Gutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Unfallkasse Nord

Personalverwaltung, Rehabilitation und Leistung, Regress, Schnittstelle Prävention – Arbeitsschutz, allgemeine Datenverarbeitung

Erstellungszeitraum: 2016-2018

ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Tel.: 0431-9881200
Fax: 0431-9881223
E-Mail: mail@datenschutzzentrum.de
Datum: 24.05.2018
Version: 1.0

Inhaltsverzeichnis

1 Gegenstand des Audits

1.1 Vereinbarung

Entsprechend dem Auditvertrag vom Januar 2016 reauditiert das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) die Datenverarbeitung bei der Unfallkasse Nord hinsichtlich der Versicherten- bzw. Betroffenendaten sowie der Personalaktenverwaltung. Gegenstand ist aus technischer Sicht auch die Sicherheit und Ordnungsmäßigkeit der allgemeinen Datenverarbeitung bei der Unfallkasse Nord.

Konkret umfasst das Audit folgende Bereiche:

- Personalverwaltung,
- Leistungsgewährung Leicht-, Mittel-, Schwerfall,
- Berufskrankheiten,
- Teilhabe und Rehabilitation,
- Regress,
- Schnittstelle zwischen Prävention und Arbeitsschutz,
- Allgemeine Datenverarbeitung

Es handelt sich um eine Reauditierung des ursprünglich am 20. März 2013 erteilten Zertifikats. Der Bereich des häuslichen Arbeitsplatzes gehört nicht zum Auditgegenstand. Zwar wurde dieses in einem Pilotverfahren getestet; laut Aussage der Unfallkasse Nord ist aktuell aber keine weitere Nutzung von Heimarbeitsplätzen geplant. Es laufen allerdings Prüfungen, ob die Regelungen des Landes Schleswig-Holstein für die Einrichtung mobiler Arbeitsplätze für die Unfallkasse Nord umgesetzt werden können. Diese sind jedoch nicht Auditgegenstand.

1.2 Vorgehen bei der Auditierung

Die Auditierung erfolgte unter Berücksichtigung der „Hinweise des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG“.

Die Durchführung des Datenschutz-Behördenaudits erfolgt in den folgenden Schritten:

- Überprüfung der Abgrenzung des Auditgegenstands,
- Analyse der Dokumentation (Datenschutzkonzept),
- Begutachtung der Wirkungsweise des Datenschutzmanagementsystems und der Erreichung der festgelegten Datenschutzziele,
- Hervorhebung von anerkennenswerten und datenschutzfreundlichen Datenverarbeitungsprozessen,
- stichprobenartige Überprüfung der Umsetzung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen und

- Überprüfung der Einhaltung datenschutzrechtlicher und bereichsspezifischer Vorschriften in Bezug auf den Auditgegenstand.

1.3 Datenschutz- und Datensicherheitsziele

Die Unfallkasse Nord hat, wie im bei der ersten Auditierung, in einem Sicherheitskonzept Ziele für den sicheren und datenschutzkonformen Einsatz festgelegt.

Die Ordnungsmäßigkeit der automatisierten Datenverarbeitung der Unfallkasse Nord soll unter Berücksichtigung

1. der Integrität (Daten bleiben unversehrt, vollständig, zurechenbar und aktuell),
2. der Vertraulichkeit (es kann nur befugt auf Verfahren und Daten zugegriffen werden),
3. der Verfügbarkeit (Verfahren und Daten können zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden),
4. der Transparenz (die Verarbeitung von personenbezogenen Daten kann mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden),
5. der Nicht-Verkettbarkeit (personenbezogene Daten können nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden) und
6. der Intervenierbarkeit (Verfahren sind so gestaltet, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den §§ 26 bis 30 LSDG-SH wirksam ermöglichen)

der zur Aufgabenerfüllung notwendigen personenbezogenen Daten gewährleistet werden.

Die Unfallkasse Nord hat festgelegt, dass die Erforderlichkeit und Angemessenheit der Sicherheitsmaßnahmen durch eine Risikoanalyse möglicher Gefährdungen unter Berücksichtigung der tatsächlichen örtlichen und personellen Gegebenheiten geprüft und durch eine modularisierte Dokumentation der technischen und organisatorischen Sicherheitsmaßnahmen nachgewiesen werden muss.

Seit der Erstauditierung wurde u. a. laut Aussage des Datenschutzbeauftragten eine Sensibilisierungskampagne für die Beschäftigten erfolgreich durchgeführt. Der Datenschutzbeauftragte sei eng in alle relevanten Datenverarbeitungsvorgänge eingebunden; und auch die Zusammenarbeit mit der IT funktioniere gut.

1.4 Dienstanweisungen

1.4.1 Dienstanweisung Datenschutz

Zentrales Dokument bei der Unfallkasse Nord ist weiterhin die „Dienstanweisung zum Datenschutz und zur Sicherheit beim Einsatz der automatisierten Datenverarbeitung der Unfallkasse Nord“. Die aktuelle Version wurde am 13. Februar 2017 in Kraft gesetzt. Mit Verweis auf die einschlägigen Normen finden sich hierin folgende Regelungen

- Erhebung von Sozialdaten,

- Verarbeitung und Nutzung von Sozialdaten (insbesondere zur Übermittlung),
- Einwilligung des Betroffenen
- Verarbeitung oder Nutzung von Sozialdaten im Auftrag,
- Auskünfte an den Betroffenen,
- Hinweis- und Unterrichtungspflichten des Unfallversicherungsträgers,
- Berichtigung, Löschung, Sperrung und Wiederauffrischung von Sozialdaten,
- Personenbezogene Daten im Fachbereich Staatlicher Arbeitsschutz,
- Interner Datenschutzbeauftragter,
- Ergänzende Erfordernisse nach § 17 SVRV und § 40 SRVwV,
- Anweisungen für Benutzer von IT-Systemen.

Dies Dokument wird ergänzt um eine „Dienstanweisung für die Aufbewahrung von Akten und Unterlagen der Unfallkasse Nord". Hierin werden genaue Angaben gemacht, wann Unterlagen und gespeicherte Daten zu vernichten bzw. zu löschen sind. Das Dokument entspricht den Empfehlungen des Dachverbands (Deutschen Gesetzlichen Unfallversicherung (DGUV)).

Neu hinzugekommen ist das Kapitel „Personenbezogene Daten im Fachbereich staatlicher Arbeitsschutz", das insbesondere auf Geheimhaltungspflichten und Unterrichtungspflichten eingeht.

Hingegen wurde der Punkt „Sicherung des Rechenzentrums" gestrichen, da die Unfallkasse Nord kein eigenes Rechenzentrum mehr betreibt (siehe Kapitel 4.1.3.3).

Die Dokumente sind in der vorgelegten Form nicht zu beanstanden. Sie geben eine gute Hilfe dabei, die beteiligten Personen bei der ordnungsgemäßen Datenverarbeitung zu unterstützen.

1.4.2 Dienstanweisung Arbeitszeit

Neu ist auch die Dienstanweisung über die Durchführung einer flexiblen Arbeitszeit vom 29.03.2016. Aktuell werden eine analoge Stempelanlage und eine elektronische Zeiterfassung parallel eingesetzt: Aus technischen Gründen ist an den Standorten Hamburg, Lübeck und Itzehoe eine Stempelanlage im Einsatz, in Kiel wird eine elektronische Zeiterfassung eingesetzt. Ein einheitliches elektronisches Zeiterfassungssystem ist aufgrund des IT-Harmonisierungsprozesses noch nicht umgesetzt; aktuell wird geprüft, welches einheitliche System eingeführt werden könnte. Zeiterfassungsbelege und Zeitkarten sind sechs Monate lang aufzubewahren und werden danach vernichtet. Zeiterfassungsdaten sind nach Ablauf der Aufbewahrungsfrist durch das Sachgebiet Personal zu löschen.

Auch dieses Dokument war datenschutzrechtlich nicht zu beanstanden.

1.5 Schwerpunkte der Prüfungen

Schwerpunkt des Audits war die Implementierung von Verfahren zur Umsetzung der folgenden Punkte:

- Beachtung des Grundsatzes der Erforderlichkeit (vgl. § 67a Abs. 1 S. 1 SGB X),

- Transparenzpflicht gegenüber den Betroffenen (insbesondere Unterrichtung über die Zweckbestimmung und Rechtsgrundlagen der Datenerhebung beim Betroffenen – vgl. § 67a Abs. 3 SGB X),
- Beachtung des Grundsatzes der vorrangigen Datenerhebung beim Betroffenen (vgl. § 67a Abs. 2 S. 2 SGB X),
- Beachtung der Möglichkeiten für eine direkte Datenerhebung bei Dritten oder externen Stellen (§ 67a Abs. 2 S. 2 SGB X),
- Beachtung der Unterrichtungspflicht bei einer Datenerhebung nach § 67a Abs. 2 S. 2 SGB X (vgl. § 67a Abs. 5 SGB X),
- Beachtung der Erforderlichkeit der Datenspeicherung (§ 67c SGB X) und
- Beachtung der Befugnisregelungen für die Datenübermittlung (§ 67d SGB X).

2 Ergebnisse der Auditierung

2.1 Personalaktenführung

Erneut wurden stichprobenartig einige Personalakten bei der Unfallkasse Nord gesichtet. Drei Akten haben wir uns angesehen, wobei zwei davon Angestellte betrafen und eine einen Beamten. Hierbei ergaben sich keine Auffälligkeiten. Rechtliche Grundlage für die Personalaktenführung ist weiterhin vor allem das Landesbeamtengesetz (§§ 85 ff.) Als Grundlage der Beratung zu der sich heraus ergebenen überarbeiteten Dienstanweisung diente u. a. die „Dienstanweisung zur Führung von Personalakten bei dem Landesarbeitsgericht Schleswig-Holstein und dem Arbeitsgerichten des Landes Schleswig-Holstein“ vom 30. Oktober 2007. Vorbildlich ist weiterhin die Aufteilung in Hauptakte und Teilakten (Entgelt, Beurteilung/Fortbildung, Ausbildung, Nebentätigkeiten, Reisekosten, Abwesenheiten, Betriebliches Eingliederungsmanagement etc.).

Insgesamt waren die gesichteten Akten übersichtlich gestaltet und orientierten sich an den Empfehlungen aus dem ersten Audit.

2.2 Verfahren

Bzgl. der Verfahren zur „Leistungsgewährung Leicht- Mittel-, Schwerfall“, Berufskrankheiten, Teilhabe und Rehabilitation und Regress haben sich nach Aussage des Datenschutzbeauftragten keine relevanten Änderungen im Verfahren gegeben. Dies wurde uns auf Nachfrage am 23. Mai 2018 erneut bestätigt. Auch die eingesetzten Dokumente, die während des ersten Auditierungsverfahrens teilweise umfangreich überarbeitet wurden, werden weiterhin eingesetzt. So kommt z. B. der Aufkleber für die Verbandbücher zum Einsatz, der auf notwendige Löschungen der Daten hinweist. Auch gab es laut Aussage des Datenschutzbeauftragten beim Einsatz dieser Dokumente und Umsetzung der Verfahren keine Auffälligkeiten; es sei weiterhin von einer ausreichenden Sensibilität der Beschäftigten im Umgang mit den Daten auszugehen. Diese Ausführungen erschienen und plausibel.

Herauszustellen ist, dass inzwischen eine optisch und inhaltlich ansprechende Broschüre („MITDENKEN“) von der Unfallkasse Nord an die Beschäftigten verteilt wird, die für Datenschutz und Datensicherheit sensibilisieren soll. Insbesondere enthält sie Informationen zu Passwörtern, Sozialen Netzwerken, E-Mail und mobiles Arbeiten. Verwiesen wird für Fragen auch auf den Datenschutzbeauftragten.

3 Datenschutzrechtliche Bewertung

Die „Dienstanweisung zur Führung von Personalakten bei der Unfallkasse Nord“ entspricht weiterhin weitgehend den vom ULD empfohlenen Mustern und deckt die gesetzlichen Forderungen hinsichtlich der Aktenführung ab.

Auch die geprüften Fachverfahren entsprechen weiterhin den rechtlichen Vorgaben. Da sich hier keine nennenswerten Änderungen ergeben haben, wird diesbezüglich auf den Auditbericht von 2013 verwiesen.

Begrüßenswert ist die genannte Broschüre „MITDENKEN“.

4 Allgemeine Datenverarbeitung

4.1 Datenschutzmanagement

4.1.1 Aufbau- und Ablauforganisation

4.1.1.1 Leitlinien zum Datenschutz und der Datensicherheit

Die Unfallkasse Nord hat seit dem letzten Audit die im Rahmen einer Sicherheitsleitlinie festgelegten Grundzüge des Datenschutz- und des IT-Sicherheitsmanagements fortgeschrieben und somit den Stellenwert des Datenschutzes und der IT-Sicherheit in der Organisation bekräftigt.

Die in der Sicherheitsleitlinie erfassten Ziele umfassen die Vertraulichkeit, die Verfügbarkeit und die Integrität der zur Verarbeitung genutzten IT-Systeme. Die Unfallkasse Nord orientiert sich weiterhin an den Vorgaben des IT-Grundschutzes, um ein angemessenes Schutzniveau innerhalb der Organisation zu erreichen und aufrechtzuerhalten. Das Dokument selbst beschreibt ausführlich die verschiedenen Aspekte des Sicherheitsmanagements, des zugrundeliegenden Konzeptes sowie der modularen Dokumentation.

Es werden im Rahmen des Dokuments Aussagen zu den Aufgaben und Verantwortlichkeiten der für den Datenschutz und die IT-Sicherheit verantwortlichen Personen getroffen. Ferner gibt es Ausführungen zum Stellenwert der Leitlinie im Hinblick auf andere Dokumente sowie zur Fortschreibung des Dokuments selbst.

Die Leitlinie entspricht somit den Anforderungen anerkannter Standards. Die Umsetzung der Regelungen wurde durch das ULD im Rahmen eines Vor-Ort-Termins stichprobenartig überprüft.

4.1.1.2 Datenschutzbeauftragter

Der behördliche Datenschutzbeauftragte bei der Unfallkasse Nord wurde gemäß § 10 LDSG schriftlich bestellt und ist in seiner Position unmittelbar der Leitung der Unfallkasse unterstellt. Er unterliegt in seiner Tätigkeit als Datenschutzbeauftragter keinen fachlichen Weisungen durch die Organisationsleitung, und er verfügt über die erforderliche Fachkunde.

Im Zusammenhang mit seinen anderen dienstlichen Aufgaben konnte kein Interessenkonflikt festgestellt werden.

Somit sind die Voraussetzungen des § 10 Abs. 1 bis 3 LDSG erfüllt.

4.1.1.3 IT-Sicherheitsbeauftragter

Die Aufgaben des IT-Sicherheitsbeauftragten bei der Unfallkasse Nord sind ebenfalls im Rahmen der IT-Sicherheitsleitlinie festgeschrieben.

4.1.1.4 Kontrollen und Integration von Datenschutz und Datensicherheit in betriebliche Prozesse

Der Datenschutzbeauftragte führt im Rahmen seiner Tätigkeit sowohl anlassbezogene als auch anlasslose, regelmäßige Kontrollen innerhalb der Organisation durch. Er berät hierbei und im Rahmen regelmäßiger Besprechungen mit den einzelnen Fachabteilungen in datenschutzrechtlichen Fragen und hilft, datenschutzrechtliche Probleme zu erkennen und geeignete Lösungen zu erarbeiten.

Er ist darüber hinaus frühzeitig in die Planung und die Umsetzung neuer Verfahren sowie allgemeiner technischer und organisatorischer Maßnahmen zum Datenschutz und der IT-Sicherheit eingebunden.

Er führt ferner regelmäßige Schulungen der Beschäftigten der Unfallkasse Nord durch.

Hierdurch sind die Anforderungen des § 10 Abs. 4 Nr. 1 bis 3 LDSG erfüllt.

4.1.1.5 Sicherheits- und Datenschutzvorfälle

Bestandteil der Sicherheitsleitlinie sind ebenfalls Regelungen, die das Vorgehen, die Ansprechpartner, die Dokumentation und die Nachbearbeitung von Sicherheits- und Datenschutzvorfällen festlegen. Für die Bearbeitung solcher Vorfälle gibt es bei der Unfallkasse Nord ein abgestuftes System, bei dem die jeweils zuständigen Administratoren entsprechende Meldungen entgegennehmen und zunächst eigenverantwortlich entscheiden, ob es sich um ein Sicherheitsproblem handelt, welches selbstständig und eigenverantwortlich gelöst werden kann, oder ob sie die nächsthöhere Eskalationsstufe zu unterrichten haben.

Ist dies der Fall, so wird der Sicherheitsvorfall an den Sicherheitsbeauftragten gemeldet, der den Vorfall untersucht und bewertet. Im Anschluss daran werden notwendige und geeignete Maßnahmen identifiziert und durch die Administratoren umgesetzt.

Je nach Schwere des Vorfalls erfolgt ggf. eine weitere Abstimmung mit dem Leiter der Stabsstelle IT/Zentrale Planung und Steuerung (ZPS).

Sicherheitsvorfälle werden im Nachgang schriftlich aufgearbeitet.

Die Unfallkasse Nord hat somit geeignete Prozesse implementiert, um auf Sicherheitsvorfälle angemessen zu reagieren und mit diesem umgehen zu können.

Gleiches gilt für die Umsetzung der Vorgaben des § 27a LDSG. Auch hier hat die Unfallkasse Nord geeignete Prozesse definiert und implementiert, die ihr den Umgang mit den Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten ermöglichen.

4.1.1.6 Betroffenenrechte

Für die Bearbeitung von Auskunftsansprüchen nach § 27 LDSG sowie für die Umsetzung weiterer gesetzlich geregelter Betroffenenrechte ist der Datenschutzbeauftragte der Unfallkasse Nord zuständig. Er prüft in diesem Rahmen regelmäßig die Umsetzung geeigneter technisch-organisatorischer Maßnahmen im Hinblick auf die Regelungen des § 28 LDSG.

4.1.2 Dokumentation

Die von der Unfallkasse Nord vorgehaltene Dokumentation ist entsprechend den Empfehlungen des ULD modular aufgebaut und umfasst nach Aussagen des Datenschutzbeauftragten (und in Fortschreibung der Ergebnisse des Audits aus dem Jahr 2013) alle nach LDSG und DSVO notwendigen Bestandteile.

Wie bereits dargestellt, orientiert sich die Unfallkasse Nord bei der Auswahl und Implementierung geeigneter technisch-organisatorischer Maßnahmen an der Vorgehensweise des IT-Grundschutzes. Eine erfolgte Grundschutzerhebung umfasst alle für eine vollständige Abbildung der Organisationsstruktur relevanten Bausteine und die mit diesen Bausteinen verbundenen Maßnahmen.

4.1.2.1 Verfahrensverzeichnis

Zu den Aufgaben des Datenschutzbeauftragten der Unfallkasse Nord zählt das Führen und Pflegen der Verfahrensverzeichnisse gemäß § 7 LDSG, die dem ULD übersendet wurden und die das ULD im Rahmen des Audits stichprobenartig eingesehen und geprüft hat. Es konnte festgestellt werden, dass die übersendeten Dokumente aktuell sind und den Anforderungen des § 7 LDSG entsprechen.

4.1.2.2 Dienstanweisungen und Auftragsdatenverarbeitung

Um den Beschäftigten belastbare Regelungen an die Hand zu geben, hat die Unfallkasse Nord relevante Sachverhalte beim Umgang mit personenbezogenen Daten in Dienstanweisungen geregelt.

Zentrales Dokument in diesem Zusammenhang ist die „Dienstanweisung zum Datenschutz und zur Sicherheit beim Einsatz der automatisierten Datenverarbeitung bei der Unfallkasse Nord". Dieses Dokument regelt u. a. umfassend die Anforderungen bei der Erhebung und Verarbeitung von Sozialdaten, die Rechte des Betroffenen auf Auskunft, Sperrung, Löschung und Berichtigung, die Aufgaben und die Stellung des Datenschutzbeauftragten sowie Anforderungen an die Nutzer von IT-Systemen, beispielsweise im Hinblick auf die Grundsätze der Erforderlichkeit, die Speicherung von Daten, die Verwendung und Gestaltung von Passwörtern sowie die Verwendung von Telefax, E-Mail und Internet. Weitere Dienstanweisungen beschäftigen sich u. a. mit dem Einsatz von Notebooks und der Verwendung von USB-Sticks, der Nutzung von Internet-Terminplanern sowie mit den Anforderungen an die Umsetzung flexibler Arbeitszeiten. Diese Dokumente wurden vom ULD im Rahmen des Audits ebenfalls stichprobenartig geprüft.

Die Unfallkasse Nord lässt darüber hinaus verschiedene Auftragsverarbeitungen durchführen. Wie bereits im vorangegangenen Audit sind die im Rahmen einzelner Fachverfahren durchgeführten Auftragsverarbeitungen Gegenstand entsprechender schriftlicher Vereinbarungen zwischen der Unfallkasse und den jeweiligen Auftragnehmern.

Darüber hinaus lässt die Unfallkasse Nord die Vernichtung personenbezogener Daten (von Kunden, Geschäftspartnern und Beschäftigten) durch das vom ULD zertifiziertes Aktenvernichtungsverfahren der Rhenus Data Office GmbH durchführen. Der hierzu vorgelegte Auftragsdatenverarbeitungsvertrag wurde ebenfalls vom ULD geprüft.

4.1.2.3 Netzplan

Die für die Verarbeitung eingesetzten IT-Systeme sowie ihre physikalischen und logischen Verbindungen sind in einem Netzplan dokumentiert, der den Anforderungen des § 4 Abs. 2 Punkt 4 DSVO entspricht.

4.1.2.4 Weitere Dokumentationsbestandteile

Insgesamt sind die für die Verarbeitung verwendeten IT-Systeme und Programme bei der Unfallkasse Nord umfangreich dokumentiert. Es existieren in diesem Zusammenhang Dokumente zur Installations- und Konfigurationsdokumentation sowie entsprechende Betriebs- und Notfallhandbücher. Ein Zentraldokument verweist auf den jeweiligen Standort des entsprechenden Dokuments, so dass der modulare Aufbau der Dokumentation nachvollziehbar ist.

Insgesamt erfüllt die Dokumentation der Unfallkasse Nord, wie bei der vorangegangenen Auditierung, die Anforderungen des § 3 Abs. 2 Punkt 2 und 3 DSVO.

4.1.3 Sicherheitsmaßnahmen

4.1.3.1 Risikoanalyse

Die Vorgehensweise der Unfallkasse Nord hat sich, nach Aussagen der zuständigen Personen (IT-Sicherheitsbeauftragter und Datenschutzbeauftragter), im Hinblick auf die Identifikation und Analyse von Risiken nicht verändert. Die vom IT-Grundschutz vorgeschlagene Vorgehensweise kommt somit bei der Unfallkasse Nord weiterhin zum Einsatz. Es kann somit davon ausgegangen werden, dass die Umsetzung der Anforderungen zur Risikoanalyse und die Auswahl konkreter Maßnahmen noch immer den Ausführungen von § 4 Abs. 2 und 3 DSVO entspricht.

4.1.3.2 Räume und Gebäude

Die Unfallkasse Nord ist weiterhin an den Standorten Hamburg und Kiel ansässig.

Ferner wurden die Maßnahmen zur Zutritts-, Zugangs- und Zugriffskontrolle an den zwei Standorten in Kiel begutachtet. Generell sind die ergriffenen Maßnahmen ausreichend, um die jeweils verfolgten Ziele zu erreichen.

4.2 Datenschutzrechtliche Beurteilung

4.2.1 Prüfungsverlauf

Die Auditierung erfolgte unter Berücksichtigung der „Hinweise des Unabhängigen Landeszentrums für Datenschutz zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 LDSG“.

Da es sich hier um eine Reauditierung handelt und die Verfahren nach Aussage der Unfallkasse Nord seit dem letzten Audit im Jahre 2013 nur geringfügig geändert wurden, konnte auf ein Vor-Audit verzichtet werden. Bzgl. der Schritte der Durchführung des Datenschutz-Behördenaudits

wird auf Kapitel 1.2 verwiesen.

Nach Prüfung der Dokumente wurde in einem Vor-Ort-Termin die Angemessenheit und Wirksamkeit der in den Dokumenten beschriebenen Sicherheitsmaßnahmen stichprobenartig überprüft. Diese Prüfung diente dazu, festzustellen, ob die in den Dokumenten dargestellten Maßnahmen seitens der Unfallkasse Nord angemessen und wirksam umgesetzt werden.

4.2.2 Vorbereitung Datenschutz-Grundverordnung (DSGVO)

Ab dem 25. Mai 2018 wird die Datenschutz-Grundverordnung angewendet. Die aktuelle Prüfung der Unfallkasse Nord erfolgte auf Basis der Rechtslage zum Zeitpunkt der Auditierung und damit noch nicht nach DSGVO. Jedoch hat die Unfallkasse Nord in dem Auditzeitraum schon Vorarbeiten zur Umsetzung der neuen Anforderungen getroffen. Unter anderem wurde den Auditoren eine Aufstellung vorgelegt, die die kommenden Schritte zur Umsetzung der DSGVO beschreibt. Dies umfasst u. a. die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten, die Datenschutz-Folgenabschätzung unter Heranziehung auch des Standarddatenschutzmodells, Risikobewertungen etc. Dieses Dokument war nicht Prüfgegenstand. Es zeigt jedoch, dass abzusehen ist, dass das Datenschutzmanagement auch nach dem neuen Recht ordnungsgemäß umgesetzt werden kann.

5 Zusammenfassung und Bewertung

Im Verlaufe des Auditprozesses konnte festgestellt werden, dass die Unfallkasse Nord für ihre allgemeine Datenverarbeitung und die genannten Fachverfahren über angemessene und wirksame Maßnahmen zum Datenschutz und zur Datensicherheit verfügt.

Das Management beider Bereiche orientiert sich auch bei der jetzt durchgeführten Reauditierung an internationalen Standards. Hierbei ist insbesondere das Informationssicherheitsmanagement auf Basis von IT-Grundschutz zu nennen.

Wie beim vorangegangenen Audit sind hier folgende Aspekte einer datenschutzkonformen und datenschutzfreundlichen Gestaltung der Organisation und der eingebundenen Technik zu erwähnen:

- Der bestellte Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte arbeiten eng miteinander und mit der Leitung der Unfallkasse Nord zusammen. Das eingesetzte Datenschutzmanagementsystem gewährleistet zusammen mit den durchgeführten regelmäßigen und anlassbezogenen Kontrollen ein hohes Maß an Datensicherheit und Datenschutz. Dies wird durch sauber definierte und gelebte Prozesse, auch im Hinblick auf die Erkennung und Bearbeitung von Datenschutz- und Sicherheitsvorfällen, unterstützt. Darüber hinaus werden beide Beauftragte frühzeitig in die Planung von IT-Projekten eingebunden und können so mithelfen, das etablierte Niveau an Datenschutz und Datensicherheit in der Organisation aufrecht zu erhalten.
- Sowohl technische als auch organisatorische Prozesse zum Datenschutz und zur Datensicherheit sind umfassend und nachvollziehbar beschrieben.
- Das Management von Datenschutz und Datensicherheit orientiert sich an den Vorgaben zur Ordnungsmäßigkeit der Datenverarbeitung (DSVO) und internationalen Standards (IT-Grundschutz).

Die Verleihung des Auditzeichens nach § 43 Abs. 2 LDSG ist damit gerechtfertigt.