassenberg in: Sydow, DSGVO, Artikel 33 Rn. 27). Indem Absatz 2 die (auch zwingend in dem Auftragsverhältnis vorzusehende) Pflicht (vgl. Artikel 28 Absatz 3 Buchstabe f)) als unmittelbare gesetzliche Pflicht des Auftragsverarbeiters festschreibt, ist diese aber selbständig sanktionierbar (vgl. Artikel 83 Absatz 4 Buchstabe a)).

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.

Literaturhinweise: DSK-Kurzpapier Nr. 5: „Datenschutz-Folgenabschätzung nach Art. 35 DSGVO"; BfDI: Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO; Artikel-29-Datenschutzgruppe: WP248Rev.01 („Leitlinien zur Datenschutzfolgenabschätzung und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt")

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 Geben die Aufsichtsbehörden 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 die Aufsichtsbehörden zum einen auf das von der Datenschutzkonferenz (DSK) herausgegebene Arbeitspapier Nr. 5 zur Datenschutz-Folgenabschätzung und auf das Working Paper der Artikel 29-Gruppe [„WP 248 rev.01"], das sich mit dem Thema Datenschutz-Folgenabschätzung befasst und am 04.10.2017 in überarbeiteter Version veröffentlicht wurde.

9.3 Ist die Datenschutz-Folgenabschätzung immer dann durchzuführen, wenn ein Risiko bestimmt wurde (was bei Gesundheitsdaten grundsätzlich gilt) oder nur, wenn neue Technologien eingeführt werden?

Aus der Formulierung in Artikel 35 Absatz 1 DSGVO (Wortwahl „…insbesondere bei Verwendung neuer Technologien“) ergibt sich, dass eine Datenschutz-Folgenabschätzung nicht nur bei der Einführung neuer Technologien durchzuführen ist, sondern immer, wenn ein Risiko besteht. Für die Beurteilung kann hilfreich sein, dass die Datenschutz-Folgenabschätzung häufig mit der bisherigen Vorabkontrolle des § 4d BDSG a.F. gleichgesetzt wird. Weitere Informationen können dem Kurzpapier Nr. 5 der DSK entnommen werden.

9.4 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 meint jedoch nicht die Aufsichtsbehörden der Sozialversicherungsträger, sondern die jeweiligen Datenschutzaufsichtsbehörden (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bzw. die jeweiligen Landesdatenschutzaufsichten). Seit dem 23. Mai 2018 wurde seitens der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eine solche Liste veröffentlicht. Sofern die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder eine gemeinsame Liste gemäß Artikel 35 Absatz 4 DSGVO beschließt, wird die bisherige Liste durch die gemeinsame Liste ersetzt.

9.5 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 meint jedoch nicht die Aufsichtsbehörden der Sozialversicherungsträger, sondern die jeweiligen Datenschutzaufsichtsbehörden (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bzw. die jeweilige Landesdatenschutzaufsicht). Ob und wann es eine solche Liste geben wird, ist den Aufsichtsbehörden der Sozialversicherungsträger nicht bekannt.

9.6 In welchen Fällen findet die Ausnahmeregelung des Artikels 35 Absatz 10 DSGVO Anwendung?

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.

9.7 Muss in einem laufenden Verfahren eine Datenschutzfolgenabschätzung gem. Artikel 35 DSGVO erfolgen bzw. muss geprüft werden, ob diese erforderlich ist und dann gegebenenfalls nachgeholt werden?

Ob in einem bestehenden Verfahren bzw. einem Datenverarbeitungsprozess ebenfalls eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO durchzuführen ist, ist grundsätzlich eine Frage des Einzelfalls. Allerdings führt die Artikel 29-Gruppe hierzu in ihrem Working-Paper „WP 248 rev.01“aus, dass ein Bestandsverfahren von der Datenschutzfolgenabschätzung ausgenommen ist, wenn

- es bereits eine Vorabkontrolle durch den Datenschutzbeauftragten gab und
- der Verarbeitungsvorgang immer noch auf dieselbe Art durchgeführt wird und
- sich das mit der Verarbeitung verbundene Risiko nicht verändert hat.

Solange diese Voraussetzungen vorliegen, bedarf es keiner Datenschutzfolgenabschätzung für Bestandsverfahren. Werden Änderungen am Verarbeitungsvorgang vorgenommen oder ändert sich das Risiko, ist eine Datenschutzfolgenabschätzung durchzuführen.

9.8 Was ist eine „wesentliche Änderung“, dass eine Datenschutzfolgenabschätzung wiederholt werden muss (Artikel 35 Absatz 11 DSGVO)?

Erforderlich ist eine Überprüfung dann, wenn das tatsächliche von dem kalkulierten Verarbeitungsrisiko abweicht. Nach dem Wortlaut der DSGVO genügt dabei jede „Änderung“ des Risikos im Sinne der Risikobewertung nach Artikel 35 Absatz 7 lit. c; diese muss nicht substanziell sein. Solche Änderungen können etwa durch technische Entwicklungen und neue Sicherheitsrisiken auftreten. Ein Fall des Absatzes 11 tritt jedenfalls immer dann ein, wenn sich die ursprüngliche Annahme als von vornherein fehlerhaft erweist oder wenn eine relevante Verände-

rung der tatsächlichen oder rechtlichen Umstände, insbesondere eine Änderung von Rechtsvorschriften oder eine Ausweitung des Verarbeitungsumfangs, eintritt (vgl. Paal/Pauly, Art. 35 Rn. 72/73).

10 Der bzw. die Datenschutzbeauftragte

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

Literaturhinweise: DSK-Kurzpapier Nr. 12: „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“

10.1 Ist die gem. Art. 37 Absatz 7 DSGVO zu erfolgende Mitteilung über den Datenschutzbeauftragten gegenüber den Aufsichtsbehörden der Sozialversicherungsträger zu machen?

Gemäß Art. 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 sind die zuständigen Aufsichtsbehörden der Sozialversicherungsträger. Daher hat die gemäß Art. 37 Absatz 7 DSGVO vorgeschriebene Meldung vorrangig an die Datenschutzaufsichtsbehörde zu erfolgen.

11 Besondere Arten von Daten

Literaturhinweise: DSK-Kurzpapier Nr. 17: „Besondere Kategorien personenbezogener Daten“

11.1 Betriebs- und Geschäftsgeheimnisse

§ 67 Absatz 2 Satz 1 SGB X definiert Sozialdaten als „personenbezogene Daten (Artikel 4 Nr. 1 DSGVO), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden“. Nach § 67 Absatz 2 Satz 2 SGB X sind Betriebs- und Geschäftsgeheimnisse alle betriebs- und geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben. Aus § 35 Absatz 4 SGB I ergibt sich eine Gleichstellung von Betriebs- und Geschäftsgeheimnissen mit Sozialdaten. Damit wird die bisherige Gleichstellung von Betriebs- und Geschäftsgeheimnissen mit Sozialdaten fortgesetzt, sodass sich grundsätzliche keine neue Bewertung für Betriebs- und Geschäftsgeheimnisse ergibt.

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 X auch auf Betriebs- und Geschäftsgeheimnisse Anwendungen finden.

Das bedeutet praktisch, dass auch gem. § 83 a SGB X Meldungen über Datenschutzverletzungen auch bei der Verletzung von Betriebs- und Geschäftsgeheimnissen erfolgen müssen. Dies hat aber ausschließlich gegenüber der Rechts- und Fachaufsichtsbehörde zu erfolgen. Auch sind gem. § 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 Perspnenn 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, Mit-

gliedstaaten 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.

12 Die Aufsichtsbehörden

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

Literaturhinweise: DSK-Kurzpapier Nr. 2: „Aufsichtsbefugnisse/ Sanktionen“

12.1 Welche Rolle spielen die Aufsichtsbehörden der Sozialversicherungsträger, 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 Art. 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. Dies erfolgt zur Gewährung rechtlichen Gehörs. Es soll die Gefahr divergierender Entscheidungen zwischen Rechts- und Fachaufsichtsbehörde reduzieren. Widersprüchliche Auffassungen der Aufsichtsbehörde und der Fachaufsicht sollen dem Gerichtsweg zugewiesen werden. Widerspricht die Verfügung der Datenschutzaufsichtsbehörde der Rechtsauffassung der Fachaufsichtsbehörde, soll diese den Verantwortlichen zur gerichtlichen Klärung anweisen (vgl. Wieczorek in: Kühling/ Buchner, DSGVO/ BDSG, 2. Aufl. 2018, § 16 BDSG Rn. 7).

Somit sind die Aufsichtsbehörden der Sozialversicherungsträger am Verfahren zu beteiligen, wenn die Datenschutzaufsichtsbehörde von ihren Befugnissen gem. Art. 58 Absatz 2 Buchstabe b bis g, i und j DSGVO Gebrauch macht und entsprechende Maßnahmen gegenüber den Sozialversicherungsträgern einleitet.