



## Datenschutz – Menschen, Prozesse, IT-Systeme

In den vergangenen Monaten wurde durch Pressenachrichten deutlich, dass das Thema Datenschutz auch bei den Krankenkassen wiederholt vernachlässigt wurde. Die Vorkommnisse bewirken eine Verunsicherung der Versicherten, Nachrichten über die Offenbarung von Sozialdaten wirken sich zunehmend negativ auf die Öffentlichkeitsarbeit der Krankenkassen aus. Zugriffsrechte werden bei den Krankenkassen häufig unkontrolliert vergeben, gegenüber dolosen Handlungen ist man nicht ausreichend geschützt. Leicht können Beschäftigte Versichertendaten an Konkurrenten oder private Versicherungen veräußern. Auch die Auslagerung von Aufgaben auf Dritte führt zu einer Überlassung von sehr sensiblen Sozialdaten an private Dienstleister. Grund genug, sich den Aufgaben des externen und internen Datenschutzes zu stellen. Vorstand und IT-Leiter haften bei Vorsatz und grober Fahrlässigkeit auch persönlich. Insoweit besteht die Notwendigkeit, dass den Verantwortlichen der Nachweis gelingt, durch Vorkehrungen aktiv gehandelt zu haben. Hierzu haben die Krankenkassen im Zuge ihres Information-Sicherheits-Management-Systems (ISMS) regelmäßig Audits bei sich und ihren externen Dienstleistern, die Sozialdaten verarbeiten, durchzuführen. Die Novellierung II des BDSG (in Kraft ab dem 1. September 2009) führte zu weitreichenden Konsequenzen, auch die Krankenkassen hatten ihre Datenschutzrichtlinien und Maßnahmen zu überarbeiten. Udo Polaszek

## Rechtliche Rahmenbedingungen

Im August 2008 wurde der Verbraucherzentrale in Schleswig-Holstein eine CD mit 17.000 Kundendaten und Bankverbindungen übergeben. Der Skandal um den Missbrauch von Millionen sensibler Kundendaten sorgte für großes Aufsehen in der Bevölkerung. Die Politik reagierte umgehend mit der Novellierung des Bundesdatenschutzgesetzes (BDSG). Bei der Angleichung der internen Richtlinien und Dienstanweisungen sollten die Krankenkassen auch beachten, dass neue technische Möglichkeiten die Risiken der Datenoffenbarung bzw. des -verlustes erhöht haben. Mit einfachen Datenspeichern (Sticks, CD, DVD) können sensible Massendaten (Sozialdaten, Geschäftsgeheimnisse) kopiert, offenbart und veräußert werden. Durch DV-gestützte Geschäftsprozesse (Workflow) entstanden neue Gefahren durch die fehlerhafte oder missbräuchliche Verwendung sensibler Informationen. Diese neuartigen Risiken erhöhten das Bedürfnis nach eindeutigen und nachvollziehbaren Regelungen bei den Sozialversicherungsträgern.

Anders als die Bezeichnung Datenschutz vermuten lässt, dient sie nicht dem Schutz von Daten, sondern von Persönlichkeitsrechten.

Doch zunächst ein Rückblick. Das Datenschutzrecht ist noch jung, seine Anfänge liegen in den 60er-Jahren des vergangenen Jahrhunderts. Anders als die Bezeichnung Datenschutz vermuten lässt, dient der Datenschutz nicht dem Schutz von Daten, sondern dem Schutz von Persönlichkeitsrechten. Dem Datenschutzrecht liegt die Idee zugrunde, dass jeder Mensch grundsätzlich selbst entscheiden darf, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Insofern soll das Datenschutzrecht den Einzelnen vor den Gefahren schützen, die durch einen unkontrollierten Umgang mit persönlichen Daten drohen. In letzter Konsequenz soll der „gläserne Mensch“ verhindert werden, insbesondere, wenn Sozialdaten betroffen sind.

Von entscheidender Bedeutung für die Entwicklung des deutschen Datenschutzrechts war die als „Volkszählungsurteil“ bekannte Entscheidung des Bundesverfassungsgerichts aus dem Jahr 1983. In diesem Urteil hob das Gericht die „informationelle Selbstbestimmung des Einzelnen“ in den Rang eines Grundrechts.

Das Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistet insoweit die Befugnis des Einzel-

nen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nur zulässig, wenn sie im überwiegenden Allgemeininteresse erforderlich sind und eine gesetzliche Grundlage haben. Dementsprechend gelten für den Umgang mit personenbezogenen Daten die folgenden Grundsätze:

- **Datenvermeidung und Datensparsamkeit:** Die Datenverarbeitung hat sich an dem Ziel auszurichten, keine oder möglichst wenige personenbezogene Daten zu verwenden.
- **Erforderlichkeit:** Die Erforderlichkeit der Nutzung personenbezogener Daten muss nachweisbar sein.
- **Zweckbindung:** Personenbezogene Daten dürfen grundsätzlich nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Eine Verarbeitung für andere Zwecke bedarf der gesonderten Ermächtigung.

Zu den personenbezogenen Daten zählen unmittelbar mit einer Person verknüpfte Angaben wie Name, Vorname, Geburtsdatum, Geschlecht, Familienstand oder Adresse ebenso wie medizinische Informationen (z. B. die Blutgruppe und Laborwerte) oder berufliche Daten (z. B. Personalnummer, Vergütungsgruppe, Beurteilungen und Zeugnisse). Krankenkassen haben die Vorschriften des SGB X zum Sozialdatenschutz vorrangig zu beachten.

## Abgrenzung Datenschutz und Datensicherheit

Datensicherheit und Datenschutz ergänzen sich, stehen aber auch in einem Spannungsfeld zueinander. So ist der Schutz der Vertraulichkeit ein wesentliches Informationssicherheitsziel und von grundlegender Bedeutung für diejenigen Daten, auf die der Datenschutz gerichtet ist. Datenschutzziele lassen sich ohne angemessene Sicherheitsmaßnahmen nicht erreichen; insofern setzt Datenschutz Datensicherheit voraus. Umgekehrt bringen die Erfordernisse des Datenschutzes aber auch Beschränkungen für die möglichen Sicherheitsmaßnahmen mit sich. Dies trifft immer dann zu, wenn Protokollierungen und Überwachungen auf ein datenschutzgerechtes Ausmaß begrenzt werden müssen.

Entsprechend gibt es damit sowohl Überschneidungen als auch Konfliktfelder in den Tätigkeitsbereichen von Datenschutz- und IT-Sicherheitsbeauftragten, deren Aufgabe die Unterstützung der Geschäftsführung bei der Erarbeitung von Sicherheitszielen und der Behandlung von Unternehmensrisiken aus der Informationstechnik ist. Zwischen bei-

den Zuständigkeiten empfiehlt sich folglich eine enge Zusammenarbeit, um mögliche Konfliktfelder von vorneherein zu begrenzen und von der Kompetenz des jeweils anderen im eigenen Zuständigkeitsbereich zu profitieren. Bei einer Ausübung der Tätigkeiten des Datenschutz- und des IT-Sicherheitsbeauftragten in Personalunion sind diese potenziellen Konfliktlagen zu berücksichtigen.



Bei der Übermittlung von Daten jeglicher Art soll künftig immer von der Möglichkeit sicherer Verschlüsselung Gebrauch gemacht werden.

### **Novellierung des BDSG**

Das BDSG ist 2009 durch Gesetzesbeschlüsse des Deutschen Bundestages mit drei Novellen geändert worden. Am 29. Mai 2009 hat der Bundestag mit der „Novelle I“ (BT-Drs. 16/13219, 16/10581) die Tätigkeit von Auskunfteien und ihrer Vertragspartner (insbesondere Kreditinstitute) sowie das Scoring neu geregelt. Am 10. Juli 2009 hat der Bundesrat die sogenannte BDSG-Novelle II (in Kraft ab dem 1. September 2009) verabschiedet. Einen Tag zuvor hatte der Bundestag mit der „Novelle III“ als kleinen Unterpunkt im Rahmen des Gesetzes zur Umsetzung der EU-Verbraucherkreditrichtlinie den § 29 BDSG um zwei Absätze erweitert. Von besonderer Bedeutung für die Sozialversicherungsträger ist die Datenschutznovelle II von 2009, die u. a. zu Änderungen in den folgenden Bereichen führte:

#### **Datenverschlüsselung**

Bei der Übermittlung von Daten jeglicher Art soll künftig immer von der Möglichkeit sicherer Verschlüsselung Gebrauch gemacht werden. Ferner sind Daten zu anonymisieren, sobald es der Zweck zulässt. Die Unternehmen unterliegen somit einer Sorgfaltspflicht.

#### **Stärkung der Rechte des Datenschutzbeauftragten**

Bisher ist der interne Datenschutzbeauftragte arbeitsrechtlich allein durch ein Benachteiligungsverbot und eine erschwerte Abberufung geschützt. Mit der Novellierung des BDSG stellt der Gesetzgeber den Kündigungsschutz des Datenschutzbeauftragten privilegierten Funktionsträgern aus anderen Bereichen (z. B. Betriebsrat) gleich. Dieser Kündigungsschutz wird auf ein Jahr nach der Abberufung des internen Datenschutzbeauftragten erweitert.

Zur Wahrnehmung seiner Pflichten muss sich der interne Datenschutzbeauftragte permanent fortbilden. Das Unternehmen oder die Behörde muss die Teilnahme an Fortbildungen ermöglichen und die entstehenden Kosten übernehmen.

#### **Auftragsdatenverarbeitung**

Werden personenbezogene Daten nicht durch die Behörde, sondern durch Dritte (Outsourcing) verarbeitet, wird von Auftragsdatenverarbeitung gesprochen. Mit der Novellierung des BDSG wird vom Auftraggeber vor der Erteilung eines Auftrags zur Auftragsdatenverarbeitung gefordert, die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen zu überprüfen. Bei längerfristigen Verträgen zur Auftragsdatenverarbeitung sind diese Prüfungen in regelmäßigen Intervallen zu wiederholen. Als Nachweis gegenüber den Aufsichtsbehörden sind die Prüfungen zu dokumentieren. Die Anforderungen an den Vertrag zur Auftragsdatenverarbeitung werden in einem 10-Punkte-Katalog (siehe nachfolgend Outsourcing) konkretisiert. Danach müssen diese Punkte schriftlich in dem Vertrag behandelt werden. Verstöße gegen die Pflicht, Datenverarbeitungsaufträge ordnungsgemäß und in Übereinstimmung mit dem überarbeiteten § 11 BDSG zu erteilen, können mit einem Bußgeld von bis zu 50.000€ geahndet werden.

#### **Arbeitnehmerdatenschutz**

Als Reaktion auf verschiedene Datenschutzvorfälle der jüngsten Vergangenheit wird eine Grundregel zum Arbeitnehmerdatenschutz eingeführt, die vor allem die eigenständige Aufklärung von Straftaten durch Unternehmen behindert. So werden beispielsweise präventive Maßnahmen zur Korruptionsbekämpfung verboten. Weiterhin darf ein Arbeitgeber, um etwaigen Rechtsverstößen in seinem Unternehmen oder in seiner Behörde nachzugehen, nur dann aktiv werden, wenn die im Gesetz beschriebenen Voraussetzungen gegeben sind. Diese Vorgaben sind inhaltlich jedoch bereits ohnehin geltendes Recht und stellen somit keine wesentlichen Neuerungen dar.

### Mitteilungspflichten

Besondere Risiken wird für die Wirtschaft eine weitere Neuerung mit sich bringen. Zukünftig werden Unternehmen und Behörden die Datenschutzaufsichtsbehörden und die Betroffenen über Datenschutzverstöße informieren müssen. Diese Pflicht bezieht sich auf besonders sensible, personenbezogene Daten. Die Mitteilung an die zuständigen Stellen hat grundsätzlich unverzüglich zu erfolgen. Die Meldung an den Betroffenen erfolgt im Rahmen einer verantwortungsvollen Offenlegung. Dies bedeutet, dass der Betroffene erst informiert werden darf, wenn ein etwaiger polizeilicher Ermittlungserfolg durch die Informierung nicht mehr gefährdet wird.

Für alle Behörden stellt sich die Frage nach den „schwerwiegenden Beeinträchtigungen der Rechte des Betroffenen“ im Sinne des § 42a BDSG. Wenn diese Frage nicht eindeutig beantwortet werden kann, sollte vorsorglich die Mitteilung an die zuständige Behörde erfolgen, um ein mögliches empfindliches Bußgeld zu vermeiden.

### Erhöhung der Bußgelder

Künftig sind bei einfachen Verstößen gegen das Bundesdatenschutzgesetz Bußgelder bis zu 50.000€ und bei schwerwiegenden Verstößen Bußgelder bis zu 300.000€ möglich. Wenn Verstöße zu weitergehenden Gewinnen führen, kann das Bußgeld entsprechend erhöht werden.

Bei der Verhängung von Bußgeldern gegen eine Behörde wird die Frage der Haftung unweigerlich gestellt werden. In diesem Zusammenhang ist auch der Verweis des § 82 SGB X auf die §§ 7 und 8 BDSG von Bedeutung. Wenn ein Sozialversicherungsträger einem Betroffenen durch unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Sozialdaten einen Schaden zufügt, entsteht ein Schadenersatzanspruch gegenüber der Behörde unabhängig von einem Verschulden.

### Durchführung von regelmäßigen Audits

Jede Behörde sollte im Zuge ihres Information-Sicherheits-Management-Systems (ISMS) regelmäßig Audits bei sich und ihren Dienstleistern, die Sozialdaten bzw. sensitive Informationen verarbeiten, durchführen. Für die Sozialversicherungsträger bestand diese Notwendigkeit bereits seit längerer Zeit durch die Regelung in § 78c SGB X.

In der Praxis werden Audits jedoch oft vernachlässigt. Durch die Novellierung des BDSG werden Audits zumindest bezüglich personenbezogener Daten gesetzlich gefordert. Ein derartiges Audit muss entsprechend geplant und umgesetzt werden.

Auch einige Landesdatenschutzgesetze fordern Audit-Verfahren. In Nordrhein-Westfalen wird das Verfahren durch § 10a DSGVO NRW auch weiter konkretisiert: „Die öffentlichen Stellen können zur Verbesserung von Datenschutz und Datensicherheit sowie zum Erreichen größtmöglicher Datensparsamkeit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen.“

Aufgrund dieser rechtlichen Vorgaben ist nicht auszuschließen, dass Gerichte das Fehlen von Datenschutzaudits als grobe Fahrlässigkeit bewerten.

Zukünftig müssen Unternehmen und Behörden die Datenschutzaufsichtsbehörden und die Betroffenen über Datenschutzverstöße informieren.

### IT-Grundschutzhandbuch des BSI

Das IT-Grundschutzhandbuch des BSI (Bundesamt für Sicherheit in der Informationstechnik) bietet eine wertvolle Hilfestellung für die Analyse und Bewertung der IT-Sicherheit und die kontinuierliche Umsetzung von Standard-Sicherheitsmaßnahmen bei der täglichen Arbeit. Neben konkreten Maßnahmen wird auch der Prozess beschrieben, mit dem Defizite erkannt und dauerhaft beseitigt werden können. Das IT-Grundschutzhandbuch umfasst neben einer Vielzahl von Sicherheitskriterien und konkreten Maßnahmenvorschlägen für die Behebung von Missständen auch eine Methodenbeschreibung, wie ein angemessenes IT-Sicherheitsniveau erreicht und aufrechterhalten werden kann. Es orientiert sich an den klassischen Zielen der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) und stellt nicht nur kritische Fragen, sondern liefert auch Antworten, wie gefundene Defizite beseitigt werden können. Mit seiner Hilfe können Soll- und Ist-Zustand des IT-Systems genau und sehr detailliert be- und fortgeschrieben werden.

Ausgangspunkt der Anwendung des Grundschutzhandbuches ist die Initiierung des IT-Sicherheitsprozesses, der zunächst übergreifende (strategische) IT-Sicherheitsziele festlegen und ein Sicherheitsmanagement einrichten muss. Verantwortlich für die Initiierung ist die Leitungsebene.

Die Aufgabe des Sicherheitsmanagements besteht zunächst in der Erstellung des Sicherheitskonzeptes. Nach ei-

ner Abschätzung von Schadensauswirkungen wird festgelegt, welchen Schutzbedarf die einzelnen Elemente der IT-Struktur haben (z. B. niedriger Schutzbedarf bei nur begrenzten Schadenswirkungen bis hin zu sehr hohem Schutzbedarf, wenn die Schadensauswirkungen ein katastrophales Ausmaß erreichen können).

Anschließend wird die IT-Struktur mithilfe von Bausteinen des Grundschutzhandbuches modelliert. Diese Bausteine enthalten auch Soll-Vorgaben für Sicherheitsmaßnahmen. Ein Basis-Sicherheitscheck (Soll-Ist-Vergleich) deckt Lücken einer unzureichenden Umsetzung von Sicherheitsmaßnahmen auf und findet Bereiche, in denen (etwa wegen eines erhöhten Schutzbedarfes) eine zusätzliche Sicherheitsanalyse nötig ist. Durch den Soll-Ist-Vergleich werden gleichzeitig die nötigen, aber derzeit nicht umgesetzten Sicherheitsmaßnahmen erkannt und es kann ein Realisierungsplan (mit Prioritätensetzung) erstellt werden.

In der Umsetzungsphase werden fehlende Maßnahmen gemäß dem Realisierungsplan umgesetzt. Wichtig sind Fortschreibung des Konzeptes und Umsetzung dieser Fortschreibung auch im laufenden Betrieb.

Das IT-Grundschutzhandbuch ist auf die Belange des Sozialversicherungsträgers anzupassen. Anlässlich einer Datenschutztagung in Berlin führte Tobias Niemann, Vorstand der HBSN AG, hierzu aus: „Vorhandene Konzepte und Vorgehensmodelle, wie die BSI-Grundschutzertifizierung oder die Zertifizierung nach DIN 27001, decken die Prozesse und den individuellen Handlungsrahmen der gesetzlichen Krankenversicherung nicht vollständig ab. Auf der Grundlage eines speziellen Praxishandbuches für Aufbau, Zertifizierung und nachhaltige Umsetzung kann die Entwicklung eines praxismgerechten Information-Security-Management-Systems (ISMS) erfolgen. Zur Einschätzung der Risiken und Festlegung der Maßnahmen wird zunächst eine relativ unaufwändige Analyse durchgeführt. In Abhängigkeit von den Ergebnissen können der Aufwand und die Dauer bis zur Zertifizierung bestimmt werden.“

## **Prägnante Problemstellungen in der Krankenversicherung**

### **Datenverarbeitung im Auftrag (Outsourcing)**

Die Wettbewerbskriterien führen immer häufiger zur Auslagerung von Aufgaben der Sozialversicherungsträger auf Arbeitsgemeinschaften und Dritte. Die Grundanforderung des Gesetzgebers aus § 197b SGB V, „Wesentliche Aufgaben zur Versorgung der Versicherten dürfen nicht in Auftrag gegeben werden“, bleibt dabei häufig außer Betracht. Da-

tenschutzbeauftragte beanstanden häufig, dass wegen fehlender Aufgabenbeschreibung eine unzulässige Funktionsübertragung stattfindet.

Wenn eine Institution die Verarbeitung personenbezogener Daten an einen externen Dienstleister auslagert, bleibt die Institution für den Datenschutz verantwortlich. Sie hat sicherzustellen, dass Rechtsanwendungen, die die Krankenkasse betreffen, auch von dem Auftragnehmer beachtet werden. Die Institution muss den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählen und sich vor der Erteilung eines Auftrags und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers überzeugen. Der Auftraggeber sollte die Zeitabstände der Prüfung von der Sensibilität der Daten sowie dem Verhalten des Auftragnehmers abhängig machen. Die Erhebungen sollten mindestens alle zwei Jahre stattfinden, bei vermutetem Fehlverhalten eines Auftragnehmers entsprechend kürzer.

In diesem Zusammenhang ist es für den Auftraggeber von Vorteil, wenn der Auftragnehmer ein Zertifikat über die Einhaltung der Datenschutzrichtlinien vorweisen kann.

Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

- der Gegenstand und die Dauer des Auftrags,
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die nach Abs. 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Die Anpassungen des BDSG zur Datenverarbeitung im Auftrag werden durch das 3. Gesetz zur Änderung des SGB IV und anderer Gesetze aktuell in den § 80 SGB X übernommen.

Der Auftragnehmer darf die Daten ferner nur im Rahmen der Weisungen des Auftraggebers und für den vorgegebenen Zweck erheben, verarbeiten oder nutzen.

Aus dem Vertrag muss sich zweifelsfrei ergeben, welche Rechte und Pflichten die einzelnen Vertragspartner haben (Pflichtenheft). Im Vertrag sollte für die ausgelagerten Tätigkeiten dezidiert beschrieben sein, wer (Krankenkasse/Auftragnehmer) welche Aufgaben wahrzunehmen hat.

Es sollte darauf geachtet werden, dass die richtigen Bezeichnungen verwandt werden (z. B. „persönliche Daten“ stellt kein Synonym für „Sozialdaten“ dar etc.). Die von dem Auftragnehmer/von der Krankenkasse geschuldete Leistung sollte so exakt wie möglich beschrieben werden (Leistungsgegenstand, -umfang, -ort, -zeit). Hierzu gehört beispielsweise auch, dass Gesetze, Verordnungen, Verträge etc., die vom Auftragnehmer bei der Aufgabenerfüllung zu beachten sind, genannt werden. Nur so ist sichergestellt, dass die ausgelagerte Aufgabe komplett beschrieben wird. Auslegungsbedürftige oder -fähige Begriffe sind darüber hinaus zu vermeiden oder im Vertrag zweifelsfrei zu erklären.

Die Anpassungen des BDSG zur Datenverarbeitung im Auftrag werden durch das 3. Gesetz zur Änderung des SGB IV und anderer Gesetze aktuell in den § 80 SGB X übernommen.



Der Sozialversicherungsträger kann seiner Verantwortung nur gerecht werden, wenn er das Recht hat, dem Dritten hinsichtlich der Durchführung der Aufgaben Weisungen zu erteilen. Würde der Krankenkasse im Vertrag ein solches Recht nicht eingeräumt, bliebe ihr bei Meinungsverschiedenheiten mit dem Dritten nur die zeitaufwändige gerichtliche Auseinandersetzung.

Der Sozialversicherungsträger muss auch das Recht haben, die Geschäftsräume, in denen der Auftragnehmer für ihn Aufgaben wahrnimmt, jederzeit betreten zu können, von dem Auftragnehmer bzw. seinem Personal die Auskünfte und Unterlagen zu fordern und zu erhalten und auf die elektronische Datenverarbeitung des Auftragnehmers zugreifen zu können, sofern dies für seine Prüfungen erforderlich ist. Dieses Recht muss sich auch auf die Aufsichtsbehörden und Prüfdienste erstrecken.

Auch für die Zeit nach Beendigung des bestehenden Vertragsverhältnisses müssen diese Rechte Bestand haben. Der Auftragnehmer muss sich auch für die Zeit nach Beendigung des Vertragsverhältnisses zur Geheimhaltung der im Rahmen der Auftragsdurchführung erlangten Sozialdaten verpflichten.

Wurde die Einschaltung von Subunternehmern durch den Auftragnehmer vereinbart, muss sichergestellt sein, dass alle Anforderungen und Rechte auch für diese gelten.

### Zugriffsberechtigung

Die Vergabe von Zugriffsrechten sowie deren Prüfung stellt auch in den aktuellen Standardverfahren ein Problem für die Krankenversicherungsträger dar.

Viele Vorstände sind entsetzt, wenn sie erfahren, dass ein großer Teil der Mitarbeiter Zahlungen anweisen und freigeben kann. Noch extremer ist die Vergabe von Administrationsrechten. Nicht selten werden bei einer Krankenkasse 50 Personen und mehr diese umfassenden Rechte eingeräumt. Auch die Rechenzentren lassen sich derartige Rechte sichern. So kann auch von außen weitgehend unbemerkt auf sensible Daten zugegriffen werden. Datensicherheit und Datenschutz sind bei derartig fahrlässiger Handlungsweise erheblich gefährdet.

Die eingesetzten Standardverfahren tragen nicht zur Transparenz hinsichtlich der vergebenen Zugriffsrechte bei. Unübersichtliche Tabellensteuerungen und Rollenkonzepte machen die Prüfungen aufwändig, differenzierte Programmkenntnisse sind erforderlich, um die Rechtmäßigkeit zu beurteilen. Durch Selektionsprogramme und verbessertes Reporting sollten die Revisionsmöglichkeiten verbessert werden.

## Datenadministration

Durch den Einsatz von Selektionsprogrammen werden in den Krankenkassen sensible Listen erzeugt. Es muss verhindert werden, dass diese Daten anderen Personen unzulässig übermittelt werden. Bei der Absicherung sind u. a. die Zuweisung der Drucker, die Versendung von Massendaten per E-Mail sowie die Möglichkeit, Daten auf Speichermedien zu kopieren, einzubeziehen.

Datenträger müssen immer verschlossen aufbewahrt werden. In den sensiblen Bereichen muss ein Vier-Augen-Prinzip gewährleistet sein. Die Funktionen Programmierung, Systemverwaltung und Operating/Arbeitsvorbereitung sind auf jeden Fall zu trennen. Die Anforderungen an die Geschäftsprozesse sind in einem Organisationshandbuch darzulegen.

## Sichere E-Mail-Kommunikation

Die Nutzung von E-Mail führt zu Sicherheitsproblemen, der unbedachte Umgang kann auch zur Offenbarung von Sozialdaten bzw. zum Missbrauch führen.

Das Bundesamt für Sicherheit in der Informationstechnik hat zwei neue Schriften zur E-Mail-Sicherheit veröffentlicht. Die beiden Dokumente thematisieren die „Sichere Nutzung von E-Mail“ und den „Sicheren Betrieb von E-Mail-Servern“. Die Studie (ISi-S) zum E-Mail-Client beschreibt, wie bestehenden Gefährdungen bei normalem Schutzbedarf mit geeigneten Maßnahmen begegnet werden kann. Diese Maßnahmen beziehen sich dabei auf eine sichere Architektur des E-Mail-Clients, eine geschützte Anbindung an den E-Mail-Server und einen sicheren Austausch von Informationen zwischen den einzelnen Kommunikationspartnern.

Darüber hinaus wird empfohlen, eine E-Mail-Richtlinie zu erstellen, die beschreibt, wie sich Anwender bei der Nutzung von E-Mail zu verhalten haben. Für den sicheren Austausch von Informationen zwischen den einzelnen Kommunikationspartnern sollten Verfahren zur Verschlüsselung und zur Erstellung digitaler Signaturen von E-Mails verwendet werden. Weiterhin ist sicherzustellen, dass Dateien mit schutzwürdigen Daten nicht an unbefugte Stellen übersandt werden.

## Kooperation mit privaten Krankenkassen

Nach der Gesetzesbegründung zu § 194 Abs. 1a SGB V soll den Krankenkassen die Möglichkeit der Kooperation mit einem Unternehmen der privaten Krankenversicherungswirtschaft gegeben werden. Gegenstand der Kooperation soll die Vermittlung zwischen den Versicherten der Krankenkasse und den Versicherungsunternehmen sein. Damit soll



Es ist sicherzustellen, dass Dateien mit schutzwürdigen Daten nicht an unbefugte Stellen übersandt werden.

dem Wunsch der Versicherten entsprochen werden, ergänzende Versicherungen abschließen zu können. Fraglich ist, welche Datenverarbeitung im Rahmen dieser Vermittlungstätigkeit zulässig ist, insbesondere, welche Daten von den Kassen an das private Unternehmen weitergegeben werden dürfen.

Die Vermittlung von privaten Zusatzversicherungen stellt eine neue Aufgabe der gesetzlichen Krankenkassen als Sozialleistungsträger dar. Insoweit sind die Vorschriften des Sozialdatenschutzes (§ 35 SGB I, §§ 67 ff. SGB X, SGB V) anzuwenden. Die Krankenkasse ist nicht Auftragnehmerin und wird auch nicht privatrechtlich als Vermittlerin tätig, sondern als öffentlich-rechtliche Vermittlerin für die privaten Versicherungen.

Die Krankenkasse darf bei ihrer Vermittlungstätigkeit auf den aktuellen Versichertenbestand zurückgreifen (§§ 186 ff. SGB V). Daten, die unter Umständen bei den Krankenkassen ausschließlich zum Zweck der Weiterleitung (Renten-, Arbeitslosenversicherung) erhoben werden, werden von der Vermittlungsbefugnis nicht mit umfasst. Die Erhebung von Adressaten ist unzulässig, wenn ausschließlich das Ziel verfolgt wird, Zusatzversicherungen zu vermitteln.

Genutzt werden dürfen Daten wie Name, Vorname, Anschrift, Geburtsdatum, Geschlecht, Versicherungsart/Angaben zu Familienversicherung. Eine Erforderlichkeit für die Nutzung der Krankenversicherungsnummer besteht nicht. Sollen darüber hinausgehend im Rahmen der Vermittlung

weitere Daten zwischen den Versicherungsunternehmen und der Krankenkasse ausgetauscht werden, so bedarf es hierfür einer ausdrücklichen Einwilligung des oder der Betroffenen.

Die Rechtsvorschrift begründet keine direkte Übermittlungsbefugnis. Übermittlungen von der Kasse an das private Versicherungsunternehmen müssen vielmehr durch die Einwilligung des Kassenmitglieds bzw. durch den Vermittlungsantrag mit diesem legitimiert werden.

### IT-Risikomanagement zur Konvergenz von Datenschutz und Datensicherheit

Im Rahmen des Finanzcontrollings sind die Krankenkassen gehalten, ein Risikomanagementsystem einzuführen.<sup>1</sup> Derartige Systeme eignen sich auch für die Aufnahme und Bewertung von Risiken im Bereich des Datenschutzes. Das Thema Datenschutz als Bestandteil eines unternehmensinternen Risikomanagements hat in den letzten Jahren zunehmend an Bedeutung gewonnen.

Die Krankenkasse hat nach der Implementierung eines Risikomanagements die Schritte der Risikoanalyse für den Bereich Datenschutz festzulegen:

- Erstellung der Gefährdungsübersicht.
- Ermittlung zusätzlicher Gefährdungen: Es ist für jedes Zielobjekt zu prüfen, ob weitere Gefährdungen zu berücksichtigen sind, die sich aus dem spezifischen Einsatzszenario ergeben.
- Es ist eine Gefährdungsbewertung für jedes Zielobjekt vorzunehmen und für jede Gefährdung zu prüfen, ob die bislang vorgesehenen Sicherheitsmaßnahmen einen ausreichenden Schutz bieten.

Für jedes nicht hinreichend abgesicherte Risiko entscheidet die Leitung, wie mit ihm zu verfahren ist:

- **Risiko-Reduktion:** durch Ergänzung der Sicherheitsmaßnahmen.
- **Übernahme des Risikos:** Die Risiken werden akzeptiert, weil die Gefährdung nur unter äußerst speziellen Bedingungen zu einem Schaden führen könnte, keine hinreichend wirksamen Gegenmaßnahmen bekannt sind oder der Aufwand für mögliche Schutzmaßnahmen unangemessen hoch wäre.
- **Risiko-Transfer:** Die Risiken werden verlagert. Durch Abschluss von Versicherungen oder durch Auslagerung der risikobehafteten Aufgabe an einen externen Dienstleister kann z. B. ein möglicher finanzieller Schaden auf Dritte abgewälzt werden.
- **Risiken beobachten:** Sollten bei der Risikoanalyse Gefähr-

dungen identifiziert werden, die zukünftig riskant werden können, sollten vorsorglich ergänzende Sicherheitsmaßnahmen vorbereitet werden.

### Kompensierende Kontrollen (Compensating Controls) und ISMS

Sicherheitsmaßnahmen gliedern sich bekanntermaßen in organisatorische und technische Bereiche. Wichtig hierbei ist, dass die organisatorischen und technischen Sicherheitsmaßnahmen ineinandergreifen und sich gegenseitig unterstützen. Neben einem funktionierenden Information-Sicherheits-Management-System (ISMS), mit den entsprechenden Prozessen und Sensibilisierungsmaßnahmen für die Mitarbeiter, können technische Hilfsmittel den Datenschutz unterstützen. Das ISMS ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Die Einführung eines ISMS wirkt dabei nach innen, die Zertifizierung nach außen.

Falls bei der Krankenkasse noch Defizite vermutet werden, sind kompensierende Kontrollen (Compensating Controls) zulässig.

Gemäß § 9a BDSG bzw. § 78c SGB X kann eine Behörde ihre technischen Einrichtungen sowie ihr Datenschutzkonzept durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das dabei erzielte Prüfergebnis ver-

Im Rahmen des Finanzcontrollings sind die Krankenkassen gehalten, ein Risikomanagementsystem einzuführen.



öffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung sowie das Verfahren selbst sind einem besonderen Gesetz vorbehalten, das auf Bundesebene noch nicht verabschiedet wurde.

Die Vorbereitung eines Audits geschieht auf der Grundlage des ISMS. Ein ISMS muss entsprechend geplant und umgesetzt werden. Dazu gehören u. a.

#### Erstellung einer Informationssicherheitsleitlinie

- Berücksichtigung der Anforderungen der elektronischen Gesundheitskarte (eGK) (in Vorbereitung)

#### Erarbeitung einer Schutzbedarfsanalyse

- Identifikation der Informationsobjekte
- Bestimmung von Schutzklassen in Anlehnung an das Sicherheitskonzept der gematik
- Identifizierung von Zielobjekten für die Risikoanalyse

#### Durchführung einer Risikoanalyse

- Identifizierung von Bedrohungen
- Definition von Schadenspotenzialen
- Definition von Eintrittswahrscheinlichkeiten

#### Erstellung von

- Datenschutz-,
- Datensicherheits-,
- Notfall- und
- Audithandbuch

#### Implementierung von

- Maßnahmen und Strukturen zur Sicherstellung der Nachhaltigkeit

#### Vorbereitung und Durchführung von

- internen und
- externen Audits

Das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein hat die folgende Checkliste (Auszug) veröffentlicht, die bei der Entscheidung helfen soll, ein Audit durchzuführen:

- Betrifft das Verfahren, das auditiert werden soll, die Verarbeitung personenbezogener Daten und hat es einen präzise beschreibbaren und überschaubaren Umfang?
- Kann die datenverarbeitende Stelle das Verfahren bei Bedarf durch vertretbare Maßnahmen und Änderungen so gestalten, dass Datenschutz und Datensicherheit optimal gewährleistet sind?
- Ist das zu auditierende Verfahren dokumentiert, sind z. B. die im Rahmen des Auditverfahrens benötigten Unterla-

gen (Verfahrensverzeichnisse, Verfahrensdokumentation) vorhanden?

- Beschäftigt die datenverarbeitende Stelle Mitarbeiter, die in der Lage sind, die im Auditverfahren vorzunehmenden Schritte durchzuführen, z. B. einen behördlichen Datenschutzbeauftragten oder andere Mitarbeiter mit entsprechender Kompetenz?
- Hat die datenverarbeitende Stelle sich bereits Gedanken darüber gemacht, welche Datenschutzziele im Sinne einer datenschutzrechtlichen Verbesserung des zu auditierenden Bereichs sie anstreben möchte?
- Hat die datenverarbeitende Stelle bereits Vorstellungen über ein sachgerechtes Datenschutzmanagementsystem, d. h. über sinnvolle Organisationsstrukturen für die dauerhafte Sicherstellung eines guten Datenschutzniveaus, entwickelt?



Die Krankenkassen sollten ihre Handlungen durch einen autorisierten Dienstleister auch zertifizieren lassen.

#### Zertifikat „Datenschutz bei Krankenkassen“

Die Krankenkassen sollten ihre Handlungen durch einen autorisierten Dienstleister auch zertifizieren lassen. Der TÜV Rheinland hat auf der Grundlage des § 78c SGB X – Datenschutzaudit – die technischen und organisatorischen Anforderungen für das Zertifikat „Geprüfter Datenschutz bei Krankenkassen“ im September 2009 vorgestellt. Neben den Datenschutzgesetzen beinhalten die Anforderungen auch die Kriterien des BSI-Grundschriftbuches sowie die technischen Anforderungen der Gesellschaft für Telematik-Anwendungen der Gesundheitskarte mbH (gematik) und die organisatorischen und technischen Anforderungen aus dem Standard ISO IEC 27001.

Der Anforderungskatalog enthält die Voraussetzungen, unter denen das Prüfzeichen an Krankenkassen vergeben wird. Der Anforderungskatalog definiert technische und organisatorische Anforderungen an die Erhebung, Speicherung, Verarbeitung und die Weitergabe von personenbezogenen Daten im Bereich der Krankenkassen, die vor der Vergabe des Prüfsiegels erfüllt sein müssen. Das Prüfsiegel erhalten Krankenkassen erst nach einer sorgfältigen Prüfung gegen diese Anforderungen.

Die Anforderungen wurden gewählt, um die Erhebung, Speicherung, Verarbeitung und die Weitergabe personenbezogener Daten im Bereich der Krankenkassen in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sicherzustellen. Für die Effektivität der Sicherheitsziele, ist ein Nachweis mittels folgender Prüfverfahren durchzuführen:

- organisatorische Erfüllung/Richtlinien und operative Sicherheit,
- technische Erfüllung,
- Einhaltung der Datenschutzrichtlinien.

Inhaltlich werden die folgenden Sachverhalte bewertet:

#### **Datenschutz-Grundlagen**

Das Modul „Datenschutz-Grundlagen“ behandelt die Einhaltung der grundlegenden rechtlichen Anforderungen, vom Verfahrensverzeichnis über die relevanten Verträge mit Auftragsdatenverarbeitern bis zu den Sensibilisierungsmaßnahmen für Mitarbeiter, und beinhaltet die Abschnitte:

**Prozess gemanagter Datenschutz.** Im Modul „Prozess gemanagter Datenschutz“ wird die Umsetzung der Anforderungen an interne Selbstkontrollmechanismen geprüft, insbesondere die regelmäßige und systematische Auditierung der eigenen Prozesse und Systeme sowie die dokumentierte Überwachung von Auftragnehmern:

- **Betroffenenrechte:** Das Unternehmen hat die Einhaltung und Implementierung gesetzlicher Regelungen zur Ausübung von Betroffenenrechten in Bezug auf gespeicherte personenbezogene Daten sowie auf die geplante eGK zu gewährleisten, insbesondere die Bearbeitung von Auskunftersuchen in Bezug auf die gespeicherten Daten.
- **Datawarehousing:** Das Unternehmen hat die Prozesse zum Datawarehousing und Datamining sowie die Datenverarbeitung im Zuge der Rechnungslegung (unter besonderer Berücksichtigung der Abrechnung über Hausarztprogramme) datenschutzoptimiert auszulegen.

**Kooperation mit privaten Krankenkassen.** Das Modul „Kooperation mit privaten Krankenkassen“ hat den Datenaustausch zum Zwecke des Abschlusses von Zusatzversicherungen zum Gegenstand. Hier wird besonders auf die Einholung der Einwilligung von Betroffenen sowie die Modi von Datenauswahl und -übertragung Wert gelegt.

**Versorgungsmanagement-Programme.** Im Modul „Versorgungsmanagement-Programme“ werden die DMP-Kampagnen gemäß §§ 137f, 137g SGB V und weitere Verträge im Rahmen des Versorgungsmanagements (Hausarztverträge) fokussiert. Im Mittelpunkt stehen dabei die im Modul „Datawarehousing“ gegebenenfalls bereits thematisierten Dataminingprozesse sowie die Teilnahmemodalitäten und Art und Umfang der Datenhaltung.

**Kundenservice/Callcenter.** Das Modul „Kundenservice/Callcenter“ betrifft die Datenerhebung beim Kunden und die Verarbeitung seiner Daten in Niederlassungen bzw. durch eigene oder externe Callcenter. Schwerpunkt sind die vertraglichen Regelungen und dokumentierten Prozesse.

**Technisch-organisatorische Maßnahmen.** Nach § 9 BDSG in Verbindung mit § 78a SGB X haben Sozialversicherungsträger die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Mit präventiven Maßnahmen muss der Schutz der Daten gegen Diebstahl, fahrlässigen und vorsätzlichen Datenabfluss gewährleistet werden.

Der TÜV Rheinland hat hierzu den folgenden Anforderungskatalog erstellt:

# Anforderungskatalog Datenschutz bei Krankenkassen

## Informationssicherheitsleitlinie

Das Unternehmen muss ein Dach-Dokument erlassen, das die Sicherheits- und Datenschutzziele des Unternehmens definiert und zu deren Erreichung mindestens die Umsetzung der Anforderungen dieses Kataloges vorschreibt.

## Sicherheitsrichtlinien

Die im Folgenden dargelegten Sicherheitsmaßnahmen sind in dezidierten Sicherheitsrichtlinien zu dokumentieren. Die Richtlinien sind Gegenstand regelmäßiger (jährlicher) Reviews und müssen bei entsprechender Änderung der Prozesse angepasst werden.

Zudem ist ein Auszug der Sicherheitsmaßnahmen als End-User-Policy für alle Mitarbeiter sowie Externe zu erstellen und diesen auszuhändigen.

## Verantwortung für Informationssicherheit

Das Unternehmen muss einen Informationssicherheitsbeauftragten (ISB) ernennen, der über die nötige Fachkunde verfügt, um kontinuierlich die Aufrechterhaltung des in der ISL angestrebten Sicherheitsniveaus zu überwachen und anzusteuern. Dabei darf der ISB keine Interessenkonflikte aufgrund einer anderen Position haben.

## Beschaffungsprozesse

Die Beschaffung neuer Hardware und Software jeglicher Art durch die Abteilungen des Unternehmens bedarf der Freigabe durch eine verantwortliche Stelle und muss dokumentiert erfolgen. Der Anforderer darf nie zugleich die Freigabe erteilen. Geräte, die durch Fremdfirmen im Netzwerk des Unternehmens genutzt werden, sind zu melden und bedürfen einer gesonderten Freigabe.

## Inventarisierung

Sämtliche Informationswerte (Hardware, Software, Datenbestände) sind zu inventarisieren und einem verantwortlichen Mitarbeiter zuzuweisen. Die Aktualität des Inventars ist durch geeignete Reviews sowie die Einbettung in entsprechende Prozesse (z. B. Einkaufsprozesse) sicherzustellen. Personenbezogene und unternehmenskritische Daten in Systemen sind zu identifizieren.

## Klassifizierungsrichtlinie

Für relevante Daten, deren Vertraulichkeit ungeachtet des Vorhandenseins personenbezogener Merkmale von großer Bedeutung für das Unternehmen ist, muss eine Klassifizierungsrichtlinie erstellt werden, die zugleich grundlegende Kennzeichnungs- wie auch Handhabungsvorschriften enthält.

## Personelle Sicherheit

Neue Mitarbeiter, die personenbezogene Daten bearbeiten, sind mit angemessener Sorgfalt auszuwählen, d. h. es ist mindestens ein polizeiliches Führungszeugnis des Mitarbeiters einzuholen. Bei Systemadministratoren sind Führungszeugnisse auch nachträglich einzuholen.

## Zutrittskontrolle

Die Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden, müssen durch ein Zutrittskontrollsystem gesichert werden. Zutritt ist nur auf Antrag und durch gezielte Rechtevergabe möglich. Die Vergabe, Änderung und Löschung von Zutrittsrechten sind in einem Laufzettel hinterlegt, der bei Änderungen des Anstellungsverhältnisses berücksichtigt wird. Zudem finden jährliche Reviews der vergebenen Rechte statt (Stichprobenmenge 10%), um Abweichungen zu identifizieren. Bei kartenbasierten Zutrittskontrollsystemen sind ebenfalls regelmäßig die Protokolldateien zu überprüfen.

Büros und andere Räumlichkeiten, in denen personenbezogene Daten verarbeitet werden, sind bei Verlassen regelmäßig abzuschließen, wenn sich kein weiterer Mitarbeiter dort aufhält.

## Besucherrichtlinie

Zudem ist eine Besucherrichtlinie zu definieren und zu implementieren, nach der alle Besucher zentral unter Angabe der Daten des besuchten Mitarbeiters anzumelden sind. Besucher sind durch den Mitarbeiter oder einen Vertreter abzuholen und während der Dauer des Aufenthalts zu begleiten. Besucher mit häufigeren Aufenthalten können auf Antrag zeitlich und räumlich begrenzte Zutrittsrechte erhalten.

## Außenhautsicherung

Die Außenhaut des Gebäudes/der Gebäude ist mit einem angemessenen Perimeterschutz zu sichern.

### Sicherheitsbereiche

Bereiche mit erhöhten Sicherheitsanforderungen sind zu identifizieren. Hierzu gehören mindestens Server- und Archivräume sowie gegebenenfalls Räume mit Arbeitsplätzen, die vollen Zugriff auf alle personenbezogenen Daten erlauben. Diese Räume sind durch geeignete Eingangskontrollen und Ausstattungen zusätzlich zu sichern.

### Informations- und kommunikationstechnische Infrastruktur

Die für die Aufrechterhaltung der Geschäftsprozesse kritischen technischen IT-Systeme müssen dem Bedarf, der angestrebten Verfügbarkeit und der sich aus dem Schutzbedarf ergebenden Vertraulichkeit und Integrität der Daten entsprechend ausgelegt sein.

Es muss ein Plan über die IT-Netzwerkstruktur gepflegt werden.

### Bautechnische Infrastruktur

Die für die Aufrechterhaltung des Geschäftsbetriebs kritischen Versorgungseinrichtungen (Kommunikation, Strom, Klima) müssen der Beanspruchung, dem Ausfallrisiko, der notwendigen Verfügbarkeit und dem Schutzbedarf entsprechend ausgelegt sein. Server- und Archivräume sind zudem mit Brandmeldeanlagen und geeigneten Löschvorrichtungen sowie mit Videoüberwachung und Bewegungsmeldern oder einer Alarmanlage zu sichern. Es müssen dem Schutzbedarf/dem Risiko entsprechende, wirksame physische Schutzeinrichtungen vorhanden sein, die möglichen Bedrohungen entgegenwirken.

### Change Management

Sämtliche sicherheitsrelevanten Änderungen an Systemen mit personenbezogenen Daten sind zu dokumentieren und im Vier-Augen-Prinzip freizugeben. Änderungen müssen vor dem Rollout stets in Testumgebungen geprüft werden. Die Daten in den Testsystemen dürfen nicht identisch mit den Produktionsdaten sein. Für zeitkritische Patches muss ein dokumentierter Umgehungsmechanismus implementiert werden.

### Monitoring

Dienste Dritter sind durch geeignete Monitoring-Maßnahmen zu überwachen und bei Abweichungen entsprechend zu korrigieren. Die verfügbaren Kapazitäten von Systemen sind ebenfalls kontinuierlich zu überwachen.

### Mobiler und Schadcode

Die Systeme, auf denen personenbezogene Daten lagern oder verarbeitet werden, sind durch geeignete Virens Scanner vor mobilem und Schadcode zu sichern (Server und Client). Neue Definitionen (Patterns) müssen regelmäßig (mindestens täglich) aufgespielt werden. Updates der Engine unterliegen dem Change Management.

### Backup-Konzept

Sämtliche personenbezogenen Daten sind mindestens täglich inkrementell und wöchentlich voll zu sichern. Die Sicherungsmedien müssen sicher untergebracht in einem separaten Brandabschnitt des Gebäudes lagern. Wöchentliche Sicherungen sind an einem anderen Standort zu lagern (z. B. Banksafe).

### Lagerung und Entsorgung

Datenträger, die personenbezogene Daten enthalten, sind in geeigneter Form zu lagern und zu sichern, um sie gegen den Zugriff Unberechtigter zu schützen.

Es muss ein geeignetes Kontrollsystem für Datenträger existieren. Zu berücksichtigende Detailregelungen sind:

- eine eindeutige und einheitliche Datenträgerkennzeichnung,
- Bestandsverzeichnisse,
- Protokoll- und
- Kontrollverfahren.

Bei der Vernichtung von Datenträgern (magnetische und/oder optische Speichermedien, Papier etc.), die personenbezogene Daten enthalten oder enthalten haben, ist durch geeignete Maßnahmen sicherzustellen, dass diese nicht wieder restauriert werden können. Die Befugnisse für die Vernichtung von Datenträgern müssen festgelegt sein.

Die Sicherung der Daten bzw. der Datenträger bis zur Vernichtung muss gewährleistet sein.

Es müssen Festlegungen zur Absicherung der gespeicherten personenbezogenen Daten und ein dazugehöriges Kontrollsystem existieren. Das Sicherungskonzept muss neben der ständigen Verfügbarkeit auch die Einhaltung von verschiedenen Sicherheitsaspekten wie Zugriffsschutz, Passwortverfahren und, soweit angemessen, Verschlüsselung von Daten gewährleisten.

### Zugriffsrechte

Der Zugriff auf personenbezogene Daten (lesen, schreiben, verändern, sperren, löschen) muss für Personen und/oder Benutzergruppen festgelegt worden sein. Diesbezügliche Regelungen können u. a. enthalten:

- Administration,
- Rechte externer Mitarbeiter,
- Zugriff auf Verwaltungsdateien der jeweiligen Betriebs- und Datenbanksysteme,
- Online-Abrufverfahren,
- zeit- und/oder funktionsorientierte Einschränkung.

Bei allen Zugriffen auf personenbezogene Daten muss eine Identifizierung und Authentisierung (z. B. mittels Benutzer-ID und Passwort) vorausgegangen sein.

### Passwörter

Jeder Mitarbeiter muss sich durch geeignete Sicherungsmaßnahmen am System identifizieren. Werden hierzu Passwörter eingesetzt, so müssen diese mindestens acht Zeichen Länge haben und mindestens aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen bestehen. Die Verwendung des Passwortes und dessen Geheimhaltung regelt eine entsprechende Richtlinie. Passwörter sind mindestens alle 26 Wochen zu wechseln. Die Qualität der Passwörter sollte automatisch überprüft und die Vergabe zu schwacher Passwörter verhindert werden.

### Übertragung

Es muss festgelegt worden sein, an welche Stellen welche Daten zu welchem Zweck übertragen werden dürfen. Die Übertragung ist zu dokumentieren.

Das Unternehmen muss eine Festlegung zu Protokollierung und Speicherdauer erstellen und dokumentieren, wie die personenbezogenen Daten bei denjenigen Stellen berücksichtigt werden, an die Daten übertragen wurden.

Die Aufrechterhaltung der Vertraulichkeit und Integrität personenbezogener Daten muss während der Übertragung angemessen sichergestellt sein (gesicherte Übertragungsstrecken, Verschlüsselung etc.).

Diese Anforderung gilt – soweit anwendbar – insbesondere auch für die Verschlüsselung von Mailverkehr sowie Festplatten in mobilen Endgeräten.

### Kontrollen und Protokollierung

Im gesamten System mit Schwerpunkt auf den zentralen datenhaltenden Applikationen und Datenbanken sind Zeitpunkt, Ziel und Quelle des Zugriffs auf personenbezogene Daten zu protokollieren. Die Protokollierung erstreckt sich sowohl auf erfolgreiche wie auch auf fehlgeschlagene Anmeldungen und andere Systemmeldungen. Die Protokolldateien sind gesichert zu bewahren, Schreib- und Leserechte sind ausschließlich auf Administratoren begrenzt, Änderungen müssen nachgehalten werden.

### Privacy-by-Design

Hinsichtlich zentraler datenhaltender Applikationen sind Privacy-by-Design-Anforderungen zu implementieren, d. h., die Applikationen müssen den besonderen Anforderungen der zu schützenden Daten Rechnung tragen. Maßnahmen sind u. a.:

- restriktive Zugriffsrechte,
- umfassende Protokollierung,
- Monitoring mit definierten Schwellenwerten zur Missbrauchskontrolle,
- Minimierung von Freitextfeldern,
- Vermeidung von Code-Eingaben in Freitextfeldern,
- Incident-Management.

Das Unternehmen muss geeignete Maßnahmen treffen, um im Falle eines erkannten Datenschutz-Vorfalles (z. B. Datendiebstahl, Datenverlust etc.) schnell und angemessen reagieren zu können. Diese Maßnahmen umfassen je nach Art des Vorfalles u. a.:

- Meldewege und Verantwortlichkeiten,
- Incident-Definitionen und -Kategorien,
- geeignete Reaktionen,
- Information der zuständigen Behörden,
- Information der Betroffenen,
- Notfallprozeduren.

Das Unternehmen muss geeignete Maßnahmen treffen, um im Falle eines Notfalls (z. B. menschengemachte oder natürliche Katastrophen) schnell und angemessen reagieren zu können. Diese Maßnahmen umfassen je nach Art des Vorfalles u. a.:

- Trennung kompromittierter Systeme vom Netz,
- Wiederanlaufmaßnahmen,
- Redundanz von Systemen,
- Auslegung von Support-Systemen,
- Beweissicherungsmaßnahmen,

- Information der zuständigen Behörden,
- Information der Betroffenen.

### Technische Anforderungen

Die IT-technische Infrastruktur einer Krankenkasse besteht aus mehreren Komponenten, die getrennt voneinander oder zusammen betrieben werden.

Zu den einzelnen Systemen zählen nicht nur die eigentlichen Serversysteme, sondern alle technischen Teilkomponenten, die für den Betrieb notwendig sind. Insbesondere auch die aktiven Netzwerkkomponenten (Router, Switches) zählen dazu. Alle diese Komponenten müssen den gleichen Sicherheitsstandards entsprechen und bei den technischen Audits betrachtet werden.

Alle Systeme für den Betrieb und die Verwaltung der personenbezogenen Daten und für die Administration der Infrastruktur müssen vor unerlaubten Zugriffen aus fremden Netzen durch geeignete Maßnahmen geschützt werden. Dies kann beispielsweise durch Segmentierung mittels Firewall-Systemen erreicht werden. Die Sicherungsmaßnahmen dürfen sich jedoch nicht nur auf das Internet beschränken, sondern müssen alle angeschlossenen Netze (drahtgebunden und drahtlos) berücksichtigen.

Die Vertraulichkeit und Integrität übermittelter sensibler Daten, beispielsweise personenbezogene Daten oder Logindaten, muss durch geeignete Maßnahmen sichergestellt werden.

### Anforderungen an Firewallsysteme

Unter einer Firewall werden in diesem Zusammenhang alle Systeme verstanden, deren Aufgabe es ist, den netzwerktechnischen Zugriff auf personenbezogene Daten zu kontrollieren. Dazu gehören gegebenenfalls auch auf Telekommunikation basierende Systeme.

Für alle Firewallsysteme sind Konfigurationsstandards zu entwickeln, welche die Dokumentation, Administration und die Überwachung mit einschließen.

Die sensiblen Daten sollten von den öffentlich erreichbaren Systemen durch eine Firewall getrennt sein.

### Systemhärtung

Für alle im Einsatz befindlichen Systeme müssen Standards entwickelt sein, nach denen diese Systeme installiert und gehärtet werden. Diese Standards müssen alle bekannten Sicherheitsrisiken und Best Practices beinhalten.

### Einhaltung eines Vulnerability-Management-Programmes

Es sind Maßnahmen zu implementieren, welche den effektiven Schutz vor Kompromittierung aller am Geschäftsprozess beteiligten Systeme sicherstellen. Dazu gehören u. a. Antivirus-Maßnahmen, ein effektiver Patchmanagementprozess und die Trennung der Test- und Entwicklungsumgebungen von Produktivsystemen.

### Entwicklung und Betrieb von sicheren Applikationen

Die Entwicklung von Software und Applikationen ist auf Basis von Best-Practice-Richtlinien zu erstellen, z. B. dem Open Web Application Security Project ([www.owasp.org](http://www.owasp.org)). Es ist ein Review zur Identifizierung potenzieller Schwachstellen in selbst entwickelten Applikationen durchzuführen, um generelle Programmierfehler aufzudecken.

### Anforderung an die Administration der Infrastruktur

Aufgrund der weitreichenden Rechte von Administratoren sind weitergehende Maßnahmen erforderlich, z. B. genereller Einsatz von verschlüsselten Administrationsdiensten, administrativer Zugriff erfolgt aus einer gesonderten Management-DMZ, die Adminsysteme besitzen keine Verbindung ins Intern

## Sensibilisierung und Schulungen erforderlich

Die Konsequenzen aufgrund der BDSG-Novellierungen können beträchtlich sein. Daher sollten die organisatorischen und technischen Maßnahmen in Behörden so angepasst werden, dass die Anforderungen des neuen BDSG erfüllt werden bzw. gewisse Vorschriften, wie z. B. die Mitteilungspflicht nach § 42a BDSG, erst gar nicht angewendet werden müssen. Mit präventiven Maßnahmen muss der Schutz der Daten gegen Diebstahl, fahrlässigen und vorsätzlichen Datenabfluss gewährleistet werden.

Die Einhaltung der Datenschutzbestimmungen – insbesondere die Kontrolle der technischen und organisatorischen Maßnahmen – wird allerdings unzureichend bleiben, wenn darin allein ein unproduktiver Kostenfaktor gesehen wird.

Eine effektive Datenschutzkontrolle setzt voraus, dass das Personal – insbesondere der Datenschutzbeauftragte – ausreichend geschult und informiert ist. Die Sensibilisierung der Beschäftigten für Risiken der Informationssicherheit und sicherheitsgerechtes Verhalten sollte daher fester Bestandteil eines Sicherheitskonzepts sein.

Technische Sicherheitsmaßnahmen zum Datenschutz führen häufig zu einer Einschränkung der Benutzerfreundlichkeit. Nur wenn Benutzer verstehen, warum Einschränkungen nötig sind, sind sie bereit, diese auch zu akzeptieren. Nur dann, wenn die Beschäftigten die Kenntnisse und Kompetenz für einen sicherheitsgerechten Umgang mit der Informationstechnik haben, können sie die implementierten ganzheitlichen Sicherheitsrichtlinien auch tatsächlich einhalten.

Die Sensibilisierung der Mitarbeiter für Informationssicherheit soll Verständnis vermitteln, warum Sicherheit wichtig ist, das Bewusstsein stärken, dass die gewissenhafte Umsetzung der Sicherheitsmaßnahmen die selbstverständliche Pflicht eines jeden Mitarbeiters ist, die Eigenverantwortlichkeit erhöhen, die Kenntnisse über Informationssicherheit verbessern sowie ein frühzeitiges Erkennen von sicherheitsrelevanten Zwischenfällen fördern.

Audits tragen dazu bei, die Kenntnisse über das eigene Verhalten auf eine gesicherte Grundlage zu stellen. In der Praxis werden Audits häufig vernachlässigt. Nun wird ein solches Audit zumindest bezüglich personenbezogener Daten gesetzlich gefordert. Die Mitteilungspflichten, die sich aus der Datenschutznovelle II ergeben, zwingen jedes Unternehmen und jede Behörde bei Datenpannen, Informationen über diesen Vorfall bekannt zu geben. In jedem Fall wird der Vorfall veröffentlicht, und es kann ein erheblicher, finanziell nur schwer zu beziffernder Vertrauensverlust entstehen. Die Bekanntgabe von Datenpannen wird sicherlich die Presse dankend übernehmen.

Vorstand und IT-Leiter haben die Verantwortung und haften bei Vorsatz und grober Fahrlässigkeit auch persönlich. ISMS Einführung und Zertifizierung der Maßnahmen dienen der Risikominimierung und dem Nachweis, dass die verantwortlich Haftenden zu ihrer Entlastung aktiv gehandelt haben.

Die Schwerpunkte der internen und externen Prüfung müssen aufgrund der Datenschutzverletzungen bei Krankenkassen verändert werden. Priorität müssen dabei die Auslagerung von Aufgaben auf Dritte, Telearbeitsplätze, der Einsatz von Telekommunikation (u. a. Smartphones) sowie die Sicherheit der Informationsverarbeitung und der Datenschutz nach Einführung neuer DV-Verfahren (z. B. oscore, IS KV 21c) erhalten.

■ **Udo Polaszek, Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen, Essen**  
Kontakt: [Udo.Polaszek@mags.nrw.de](mailto:Udo.Polaszek@mags.nrw.de)

### Anmerkung

<sup>1</sup> Siehe u. a. Polaszek, U., M. Zellmann, Krankenkassen im Fokus des Insolvenzrechts – die neuen Pflichten nach dem GKV-OrgWG, in: *Die BKK* 04/2009, S. 137–142.