

**Lernbrief**

# **Datenschutz und Datensicherheit**

**C**

**Prozess-  
übergreifende  
Themen**

Prozesshandbuch, Stand: August 2025

Herausgeber:

AOK-Bundesverband, Rosenthaler Straße 31, 10178 Berlin

Redaktion: Referat Berufliche Bildung

Ansprechpartnerin: Anja Michelchen, Tel.: 030 34646-2175

Druck und Vertrieb durch

Bonndruck GmbH, Frankfurter Straße 51, 57074 Siegen.

Vervielfältigung der Materialien oder einzelner Beiträge daraus  
(auf fotomechanischem oder sonstigem Wege) ist nur mit vorheriger  
Genehmigung des Herausgebers gestattet.

# Gliederung

<b>1 Einleitung</b>	<b>3</b>
<b>2 Lernziele</b>	<b>4</b>
<b>3 Informations- und Datenverarbeitungsabläufe in der GKV</b>	<b>5</b>
3.1 Entwicklung und aktueller Stand	5
3.2 Wahrung der Vertraulichkeit am Arbeitsplatz	6
3.3 Auswirkungen des Einsatzes von Informationstechnologien am Arbeitsplatz	8
3.4 Rechtmäßigkeit der Datenverarbeitung	9
3.5 (Weiter-)Entwicklung und Forschung für die Krankenversicherung	9
3.6 Informations- und Kommunikationstechniken im betrieblichen Ablauf	10
3.7 Kurzer Einblick in die Informationssicherheit	11
3.8 Übungen zum Lernabschnitt 3	13
<b>4 Datenschutz</b>	<b>14</b>
4.1 Allgemeines	14
4.2 Gesetzliche Grundlagen	14
4.3 Sozialdatenschutz	15
4.3.1 Rechtsquellen	15
4.3.2 Sozialdaten	15
4.3.3 Sozialgeheimnis	16
4.4 Begriffsdefinitionen	17
4.5 Verarbeitung von Sozialdaten	19
4.5.1 Zulässigkeit von Datenverarbeitung und -nutzung	19
4.5.2 Sozialdaten bei den Kranken- und Pflegekassen	20
4.5.3 Datenübermittlung	23
4.5.3.1 Einschränkung der Übermittlungsbefugnis bei besonders schutzwürdigen Sozialdaten	26
4.5.3.2 Gewährleistungsziele der Datenschutzgrund- verordnung (DSGVO)	27
4.5.3.3 Technische und organisatorische Maßnahmen (TOM) zur Datensicherheit	27
4.5.4 Betroffenenrecht	30
4.5.5 Umgang mit Datenschutzverstößen	30

4.6 Gewährleistungsziele des Datenschutzes	31
4.7 Innerbetriebliche Datenschutzorganisation	32
4.8 Risikoanalyse aus der Perspektive Datenschutz	33
4.9 Social Media und Datenschutz	36
4.10 Übungen zum Lernabschnitt 4	37
<b>5 Zusammenfassende Selbstkontrolle</b>	<b>38</b>
<b>6 Lösungen zu den Übungen im Text</b>	<b>46</b>
<b>7 Lösungen zur zusammenfassenden Selbstkontrolle</b>	<b>49</b>

# 1 Einleitung

In der digitalen Welt sind Datenschutz und Datensicherheit essenzielle Themen, die jeden betreffen – von Privatpersonen über Unternehmen bis hin zu staatlichen Institutionen.

Während der Datenschutz sich mit der Frage beschäftigt, welche personenbezogenen Daten erhoben, gespeichert und weitergegeben werden dürfen (Datenverarbeitung), geht es bei der Datensicherheit um technische und organisatorische Maßnahmen zum Schutz dieser Daten vor unbefugtem Zugriff, Verlust oder Manipulation im Zuge der Datenverarbeitung.

Angeichts zunehmender Cyberangriffe, Datenlecks und der wachsenden Bedeutung von Künstlicher Intelligenz ist der Schutz personenbezogener Daten und insbesondere sensibler Daten (z.B. Gesundheitsdaten) wichtiger denn je.

Ein bewusster Umgang und die Einhaltung datenschutzrechtlicher Vorschriften (DSGVO, BDSG, SGB X) sind daher unerlässlich, um Vertrauen und Sicherheit in die Geschäftsprozesse der Krankenversicherung zu gewährleisten.

Das Ziel des Lernbriefs ist es, das grundlegende Wissen zum Thema Datenschutz und Datensicherheit zu vermitteln und Sensibilität im Umgang mit personenbezogenen Daten zu schaffen.

Darüber hinaus soll ein gutes Verständnis im Umgang mit Betroffenenrechten, bei der Verarbeitung von personenbezogenen Daten im Auftrag sowie bei Verstößen gegen die gesetzlichen Vorgaben zum Datenschutz erlangt werden.

## 2 Lernziele

Der Lernbrief soll Sie in der Entwicklung folgender Kompetenzen unterstützen:

- umfangreiche Kenntnisse zu den datenschutzrechtlichen Vorschriften
- ausgeprägtes Verständnis zur Wahrung der Vertraulichkeit
- Sensibilisierung im Umgang mit Betroffenenrechten und Verstößen gegen die gesetzlichen Vorschriften
- Umsetzung der Rechenschaftspflichten (u.a. Datenschutzfolgenabschätzungen, Verarbeitungsverzeichnis, Datenschutzkonzept)
- Verständnis zur Datenschutzorganisation
- Anwendung betrieblicher Regelungen zum Datenschutz
- richtiger Umgang mit externen Diensten und Dienstleistern
- Abgrenzung Datenschutz und Informationssicherheit
- allgemeine Vorschriften zum Sozialdatenschutz kennen und beachten
- Wahrung des Sozialgeheimnisses bei der Kommunikation über digitale Kanäle (u.a. Versicherten, Leistungserbringern, Firmenkunden)

### Hinweis

Haben Sie Tipps, Anregungen oder Verbesserungsvorschläge zu den Inhalten des Lernbriefs? Dann zögern Sie nicht, uns anzusprechen.

## 3 Informations- und Datenverarbeitungsabläufe in der GKV

### 3.1 Entwicklung und aktueller Stand

Bis in die 70er Jahre mussten alle Vorgänge bei der Krankenkasse „von Hand“ erledigt werden. Die Mitarbeitenden in der Sachbearbeitung und Kundenberatung führten den Versicherungsverlauf und die Leistungsdaten unserer Kundschaft auf Karteikarten.

Ab diesem Zeitpunkt liefen die ersten Bestrebungen, die Möglichkeiten der EDV auch zur Arbeitsentlastung der Mitarbeitenden zu nutzen. Die EDV konnte Mitgliedschaftszeiten speichern und wiederkehrende Berechnungen, z.B. im Arbeitsunfähigkeitsfall, durchführen.

Ausdrucke der verarbeiteten Daten wurden ausschließlich im Rechenzentrum selbst erzeugt und per Post an die Geschäftsstellen weitergeleitet. Als Verarbeitungsprogramm hatte sich dann im Laufe der Jahre das IDVS II (Informations- und Datenverarbeitungssystem Stufe II) im AOK-Bereich durchgesetzt. Das IDVS II wurde immer wieder verbessert, an die jeweiligen Gesetzesänderungen angepasst und blieb bis Mitte der 90er Jahre das alleinige Datenverarbeitungssystem. Parallel wurden ab den 80er Jahren erste Textverarbeitungssysteme eingesetzt, die das Erstellen von Briefen erleichtern sollten.

Nach einiger Zeit zeigte sich jedoch, dass nicht jede AOK ihr eigenes EDV-System wirtschaftlich betreiben konnte. So konzentrierte sich im Laufe der Zeit die EDV-Produktion auf immer weniger, aber immer größere Rechenzentren. Außerdem fusionierten die bis dahin selbstständigen AOKs zu größeren Gebilden, den elf Landes-AOKs.

Durch die neuen Anforderungen wurde auch die Kommunikation zum AOK-Bundesverband und zwischen den AOKs immer notwendiger und es wurde ein AOK-weites Netzwerk geschaffen.

Mitglieds- und Leistungskarte		Nr.	Mitgl. Nr.	Vers.Nr.	Beschäftigungsverhältnis		Austritt		AG Kto. Nr.	
Eintritt	Nr. der Anmeldung				Arbeitsgeber	A + B Schlüssel Beschäftigungsverhältnis	Austritt	Nr. der Abmeldung		
5.11.74	45483	AOK				66	22.80	10.5.75	63882	061.175240
12.5.75	21.5.75	AOK				60	64.86	10.5.75	8.6.	
11.5.75	66161	AOK				44	24.80	10.4.75	72584	K-Ad.
31.4.75	11.8.75	8331				9	8.75	11.8.75		
11.8.75	46078	AOK				46	24.80	9.4.75	77715	
10.9.75	86446	AOK				46	27.80	7.4.75	88852	
11.8.76	91032	M.B.				204	27.1	19.7.15	215028	8
10.12.75	48168	AOK				46	11.80	1.1.76	96104	
15.08.77	21111	Deu				355	11.1	22.3.73	19473	21583.026
26.4.79	3.05.79	Y11				48	53.10	3.05.83	25523	44 (sonstige)
10.3.80	22.4.80	AOK				48	34.20	2.10.80	141080	44
17.11.80	31.12.80	AOK				48	31.40	10.2.81	172.81	43
23.10.80	28.2.81	AOK				48	31.40	15.11.80	182.81	44

Ruhegeld/BR/ER/Witwen R.		Ersatzanspruch LVA - BIA angem. am		Ehefrau S. Karte II geb.	
Weisen R.		Fall Nr.:		Kinder	
Beantragt:				1.	
Rentenbeginn:				2.	
AV Rentenzeichen IV				3.	
				4.	
				5.	
				6.	
				7.	
				8.	
				9.	

Rentenleiden / Leistungsausschluss nach § 310/2 RVO	

In den Geschäftsstellen sind heutzutage alle Arbeitsplätze über ein LAN (Local-Area-Network) verbunden. Auf dem Server wird Speicherplatz für alle Daten bereitgestellt. Hier erfolgt auch eine regelmäßige Datensicherung. Die Daten werden gespeichert, damit bei Defekten die Informationen wiederhergestellt werden können.

Weiterhin wurde für die Entwicklung von Programmen eine eigene Gesellschaft, die AOK-Systems GmbH, gegründet.

Hieraus hat sich eine Entwicklungspartnerschaft zwischen der AOK-Systems und der Firma SAP entwickelt. Das Hauptanwendungsprogramm im AOK-Bereich ist oscar®. Das betrifft die komplette integrative Verarbeitung aller Aufgaben der Krankenversicherung, die Mitgliederbestandsführung, wie auch die Leistungsgewährung. Eine tiefergehende Betrachtung ist in diesem Lernbrief nicht möglich. Der Umgang mit dieser Software wird innerhalb der fachlichen Ausbildung direkt am Arbeitsplatz erlernt. Zur Information ihrer Mitarbeitenden stellt jede AOK ein eigenes Intranetangebot zur Verfügung. Dieses beruht technisch auf der gleichen Basis wie das Internet, stellt aber speziell auf die eigenen Bedürfnisse angepasste Informationen bereit.

Hier finden Sie in elektronischer Form z.B.:

- relevante Gesetzestexte
- Dienstanweisungen
- Dienstvereinbarungen
- Beschreibungen von Arbeitsabläufen
- interne Telefonverzeichnisse
- Stellenausschreibungen
- aktuelle, dienstlich erforderliche Informationen

In der Regel wird über dieses Medium auch ein Zugriff ins Internet ermöglicht, wobei die Zugriffsrechte in den einzelnen AOKs unterschiedlich gehandhabt werden. Zu Schutzzwecken werden in der Service-Area automatisiert sexuelle, rassistische Inhalte sowie Aufrufe zur Gewalt ausgefiltert. Die Nutzung erfolgt generell zu dienstlichen Zwecken. Einzelheiten sind für jede AOK in Internetdienstanweisungen oder -vereinbarungen verbindlich geregelt.

### 3.2 Wahrung der Vertraulichkeit am Arbeitsplatz

In der Regel steht für jeden Mitarbeitenden ein PC am Arbeitsplatz zur Verfügung. Für das Verständnis zum Umgang mit der EDV sind hierzu noch weitere Grundlagen erforderlich.

#### Benutzeranmeldung

Die aktuellen EDV-Systeme der AOK sind gegen unbefugte Benutzung geschützt. Das bedeutet, eine Nutzung ist nur dann möglich, wenn Sie dazu befugt sind. Hierzu erhalten Sie durch die EDV-Benutzerverwaltung eine sogenannte Benutzer-ID (engl. User-ID). Diese wird in jeder AOK nach eigenen Regeln vergeben. Sie kann sich aus der Personalnummer oder aus Teilen Ihres Namens oder Ihrer Funktion in der AOK zusammensetzen.

Für den oscar®-Einsatz werden bundesweit einheitliche und somit eindeutige siebenstellige Benutzer-ID in Form von zwei Buchstaben und fünf Ziffern (z.B. XI88888) verwendet. Dabei ist aus der ersten Stelle die AOK erkennbar, die zweite Stelle steht für I = intern „eigener Mitarbeiter“ oder E = extern, z.B. Servicemitarbeiter



einer Wartungsfirma. Die fünf Ziffern werden frei durch die oscar®-Benutzerverwaltung erzeugt.

Damit andere Mitarbeitende Ihre Benutzer-ID nicht nutzen können, ist diese geschützt. Im AOK-Bereich geschieht das noch zu fast 100 % mittels eines persönlichen Passworts, das nur Ihnen bekannt sein darf. Die gesamte Sicherheit beruht darauf, dass keine andere Person Ihr Passwort kennt. Daher sollten hier einige Grundregeln im Umgang mit dem Passwort beachtet werden:

- Wechseln Sie direkt nach der erstmaligen Anmeldung an einem EDV-System oder Programm Ihr Passwort (wird in der Regel automatisch veranlasst).
- Verwenden Sie keine Trivialpasswörter (z.B. AOK, Sommer, Montag, September) oder Bezüge zu Ihrem Namen oder Ihren Familienangehörigen.
- Nutzen Sie die maximale Passwortlänge, die Ihr EDV-System zulässt, zwölf Zeichen sollten Minimum sein. Relativ sicher ist eine Kombination aus Zahlen und Buchstaben. Dazu zählen: Großbuchstaben (A bis Z), Kleinbuchstaben (a bis z), Zahlen (0 bis 9) und nicht alphabetische Zeichen/Sonderzeichen (z. B.: !, \$, %, #). (vgl. Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu sicheren Passwörtern.)
- Eine sichere Alternative ist, sich eine „Eselsbrücke“ zu bauen und einen einstudierten, zeichenweise veränderten Satz wie z. B.: „lejT-2Bu1A!“ zu verwenden. Dieser wird gebildet aus den fett hervorgehobenen Zeichen von: „Ich esse jeden Tag - **2** Bananen und **1** Apfel!“
- Schreiben Sie Ihr Passwort nirgendwo auf (unter der Tastatur oder am Bildschirm schaut jeder nach).

- Geben Sie Ihr Passwort nicht an Kolleginnen oder Kollegen, Teammitgliedern oder Führungskräften weiter (auch die EDV benötigt diese Kenntnis nicht, um Ihnen im Fehlerfall helfen zu können).
- Sollten Sie den Verdacht haben, dass jemand Kenntnis von Ihrem Passwort hat, wechseln Sie sofort das Passwort. Die konkreten Regelungen zum Passwortgebrauch (z. B. über die Passwortrichtlinie) können in ihrem Haus eingesehen werden.

Zur sicheren Verwaltung von Accountdaten können sogenannte Passwortmanager-Software wie z. B. „KeePass 2“ verwendet werden. Diese ist bereits von der AOK vorinstalliert.

Wenn Sie Ihre User-ID und Passwort eingegeben haben, wird es automatisch durch das Betriebssystem geprüft und Sie erhalten Zugriffsmöglichkeiten auf Ihre EDV. In der Regel ist das System so eingestellt, dass Ihre User-ID nach dreimaligem Fehler bei der Passworteingabe gesperrt wird und erst durch EDV-Mitarbeitende wieder freigeschaltet werden kann.

Durch die Benutzerverwaltung wird bei der Ersteinrichtung Ihrer User-ID auch eingestellt, welche Ressourcen/Programme der EDV Sie benutzen dürfen. Das geschieht grundsätzlich analog zur Organisation Ihrer AOK.

### Merke

Schützen Sie Ihre Passwörter!  
Eine Weitergabe an Dritte darf unter keinen Umständen erfolgen.

### 3.3 Auswirkungen des Einsatzes von Informationstechnologien am Arbeitsplatz

Die IT-Lösung oscar® bietet aktuell u.a. folgende Unterstützung:

- Abrechnungen mit Leistungserbringern:

Hier ist ein elektronischer Datenaustausch möglich. Abrechnungen können per Datenträger oder auch per Internet angeliefert und direkt ins oscar® eingespielt werden.

- Geldtransfer läuft bargeldlos:

Zahlungen der AOK werden im oscar®- System gebucht und elektronisch an die Banken übermittelt.

- Zahlungseingänge werden automatisch offenen Forderungen zugeordnet und in oscar® verarbeitet.
- Fallmanagementprogramme unterstützen die Sachbearbeiterinnen und Sachbearbeiter durch automatische Plausibilitätsprüfungen und dem Führen einer elektronischen Wieder-vorlage.
- Rechnungsprüfprogramme prüfen automatisch Abrechnungen auf ihre Richtigkeit.
- Durch E-Mail-Systeme können schnell Fragen und Abstimmungen zwischen Kolleginnen und Kollegen erfolgen.
- Austausch mit Versicherten über das Postfach der Online-Geschäftsstelle (OGS)/ Meine AOK als E-Mail-System nach außen.
- In Textverarbeitungssystemen sind Musterbriefe für viele Standardsachverhalte vorhanden, die automatisch Versichertendaten (z.B. Adressen) aus oscar® in Briefe übertragen.

Das bedeutet, dass Mitarbeitende durch die EDV immer mehr von Regelarbeiten entlastet werden. Es bleibt mehr Zeit zur Bearbeitung von Sonderfällen und zur Kundenbetreuung. Hierdurch ändern sich aber auch die Anforderungen an die Qualität der Mitarbeitenden. Es werden gegenüber früher für die Betreuung der gleichen Anzahl von Versicherten weniger, aber dafür umfassend qualifizierte Mitarbeitende benötigt.

- Kundinnen und Kunden können Adressänderungen per Internet direkt erfassen.

Schriftliche Verwaltungsakte können auch elektronisch erlassen werden. Hier müssen jedoch bei den Sozialversicherungsträgern weitere Vorkehrungen zur elektronischen Signatur sowie zur ordnungsgemäßen Identifizierung und Authentifizierung des Versicherten getroffen werden.

§ 33 Abs. 2  
SGB X

Das E-Mail-System stellt grundsätzlich eine offene Übermittlung dar, sodass der Inhalt von E-Mails auf dem Übertragungsweg problemlos mitgelesen und manipuliert werden kann. E-Mail-Adressen sind nicht eindeutig bestimmten Personen zugeordnet. Die Risiken zur unbefugten Offenlegung oder der Manipulation der Korrespondenz kann durch geeignete technische Maßnahmen begegnet werden, um das Risiko zu minimieren. Nichtsdestotrotz ist die Übersendung von Sozialdaten per E-Mail risikobehaftet, sodass nur auf die bestehenden sicheren Kommunikationswege zurückgegriffen werden soll (z.B. Online-Geschäftsstelle und Telefon nach erfolgter Authentifizierung).

**Merke**

Nicht alles, was in der EDV technisch möglich ist, ist in der AOK auch erlaubt.

### 3.4 Rechtmäßigkeit der Datenverarbeitung

Die AOK benötigt von ihren Kunden und Vertragspartnern Daten, um die gesetzlichen Aufgaben nach dem SGB bewältigen zu können (vgl. § 284 Abs. 1 SGB V).

Die Grundsätze der Datenverwendung bei den Pflegekassen ergeben sich aus den §§ 93, 94 SGB XI.

Um die Zugangsmöglichkeiten zu erläutern, ist die Einteilung in zwei Bereiche sinnvoll:

- regelmäßiger Datenaustausch
- anlassbezogener Datenaustausch (Einzelfälle)

Der regelmäßige Datenaustausch erfolgt bereits maschinell. Hier werden die per E-Mail oder Dateitransfer gelieferten Daten von Arbeitgebern, anderen Sozialleistungsträgern oder Geschäftspartnern direkt in oscore® eingespielt. So können die Ergebnisse am Bildschirm oder per Fehler- oder Hinweisliste kontrolliert werden. Sie haben hier kaum Beeinflussungsmöglichkeiten.

Die Einzelfälle (anlassbezogener Datenaustausch) treffen auf Ihre Arbeit eher zu. Auch hier sind wieder zwei Varianten zu nennen. In der Regel gibt es in Ihrer AOK Musterbriefe und Anfragen für die meisten Sachverhalte. Wenn Sie diese verwenden, sind Sie auf der sicheren Seite. Durch diese Muster können aber nicht alle Fälle abgedeckt werden. Im übrigen Bereich sind Sie auf die eigene Kreativität angewiesen. Hier müssen Sie auch die rechtlichen Rahmenbedingungen prüfen, d.h., ob, wen und wie Sie fragen dürfen. Diese gesetzlichen Rahmenbedingungen werden im Kapitel Datenschutz gezielt erklärt (vgl. Punkt 4 dieses Lernbriefs).

**Merke**

Wenn Sie mit jemandem elektronisch bzw. telefonisch kommunizieren, sollten Sie sich sicher sein, wer Ihr Gegenüber tatsächlich ist (Nutzung Authentifizierungstool).

§ 217f Nr. 4b SGB V

### 3.5 (Weiter-)Entwicklung und Forschung für die Krankenversicherung

Um die AOK steuern zu können, muss der Vorstand immer aktuelle Informationen über den Stand des Unternehmens haben. Er muss wissen, wo es reibungslos läuft und viel wichtiger, er muss frühzeitig erfahren, wo Probleme auftauchen, um rechtzeitig gegensteuern zu können.

Aber auch für die alltägliche Sachbearbeitung ist es für die Mitarbeitenden wichtig zu wissen, ob

- die Betreuung der Kundschaft problemlos läuft,
- eventuell Kundinnen und Kunden zu anderen Krankenkassen wechseln wollen,
- überdurchschnittlich viele Arbeitsunfähigkeitszeiten vorliegen,
- immer der günstigste Anbieter für Hilfsmittellieferungen den Zuschlag erhält, usw.

Um hier zu unterstützen, müssen die vorhandenen Daten bestmöglich aufbereitet und ausgewertet werden.

In einem standardisierten Berichtswesen, dessen Einzelheiten jede AOK für sich festlegt, ist festgeschrieben, welche Auswertungen in welchem Zeitraum an wen geliefert werden.

Hierzu gehören u.a. Auswertungen über:

- die Mitgliederstruktur (gibt es regionale Auffälligkeiten, z.B. höhere Mitgliederverluste, andere Altersstruktur, etc.)
- die Leistungsstruktur (gibt es regionale Auffälligkeiten, z.B. längere Arbeitsunfähigkeitszeiten, längere Krankenhausaufenthalte, sind bestimmte Abteilungen von Krankenhäusern auffällig)
- die durchschnittlichen Kosten für Hilfsmittelbeschaffung (um Preisvergleiche anstellen zu können)
- die finanzielle Situation (gibt es Kostensteigerungen in bestimmten Bereichen gegenüber dem gleichen Vorjahreszeitraum und ist zu erwarten, dass die Haushaltsplanung eingehalten wird)

Seit der oscar®-Auslieferung steht für Auswertungen zusätzlich das SAP-Businesswarehouse zur Verfügung. Dieses beinhaltet eine Kopie der notwendigen Daten aus produktiven EDV-Systemen mit bereits vorkonfigurierten Abfragemöglichkeiten und ermöglicht es allen Beteiligten, vom Vorstand bis zum Sachbearbeiter, direkt online auf die für ihn relevanten Auswertungen und Analysen zuzugreifen. Durch ein Rollen- und Berechtigungskonzept wird sichergestellt, dass jeweils nur die benötigten Daten angezeigt werden sowie der Mitarbeiterdatenschutz auch dort eingehalten wird.

Wenn im Vertriebsbereich die in der AOK vorhandenen Datenbestände nicht ausreichend sind, um Prognosen treffen zu können, wird hier die Datengrundlage durch Kundenbefragungen ergänzt. Hiermit werden teilweise auch externe Unternehmen beauftragt.

#### **Merke**

Ohne aktuelle, aussagekräftige Auswertungen kann die AOK nicht geführt werden. Dazu zählen Auswertungen zur Mitglieder- und Leistungsstruktur.

### **3.6 Informations- und Kommunikationstechniken im betrieblichen Ablauf**

Wichtig ist, dass Sie nur dann optimal arbeiten können, wenn Sie die AOK-Anwendungen nicht nur bedienen können, sondern auch den vorhandenen Leistungsumfang kennen. Bei oscar® gibt es aufgrund der hohen Funktionalität und des Gesamtumfangs sehr viele Eingabemöglichkeiten.

### Beispiel

Bei der Abarbeitung eines Krankenhausfalls wird ein bestimmter Verarbeitungsgrund gesetzt, um eine Fehler- oder Hinweisliste zu vermeiden.

### Folge

Dadurch werden interne Plausibilitätsprüfungen der EDV ausgeschaltet, sodass eventuell Gelder zu Unrecht ausgezahlt werden.

Es ist demnach erforderlich, die Hintergründe zu verstehen und die Verarbeitungsgründe genau zu kennen.

Weiterhin müssen Sie alle Informationsquellen in Ihrer AOK kennen:

- Welche Information werden zu Ihrem Aufgabenbereich im Intranet bereitgestellt?
- Gibt es aktuelle Handlungsanleitungen?
- Welche Standardauswertungen werden im standardisierten Berichtswesen für Ihren Bereich bereitgestellt?

Nutzen Sie die durch das zentrale Controlling bereitgestellten Berichte als Hilfestellung für Ihre tägliche Arbeit.

Darüber hinaus können Sie neben dem Intranet Ihrer AOK auch das Intranet des AOK-Bundesverbandes für fachliche Informationen nutzen.

Sehr wichtig ist auch der „sichere“ Umgang mit dem Betriebssystem und der Standardsoftware im Bürobereich. Es darf Ihnen z.B. keine Schwierigkeiten bereiten, einen neuen Ordner anzulegen oder ein Dokument als Anlage

in eine E-Mail einzufügen. Sie müssen in der Lage sein, einen Kundenbrief in Word zu verfassen. Zur Zusammenarbeit im Team sollte Ihnen auch die Überarbeitungsfunktionalität bekannt sein.

Immer wichtiger wird auch Ihre persönliche interne Qualitätssicherung, d.h. Selbstüberprüfung der Arbeitsergebnisse. Hier sollten Sie mit Excel oder Access einfache Auswertungen, z.B. über Hilfsmittelausgaben innerhalb Ihres Aufgabenbereichs, erstellen können oder mit Access Zielkunden selektieren, um die Daten mit Word zu einem Serienbrief zu koppeln.

Sie sollten in der Lage sein, Ihre Arbeitsergebnisse mithilfe von Power Point zu präsentieren und dazu eine Excel-Grafik einbinden können.

### Hinweis

Zur Bürokommunikation werden ggf. in Ihrer AOK Kurse angeboten. Wenn Sie hier Schwächen erkennen, sprechen Sie mit Ihrem Ausbildungsleiter.

### Merke

Nur wenn Sie wissen, wo Sie alle zu Ihrem Arbeitsbereich vorliegenden Informationen finden, können Sie gut arbeiten.

## 3.7 Kurzer Einblick in die Informationssicherheit

Die Informationssicherheit und der Datenschutz haben einen ähnlichen, aber dennoch klar zu differenzierenden Fokus. Während die Informationssicherheit die im Unternehmen befindlichen Informationen grundsätzlich betrachtet, besitzt der Datenschutz

einen deutlich fokussierten Blick auf die Informationen mit Personenbezug. Aufgrund der stetigen Vernetzung und Systematisierung der Geschäftsprozesse sowie der Standardisierung der IT-Lösungen im Zuge der Digitalisierung werden jedoch in nahezu jedem Geschäftsprozess auch personenbezogene Daten verarbeitet und der Datenschutz bzw. die Gewährleistungsziele des Datenschutzes sind daher immer zu berücksichtigen. Dennoch gilt, dass ein Sicherheitsvorfall nicht immer einen Datenschutzvorfall darstellt, ein Datenschutzvorfall jedoch immer auch ein Sicherheitsvorfall ist.

Beide Disziplinen haben jedoch einen unbestreitbaren gemeinsamen Nenner, nämlich den Schutz der Informationen. Dieser Schutz wird gewährleistet durch die Risikoanalyse und der Ableitung wirksamer technisch-organisatorischer Maßnahmen (TOM) zur Risikobehandlung (z.B. in Form einer DSFA gemäß Art. 35 DSGVO). Diese TOM stellen die Sicherheit bei der Datenverarbeitung her und sollten unbedingt für die Implementierung abgestimmt werden. Die avisierten TOM zur Gewährleistung der Datensicherheit unterstützen den Fachverantwortlichen bei der Erfüllung der (unter-) gesetzlichen Anforderungen zum Datenschutz und zur Informationssicherheit.

Die folgende Aufzählung zeigt Ihnen eine nicht abschließende Auflistung von technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit:

- Erheben, verarbeiten (speichern, verändern, übermitteln, sperren, löschen) oder nutzen Sie die Ihnen anvertrauten personenbezogenen Daten nur im Rahmen Ihrer Aufgabenstellung.

- Wählen Sie bei der Übertragung von Sozialdaten (z.B. Diagnosen / Befunde) nur geschützte Übertragungswege – nach Möglichkeit zusätzlich verschlüsselt.
- Speichern Sie auf Ihrem lokalen Datenträger (z.B. Festplatte) – sofern es nicht zu Ihrem Aufgabenbereich gehört – keine personenbezogenen Daten, solange eine Festplattenverschlüsselung nicht umgesetzt ist.
- Halten Sie die Ihnen anvertrauten Datenträger, wenn Sie nicht unmittelbar daran arbeiten, unter Verschluss (USB-Sticks, CDs, DVDs und andere Datenträger sind wegzuschließen).
- Machen Sie Ihren PC und Ihre Anwendungen keinem Unbefugten zugänglich.
- Sorgen Sie dafür, dass Ihre Passwörter niemandem, auch nicht Ihrer Vertretung, bekannt werden.
- Sperren Sie vor Verlassen des Büros den PC (Tastenkombination: Windows-Taste + L) oder benutzen Sie eine sichere „Pausenschaltung“.
- Vernichten Sie nicht mehr benötigte Datenträger datenschutzgerecht, damit eine missbräuchliche Weiterverwendung nicht möglich ist.
- Setzen Sie zur Verarbeitung personenbezogener Daten ausschließlich solche Hard- und Software-Produkte ein, die vom Arbeitgeber für diesen Zweck vor- und freigegeben sind.
- Sie dürfen weder nicht freigegebene, nicht lizenzierte Software sowie Public-Domain-Programme nutzen, noch dürfen Sie Shareware und Freeware einsetzen. Das gilt auch für Programme, die aus dem oder über das Internet beschafft werden.
- Nehmen Sie an der bereitgestellten Hardware keinerlei Veränderung vor.
- Geben Sie Software und Daten nicht unbefugt an Dritte weiter.
- Sie dürfen weder Kettenbriefe versenden, noch beantworten.

- Eigene Unterschriften dürfen nicht eingescannt und z.B. als BMP-Datei an Dokumente oder E-Mails angehängt werden, da diese vom Empfänger ansonsten weiter genutzt werden könnten.
- Sichern Sie beim mobilen Einsatz von Laptops (ausgedockt) die erfassten Daten bei nächstmöglicher Gelegenheit (eingedockt) auf dem Server.
- Führen Sie keine an E-Mails angehängte Dateien – insbesondere mit der Endung „.vbs“ oder „.exe“ aus.
- Öffnen Sie keine Dokumente, an deren Herkunft oder Zuverlässigkeit Sie Zweifel haben und leiten Sie diese auch nicht weiter.
- Leiten Sie keine Virenwarnungen weiter, sondern wenden Sie sich umgehend an die zuständige IT-Abteilung Ihrer AOK.
- Stellen Sie sicher, dass regelmäßig eine Virenprüfung auf Ihrem PC durchgeführt wird und dass Ihr Virens Scanner aktuell ist. Wenn Sie Zweifel haben, ob Ihr Virens Scanner richtig eingestellt ist, wenden Sie sich an Ihre IT-Abteilung.

**Verhalten im Fall eines Virusbefalls**  
(Virens Scanner meldet Virus):

- Stellen Sie augenblicklich die Arbeit an Ihrem PC ein.
- Melden Sie umgehend den Virenbe-  
fall an die IT-Abteilung.

### 3.8 Übungen zum Lernabschnitt 3

#### Übung 1

Wie unterscheidet sich der Daten-  
schutz und die Informationssicherheit?

#### Übung 2

Erläutern Sie, warum Sie Ihr Passwort  
geheim halten sollen.

#### Übung 3

Nennen Sie Grundregeln für den Um-  
gang mit Passwörtern.

#### Übung 4

Nennen Sie drei technisch-organisa-  
torische Maßnahmen, die Sie bei ihrer  
täglichen Arbeit umsetzen sollten?

## 4 Datenschutz

### 4.1 Allgemeines

Jetzt wird es schwer, in wenigen Kapiteln zu verdeutlichen, was eigentlich hinter der komplexen Materie Datenschutz steckt. Häufig ist das Wort bereits negativ besetzt. Immer, wenn Vorgehensweisen, z.B. Mitgliederwerbung oder Anfragen wegen Arbeitsunfähigkeitszeiten, rechtlich unsicher sind, wird der Datenschutz als Arbeitsbehinderung dargestellt.

Doch man kommt schnell darauf, dass der Datenschutz nicht Selbstzweck ist, wenn man sich bei jeder Tätigkeit, die man in der Krankenkasse ausführt, vorstellt, dass hiervon die eigenen Daten betroffen sind.

Wäre es z.B. o.k., wenn

- Ihre eigene Diagnose- und/oder Befunddaten offen und unverschlüsselt über das Internet verschickt würden?
- Ihr eigener Krankheitsverlauf offen in der Geschäftsstelle ausdiskutiert würde?
- Jemand, der sich telefonisch unter Ihrem Namen meldet, Informationen über Ihre persönlichen Daten erhält?

### 4.2 Gesetzliche Grundlagen

Die Thematik Datenschutz wurde in den 70er-Jahren erstmals im größeren Rahmen diskutiert, als die Verwaltung automatisiert werden sollte und somit die ersten Großrechner eingesetzt wurden. Hier kam zum ersten Mal die Angst auf, jeder Bürger könnte eine eindeutige Personennummer bekommen, über die er in jedem EDV-System erkennbar ist. Aus dieser Grundstimmung heraus wurden die ersten Datenschutzgesetze mit dem Hauptzweck erlassen, den Bürger vor der Willkür des Staates zu schützen.

Das Bundesverfassungsgericht hat im Volkszählungsurteil vom 15. 12. 1983 den Begriff „Recht auf informationelle Selbstbestimmung“ erstmals in dem Sinne verwendet, dass es sich bei dem Datenschutz um ein Grundrecht handelt, also im Grundgesetz verankert ist.

Im 1. und 2. Leitsatz hat das Gericht dazu ausgeführt, dass der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann. Einschränkungen dieses „Rechts auf informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig.

Die EU hat in der Charta der Grundrechte den Schutz personenbezogener Daten in Art. 8 aufgenommen. „Jede Person hat das Recht auf Schutz der sie betreffenden Daten“

Abs. 2 spiegelt einige der Grundsätze der Verarbeitung von personenbezogenen Daten wieder, wie sie 2016 in der DSGVO übernommen worden.

Das SGB X enthält zudem datenschutzrechtliche Vorgaben, welche als „lex specialis“ für die genannten Leistungsträger gemäß § 12 SGB I greifen. Das SGB V enthält weitere datenschutzrechtliche Vorgaben für die Krankenversicherung, das SGB XI für die Pflegeversicherung.

Insbesondere § 284 SGB V und § 94 SGB XI regeln zu welchen Zwecken die Versicherungen Sozialdaten erheben und speichern dürfen.

Zudem sind noch zu erwähnen:

- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetz (LDSG)

BVerfG-Urteil v. 15. 12. 1983, 1 BvR 209, 269, 362, 420, 440, 484/83

Art. 1, 2 GG



Das Telekommunikation-Digitale-Dienste-Gesetz (TDDDG) regelt die datenschutzrechtlichen Vorgaben für Anbieter von digitalen Diensten.

In diesem Lernbrief wird größtenteils auf die Regelungen des Sozialgesetzbuchs eingegangen. Im Zuge einer EU-weiten Harmonisierung wurden auch diese speziellen Datenschutzregeln angepasst (vgl. DSGVO).

### Merke

Der Datenschutz (Recht auf informationelle Selbstbestimmung) wurde als Grundrecht anerkannt und als das Recht definiert, selbst über die Verwendung der eigenen Daten zu entscheiden. Staatliche Eingriffe in dieses Recht sind nur aufgrund einer gesetzlichen Rechtsgrundlage zulässig.

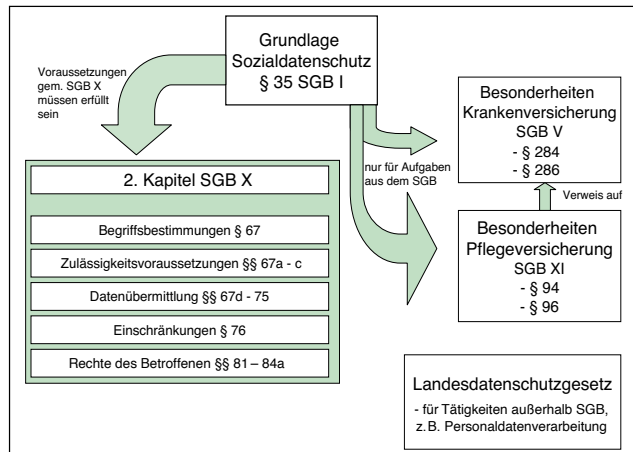
## 4.3 Sozialdatenschutz

### 4.3.1 Rechtsquellen

Genau wie alle anderen Regelungen, die für alle Sozialleistungsträger gleichermaßen gelten, sind die Grundregeln des Sozialdatenschutzes im SGB I und SGB X aufgeführt. Bereichsspezifische Regelungen zum Datenschutz für die Krankenversicherung stehen im SGB V, für die Pflegeversicherung im SGB XI.

Es ist also die richtige Reihenfolge der Paragraphen zu beachten.

## Gesetzliche Bestimmungen zum Sozialdatenschutz



Mit der seit Mai 2018 anwendbaren Datenschutz-Grundverordnung (DSGVO) haben sich die gesetzlichen Anforderungen an die Verwendung und Verarbeitung von Daten mit Personenbezug nochmals verschärft. Sie findet Anwendung auf die Verarbeitung personenbezogener Daten innerhalb der EU.

Art. 3 DSGVO

Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der ganz oder teilweisen automatisierten Verarbeitung personenbezogener Daten und Regelungen zum freien Verkehr solcher Daten.

Art. 1 DSGVO

### 4.3.2 Sozialdaten

In unserer täglichen Arbeit, müssen wir zwischen personenbezogenen Daten nach Art. 6 DSGVO, besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO und Sozialdaten gemäß dem SGB unterscheiden.

Sozialdaten sind gemäß § 67 Abs. 2 SGB X personenbezogene Daten, welche von einer nach § 35 SGB I genannten Stelle (bspw. die Träger der Kranken- oder Pflegeversicherung) im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden.

Zusammengefasst - personenbezogene Daten welche zur Erfüllung einer Aufgabe im SGB verarbeitet werden, sind Sozialdaten.

Betriebs- und Geschäftsgeheimnisse sind diesen gleichgestellt (§ 35 Abs. 4 SGB I). Diese werden in § 67 Abs. 2 SGB X definiert.

#### 4.3.3 Sozialgeheimnis

§ 35 SGB I

Der § 35 SGB I stellt die Grundlage des Sozialdatenschutzes dar. Hier sind exemplarisch daraus die wichtigsten Prinzipien dargestellt:

- Sozialdaten sollen von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden.
- Der Leistungsträger hat sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden.

Leistungsträger in diesem Sinne sind alle Träger der gesetzlichen Sozialversicherung und deren Verbände und Arbeitsgemeinschaften, also insbesondere Krankenkassen, Pflegekassen, Rentenversicherungsträger, Agenturen für Arbeit, Sozialämter, aber auch Berufsgenossenschaften für bestimmte Bereiche.

Die Beurteilung, welche Institution als Leistungsträger unter die Definition des § 35 SGB I fällt, ist später in vielen Fällen für die Frage wichtig, ob eine Auskunft erteilt werden darf.

Sozialdaten der Beschäftigten und ihrer Angehörigen dürfen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein, noch von Zugriffsberechtigten weitergegeben werden (Mitarbeiterdatenschutz).

Hier hat jede Krankenkasse individuelle Regelungen getroffen, mit denen man sich vertraut machen sollte, da diese oft eine Mitarbeit voraussetzen (z.B. Mitarbeitergeschäftsstelle).

Die Beschäftigten haben auch nach Beendigung ihrer Tätigkeit bei den genannten Stellen das Sozialgeheimnis zu wahren.

Hier ist ein großer Unterschied zum BDSG bzw. den LDSG erkennbar, die „nur“ natürliche Personen schützen. Im SGB sind somit auch reine Firmendaten geschützt (Abrechnungsdaten, Umsätze, usw.).

Sozialdaten Verstorbener dürfen nach Maßgabe des zweiten Kapitels des SGB X verarbeitet oder genutzt werden. Sie dürfen außerdem verarbeitet oder genutzt werden, wenn schutzwürdige Interessen des Verstorbenen oder seiner Angehörigen dadurch nicht beeinträchtigt werden können.

Dieses führt oft bei Erbschaftsstreitigkeiten zu Problemen. Hier ist darauf zu achten, dass Daten grundsätzlich an Erbberechtigte weitergegeben werden dürfen.

In der Regel erfolgt bei jeder Neueinstellung von Mitarbeitenden eine schriftliche Verpflichtung, dieses Sozialgeheimnis zu wahren.

### Merke

Im § 35 SGB I steckt die Grundaussage des Sozialdatenschutzes. Jeder hat Anspruch darauf, dass seine Sozialdaten nicht unbefugt erhoben, verarbeitet oder genutzt werden.

## 4.4 Begriffsdefinitionen

§ 67 Abs. 2  
Satz 1  
SGB X, Art. 4  
Nr. 1  
DSGVO

**Sozialdaten** sind personenbezogene Daten, die wir als Kranken- bzw. Pflegeversicherungsträger erhalten. Dieses muss nicht schriftlich sein, auch was Sie in der Kundenberatung im persönlichen Gespräch von den Kunden erfahren, gehört bereits dazu. Wichtig in diesem Zusammenhang ist auch, dass bereits die Adressdaten (Anschrift, Straße, Hausnummer, usw.) unter dieses Gesetz fallen und auch hier die gleichen, hohen Sicherheitsbestimmungen gelten. Es ist daher erforderlich, dass vor jeder Datenverwendung geprüft wird, ob die Daten wie geplant verwendet und verarbeitet werden dürfen.

§ 284 SGB V

Bei der Menge und Art der Daten, die wir speichern dürfen, sind wir als Krankenversicherung zusätzlich durch das SGB V eingeschränkt.

§ 67 Abs. 2,  
Abs. 3 SGB X

**Aufgaben nach diesem Gesetzbuch** sind neben den direkt im Gesetz genannten, natürlich auch Aufgaben, die sich aus Verordnungen ergeben sowie aufgrund über- und zwischenstaatlichem Recht und Aufgaben, die einem Leistungsträger durch andere Gesetze zugewiesen wurden.

Des Weiteren wird definiert, dass sich die Datenverarbeitung aus zwei Hauptgebieten zusammensetzt:

- verarbeiten
- erheben

**Verarbeitung** wird nach dem Gesetz u.a. in folgende Schritte unterteilt:

- erheben
- speichern
- verändern
- übermitteln
- sperren
- löschen

Art. 4 Nr. 2  
DSGVO

**Erheben** ist das erstmalige Beschaffen von Daten über den Betroffenen, also z.B. Abfragen von Sachverhalten im Telefonat oder per Mail mit Kundinnen oder Kunden, im persönlichen Gespräch oder per Fragebogen. Aber auch im Austausch mit anderen Leistungserbringern, Sozialleistungsträgern, Arbeitgebern und Geschäftspartnern können Daten erhoben werden

Hierbei ist **Speichern** das erstmalige Erfassen von neuen Daten im EDV-System. Das kann sowohl die manuelle Eingabe von Daten in eine Erfassungsmaske als auch das maschinelle Einspielen von Daten (z.B. von CD, USB-Stick oder die Dunkelverarbeitung) sein.

**Verändern** hingegen ist das inhaltliche Umgestalten gespeicherter Sozialdaten (z.B. Adressänderung).

**Übermitteln** ist das Bekanntgeben von Sozialdaten an einen Dritten. Dieses kann durch Weitergabe (Brief, E-Mail, usw.) oder durch Bereitstellen zum Abruf (z.B. Internetseite) geschehen. Hierunter fällt auch das Bekanntgeben nicht gespeicherter Sozialdaten (z.B. Gespräch mit persönlichen Informationen des Kundenberaters).

**Sperren** ist das vollständige oder teilweise Untersagen der weiteren Verarbeitung oder Nutzung von Sozialdaten durch entsprechende Kennzeichnung. Das ist anzuwenden, wenn bestimmte Daten eigentlich gelöscht werden müssten, dies aber technisch nicht möglich ist. Dann sollte der Zugriff auf diesen Datensatz technisch verhindert werden.

**Löschen** ist das Unkenntlichmachen gespeicherter Sozialdaten (z.B. Vernichten des Datenträgers, Löschen eines Datensatzes in einer Datenbank).

Der Begriff „**Nutzen**“ wurde als Auffangbecken geschaffen, da festgestellt wurde, dass es außer den Definitionen von Erheben und Verarbeiten noch andere Prozesse gibt (z.B. Weitergabe innerhalb der verantwortlichen Stelle), bei denen das Gesetz ansonsten nicht greifen würde. Nutzen ist somit jede Verwendung von Sozialdaten, soweit es sich nicht um Verarbeitung handelt.

**Anonymisieren** bedeutet, dass Daten so verändert werden, dass mit normalem Aufwand keine Möglichkeit besteht, den Bezug zu einer Person herzustellen. Das ist vor allem im Bereich Statistik und Forschung wichtig. Es ist z.B. ausreichend, wenn bekannt ist, wie viele Krankengeldfälle in einem Monat aufgetreten sind. Der einzelne Krankengeldbezieher ist jedoch unwichtig. Da kein Personenbezug vorhanden ist, können für diese Daten die hohen Schutzanforderungen entfallen.

Es ist jedoch wichtig zu ergänzen, dass das Anonymisieren von personenbezogenen Daten eine eigene Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO darstellt, die einer eigenständigen Rechtsgrundlage bedarf.

**Pseudonymisieren** ist eine spezielle Form des Anonymisierens. Hier werden personenbezogene Daten nicht gelöscht, sondern durch andere Daten ersetzt. Hierdurch weiß der Empfänger auch nicht, um wen es sich handelt. Es können aber z.B. für längere Forschungsvorhaben mehrere zeitlich gestaffelte Datenlieferungen zu einer Person zusammengeführt werden, wenn immer das gleiche Ersatzmerkmal verwendet wird.

Jede AOK ist als eine **verantwortliche Stelle** im Sinne des Gesetzes zu sehen. Damit entspricht eine Datenweitergabe von einer Geschäftsstelle zu einer anderen keiner Datenübermittlung. Auch können somit die Zugriffsmöglichkeiten der Mitarbeitenden auf den Datenbestand nach jeweiliger Zuständigkeit in einer AOK frei vergeben werden. Wird ein Teil der Datenverarbeitung im Auftrag an andere vergeben (z.B. Mailing-Aktion, Versand von Zeitschriften), so gilt die auftragnehmende Person rechtlich hier auch als Teil der verantwortlichen Stelle.

**Empfänger** ist jede Person oder Stelle, die Sozialdaten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle, mit Ausnahme der/s Betroffenen und einer Datenverarbeitung im Auftrag (vgl. auch „Verantwortliche Stelle“).

Der Begriff **besondere Arten personenbezogener Daten** wurde erst in jüngerer Vergangenheit ins Gesetz aufgenommen. Hierdurch sollte deutlich gemacht werden, dass nicht alle personenbezogenen Daten gleich schützenswert sind und gerade die hier aufgezählten Daten besonders sensibel zu behandeln sind:

- die rassische und ethnische Herkunft
- politische Meinungen

Art. 4 Nr. 5  
DSGVO

Art. 4 Nr. 7  
DSGVO

Art. 4 Nr. 9  
DSGVO

- religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit oder Sexualleben

284 SGB V regelt die Zwecke zu welcher die Krankenversicherung Sozialdaten erheben und speichern darf.

§ 94 SGB XI regelt dies analog für die Pflegeversicherung.

## 4.5 Verarbeitung von Sozialdaten

In § 35 SGB I wird darauf verwiesen, dass eine Erhebung, Verarbeitung und Nutzung von Sozialdaten nur unter den Voraussetzungen des Zweiten Kapitels SGB X zulässig ist. Die Kernpunkte dieses Kapitels sind:

- Begriffsbestimmungen
- Rechtmäßigkeit der Datenverarbeitung
- Datenübermittlung
- Einschränkungen bei besonders schutzwürdigen Daten
- Rechte des Betroffenen
- Umgang mit Datenschutzverstößen

### 4.5.1 Zulässigkeit von Datenverarbeitung und -nutzung

§ 67a – c  
SGB X

Im SGB X werden Aussagen zu folgenden Hauptbereichen getroffen:

- Wann ist Verarbeitung zulässig?
- Wo und wie dürfen Daten erhoben werden?
- Wie muss das Einverständnis der Kundin oder des Kunden nachgewiesen werden?
- Daten dürfen nur zweckgebunden verarbeitet werden.

Für eine Datenverarbeitung und -nutzung durch einen Sozialleistungsträger muss immer eine gesetzliche Grundlage vorhanden sein (vgl. Begriff „Aufgaben nach diesem Gesetzbuch“) oder die betroffene Person hat eingewilligt.

Eine Datenerhebung hat grundsätzlich bei der betroffenen Person selbst zu erfolgen, es sei denn, die benötigten Daten liegen bereits bei einem anderen Sozialleistungsträger vor und dieser darf sie uns übermitteln (Ersterhebungsgrundsatz). Sobald eine Datenerhebung nicht bei der betroffenen Person erfolgt, ist sicherzustellen, dass hierdurch keine überwiegenden schutzwürdigen Interessen der betroffenen Person beeinträchtigt werden. Dieser Begriff wird im Gesetz nicht näher erläutert, sodass dies in jedem Einzelfall zu prüfen ist.

Die betroffene Person ist bei der Erhebung über den Zweck zu unterrichten. Weiterhin muss die gesetzliche Grundlage sowie Folgen bei Verweigerung der Auskunft und die Freiwilligkeit von bestimmten Angaben genannt werden. Eine Einwilligung muss auf dem freien Willen der oder des Betroffenen beruhen, ansonsten ist diese unwirksam. Die Einwilligung sollte grundsätzlich schriftlich erfolgen, damit eine entsprechende Dokumentation vorgenommen werden kann.

Muster für einen entsprechenden Hinweis:

Damit wir unsere Aufgaben (Beschreibung der konkreten jeweiligen Aufgabe) rechtmäßig erfüllen können, ist Ihr Mitwirken nach (Angabe der Vorschrift, aus der sich eine Pflicht des Versicherten zur Mitwirkung ergibt, z.B. § 60 SGB I) erforderlich. Ihre Daten

§ 67b Abs. 1  
Satz 1 SGB X,  
Art. 6 Abs. 1  
Buchst. a  
DSGVO

§ 67a Abs. 2  
SGB X

§ 67b Abs. 2  
SGB X, Art. 6  
Abs. 1  
Buchst. a, c, e  
DSGVO

sind im vorliegenden Fall aufgrund (Angabe der Vorschrift, für deren Vollzug die Daten erhoben werden) zu erheben. Fehlende Mitwirkung kann zu Nachteilen (z.B. bei den Leistungsansprüchen) führen. Die Angabe der Telefonnummer erfolgt freiwillig.

§ 67c Abs. 1–4 SGB X

Im Bereich der Sozialversicherung gilt zusätzlich das Gebot der Zweckbindung. Das bedeutet, Daten dürfen grundsätzlich nur für den Zweck verwendet werden, für den sie auch erhoben worden sind.

Gemäß § 67c Abs. 2 Nr. 1 SGB X, können rechtmäßig gespeicherte Daten unter bestimmten Bedingungen zu anderen Aufgaben nach dem SGB verarbeitet werden.

#### Beispiel

Mit der Krankenhausabrechnung werden auch Diagnosedaten des Versicherten geliefert. Diese dienen der Abrechnungsprüfung und der Berechnung von Vorerkrankungszeiten.

#### Folge

Eine Nutzung dieser Daten für eine Risikoselektion ist nicht zulässig. Selbst die Nutzung dieser Daten, den Versicherten gezielt zu informieren (z.B. spezielle Informationen zu einer Diabetikerschulung), wird von einigen Aufsichtsbehörden als kritisch bewertet.

#### 4.5.2 Sozialdaten bei den Krankenkassen und Pflegekassen

Im Unterschied zu anderen Sozialleistungsträgern, sind für den Bereich der gesetzlichen Krankenversicherung spezielle Zusatzregeln in das SGB V aufgenommen worden. In diesen wird genau definiert, was gespeichert werden darf, wie eine Übersicht bereitzustellen ist und wie diese zu schützen ist.

Die Krankenkasse darf laut gesetzlicher Regelung nur für folgende Zwecke Daten erheben und speichern:

- die Feststellung des Versicherungsverhältnisses und der Mitgliedschaft, einschließlich der für die Anbahnung eines Versicherungsverhältnisses erforderlichen Daten
- die Ausstellung des Berechtigungsscheins und der elektronischen Gesundheitskarte
- die Feststellung der Beitragspflicht und der Beiträge, deren Tragung und Zahlung
- die Prüfung der Leistungspflicht und der Erbringung von Leistungen an Versicherte, die Bestimmung des Zuzahlungsstatus und die Durchführung der Verfahren bei Kostenerstattung, Beitragsrückzahlung und der Ermittlung der Belastungsgrenze
- die Unterstützung der Versicherten bei Behandlungsfehlern
- die Übernahme der Behandlungskosten in den Fällen des § 264 SGB V
- die Beteiligung des Medizinischen Dienstes oder des Gutachterverfahrens

§ 284 Abs. 1 SGB V

§ 278 SGB V

- die Abrechnung mit den Leistungserbringern, einschließlich der Prüfung der Rechtmäßigkeit und Plausibilität der Abrechnung
- die Überwachung der Wirtschaftlichkeit der Leistungserbringung
- die Abrechnung mit anderen Leistungsträgern
- die Durchführung von Erstattungs- und Ersatzansprüchen
- die Vorbereitung, Vereinbarung und Durchführung von ihnen zu schließenden Vergütungsverträgen
- die Vorbereitung und Durchführung von Modellvorhaben, die Durchführung des Versorgungsmanagements nach § 11 Abs. 4 SGB V, die Durchführung von Verträgen zur hausarztzentrierten Versorgung, zu besonderen Versorgungsformen und zur ambulanten Erbringung hochspezialisierter Leistungen, einschließlich der Durchführung von Wirtschaftlichkeitsprüfungen und Qualitätsprüfungen
- die Durchführung des Risikostrukturausgleichs nach den §§ 266, 267 SGB V sowie zur Gewinnung von Versicherten für die Programme nach § 137g SGB V und zur Vorbereitung und Durchführung dieser Programme
- die Durchführung des Entlassmanagements nach § 39 Abs. 1a SGB V
- die Auswahl von Versicherten für Maßnahmen nach § 44 Abs. 4 Satz 1 SGB V und nach § 39b SGB V sowie zu deren Durchführung
- die Überwachung der Einhaltung der vertraglichen und gesetzlichen Pflichten der Leistungserbringer von Hilfsmitteln nach § 127 Abs. 7 SGB V
- die Erfüllung der Aufgaben der Krankenkassen als Rehabilitationsträger nach dem Neunten Buch
- die Vorbereitung von Versorgungsinnovationen, die Information der Versicherten und die Unterbreitung von Angeboten nach § 68b Abs. 1 und 2 SGB V

- die administrative Zurverfügungstellung der elektronischen Patientenakte sowie für das Angebot zusätzlicher Anwendungen im Sinne des § 345 Abs. 1 Satz 1 SGB V

Dies bedeutet also, dass eine Datenverarbeitung für andere Zwecke unzulässig ist.

Im Zuge des GKV-Modernisierungsgesetzes (GMG) wurden auch die notwendigen Änderungen in den § 284 SGB V eingefügt, die der Wettbewerb zwischen den Krankenkassen erfordert (z.B. Daten zur Anbahnung eines Versicherungsverhältnisses) und die Anwendungen der elektronischen Gesundheitskarte berücksichtigt.

Auch wenn Datenverarbeitung zu Werbezwecken somit erlaubt ist, muss bei der Adressgewinnung grundsätzlich eine schriftliche Einverständniserklärung eingeholt werden, in der eine Nutzung zu Informations- und Werbezwecken erlaubt wird.

Details regelt das Gesetz gegen den unlauteren Wettbewerb (UWG). Die Telefonwerbung wird besonders restriktiv behandelt. Nur bei vorheriger ausdrücklicher schriftlicher Einwilligung ist eine Werbung am Telefon zulässig.

Die Krankenkassen haben einmal jährlich eine Datenübersicht zu erstellen und der Aufsichtsbehörde vorzulegen. Diese Übersicht muss in geeigneter Weise veröffentlicht werden. In der Regel erfolgt dieses durch einen Aushang in den Geschäftsstellen, in dem darauf hingewiesen wird, wer die datenschutzbeauftragte Person ist und wo die Übersicht eingesehen werden kann.

§ 286 SGB V

Weiterhin müssen die Krankenkassen in einer Dienstanweisung Folgendes regeln:

- die zulässigen Verfahren der Verarbeitung der Daten
- Art, Form, Inhalt und Kontrolle der einzugebenden und der auszugebenden Daten
- die Abgrenzung der Verantwortungsbereiche bei der Datenverarbeitung
- die weiteren zur Gewährleistung von Datenschutz und Datensicherheit zu treffenden Maßnahmen

#### **Elektronische Gesundheitskarte (eGK)**

Besonders die elektronische Gesundheitskarte benötigt einen hohen Sicherheitsstandard. Auf der elektronischen Gesundheitskarte sind u.a. folgende vertrauliche personenbezogene Daten gespeichert:

- Bezeichnung der ausstellenden Krankenkasse
- Name und Adresse der versicherten Person
- Geburtsdatum und Geschlecht
- Krankenversichertennummer
- Versichertenstatus
- Tag des Beginns des Versicherungsschutzes
- Gültigkeit der Karte

Aufgrund des hohen Schutzbedarfs dieser personenbezogenen Daten wird die elektronische Gesundheitskarte laufend mit neuen Funktionen und Sicherheitsmerkmalen versehen. Während die administrativen Funktionen für alle Versicherten bindend sind, basiert die Nutzung der medizinischen Funktionen wie z.B. die Übermittlung von Befunden, Diagnosen, Therapieempfehlungen sowie Behandlungsberichten in elektronischer und maschinell verwertbarer Form (elektronischer

Arztbrief) auf freiwilliger Basis. Hierbei kann jede versicherte Person frei entscheiden, welche Funktionen sie/er in welcher Weise nutzen möchte. Die Daten werden verschlüsselt gespeichert und können von den Versicherten nur durch eine PIN-Eingabe freigegeben werden.

Weitere Informationen über die elektronische Gesundheitskarte finden Sie im § 291a SGB V.

Da die Aufgaben der Pflegeversicherung durch die Krankenversicherung übernommen werden, müssen auch hier vergleichbare Datenschutzregelungen gelten. Das bedeutet, der § 35 SGB I sowie die Regelungen im zweiten Kapitel SGB X sind auch in der Pflegeversicherung anzuwenden. Die gemeinsame Nutzungsmöglichkeit der Daten ist im § 96 SGB XI ausdrücklich erlaubt.

§ 96 SGB XI

Die Einschränkungen des § 76 SGB X (besonders schützenswerte Sozialdaten und Widerspruchsrecht) gelten nicht für den Austausch zwischen Kranken- und Pflegeversicherung.

Entsprechend dem § 284 SGB V sind auch die Zwecke, zu denen Daten verarbeitet und genutzt werden dürfen, vollständig aufgelistet.

§ 94 SGB XI

- die Feststellung des Versicherungsverhältnisses (§§ 20 bis 26 SGB XI) und der Mitgliedschaft (§ 49 SGB XI),
- die Feststellung der Beitragspflicht und der Beiträge, deren Tragung und Zahlung (§§ 54 bis 61 SGB XI),
- die Prüfung der Leistungspflicht und die Gewährung von Leistungen an Versicherte (§§ 4, 28 und 28a SGB XI) sowie die Durchführung von Erstattungs- und Ersatzansprüchen,
- die Beteiligung des Medizinischen Dienstes (§§ 18 bis 18c und 40 SGB XI),



- die Abrechnung mit den Leistungserbringern und die Kostenerstattung (§§ 84 bis 91 und 105 SGB XI),
- die Überwachung der Wirtschaftlichkeit, der Abrechnung und der Qualität der Leistungserbringung (§§ 79, 112, 113, 114, 114a, 115 und 117 SGB XI),
- den Abschluss und die Durchführung von Pflegesatzvereinbarungen (§§ 85, 86 SGB XI), Vergütungsvereinbarungen (§ 89 SGB XI) sowie Verträgen zur integrierten Versorgung (§ 92b SGB XI),
- die Aufklärung und Auskunft (§ 7 SGB XI),
- die Koordinierung pflegerischer Hilfen (§ 12 SGB XI), die Pflegeberatung (§ 7a SGB XI), das Ausstellen von Beratungsgutscheinen (§ 7b SGB XI) sowie die Wahrnehmung der Aufgaben in den Pflegestützpunkten (§ 7c SGB XI),
- die Abrechnung mit anderen Leistungsträgern,
- statistische Zwecke (§ 109 SGB XI),
- die Unterstützung der Versicherten bei der Durchsetzung des Herausgabeanspruchs nach § 109a Abs. 1 SGB XI Satz 2 in Verbindung mit Abs. 4 SGB XI
- die Unterstützung der Versicherten bei der Verfolgung von Schadensersatzansprüchen (§ 115 Abs. 3 Satz 7 SGB XI),
- Auswertungen nach § 25b SGB XI (soweit erforderlich)

Es wird nur zusätzlich auf die notwendige Beachtung von Zweckbindung hingewiesen.

#### 4.5.3 Datenübermittlung

Auch für die Datenübermittlung sind die entsprechenden Tatbestände sehr genau im Gesetz geregelt. Eine Übermittlung von Sozialdaten ist nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis vorliegt. Folgende Übermittlungssachverhalte sind zulässig:

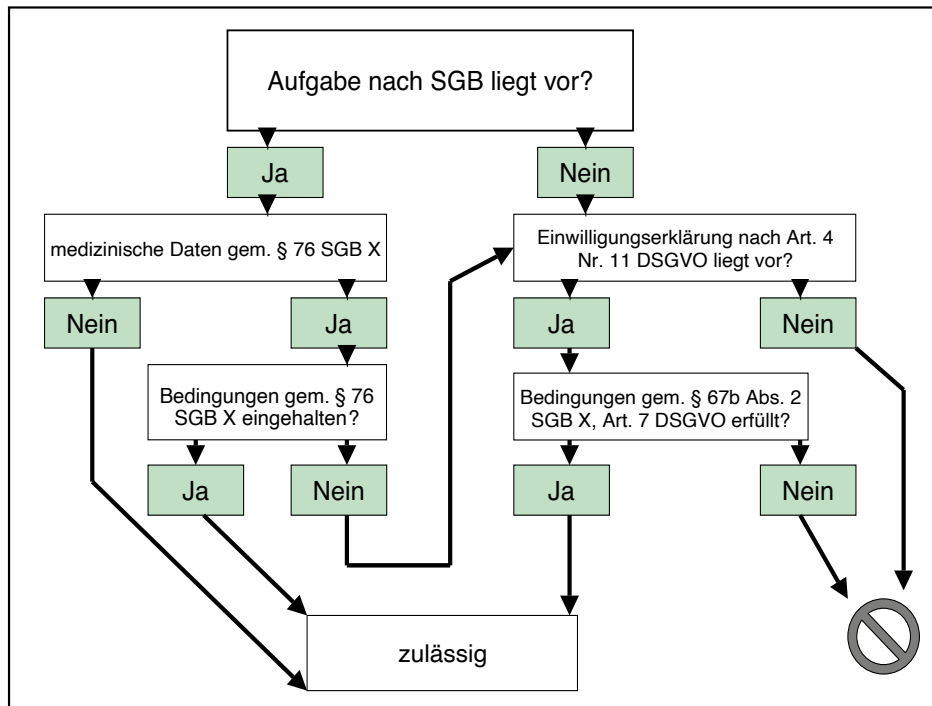
- Übermittlung für Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr oder zur Durchsetzung öffentlich-rechtlicher Ansprüche
- Übermittlung für die Erfüllung sozialer Aufgaben
- Übermittlung für die Durchführung des Arbeitsschutzes
- Übermittlung für die Erfüllung besonderer gesetzlicher Pflichten und Mitteilungsbefugnisse
- Übermittlung für den Schutz der inneren und äußeren Sicherheit
- Übermittlung für die Durchführung eines Strafverfahrens
- Übermittlung bei Verletzung der Unterhaltspflicht und beim Versorgungsausgleich
- Übermittlung zur Durchsetzung öffentlich-rechtlicher Ansprüche und im Vollstreckungsverfahren
- Übermittlung von Sozialdaten für die Forschung und Planung

§§ 68 – 75  
SGB X

Als Grundsatz über allen entsprechenden Regelungen steht:

Die Verantwortung für die Zulässigkeit trägt immer der Absender, d.h., die jeweilige Person, die den Fall bearbeitet.

### Prüfschema: Rechtmäßigkeit der Datenübermittlung



Im Tagesgeschäft sind hauptsächlich die folgenden Sachverhalte relevant:

Übermittlung für Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr oder zur Durchsetzung öffentlich-rechtlicher Ansprüche in Höhe von mindestens 500 €.

§ 68 Abs. 1,  
§ 74a Abs. 1  
SGB X

An die vorher genannten Stellen dürfen folgende Daten übermittelt werden:

- Name, Vorname
- Geburtsdatum, Geburtsort
- derzeitige Anschrift der betroffenen Person
- Namen und Anschriften ihrer derzeitigen Arbeitgeber
- derzeitiger oder zukünftiger Aufenthaltsort

Der ansonsten zwischen Behörden geltende Amtshilfeanspruch auf weitergehende Auskünfte gilt im Sozialversicherungsbereich nicht.

Zu den Behörden der Gefahrenabwehr zählen u.a. Feuerwehr, Rettungsdienste, soweit diese in öffentlicher Hand sind.

Eine Anfrage bezüglich des derzeitigen oder zukünftigen Aufenthaltsorts ist nur sechs Monate gültig.

Um die Aufenthaltsermittlung von Kindern und Unterhaltsschuldnern zu erleichtern, darf im Einzelfall der derzeitige Aufenthalt einer betroffenen Person an die zuständige Behörde übermittelt werden.

§ 68 Abs. 1a  
SGB X

§ 68 Abs. 2  
SGB X

Erhält die AOK ein Übermittlungser-suchen, hat der Leiter bzw. die Leiterin der AOK, sein bzw. ihre Stellvertreter/-in oder eine besonders bevollmäch-tigte bedienstete Person über das Ersuchen zu entscheiden und dabei zu prüfen, ob der Übermittlung schutz-würdige Belange der betroffenen Per-son entgegenstehen.

Die Verfahrensweise ist in den einzel-nen AOKs im Datenschutzhandbuch erläutert. Erkundigen Sie sich deshalb bei Ihrer AOK über die dort getroffe-nen Regelungen.

- eine gesetzliche Aufgabe des Ab-senders
- eine gesetzliche Aufgabe des Emp-fängers
- die Durchführung eines gerichtlichen Verfahrens einschließlich Strafver-fahrens

In diesen Fällen dürfen alle vorhan-denen Daten übermittelt werden. Vor der Übermittlung medizinischer Daten ist das Widerspruchsrecht der be-troffenen Person (§ 76 Abs. 2 SGB X) zu beachten (vgl. Punkt 4.4.3.1 dieses Lernbriefs).

§ 68 Abs. 3  
Satz 1 SGB X

Zur Unterstützung der nach Bundes-oder Landesrecht zulässigen Raster-fahndung wurde eine weitergehende Befugnis ins Gesetz aufgenommen. Danach dürfen folgende Angaben mit übermittelt werden:

- Angaben zur Staats- und Religionszugehörigkeit
- Angaben früherer Anschriften der bzw. des Betroffenen
- Namen und Anschriften früherer Arbeitgeber der betroffenen Person
- Angaben über an die betroffene Person erbrachte oder demnächst zu erbringende Geldleistungen

#### **Übermittlung für die Erfüllung sozia-ler Aufgaben**

§ 69 Abs. 1  
Nr. 1, 2  
SGB X

Dieses ist der häufigste Über-mittlungstatbestand. Er stellt den reibungslosen Ablauf des Daten-austauschs zwischen den Sozialleis-tungsträgern sicher. Wichtig hierbei ist, dass dieses ausschließlich für die im § 35 SGB I definierten Absender und Empfänger gilt. Im zweiten Ab-satz sind weitere Stellen aufgelistet, die denen für die Datenübermittlung gleichgestellt sind. Hier ist die Über-mittlung zulässig für:

Weiterhin ist geregelt, dass Arbeit-gebern ausschließlich die Dauer bzw. Fortdauer der Arbeitsunfähigkeit sowie die Anrechnung von Vorerkran-kungen mitgeteilt werden darf. Die Übermittlung von Diagnosedaten an den Arbeitgeber ist nicht zulässig.

Soll im Rahmen einer intensiven Kran-kengeldfallbetreuung ein weiterge-hender Kontakt mit dem Arbeitgeber aufgenommen werden, so ist unbe-dingt vorher eine schriftliche Einver-ständniserklärung der versicherten Person einzuholen.

#### **Hinweis**

Private Krankenversicherungsunter-nehmen sind keine Stellen nach § 35 SGB I.

Auch wenn in einer Satzungsregelung gemäß § 194 Abs. 1a SGB V die Ver-mittlung privater Zusatzleistungen mit einer privaten Krankenversicherung vereinbart wurde, so ergeben sich da-tenschutzrechtlich hierdurch keine Son-derregelungen und somit auch **keine** generelle Übermittlungsbefugnis.

§ 69 Abs. 4  
SGB X

### Beispiel

Ein privates Unternehmen (z.B. Bank, Versicherung, Arbeitgeber) fordert bei der AOK Daten an und legt eine Einverständniserklärung der versicherten Person vor.

### Folge

Nur wenn die Einverständniserklärung der bzw. des Versicherten aus freier Entscheidung erfolgte, ist die Datenübermittlung zulässig.

### Hinweis

Wenn Zweifel bestehen, ob diese Einverständniserklärung tatsächlich freiwillig erfolgt ist (eventuell bei Abschluss einer Lebensversicherung), aber aus Kundenfreundlichkeit die Auskunft nicht verweigert werden soll, ist es ein akzeptierter Weg, der versicherten Person die Auskunft zuzuschicken. Sie kann dann selbst entscheiden, ob sie die Daten weitergibt.

### Übermittlung für die Erfüllung besonderer gesetzlicher Pflichten und Mitteilungsbefugnisse

§ 71 Abs. 1  
Satz 1 Nr. 3  
SGB X

Wichtig ist insbesondere die Übermittlungsbefugnis an die Finanzbehörden. Diese ist zulässig zur Sicherung des Steueraufkommens nach § 22a Abs. 4 EStG und den §§ 93, 97, 105, 111 Abs. 1 und 5 und § 116 der Abgabenordnung (AO, 1977), soweit diese Vorschriften unmittelbar anwendbar sind.

Nach derzeitiger Auffassung der staatlichen Datenschutzbeauftragten ist das z.B. bei Grundsteuern, Gewerbesteuern und Gemeindeabgaben nicht zutreffend.

Im Zweifelsfall sollte hier vor einer Übermittlung die Abstimmung mit der oder dem Datenschutzbeauftragten oder den regionalen Datenschutzansprechpersonen erfolgen.

### Merke

Entweder gibt es eine gesetzliche Grundlage oder eine rechtmäßige schriftliche Einverständniserklärung der betroffenen Person, damit Sozialdaten verarbeitet, genutzt oder übermittelt werden dürfen.

### 4.5.3.1 Einschränkung der Übermittlungsbefugnis bei besonders schutzwürdigen Sozialdaten

Medizinische Daten, sowie alle Daten, die einem besonderen Berufsgeheimnis (§ 203 StGB) unterliegen, sind durch die Krankenkassen genauso gut zu schützen, wie es auch von den Ärzten, Krankenhäusern oder auch Rechtsanwälten gefordert wird. Diese Daten dürfen nur nach den gleichen Regeln weitergegeben werden, wie sie auch für die oben genannten Personen gelten.

§ 76 SGB X

Eine Ausnahme gilt für Daten, die im Zusammenhang mit einer Begutachtung wegen der Erbringung von Sozialleistungen oder wegen der Ausstellung einer Bescheinigung übermittelt worden sind. Das gilt allerdings nur, wenn die betroffene Person rechtzeitig (vor Beginn des Verwaltungsverfahrens) auf das Widerspruchsrecht hingewiesen wurde und dieses dann nicht genutzt hat.

Ist die Einschaltung des Medizinischen Dienstes (MD) notwendig (§ 275 SGB V), gilt dieses Widerspruchsrecht nicht.

#### 4.5.3.2 Gewährleistungsziele der Datenschutzgrundverordnung (DSGVO)

Die Regelungen im Datenschutz dienen dem Schutz der Rechte und Freiheiten von natürlichen Personen, konkret den Betroffenen. Die DSGVO systematisiert die Anforderungen zur Gewährleistung des Schutzes der Betroffenen durch Ableitung sogenannter Gewährleistungsziele. Diese Gewährleistungsziele verorten sich im Art. 5 DSGVO und sind auch bekannt als „Schutzziele“ des Datenschutzes. Die systematische Darlegung beschreibt der Gesetzgeber als Grundsätze für die Verarbeitung personenbezogener Daten und ist wie folgt gegliedert:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Diese Gewährleistungsziele müssen von Beginn an und damit bereits bei der Konzeption (u.a. eines Geschäftsprozess, einer Weiter-/Neuentwicklung) berücksichtigt werden. Die Gewährleistungsziele sind bei der Verarbeitung von personenbezogenen Daten grundsätzlich einzuhalten, da jede Verarbeitung von personenbezogenen Daten Risiken bergen. Diesen Risiken sind mit geeigneten technisch-organisatorischen Maßnahmen (TOM) zu begegnen (Risikoanalyse in Form der Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO).

Der Begriff „geeignet“ wurde bewusst gewählt und soll den Fokus darauf richten, bei der Ableitung TOM mit Bedacht vorzugehen und bereits bei der Entwicklung oder Justierung der Grundeinstellung (gemäß Art. 25 DSGVO) auf die Wirksamkeit und auf die Aktualität bzw. den Stand der Technik (gemäß Art. 32 DSGVO) zu achten.

Alle ergriffenen und mit Bedacht und Sorgfalt ausgewählten TOM dienen der risikoarmen respektive sicheren Verarbeitung personenbezogener Daten (Datensicherheit) und damit schlussendlich dem Schutz der Freiheiten und Rechte der Betroffenen (Datenschutz).“

#### 4.5.3.3 Technische und organisatorische Maßnahmen (TOM) zur Datensicherheit

Die Erläuterung im Gesetzestext ist sehr global gehalten, daher werden im Folgenden zum besseren Verständnis zu jedem Bereich Beispiele genannt. Die Ausgestaltung ist in jeder Krankenkasse unterschiedlich, da fast immer mehrere Maßnahmen den gleichen Schutzzweck erfüllen und die Verfahren jeweils an die genauen Erfordernisse vor Ort angepasst sind.

##### 1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet oder genutzt werden, zu verwehren.

### Beispiele

- Festlegung der Zutrittsberechtigten Personen
- Zutrittsregelungen für betriebsfremde Personen
- Einsatz Chipkarten anstelle Schlüssel
- Videoüberwachung
- Verschluss der EDV-Räume
- Protokollierung der Zutritte und Abgänge

## 2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

### Beispiele

- EDV-Nutzung nur mit bestimmter User-ID
- Sicherung der Bildschirmarbeitsplätze (Bildschirmschoner mit Kennworteingabe)
- Abschottung interner Netzwerke (LAN, Intranet, usw.) gegen ungewollte Zugriffe von außen (Firewall)
- Verschlüsselung der Übertragungsleitungen

## 3. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

### Beispiele

- Absicherung der Bereiche, in denen Datenträger aufbewahrt werden (Datenträgerarchiv)
- benutzerbezogene EDV-Zugriffsrechte (Rollen und Berechtigungen)
- Protokollierung der User und deren EDV-Aktivitäten
- Kontrolle der Systemadministratoraktivitäten
- Protokollierung des Zugriffs auf bestimmte Dateien
- Abschottung interner Netze
- Kopierkontrolle
- datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger

## 4. Weitergabekontrolle

Es ist zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist.

### Beispiele

- Prüfung der Zulässigkeit der Übermittlung
- Festlegung der Übermittlungswege und der Datenempfänger
- Protokollierung der Datenübermittlung und der Empfänger
- Dokumentation
- Datenverschlüsselung
- regelmäßige Auswertung der Protokollierung
- Beauftragung zuverlässiger Transportunternehmen
- Verwendung verschließbarer Transportbehälter/Einschreiben

#### 5. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

##### **Beispiele**

- Protokollierung von Eingabe, Veränderung und Löschung personenbezogener Daten
- Speicherung von Benutzer, Datum, Uhrzeit, PC und Grund der Eingabe, Veränderung oder Löschung
- digitale Signatur

#### 6. Auftragskontrolle

Es ist zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können.

##### **Beispiele**

- schriftlicher Vertrag nach § 80 SGB X
- klare Abgrenzung der Rechte und Pflichten zwischen Auftragnehmenden und Auftraggebenden
- sorgfältige Auswahl des Auftragnehmenden
- Definition von Sicherheitsmaßnahmen
- Kontrolle der vertragsgemäßen Durchführung
- Sanktionen bei Vertragsverletzung

#### 7. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind.

##### **Beispiele**

- regelmäßige Datensicherung
- Brandschutz
- Katastrophenvorsorge (Notfallrechenzentrum)
- Virenschutz
- ausschließlicher Einsatz von geprüfter Hard- und Software
- Mitarbeiterschulung auf aktuellem Stand
- Durchführung von Risikoanalysen für den gesamten EDV-Bereich

#### 8. Zweckbindungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden können.

##### **Beispiele**

- Dokumentation des Datenerhebungszwecks und der entsprechenden Programme
- Pseudonymisierung der Daten
- eindeutige Dienstanweisungen für die Datenverarbeitung und -nutzung
- datenschutzfreundliche Anwendung des Data Warehousing und Data Mining

#### 4.5.4 Betroffenenrecht

Kapitel 3 der DSGVO befasst sich mit den Betroffenenrechten. So ist ein Betroffener transparent u.a. über den Verantwortlichen, die Zwecke und die Rechtsgrundlage für die Verarbeitung zu informieren. Zudem müssen (falls vorhanden) die Kontaktdaten des Datenschutzbeauftragten sowie auf das Beschwerderecht gegenüber der zuständigen Aufsichtsbehörde hingewiesen werden. (Art. 13 DSGVO)

Zudem besteht ein Recht auf Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18) und auf Datenübertragbarkeit (Art. 20).

Gemäß Art. 12 DSGVO, sind die Betroffenenrechte innerhalb eines Monats zu bedienen. Die Frist kann um zwei Monate verlängert werden, unter Berücksichtigung der Komplexität der Anfrage.

§ 81 ff. SGB X konkretisieren die Betroffenenrechte im Kontext der Sozialdatenverarbeitung.

Da die AOK auf Landesebene organisiert ist, ist in der Regel die datenschutzbeauftragte Person des entsprechenden Bundeslandes (staatliche Aufsicht für den Datenschutz) zuständig.

Zur Regelung eines eventuellen Schadenersatzes wird auf die §§ 7, 8 des Bundesdatenschutzgesetzes verwiesen.

§§ 25, 83  
SGB X

Möchte jemand Auskunft über die zu seiner Person bei der AOK gespeicherten Daten bekommen, so ist ihm auf Antrag grundsätzlich unentgeltlich Auskunft zu erteilen über:

- die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten beziehen
- die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden
- den Zweck der Speicherung

Hierbei ist allerdings abzuwägen, ob eventuell überwiegende Geheimhaltungsinteressen einer dritten Person der Auskunftserteilung entgegenstehen. Die Ablehnung einer Auskunft muss nicht begründet werden.

#### 4.5.5 Umgang mit Datenschutzverstößen

Um zu klären, welche Maßnahmen bei Verstößen gegen den Datenschutz zu ergreifen sind, muss i.d.R. die datenschutzbeauftragte Person der AOK bereits beim Verdacht eines Datenschutzverstoßes informiert werden.

§ 83a SGB X,  
Art. 33, 34  
DSGVO

Stellt eine in § 35 SGB I genannte Stelle fest, dass bei ihr gespeicherte personenbezogener Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdige Interessen der betroffenen Person, hat sie dies möglichst binnen 72 Stunden der zuständigen Aufsichtsbehörde, der zuständigen Datenschutzaufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung der betroffenen Person muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen



Maßnahmen enthalten. Soweit die Benachrichtigung der betroffenen Person einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der betroffenen Person gleich geeignete Maßnahme ein.

§§ 85, 85a  
SGB X,  
§§ 41, 42  
BDSG

Im SGB X ist auch festgelegt, wie Verstöße gegen den Datenschutz zu ahnden sind. Hier wird zwischen Ordnungswidrigkeiten und Straftaten unterschieden.

Wichtig hierbei ist, dass die Strafandrohung jeweils nur für nicht allgemein zugängliche Daten gilt (Ausnahme: Weitergeben an Dritte, entgegen des Zweckbindungsgebots).

Weiterhin gilt als Ordnungswidrigkeit auch die weitergehende, zweckentfremdete Nutzung bei Stellen außerhalb des Bereichs des § 35 SGB I, denen Sozialdaten rechtmäßig übermittelt wurden und fehlende bzw. zu späte Bestellung einer datenschutzbeauftragten Person.

Bereits Fahrlässigkeit reicht in diesen Fällen für eine Bestrafung aus und kann hohe Geldbußen verursachen.

§ 42 Abs. 2  
BDSG

Wenn man eine der vorher genannten vorsätzlichen Handlungen entweder gegen Bezahlung oder in der Absicht jemanden zu schädigen bzw. sich zu bereichern durchführt, wird aus der Ordnungswidrigkeit eine Straftat, die mit bis zu zwei Jahren Freiheitsstrafe geahndet werden kann.

Hat eine Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt die verantwortliche Person vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

§ 35 DSGVO

Bei der Durchführung der Datenschutzfolgenabschätzung (DSFA) muss der bzw. die Datenschutzbeauftragte beratend eingebunden werden.

Insbesondere bei der Anzeige von Sozialdatenverarbeitungen im Auftrag nach § 80 SGB X fordern die Rechtsaufsichten die Vorlage der durchgeführten DSFA.

#### 4.6 Gewährleistungsziele des Datenschutzes

Die Regelungen im Datenschutz dienen dem Schutz der Rechte und Freiheiten von natürlichen Personen, konkret den Betroffenen. Die DSGVO systematisiert die Anforderungen zur Gewährleistung des Schutzes der Betroffenen durch Ableitung sogenannter Gewährleistungsziele. Diese Gewährleistungsziele verorten sich im Art. 5 DSGVO und sind auch bekannt als „Schutzziele“ des Datenschutzes. Die systematische Darlegung beschreibt der Gesetzgeber als Grundsätze für die Verarbeitung personenbezogener Daten und ist wie folgt gegliedert:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, - Transparenz
- Zweckbindung
- Datenminimierung

- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Diese Gewährleistungsziele müssen von Beginn an und damit bereits bei der Konzeption (u.a. eines Geschäftsprozess, einer Weiter-/Neuentwicklung) berücksichtigt werden. Die Gewährleistungsziele sind bei der Verarbeitung von personenbezogenen Daten grundsätzlich einzuhalten, da jede Verarbeitung von personenbezogenen Daten Risiken bergen. Diesen Risiken sind mit geeigneten technisch-organisatorischen Maßnahmen (TOM) zu begegnen (Risikoanalyse in Form der Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO).

Der Begriff „geeignet“ wurde bewusst gewählt und soll den Fokus darauf richten, bei der Ableitung TOM mit Bedacht vorzugehen und bereits bei der Entwicklung oder Justierung der Grundeinstellung (gemäß Art. 25 DSGVO) auf die Wirksamkeit und auf die Aktualität bzw. den Stand der Technik (gemäß Art. 32 DSGVO) zu achten.

Alle ergriffenen und mit Bedacht und Sorgfalt ausgewählten TOM dienen der risikoarmen respektive sicheren Verarbeitung personenbezogener Daten (Datensicherheit) und damit schlussendlich dem Schutz der Freiheiten und Rechte der Betroffenen (Datenschutz).

#### 4.7 Innerbetriebliche Datenschutzorganisation

Datenschutz ist ein äußerst wichtiger Aspekt, der in der heutigen digitalen Welt immer mehr an Bedeutung gewinnt. Unternehmen müssen sicherstellen, dass die Daten ihrer Kunden und Mitarbeiter angemessen ge-

schützt werden, um Vertrauen aufzubauen und rechtliche Anforderungen zu erfüllen.

Es ist daher von entscheidender Bedeutung, dass Unternehmen angemessene Maßnahmen ergreifen, um den Datenschutz zu gewährleisten und sicherzustellen, dass die Daten ihrer Kunden und Mitarbeiter geschützt sind.

Jeder Sozialleistungsträger, also auch jede Krankenkasse, muss eine oder einen Beauftragten für den Datenschutz bestellen. Dieser ist dem Vorstand direkt unterstellt. (§ 81 Abs. 4 Satz 1 SGB X; §§ 5,6 BDSG; Artikel 37, 38 DSGVO).

Der oder die Beauftragte für den Datenschutz hat den gesetzlichen Auftrag, die Einhaltung der DSGVO und der diese ergänzenden gesetzlichen Bestimmungen zu überwachen, die verantwortliche Stelle hinsichtlich der Einhaltung der gesetzlichen Regelungen zum Datenschutz zu beraten und zu unterstützen. Die Aufgaben des Datenschutzbeauftragten sind gesetzlich vorgegeben (Artikel 39 DSGVO).

Die vom Gesetzgeber geforderte Unterstützung des Beauftragten für den Datenschutz in räumlich getrennten Organisationseinheiten ist sicherzustellen (§ 81 Abs. 4 Satz 2 SGB X). Darüber hinaus können weitere Mitarbeitende benannt werden, die Mitarbeiter bei Fragestellungen zum Datenschutz unterstützen sowie auf die Einhaltung des Datenschutzes in einzelnen Organisationseinheiten achten. Im Bereich der AOK existieren hierzu unterschiedliche Organisationsstrukturen. Diese erfragen sie bei Ihrem/Ihrer Beauftragten für den Datenschutz oder entnehmen dies aus den AOK internen Medien.

Innerhalb der AOK-Gemeinschaft wurden in Arbeitsgruppen der Datenschutzbeauftragten einige Arbeitshilfen geschaffen, die das Tagesgeschäft vereinfachen sollen. Darunter fällt auch die Entscheidungshilfe zu Auskunftersuchen. In dieser wird zu den Standardanfragen, z.B. von Arbeitgebern, erläutert, was, wann und warum übermittelt bzw. nicht übermittelt werden darf. Details über diese und andere Arbeitshilfen und Leitlinien erhalten Sie bei Ihrem bzw. Ihrer Beauftragten für den Datenschutz.

### Hinweis

Oft sind es die kleinen Dinge im Arbeitsalltag, die zu Datenschutzpannen führen können. Unterstützen Sie Ihre AOK und Ihren oder Ihre Beauftragte für den Datenschutz, indem Sie bei der täglichen Arbeit einige Grundsätze berücksichtigen:

1. Machen Sie sich mit den internen Regelungen Ihrer AOK zum Datenschutz vertraut.
2. Achten Sie beim Brief auf die richtige Adressierung! Es muss auch darauf geachtet werden, dass die Daten im Text (Vorder- und Rückseite oder mehrseitige Briefe) mit denen der empfangenden Person übereinstimmen.
3. Nehmen Sie sich Besuchern und fremden Personen an! Begegnen Ihnen auf dem Flur eine Ihnen unbekannte Person, dann fragen Sie diese nach ihrem Namen und zu wem sie möchte. Wenn möglich begleite Sie die Person bis zu den zuständigen Mitarbeitenden. So tragen Sie dazu bei, dass Unbefugte nicht an Orte gelangen, an denen sie nichts verloren haben.

4. Lassen Sie keine Akten oder Unterlagen offen liegen! Spätestens nach Feierabend dürfen solche Unterlagen nicht mehr auf dem Schreibtisch zu finden sein und Aktenschränke müssen abgeschlossen werden. Schließlich gehen diese Unterlagen auch niemanden vom Reinigungspersonal etwas an (Stichwort: Clean-Desk-Policy). Entdecken Sie Unterlagen an Kopier- oder Faxgeräten, die dort vergessen wurden, dann kümmern Sie sich bitte darum, dass die Unterlagen zum zuständigen Mitarbeitenden gelangen.

### Merke

Die AOK muss sicherstellen, dass personenbezogene Daten sicher und vertraulich behandelt werden, um das Vertrauen ihrer Kunden und Mitarbeitenden zu gewinnen und zu erhalten. Die AOK ist gesetzlich verpflichtet, die Datenschutzbestimmungen einzuhalten und sicherzustellen, dass die Daten angemessen geschützt werden. Bei Verletzung des Datenschutzes kann die AOK mit rechtlichen Konsequenzen, Reputationsschäden und finanziellen Verlusten konfrontiert werden.

## 4.8 Risikoanalyse aus der Perspektive Datenschutz

Die Datenschutz-Folgenabschätzung (DSFA) ist ein zentrales Instrument der Datenschutz-Grundverordnung (DSGVO), das Unternehmen und Organisationen dabei unterstützt, die Risiken von Datenverarbeitungen für betroffene Personen frühzeitig zu erkennen und zu minimieren. Sie ist ins-

besondere dann erforderlich, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, etwa bei der umfangreichen Überwachung oder der Verarbeitung sensibler Daten. Deswegen sieht die DSGVO unabhängig von sonstigen Voraussetzungen für die Verarbeitung vor, dass durch geeignete Abhilfemaßnahmen, wie z.B. durch technische und organisatorische Maßnahmen (sog. TOMs) diese Risiken eingedämmt bzw. minimiert werden.

Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat (Artikel 35 Abs. 1 DSGVO). Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann.

Dabei bezieht sich die DSFA auf einzelne, konkrete Verarbeitungsvorgänge. Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen. Sollten mehrere ähnliche Verarbeitungsvorgänge voraussichtlich ein ähnliches Risiko aufweisen, können diese auch zusammen bewertet und in einer DSFA dargestellt werden. Ähnliche Risiken können z.B. dann gegeben sein, wenn ähnliche Technologien zur Verarbeitung vergleichbarer Daten (-kategorien) zu gleichen Zwecken eingesetzt werden.

Eine DSFA ist immer vor der Aufnahme bzw. Implementierung der zu betrachtenden Verarbeitungsvorgänge und ist auch bei bereits bestehenden

Datenverarbeitungsvorgängen durchzuführen. Ob allerdings eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge (Schwellwertanalyse). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass die Verarbeitungsvorgänge kein hohes Risiko aufweisen, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren (Nachweis- und Rechenschaftspflicht).

Die formellen Anforderungen an die Durchführung einer DSFA ergeben sich aus der DSGVO, speziell aus Artikel 35 sowie den dazugehörigen Erwägungsgründen (84, 90 - 93). An eine spezielle Form ist man nicht gebunden. Es hat sich in der Praxis jedoch etabliert die DSFA unter Zuhilfenahme eines in Excel erstellten Muster durchzuführen. Dieses Muster kann bei dem zuständigen Datenschutzbeauftragten in Ihrem Hause angefordert werden oder steht in den jeweiligen frei zugänglichen Medien (z.B. Sharepoint) zur Verfügung.

Eine DSFA enthält nach Artikel 37 Abs. 7 DSGVO zumindest die folgenden Inhalte:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Person und

- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird.

Die Erstellung einer DSFA ist kein einmaliger Vorgang. Sollten sich z.B. neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren ergeben, die in der DSFA bisher nicht berücksichtigt wurden, so ist diese zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassungen empfohlen.

Die DSFA ist immer von dem Fachverantwortlichen, in dessen Verantwortung die Verarbeitungsvorgänge durchgeführt werden, zu erstellen bzw. anzupassen. Der Fachverantwortliche holt bei der Durchführung der Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten ein (Artikel 35 Abs. 2 DSGVO).

Die DSFA ist ein sinnvolles Instrument zur systematischen Risikoeindämmung. Rechtzeitig auf den Weg gebracht hilft sie nicht nur, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen, sondern auch die Pflichten nach der DSGVO umzusetzen.

Die Verarbeitung von personenbezogenen Daten erfolgt in den allermeisten Fällen im Rechenzentrum der AOK, konkret bei dem IT-Dienstleister der Kasse. Allerdings besteht die Möglichkeit die Daten in eine andere Betriebsstruktur zu verarbeiten. Immer öfter werden für die Betriebsstruktur sogenannte Cloud-Betreiber herangezogen. Diese Dienstleister bietet die

Möglichkeit an, zentral und flexibel und skalierbar den Betrieb sicherzustellen und somit Aufwände für den eigenen Betrieb zu minimieren. Die Nutzung von derartigen Dienstleistern ist grundsätzlich möglich, jedoch verbleibt die Verantwortung für die Datenverarbeitung nach wie vor bei der AOK und somit sind auch die Anforderungen zum Datenschutz, allem voran die Wahrung der Gewährleistungsziele, zu beachten.

Wichtig ist bei der Auswahl eines Cloud-Betreibers bzw. der Nutzung von Cloud-Computing-Diensten (gemäß § 384 Nr. 5 SGB V) die Ausgestaltung wirksamer technisch-organisatorischer Maßnahmen (TOM) und die vertragliche Vereinbarung zur Umsetzung dieser ausgestalteten TOM sowie die Verarbeitung im Idealfall innerhalb der EU. Diese Informationen finden sich zumeist im Sicherheits-/ Datenschutzkonzept und in geeigneten Nachweisen (Zertifizierungen, Testaten) wieder. Folgende Nachweise sind von besonderer Relevanz:

- ISO 27001/701
- ISO 27017/018
- C5-Testat (Typ 2)

Datenschutz-Zertifizierungen gemäß Art. 42 DSGVO (z.B. EuroPrise, datenschutz cert)

Unbedingt zu betrachten ist, dass geschlossene Verträge mit dem Ziel der Verarbeitung von Sozialdaten der Aufsicht anzuzeigen sind (gemäß § 80 Abs. 3 SGB X) und eine sogenannte EXIT-Strategie ausgearbeitet werden sollte. Mit dieser Strategie sichert sich die AOK ab, sofern vertragliche Verpflichtungen (nicht nur vom Datenschutz) nicht ordnungsgemäß erfüllt werden zum Wechsel auf die ursprüngliche Betriebsstruktur.

## 4.9 Social Media und Datenschutz

Social Media ist eine Vielfalt digitaler Medien und Technologien, die es Nutzern ermöglicht, sich untereinander auszutauschen und mediale Inhalte einzeln oder in Gemeinschaft zu gestalten. Die Interaktion umfasst den gegenseitigen Austausch von Informationen, Meinungen, Eindrücken und Erfahrungen sowie das Mitwirken an der Erstellung von Inhalten.

Die AOK und wahrscheinlich auch Sie nutzen diese Medien. Aber aufgepasst, Social Media ist kein rechtsfreier Raum. Es gelten dieselben nachfolgenden Gesetze wie sonst auch.

Ohne ausdrückliche Einwilligung des Nutzers zur Kontaktaufnahme dürfen keine Nutzer über Social Media angesprochen und geworben werden.

Die grundlegenden Datenschutzanforderungen des SGB sowie der DSGVO gelten auch dann, wenn Sie dienstlich im Rahmen von Social Media aktiv sind.

Bei den AOKs gibt es diverse Richtlinien. Diese Richtlinien sollen den Mitarbeitenden Hilfestellungen geben. Es sind u.a. folgende Themen geregelt:

- vertrauliche Informationen dürfen nicht veröffentlicht werden
- erkennbares Auftreten als Privatperson oder in dienstlichen Interesse
- rechtliche Grundlagen müssen eingehalten werden

Ergänzend ist auf die „Netiquette“ zu achten.

Stellen Sie kein Material ins Intranet/ öffentliche Ordner, das von anderen Personen als anstößig, unangemessen oder respektlos angesehen werden könnte und greifen Sie auch auf kein solches Material zu.

Prüfen Sie vor dem Versand den/ die Empfängerinnen nochmals auf Korrektheit, damit Falschsendungen bei Namensgleichheiten vermieden werden (Datenschutz).

Schicken Sie keine Unterlagen (u.a. Anhänge) über Social-Media-Kanäle und nehmen Sie auch keine an.

Jede Person die bei der AOK arbeitet, ist im dienstlichen Rahmen als Nutzer von Social Media datenschutzrechtlich für die Verarbeitung ihrer/seiner eigenen personenbezogenen Daten und ggf. die anderer Personen verantwortlich, wenn sie/er diese z.B. in seinen Profilen oder auf der Pinnwand veröffentlicht. Die Nichteinhaltung der Datenschutzanforderungen, wie beispielsweise die Nichtwahrung des Sozialgeheimnisses, kann geahndet werden. Im schlimmsten Fall können Datenschutzverstöße arbeitsrechtliche- und strafrechtliche Folgen nach sich ziehen.

§ 35 SGB I

## 4.10 Übungen zum Lernabschnitt 4

### Übung 5

Beschreiben Sie, was unter dem Begriff „Informationelle Selbstbestimmung“ zu verstehen ist. Die Angabe von Rechtsvorschriften ist nicht erforderlich.

### Übung 6

Nennen Sie den Paragraphen, der die Grundlage des Sozialdatenschutzes darstellt und dessen Inhalt.

### Übung 7

#### Sachverhalt

Die Pressestelle einer Krankenkasse erhält einen Anruf von einem Journalisten. Ihm wurde eine CD mit Daten von Versicherten anonym zugespielt. Auf der CD sind Namen, Anschriften und Diagnosedaten (sog. Patientenquittung) gespeichert. Die Herkunft der Daten kann eindeutig dieser Krankenkasse zugeordnet werden. Es ist auch ein Schreiben beigelegt, dass diese Daten frei zugänglich im Internet aufrufbar sind.

#### Aufgabe

Stellen Sie sich vor, Sie würden einen solchen Anruf eines Journalisten erhalten. Welche Schritte müssen Sie einleiten. Welche rechtlichen Konsequenzen können sich aus dieser Datenpanne ergeben?

### Übung 8

Erläutern Sie, welche Daten zu welchen Zwecken zwischen AOK und Rentenversicherungsträger übermittelt werden dürfen. Die Angabe der Rechtsvorschriften ist nicht erforderlich.

### Übung 9

Erläutern Sie die Daten, die an Arbeitgeber übermittelt werden dürfen mit Angabe der Rechtsvorschrift.

### Übung 10

#### Sachverhalt

In einer Satzungsregelung einer AOK ist nach § 194 Abs. 1a SGB V die Vermittlung von Zusatzversicherungsverträgen mit einer privaten Krankenversicherung geregelt.

#### Aufgabe

Erläutern Sie, welche Besonderheiten bei der Datenübermittlung an diese Versicherung zu beachten sind mit Angabe der Rechtsvorschriften.

## 5 Zusammenfassende Selbstkontrolle

### Aufgabe 1

Nennen Sie zehn Möglichkeiten, welche Sie selbst zur Erhöhung der Datensicherheit in der AOK beitragen können.

### Aufgabe 2

Beurteilen Sie, ob in den folgenden Fällen die Daten übermittelt werden dürfen und ggf. welche Daten

#### Sachverhalt

Sie sind Auszubildender bei der „AOK – Die Gesundheitskasse.“ und erhalten von Ihrem Ausbildungsleiter folgende Anfragen (vgl. Anlagen 1 bis 5 auf den folgenden Seiten).

#### Hinweis zu Aufgabe 2

Fassen Sie Lösung und Begründung mit Angabe der Rechtsvorschriften zusammen.



Anlage 1.1 – Anfrage einer privaten Versicherung

<p>Postanschrift: Gesunda AG • Musterstr. 1 • 99999 Gesundstadt</p> <p>AOK – Die Gesundheitskasse Hermannstr. 37 56564 Neuwied</p> <p>Unsere Vers.-Nr.: 2004196088 Vers. Person: Max Manni geboren am: 15.01.1939 verstorben am: 07.12.2023</p> <p>Ihre Vers.-Nr.: leider nicht bekannt</p> <p>Sehr geehrte Damen und Herren,</p> <p>auf das Leben der o. g. versicherten Person bestand bei unserer Gesellschaft eine Risiko-Lebensversicherung.</p> <p>Um unsere Leistungspflicht prüfen zu können, benötigen wir von Ihnen eine Aufstellung der erbrachten Leistungen für den Zeitraum der letzten zehn Jahre.</p> <p>Eine Entbindungserklärung von der ärztlichen Schweigepflicht und die Einverständniserklärung der Ehefrau liegen in Kopie bei.</p> <p>Vielen Dank für Ihre Mithilfe.</p> <p>Mit freundlichem Gruß</p> <p></p> <p>Peter Meier</p> <p>Anlagen</p>	<p><b>Gesunda AG</b> <b>Lebensversicherungen</b></p> <p>Es schreibt Ihnen: Peter Meier</p> <p>Tel.: 01111 111011 Fax: 01111 111010</p> <p>Service-Zeiten: Mo.–Do. 8.00 Uhr – 19.00 Uhr Fr. 8.00 Uhr – 18.00 Uhr</p> <p>Gesundstadt, 16.01.2024</p> <p>Gesunda AG Vorstand: Rolf Bauer (Vorsitzender) Dr. Helmut Schneider Sitz der Gesellschaft: Musterstadt Handelsregister Amtsgericht Musterstadt B 4330</p>
--	---

Anlage 1.2 – Auszug aus dem Versicherungsvertrag

Ort und Datum <i>Neuwied, 02.01.97</i>	Begünstigte der Lebensversicherung: Brigitte Manni (Ehefrau)	Bei Minderjährigen: Unterschrift des gesetzlichen Vertreters
Unterschrift des Antragstellers (Versicherungsnehmers) <i>Max Manni</i>	Unterschrift der zu versichernden Person, wenn diese selbst nicht Antragsteller ist:	Unterschrift der mitversichernden Person bei Tarif E - PN

Anlage 1.3

**Gesunda AG**  
**Lebensversicherungen**

Postanschrift: Gesunda AG • Musterstr. 1 • 99999 Gesundstadt

**Einverständniserklärung**

Vers.-Nr.: 2004196088

Todesfall: Max Manni  
geboren am: 15. 01. 1939  
verstorben am: 07. 12. 2023

Auf das Leben meines Mannes bestand bei der Gesunda AG eine Lebensversicherung.  
Durch den Tod ist der Versicherungsfall eingetreten.

Damit die Gesunda AG ihre Leistungspflicht prüfen und die Auszahlung veranlassen kann,  
bitte und ermächtige ich die Ärzte, Krankenhäuser, Heilstätten, Krankenkassen, Ämter,  
Behörden und Versicherungsgesellschaften unter Hinweis auf § 35 SGB I sowie § 67 ff.  
SGB X der Gesunda AG, Einsicht in die Krankenakten zu gewähren. Es sind Angaben über  
die behandelnden Ärzte, die genauen Behandlungsdaten und Art der Beschwerden und  
Erkrankungen zu machen.

Name und Anschrift der zuständigen Krankenversicherung: AOK  
Hermannstr. 37  
56564 Neuwied

Dermbach, 04.01.2024  
(Ort, Datum)

B. Manni  
(Unterschrift der Ehefrau)

Anlage 2

<b>Bundeskriminalamt</b>			
Unser Zeichen	Fax-No. 0611 / 55 -	Nebenstelle 0611 / 55 -	Ort, Datum Wiesbaden 15.03.2024

---

<b>Telefax-Nachricht</b>	Seitenzahl (einschl. Deckblatt) - 1 -
--------------------------	--

---

An AOK Neustadt / Weinstr.  Fax: 06321 / 896100	Nr./Operator/Uhrzeit
--	----------------------

Betreff  
Ermittlungsverfahren der STA Saarbrücken AZ K-520 gegen Pfiffig GmbH  
u.a. wegen Verdacht der Bildung einer kriminellen Vereinigung, illegaler Arbeitnehmerüberlassung, illegaler  
Beschäftigung, Betrug zum Nachteil der Sozialversicherung, u.a.

hier: Auskunftersuchen gem. § 161 StPO i.V.m. § 69 Abs. 1 Nr. 2 SGB X bzgl. der Offenbarung von  
Sozialdaten

Sehr geehrte Damen und Herren,

zum o.g. Ermittlungsverfahren ersuchen wir Sie um Übermittlung von Sozialdaten zu folgender Firma,  
gegen die sich die Ermittlung, insbesondere wegen Betrugs zum Nachteil der Sozialversicherungsträger, richtet:

Firma: Pfiffig GmbH  
Anschrift: Cleverstr. 99, 11111 Musterstadt

Wir bitten um Übersendung folgender Unterlagen:

Liste sämtlicher Arbeitnehmer seit 01/2014 bzw. Kontoeröffnung  
monatliche Beitragsnachweise seit 01/2014 bzw. Kontoeröffnung  
Höhe der Beitragssätze für die entsprechenden Erhebungszeiträume

An:

Bundeskriminalamt  
Referat 999  
65173 Wiesbaden

Anlage 3.1

<hr style="border: 1px solid black;"/> <b>Betona</b> <b>Bauzentrum</b> <hr style="border: 1px solid black;"/>		<div style="border: 1px solid black; padding: 2px; display: inline-block;">Ihr Partner für Haus und Heim</div>
		Betona GmbH Musterstr. 10 12345 Musterdorf
<b>Telefax</b>		
<hr style="border: 0; border-top: 1px solid black;"/>		
Seite:		Es schreibt Ihnen:
Empfänger:		
Firma:	<u>AOK</u>	Herr / Frau:
In:	<u>Musterdorf</u>	Tel. Durchwahl
z. Hd.	<u>Hr. Muster</u>	Musterdorf, den 20.02.2024
<hr style="border: 0; border-top: 1px solid black;"/>		
Sehr geehrte Damen und Herren,		
wir beabsichtigen, Fritz Fleißig ab 01.04.2023 in unserem Hause zu beschäftigen. Hierzu wäre es von Vorteil, eine Rückmeldung über die jüngsten Krankheiten zu erhalten. Eine entsprechende Vollmacht folgt.		
Vielen Dank für Ihre Bemühungen		
<div style="display: flex; justify-content: space-between;"><div style="width: 40%;">Betona Bauzentrum Musterstr. 10 12345 Musterdorf</div><div style="width: 30%; text-align: center;">Konto Sparkasse Musterdorf BLZ 111 11 11 Konto 22 22</div><div style="width: 30%; text-align: right;">Geschäftsführer: Heinrich Muster HR Musterdorf HR 3 0</div></div>		

Anlage 3.2

Ich entbinde die Krankenkasse von den Auswirkungen des Bundesdatenschutzgesetzes sowie einer eventuellen Schweigepflicht gegenüber der Betona GmbH, Musterstr. 10, 12345 Musterdorf, bezüglich einer Auskunft über Krankheitszeiten innerhalb der letzten 36 Monate.

Name: Fleißig, Fritz  
Vers.-Nr.: 123 456 789  
Wohnort: Musterdorf  
Geboren: 12.02.1966

Musterdorf, den 08.03.2024

Fleißig  
(Unterschrift)

Anlage 4

<p style="text-align: center;"><b>Pfennig</b></p> <hr/> <p style="text-align: center;"><b>INKASSO</b></p>	<p style="text-align: right;"><small>Als Inkassobüro zugelassen</small></p>
---	---

<p><b>VERTRAULICH</b></p> <p>An AOK Rhein-Hunsrück Gartenstr. 1 55469 Simmern</p>	<p><small>Bearbeiter: Telefon-Durchwahl: Postadresse:</small></p> <p style="text-align: right;"><small>Postfach 10 10 88888 Musterhausen</small></p>
---	--

**Inkasso-Nummer:**

Bitte immer mit angeben!

Musterhausen, den 18.01.2024

Abgetretene Forderung  
gegen Frau Lydia Maier – Anschrift unbekannt

Sehr geehrte Damen und Herren,

gegen Ihre Versicherte machen wir o. g. Forderung geltend.

Um Frau Lydia Maier Kosten zu ersparen, bitten wir, folgende Fragen zu beantworten  
(nicht Zutreffendes ist zu streichen) und das Formular zurückzusenden.

1. Ist oben Genannte/r bei Ihnen im Leistungsbezug?	Ja / Nein
2. Erkennen Sie Abtretungen an?	Ja / Nein
3. Liegen Vorpfändungen vor?	Ja / Nein

Falls ja, bitten wir um Mitteilung von wann die Vorpfändung/Abtretungen datieren	.....
Restbetrag der vorrangigen Pfändungen:	€ .....
Der monatlich pfändbare Betrag beträgt:	€ .....

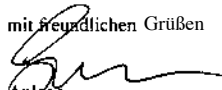
  

4. Bitte geben Sie uns die aktuelle Anschrift bekannt.

5. Bitte geben Sie auf der Rückseite dieses Briefs Ihre genaue Firmierung an.

Für Ihre Bemühungen im Voraus dankend verbleiben wir

mit freundlichen Grüßen



Anlage  
Rückumschlag

Anlage 5

Allgemeine Ortskrankenkasse  
Wittlich  
Beethovenstraße  
54516 Wittlich

**Polizeipräsidium**

Musterdorf  
Polizeiinspektion  
Musterstr. 100  
12345 Musterdorf  
Telefon:  
Telefax:  
Vorgangsnummer:  
Sachbearbeiter:  
Musterdorf, den 16.02.2024

Ermittlung wegen unerl. Entfernen v. Unfallort

Sehr geehrte Damen und Herren,

am 31.01.2023 ereignete sich in Musterdorf ein Verkehrsunfall mit erheblichem Sachschaden. Der verantwortliche Fahrzeugführer entfernte sich anschließend von der Unfallstelle, wobei das Kennzeichen des Fahrzeugs abgelesen werden konnte.  
Ein Fahrzeugführer konnte bisher nicht ermittelt werden.

Nach dem derzeitigen Stand der Ermittlungen kommt als verantwortlicher Fahrzeugführer nur ein Angehöriger/Beschäftigter der Firma Pfiffig in Betracht.  
Die Ermittlungen in der Firma blieben bisher erfolglos.

In Abstimmung mit der Staatsanwaltschaft Musterdorf bitten wir Sie, uns eine Liste der Firmenangehörigen der o.a. Firma zu übersenden.

Bei dem Straftatbestand des unerlaubten Entfernen vom Unfallort handelt es sich um eine schwerwiegende Straftat, an deren Aufklärung ein besonderes öffentliches Interesse besteht. Derzeit sind andere Möglichkeiten zur Ermittlung der Betriebsangehörigen nicht erkennbar.

Mit freundlichen Grüßen

  
Hauptkommissar

## 6 Lösungen zu den Übungen im Text

### Lösungen zu 1

Der Datenschutz schützt die personenbezogenen Daten.

Die Informationssicherheit umfasst alle schützenswerten Informationen im Unternehmen und hat damit einen breiteren Fokus als der Datenschutz.

### Lösung zu 2

Das Passwort stellt die einzige Sicherheit dar, die Sie davor schützt, dass sich Unbefugte nicht unter Ihrer USER-ID anmelden können. Wenn jemand Ihr Passwort kennt und sich unter Ihrer Kennung anmeldet, wird alles was er macht unter Ihrem Namen protokolliert. Dies kann beträchtliche Folgen haben.

### Lösung zu 3

Folgende Regeln sollten Sie im Umgang mit Passwörtern beachten:

- Wechseln Sie direkt nach der erstmaligen Anmeldung an einem EDV-System oder Programm Ihr Passwort.
- Verwenden Sie keine Trivialpasswörter (z.B. AOK, Sommer, Montag, September) oder Bezüge zu Ihrem Namen oder Ihren Familienangehörigen.
- Nutzen Sie die maximale Passwortlänge, die Ihr EDV-System zulässt, zwölf Zeichen sollten Minimum sein.
- Schreiben Sie Ihr Passwort nirgendwo auf (unter der Tastatur oder am Bildschirm schaut jeder nach).
- Geben Sie Ihr Passwort nicht an Kolleginnen oder Kollegen, Teammitgliedern oder Führungskräften weiter. Auch die EDV benötigt diese Kenntnis nicht, um Ihnen im Fehlerfall helfen zu können.

- Sollten Sie den Verdacht haben, dass jemand Kenntnis von Ihrem Passwort hat, wechseln Sie sofort das Passwort.

### Lösung zu 4

Die Gewährleistung der Datensicherheit kann u.a. durch Verwendung nur geschützter Übertragungswege oder Nutzung vom Arbeitgeber zugelassener IT-Lösungen sichergestellt werden. Auch durch das Sperren des Bildschirms beim Verlassen des Arbeitsplatzes oder der Entsorgung nicht mehr benötigter Unterlagen über die entsprechenden Papiertonnen kann die Datensicherheit gewährleistet werden.

### Lösung zu 5

Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig.

### Lösung zu 6

§ 35 SGB I ist die Grundlage des Sozialdatenschutzes und enthält folgenden Inhalt:

- Definition Sozialgeheimnis
- Geheimhaltungspflicht innerhalb des Leistungsträgers
- Mitarbeiterdatenschutz
- Wahrung auch nach Ende des Beschäftigungsverhältnisses
- Gleichstellung von Betriebs- und Geschäftsgeheimnissen mit personenbezogenen Daten
- Schutz auch für Verstorbene



## Lösung zu 7

Unverzüglich informieren Sie den Geschäftsführer und die datenschutzbeauftragte Person. Des Weiteren sind über die IT-Abteilung unverzüglich Maßnahmen einzuleiten, dass die Daten im Internet gelöscht bzw. geschützt werden. In einem weiteren Schritt ist die Datenpanne unverzüglich bei der Aufsicht anzuzeigen und die Betroffenen sind zu informieren. Es ist auch nicht auszuschließen, dass die Presse über diesen Vorfall berichtet und ein Imageschaden entsteht. Dies kann wiederum Auswirkungen auf vertriebliche Aktivitäten haben.

## Lösung zu 8

Die Deutsche Rentenversicherung Bund ist ein Sozialleistungsträger im Sinne des § 35 SGB I.

Zwischen Sozialleistungsträgern dürfen grundsätzlich alle Daten ausgetauscht werden, die für eine gesetzliche Aufgabe der AOK oder der Deutschen Rentenversicherung Bund benötigt werden. Die einzige Einschränkung ist bei medizinischen Daten, da es sich hierbei um besonders schützenswerte Sozialdaten handelt.

## Lösung zu 9

§ 69 Abs. 4 SGB X

Die Krankenkassen sind befugt, einem Arbeitgeber mitzuteilen, ob die Fortdauer einer Arbeitsunfähigkeit oder eine erneute Arbeitsunfähigkeit eines Arbeitnehmenden auf derselben Krankheit beruht. Die Übermittlung von Diagnosedaten an den Arbeitgeber ist nicht zulässig. Somit ist jegliche weitere Datenübermittlung untersagt.

## Lösung zu 10

Datenschutzrechtlich gibt es keine Sonderregelung, wenn eine Vermittlung von Zusatzleistungen mit einer privaten Krankenversicherung vereinbart wurde oder nicht. Private Versicherungen sind keine Sozialleistungsträger im Sinne des § 35 SGB I. Somit existiert keine gesetzliche Übermittlungsbefugnis.

Die Datenübermittlung ist daher nur mit schriftlicher Einwilligung des Versicherten möglich, wobei die Bedingungen von § 67b Abs. 2 SGB X zu beachten sind (§ 67b Abs. 1 Satz 1 SGB X).



## 7 Lösungen zur zusammenfassenden Selbstkontrolle

### Lösung zu 1

Möglichkeiten, wie zur Erhöhung der IT-Sicherheit in der AOK beigetragen werden kann:

- anvertraute personenbezogene Daten nur im Rahmen der Aufgabenstellung erheben, verarbeiten (speichern, verändern, übermitteln, sperren, löschen) oder nutzen
- bei der Übertragung von Sozialdaten (z.B. Diagnosen/Befunde) nur geschützte Übertragungswege (nach Möglichkeit zusätzlich verschlüsselt) wählen
- auf dem lokalen Datenträger (Festplatte, USB-Stick) – sofern es nicht zum Aufgabenbereich gehört – keine personenbezogenen Daten speichern, solange eine Festplattenverschlüsselung nicht umgesetzt ist
- anvertraute Datenträger, wenn nicht unmittelbar daran gearbeitet wird, unter Verschluss halten
- PC und Anwendungen keinem Unbefugten zugänglich machen
- Passworte niemandem, auch nicht der Vertretung bekannt geben
- vor dem Verlassen des Büros den PC sperren (Tastenkombination Windows-Taste + L) oder eine sichere „Pausenschaltung“ benutzen
- nicht mehr benötigte Datenträger datenschutzgerecht vernichten, damit eine missbräuchliche Weiterverwendung nicht möglich ist
- zur Verarbeitung personenbezogener Daten ausschließlich solche Hard- und Software-Produkte einsetzen, die vom Arbeitgeber für diesen Zweck vor- und freigegeben sind.
- nichtfreigegebene, unlizenzierte Software sowie Public Domain Programme nicht nutzen; Shareware und Freeware nicht einsetzen; das gilt auch für Programme, die aus dem oder über das Internet beschafft werden

- an der bereitgestellten Hardware keinerlei Veränderung vornehmen
- Software und Daten nicht unbefugt an Dritte weitergeben
- beim mobilen Einsatz von Laptops (ausgedockt) die erfassten Daten bei nächst möglicher Gelegenheit (eingedockt) auf dem Server sichern

### Hinweis

Es waren lediglich zehn Möglichkeiten zu nennen.

### Lösung zu 2

#### Anfrage der privaten Versicherung

#### (Anlage 1.1 – 1.3)

Eine private Versicherung (auch Krankenversicherung) stellt keinen Sozialleistungsträger im Sinne des § 35 SGB I dar, somit gibt es keinen gesetzlichen Grund für eine Übermittlung. Die Auskunft ist grundsätzlich unzulässig.

Eine Ausnahmemöglichkeit besteht bei einer Einverständniserklärung der versicherten Person (§ 67b Abs. 1 Satz 1 SGB X, Art. 6 Abs. 1 Buchst. a DSGVO). In diesem Fall ist der Versicherte bereits verstorben.

Nach § 35 SGB I gilt der Sozialdatenschutz für Verstorbene weiter. Somit darf auch hier grundsätzlich keine Auskunft erteilt werden.

Es liegt jedoch eine Einverständniserklärung der Ehefrau des Verstorbenen vor. Bei einer vorliegenden Einverständniserklärung dürfen nur die Daten bzw. Daten für den genannten Zeitraum (hier: Aufstellung der erbrachten Leistungen der letzten zehn Jahre) übermittelt werden, die konkret in der Erklärung aufgelistet

sind. Hier sind dies Angaben über die behandelnden Ärzte, die genauen Behandlungsdaten und die Art der Beschwerden und Erkrankungen.

#### **Hinweis**

Voraussetzung ist weiterhin, dass die Ehefrau auch die erbberechtigte Person ist. Es bleibt deshalb noch zu klären, ob die Ehefrau erbberechtigt ist. Sind die Voraussetzungen erfüllt, wäre eine Übermittlung der Daten zulässig.

#### **Anfrage des Bundeskriminalamts (Anlage 2)**

Grundsätzlich gilt hier § 68 Abs. 1 Satz 1 SGB X, das heißt, es dürfen ausschließlich Adressdaten des Versicherten und seines aktuellen Arbeitgebers übermittelt werden. In diesem Fall handelt es sich allerdings um die Unterstützung zu einem Strafverfahren wegen Sozialleistungsmissbrauchs. Damit greift § 69 Abs. 1 Nr. 2 SGB X. Danach dürfen grundsätzlich alle benötigten Daten übermittelt werden. Die Einschränkungen durch § 76 Abs. 2 SGB X sind zu beachten.

In diesem Fall dürfen die Daten übermittelt werden.

#### **Anfrage des Arbeitgebers (Anlage 3.1 – 3.2)**

Grundsätzlich greift hier § 69 Abs. 4 SGB X. Somit wäre die Auskunft unzulässig. Hier liegt allerdings eine Einverständniserklärung des Versicherten vor. Es greift deshalb § 67b Abs. 1 Satz 1 SGB X. Danach wäre eine Übermittlung zulässig. In diesem Fall geht man allerdings davon aus, dass es keine freie Entscheidung des Versicherten war.

Die Übermittlung ist damit unzulässig.

#### **Hinweis**

Eine Übermittlung direkt an den Versicherten ist zulässig (§ 83 SGB X).

#### **Anfrage des Inkasso-Unternehmens**

##### **(Anlage 4)**

Das Inkasso-Unternehmen stellt keinen Sozialleistungsträger im Sinne des § 35 SGB I dar, noch handelt es sich um die Durchsetzung öffentlich-rechtlicher Ansprüche. Somit liegt kein Übermittlungstatbestand nach den §§ 67e bis 75 SGB X vor. Eine Einverständniserklärung des Versicherten liegt ebenfalls nicht vor.

Die Übermittlung ist damit unzulässig.

#### **Anfrage der Polizei (Anlage 5)**

Grundsätzlich gilt für Anfragen der Polizei § 68 Abs. 1 Satz 1 SGB X; danach dürfen bestimmte Angaben zu einer Person übermittelt werden. Es handelt sich hier jedoch nicht um die Anfrage zu einer Person, sondern es sollen die Adressdaten aller Arbeitnehmer einer Firma übermittelt werden. Diese Art der Anfrage erfüllt nicht die Voraussetzungen des § 68 Abs. 1 Satz 1 SGB X (Personenbezug).

Die Übermittlung ist damit unzulässig.