Oft gestellte Fragen

Frequently Asked Questions

Inhaltsübersicht

1 Anwendbarkeit des § 80 SGB X

1.1 Aus welchem Grund wird zwischen der Erbringung von Hilfsfunktionen und einer Funktionsübertragung unterschieden? – Wann liegt eine Auftragsdatenverarbeitung gem. § 80 SGB X vor?

Der Gesetzgeber hat grds. zwei Konstellationen vorgesehen, nach denen eine Datenverarbeitung durch Dritte erfolgen kann: die Auftragsdatenverarbeitung gem. § 80 SGB X sowie die sog. Funktionsübertragung. Wichtiges Unterscheidungsmerkmal aus datenschutzrechtlicher Sicht ist, dass es bei einer Funktionsübertragung zu einer Übermittlung von Daten gem. § 67 Abs. 6 SGB X kommt. Hierfür ist eine spezielle Rechtsgrundlage erforderlich (z. B. §§ 67d ff. SGB X bzw. Spezialnorm). Die Auftragsdatenverarbeitung gem. § 80 SGB X ist hingegen datenschutzrechtlich privilegiert. Bei dieser Konstellation kommt es zu keiner Übermittlung im Rechtssinn und es bedarf keiner speziellen Übermittlungsbefugnis.

Abgrenzungsmerkmal ist die Tragweite der Aufgabe. Werden durch den Auftragnehmer lediglich Hilfsfunktionen ohne eigene Entscheidungsbefugnis wahrgenommen, die den Auftraggeber bei seiner Aufgabenwahrnehmung unterstützen, kann § 80 SGB X zur Anwendung kommen. Übernimmt die beauftragte Stelle auch die gesetzliche Aufgabe des auftraggebenden Leistungsträgers, trifft er beispielsweise eigenständige Entscheidungen mit Außenwirkung, liegt keine Hilfsfunktion vor, was zur Folge hat, dass § 80 SGB X nicht anwendbar ist. Die Zulässigkeit einer Aufgabenübertragung ist dann nach den §§ 88 bzw. 97 in Verbindung mit einer gesetzlichen Ermächtigung zu beurteilen (vgl. hierzu auch Rombach in Hauck/Noftz: Sozialgesetzbuch X, § 80 SGB X, RdNr. 20; zur weiteren Abgrenzung der Auftragsdatenverarbeitung von der einer Datenübermittlung bedingenden Funktionsübertragung siehe auch Gola/Schomerus: Bundesdatenschutzgesetz, Kommentar zu § 11, RdNrn. 9 ff.).

2 Leitfaden zur Auslegung der gesetzlichen Anforderungen

2.1 Gibt es seitens der Aufsicht einen Leitfaden oder Kriterienkataloge, die eine Auslegung der allgemein formulierten Anforderungen des § 80 Abs. 2 SGB X unterstützen?

Nein. Die Anforderungen sind relativ allgemein gehalten, damit diese im Einzelfall nach Sinn und Zweck des Datenschutzes ausgelegt werden können. Die Ausgestaltung des Verfahrens kann in der Praxis vielfach nur im Einzelfall abgewogen werden und fällt somit in den Bereich der Selbstverwaltungsautonomie.

3 Ausgestaltung der Prüferfordernis gem. § 80 Abs. 2 Satz 4 SGB X

3.1 Wie können Synergien genutzt werden, wenn insbesondere mehrere Kassen einen Dienstleister beauftragen?

Es spricht nichts dagegen, dass eine Gemeinschaft von Auftraggebern gemeinsame Prüfungen durchführen oder diese an eine unabhängige Stelle vergeben. Im Ergebnis muss der Anforderung im § 80 Abs. 2 Satz 4 SGB X Rechnung getragen werden: Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Darüber hinaus ist das Ergebnis auch zu dokumentieren. Ob eine Überzeugung durch die Anerkennung von Prüfergebnissen Dritter erreicht werden kann, muss der Auftraggeber, der schließlich auch die Verantwortung für die Auftragdatenverarbeitung trägt, selbst entscheiden. Der Gesetzgeber hat dies offen gelassen.

3.2 Welche Art von Prüfung ist erforderlich? Ist z. B. eine Vor-Ort-Prüfung vorgeschrieben oder kann die Prüfung auch dokumentenbasiert erfolgen?

Bezogen auf die Prüfverpflichtung gem. § 80 Abs. 2 Satz 4 SGB X lässt der Gesetzgeber offen, inwieweit die Prüfung vor Ort oder auch auf Basis von Dokumenten, Fragebögen, Zertifikate bzw. Prüfergebnisse Dritter erfolgen kann. Grundsätzlich halten wir beide Prüfformen für vertretbar, in der Praxis wird sich wohl eine Kombination aus beiden als verhältnismäßig herausstellen. Im Ergebnis muss sich die Kasse in geeigneter Weise überzeugt haben, dass die getroffenen technischen und organisatorischen Maßnahmen eingehalten werden.

3.3 In welchen Zeitintervallen hat die regelmäßige Überprüfung zu erfolgen?

§ 80 Abs. 2 Satz 4 SGB X enthält zwei allgemeine Vorgaben zur zeitlichen Dimension: vor Beginn der Datenverarbeitung und sodann regelmäßig. Die erste Vorgabe ist deutlich und dürfte zu keinen Interpretationsschwierigkeiten führen. Was die Regelmäßigkeit anbelangt, ist die Erforderlichkeit wiederum nach dem Einzelfall zu bestimmen. Hierzu sollten von der Kasse Bewertungskriterien erarbeitet werden, die eine nachvollziehbare Risikoabwägung ermöglicht (z. B. Schutzbedarf der Daten, zeitliche Bindung, Bedeutung für die Infrastruktur).

3.4 Wer muss die Prüfung durchführen? Ist eine eigenständige Prüfung durch den Datenschutzbeauftragten erforderlich?

Eine eigenständige Prüfung durch den Datenschutzbeauftragten ist im § 80 Abs. 2 SGB X nicht explizit vorgesehen. Vielmehr wird allgemein auf den Auftraggeber abgestellt. Wir vertreten aber die Auffassung, dass der Datenschutzbeauftragte des Auftraggebers die geeignete Stelle für eine abschließende Zulässigkeitsprüfung ist, in der die Ergebnisse der Einzelprüfungen zu

den vielfältigen Anforderungen des § 80 SGB X im Gesamtzusammenhang beurteilt werden, bevor eine Anzeige dem Bundesversicherungsamt vorgelegt wird. Dies bedeutet aber nicht, dass der Datenschutzbeauftragte auch alle Prüfungen eigenständig durchführen muss, was insbesondere hinsichtlich der technischen und organisatorischen Maßnahmen nach § 78a SGB X praktisch regelmäßig nicht der Fall sein wird.

Vor diesem Hintergrund ist unsere Anmerkung in der E-Mail vom 24. August 2010 an alle Sozialversicherungsträger (vgl. Anlage 1) zu verstehen. Zur zeitnahen Bearbeitung der Anzeigen gem. § 80 Abs. 3 SGB X halten wir es daher für sachdienlich, wenn die Durchführung der Schlussprüfung im o. a. Sinne auch zum Ausdruck kommt. Im Übrigen obliegt es dem Datenschutzbeauftragten, die Einhaltung der datenschutzrechtlichen Vorschriften im Unternehmen bzw. in der Behörde sicherzustellen (§ 4g BDSG). Das bedeutet auch, dass er bei der Auswahl eines Auftragnehmers, der Daten im Auftrag verarbeiten soll, regelmäßig zu beteiligen ist. Er sollte zudem über eine Aufstellung der verschiedenen Auftragsdatenverarbeitungsverträge verfügen (vgl. Gola/Schomerus, Kommentar zum BDSG, 8. Auflage 2005, § 11, Rn. 22).

3.5 Inwieweit muss der Auftraggeber insbesondere die Vorgaben zu § 78 a SGB X gegenüber seinem Auftragnehmer konkretisierte (und prüfen)?

In der Anlage zu § 78 a SGB X werden Maßnahmenbereiche oder auch allgemeiner gesprochen Maßnahmenziele aufgelistet. Wie diese Ziele zu erreichen sind, wird aufgrund der Vielzahl von möglichen technischen und organisatorischen Maßnahmen verständlicherweise nicht spezifiziert. Insofern würde im Rahmen einer etwaigen Aufsichtsprüfung mindestens geprüft, ob diese Maßnahmenziele in geeigneter Weise spezifiziert sind, um bezogen auf den erforderlichen Schutzbedarf entsprechende Maßnahmen einzuleiten. Diese Angaben (einschließlich Schutzbedarf) sind vom Auftraggeber zu machen, nicht zuletzt um auch deren Einhaltung prüfen zu können.

Beispielsweise könnte das Schutzziel "Zutrittskontrolle" in der Form konkretisiert werden, dass die Räume, in denen Rechensysteme aufgestellt sind, permanent verschlossen gehalten werden müssen. Ob dies nun durch ein ausgeklügeltes Schlüsselmanagement, durch kartenbasierte Öffnungssysteme oder sogar durch einen Wachdienst etc. bewerkstelligt wird, dürfte dem Auftraggeber zunächst egal sein, soweit das Sicherungssystem funktioniert. Von deren Schutzfunktion kann sich der Auftraggeber dann im Rahmen einer Vor-Ort-Prüfung überzeugen.

Diese Differenzierung ist aus unserer Sicht in der Praxis nicht unbedeutend, da ein Auftragnehmer regelmäßig mehrere und unterschiedliche Auftraggeber haben wird. Insofern wird der Auftragnehmer in der Regel Sicherheitsmaßnahmen einrichten, die ein breites Spektrum von Schutzanforderungen abdecken. Es wäre wohl in den meisten Fällen wenig aussichtsreich, eigene konkrete Maßnahmen durchzusetzen, deren Ziele auch auf anderem Wege erreichbar sind. Dies würde sich zumindest in der Kalkulation des Auftragnehmers niederschlagen, was dann wiederum Fragen der Wirtschaftlichkeit aufwirft.

4 Haftungsbeschränkungen im Kontext der Auftragsdatenverarbeitung

4.1 Wie ist die Aufsicht generell gegenüber Haftungsbeschränkungen in den Verträgen zur Auftragsdatenverarbeitung eingestellt?

Grds. ist aus unserer Sicht die Selbstverwaltungsautonomie zu beachten, zu der auch die Vertragsgestaltung zählt (Grundsatz der Vertragsfreiheit). Wir würden aber im Einzelfall Verträge bemängeln, die erkennbar zulasten der Kasse gehen, wie z. B. bei einem Haftungsausschluss.

Unser Referat I 1 hat in einem Rundschreiben an alle bundesunmittelbaren Krankenkassen vom 05.04.2007 darauf hingewiesen, dass ein Ausschluss von Schadensersatzforderungen im Zusammenhang mit Datenlieferungen (RSA) gegen § 69 Abs. 2 SGB IV verstößt.

Wir erkennen aber an, dass sich die Kasse Dienstleitungen am freien Markt beschaffen muss und insoweit fiskalisch auftritt. D. h., dass auch die wirtschaftlichen Interessen abzuwägen sind. Es ist also im Einzelfall zu prüfen, wie hoch das Risikopotenzial eingeschätzt wird und wie hoch der kalkulierte Aufschlag für eine volle Haftung ist. Im Ergebnis darf keine Schlechtstellung der Kasse vorliegen.

5 Rechtzeitigkeit der Anzeige gem. § 80 Abs. 3 SGB X

5.1 Was konkret stellt sich die Aufsicht unter einer rechtzeitigen Anzeige vor?

Vor dem Hintergrund der erweiterten Bußgeldtatbestände weisen wir auf die Bedeutung einer rechtszeitigen Anzeige hin. Welcher Zeitraum hier als angemessen angesehen werden kann, ist auch nur im Einzelfall durch die Auftraggeber abzuschätzen. Grundsätzlich stellen wir sicher, dass eingehende Anzeigen gem. § 80 Abs. 3 SGB X am Tag des Eingangs gesichtet und dann zeitnah bearbeitet werden. Dies hängt aber im Wesentlichen auch davon ab, ob die Unterlagen vollständig sind oder in problematischen Fällen die Fachabteilungen eingeschaltet werden müssen.

6 Übergangsvorschriften

6.1 Wie soll mit Verträgen umgegangen werden, die vor dem 11.08.2010 geschlossen wurden?

Der Gesetzgeber hat keine Übergangsregelungen getroffen. Insofern gelten die neuen verschärften Anforderungen für alle Verträge, die nach dem 11.08.2010 geschlossen worden sind. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) vertritt zudem die Auffassung, dass die neuen inhaltlichen Anforderungen auch gelten, wenn sich der neue Vertrag auf einen bereits vorher geschlossenen Rahmenvertrag bezieht. Letztlich gehen wir davon aus, dass Altverträge bei jeder inhaltlichen Änderung oder anstehenden Verlängerung dem neuen Recht angepasst werden müssen.