Kurzgutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Unfallkasse Nord

„Allgemeine Datenverarbeitung“

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Autor:	Sven Thomsen
Tel.:	0431-988-1211
Fax:	0431-988-1226
E-Mail:	ULD3@datenschutzzentrum.de
Datum:	18.12.2012
Version:	1.0

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits

Grundlage des Datenschutz-Behördenaudits ist der Audit-Vertrag zwischen der Unfallkasse Nord und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein.

Gegenstand des Datenschutz-Behördenaudits ist die **Sicherheit und Ordnungsmäßigkeit der allgemeinen Datenverarbeitung**.

Nicht Gegenstand dieses Teils des Datenschutz-Behördenaudits ist die Verarbeitung personenbezogener Daten in einzelnen Fachverfahren. Dieser Auditteil trifft keine Aussagen zur angemessenen und wirksamen Umsetzung datenschutzrechtlicher Bestimmungen insbesondere des Sozialgesetzbuches. Hierzu wird ergänzend auf das Gutachten „Personalverwaltung, Rehabilitation und Leistung, Regress, Schnittstelle Prävention – Arbeitsschutz“ von Henry Krasemann verwiesen.

2 Feststellung zu den sicherheitstechnischen Elementen des Datenschutzmanagementsystems

2.1 Aufbau- und Ablauforganisation

2.1.1 Leitlinie Datenschutz und Datensicherheit

Die Unfallkasse Nord hat die Grundzüge des Datenschutz- und Sicherheitsmanagements in einer Sicherheitsleitlinie festgelegt.

Die Leitlinie legt den Stellenwert der IT-Sicherheit fest und definiert IT-Sicherheitsziele. Die Sicherheitsziele umfassen die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme. Als Ziel wird weiterhin das Erreichen eines Sicherheitsniveaus in Anlehnung an die Vorgaben der IT-Grundschutzvorgehensweise des BSI festgelegt. In der Leitlinie wird das gemeinsame Sicherheitsmanagement, eine modulare Sicherheitskonzeption und –dokumentation sowie eine regelmäßige Sicherheitsrevision festgelegt.

Die Leitlinie enthält explizite Aussagen zur Verantwortung für die IT-Sicherheit und den Datenschutz. Die Bekanntgabe sowie die regelmäßige Überarbeitung der Leitlinie sind geregelt. Die Leitlinie wurde im Dezember 2012 durch den Geschäftsführer in Kraft gesetzt.

Die Leitlinie entspricht den Anforderungen internationaler und nationaler Standards. Das ULD hat die angemessene Umsetzung der Vorgaben der Leitlinie durch Kontrollen vor Ort nachvollzogen.

2.1.2 Datenschutzbeauftragter

Als behördliche Datenschutzbeauftragter ist Herr Olaf Heyduck gemäß § 10 LDSG schriftlich bestellt. Herr Heyduck ist in seiner Funktion als behördlicher Datenschutzbeauftragter der Behördenleitung unmittelbar unterstellt und unterliegt in der Ausübung seiner Tätigkeiten als behördlicher Datenschutzbeauftragter keiner fachlichen Weisung durch die Behördenleitung. Er verfügt über die erforderliche Sachkenntnis

Seine anderen dienstlichen Aufgaben stehen in keinem Konflikt mit seiner Tätigkeit als behördlicher Datenschutzbeauftragter.

Die Anforderungen des § 10 Abs. 1-3 LDSG sind erfüllt.

2.1.3 IT-Sicherheitsbeauftragter

Als IT-Sicherheitsbeauftragter ist Herr Jan Nuszkowski bestellt. Die Aufgaben des IT-Sicherheitsbeauftragten sind in einer IT-Sicherheitsleitlinie festgelegt. Herr Nuszkowski ist für die Erstellung und Fortschreibung der Sicherheitskonzeption und das Aufrechterhalten des Sicherheitsniveaus verantwortlich.

2.1.4 Anlassbezogene Kontrollen

Der behördliche Datenschutzbeauftragte führt anlassbezogene Kontrollen durch. Er wirkt beratend und unterstützend an der Behebung erkannter Mängel mit. Die Mängelbearbeitung wird schriftlich dokumentiert. Das ULD hat die Bearbeitung einzelner Mängel stichprobenartig überprüft.

2.1.5 Regelmäßige Kontrollen

Der Datenschutzbeauftragte führt regelmäßige Kontrollen durch. Im Rahmen von regelmäßigen Besprechungen mit den betroffenen Fachbereichen werden datenschutzrechtliche Probleme erläutert und Lösungswege erarbeitet.

2.1.6 Integration von Datenschutz und Datensicherheit in die betrieblichen Prozesse

Der behördliche Datenschutzbeauftragte ist in die Planung und Kontrolle der Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen einbezogen. Er pflegt regelmäßigen Kontakt zum ULD in Fragen des Beschäftigtendatenschutzes und des Schutzes der personenbezogenen Daten der Betroffenen.

Der behördliche Datenschutzbeauftragte führt regelmäßige Schulungen durch.

Durch die anlassbezogenen und regelmäßigen Kontrollen sowie die Beteiligung des behördlichen Datenschutzbeauftragten sind die Anforderungen des § 10 Abs. 4 Punkt 1-3 LDSG erfüllt.

2.1.7 Bearbeitung von Sicherheits- und Datenschutzvorfällen

Die Unfallkasse Nord hat in der Leitlinie zur IT-Sicherheit die Ansprechpartner und das Vorgehen zur Bearbeitung, Dokumentation und Nachbereitung von Sicherheits- und Datenschutzvorfällen festgelegt.

Sicherheits- und Datenschutzvorfälle werden durch ein eigens hierfür festgelegtes Sicherheitsvorfallteam bearbeitet. Zu den festen Mitgliedern des Teams gehört der behördliche Datenschutzbeauftragte, der IT-Sicherheitsbeauftragte und der technische Leiter der Unfallkasse Nord. Das Team kann durch zusätzliche Mitglieder ergänzt werden.

Die schriftliche Nachbereitung von Sicherheitsvorfällen ist zwingend vorgeschrieben.

Das ULD hat die Dokumentation von Sicherheits- und Datenschutzvorfällen und die schriftlichen Nachweise zur Bearbeitung der Sicherheitsvorfälle stichprobenartig vor Ort geprüft. Die Bearbeitung, Dokumentation und Nachbereitung von Vorfällen wurde angemessen und wirksam umgesetzt.

Die Unfallkasse Nord hat geeignete Prozesse für die Umsetzung des § 27a LDSG (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten) definiert.

2.1.8 Umsetzung der Betroffenenrechte

Der behördliche Datenschutzbeauftragte ist für die Bearbeitung von Auskunftsansprüchen von Betroffenen gemäß § 27 LDSG zuständig. Er prüft regelmäßig die angemessene Umsetzung der technischen und organisatorischen Maßnahmen zur Berichtigung, Löschung und Sperrung personenbezogener Daten gemäß § 28 LDSG.

2.1.9 Weitere organisatorischen Vorgaben

Die Zuständigkeiten für die Wartung und Weiterentwicklung der verwendeten informationstechnischen Geräte und automatisierten Verfahren sind in einem Geschäftsverteilungsplan festgelegt. Auf Ebene der jeweiligen Arbeitsgruppen liegt eine klare Aufgabenverteilung vor. Die Anforderungen des § 3 Abs. 2 Satz 5 DSVO sind erfüllt.

2.2 Dokumentation

Die Unfallkasse Nord hat die nach dem LDSG und der DSVO erforderliche Dokumentation der automatisierten Datenverarbeitung modular aufgebaut.

Die Unfallkasse Nord folgt bei der Auswahl angemessener technischer und organisatorischer Sicherheitsmaßnahmen und dem Nachweis einer ordnungsgemäßen und wirksamen Umsetzung den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der vom BSI definierten Vorgehensweise gemäß Standards 100-1 bis 100-3.

2.2.1 Verfahrensverzeichnis

Der behördliche Datenschutzbeauftragte pflegt das Verfahrensverzeichnis in Übereinstimmung mit den Anforderungen des § 7 LDSG. Das ULD hat das Verfahrensverzeichnis stichprobenartig auf Aktualität und angemessene Dokumentation der in § 7 Abs. 1 aufgeführten Sachverhalte geprüft.

Die Anforderungen des § 7 LDSG und § 10 Abs. 4 Punkt 4-5 LDSG sind erfüllt.

2.2.2 Verträge zur Auftragsdatenverarbeitung

Findet in einzelnen Fachverfahren eine Datenverarbeitung im Auftrag statt, so wird diese durch die Unfallkasse Nord ausschließlich auf Basis einer schriftlichen Vereinbarung durchgeführt. Die Vereinbarungen sind Bestandteil der Dokumentation des IT-Einsatzes. Die Anforderungen des § 3 Abs. 2 Punkt 8 und des § 4 Abs. 7 DSVO sind erfüllt.

Die Unfallkasse Nord gibt zu Zwecken der Fehlerbehebung grundsätzlich pseudonymisierte Abzüge von Datenbanken an die Hersteller der Fachverfahren. Ist in Einzelfällen der Zugriff auf personenbezogene Daten notwendig, so wird dieser datensparsam und unter Berücksichtigung der Regelungen des § 80 SGB X ausgestaltet.

Die Unfallkasse Nord schließt Wartungsverträge auf Grundlage der „Ergänzenden Vertragsbedin-

gungen für die Beschaffung von Informationstechnik (EVB-IT)“[1]. Die in den Anlagen der EVB-IT getroffenen Regelungen und Empfehlungen zur Fernwartung bzw. Teleservice werden berücksichtigt.

2.2.3 Installations- und Konfigurationsdokumentation

Für die einzelnen Verfahren verwendeten Geräte und Programme führt die Unfallkasse Nord eine detaillierte Installations- und Konfigurationsdokumentation. Die Dokumentation erfüllt die Anforderungen des § 3 Abs. 2 Punkt 3 DSVO. Sämtliche Systeme des Auditgegenstands sind inklusive des Standorts erfasst. Die Anforderungen des § 3 Abs. 2 Punkt 2 DSVO sind erfüllt.

Für jedes IT-System wird ein Betriebs- und Notfallhandbuch gepflegt, in dem neben der Installations- und Konfigurationsdokumentation der Systeme auch die wesentlichen betrieblichen Rahmendaten zur verwendeten Hardware und die für die Inbetriebnahme notwendigen Schritte festgehalten werden.

Die Grundkonfiguration der Systeme ist standardisiert und in übergeordneten Betriebshandbüchern festgelegt auf die in der Einzeldokumentation der IT-Systeme verwiesen wird.

Die verwendeten Systeme werden über zentrale Konfigurationsmechanismen mit einheitlichen Vorgaben zur Systemsicherheit versehen. Diese Vorgaben sind in eigenen Dokumenten festgehalten. Die Dokumentation wird bei Bedarf fortgeschrieben und regelmäßig geprüft.

2.2.4 Netzplan

Die Unfallkasse Nord hat die für die Verarbeitung personenbezogener Daten verwendeten Geräte sowie die physikalischen und logischen Verbindungen zwischen diesen Geräten in einem Netzplan dokumentiert. Der Netzplan erfüllt die Anforderungen des § 4 Abs. 2 Punkt 4 DSVO.

[1] http://www.cio.bund.de/DE/IT-Beschaffung/EVB-IT-und-BVB/evb-it_bvb_node.html

2.3 Sicherheitsmaßnahmen

2.3.1 Risikoanalyse und Restrisikobetrachtung

Die Unfallkasse Nord folgt der Grundschutz-Vorgehensweise. Die in Grundschutz definierten Gefährdungen wurden explizit auf eine angemessene Darstellung der Risikosituation der Unfallkasse Nord geprüft. Für einzelne Risiken wurden über Grundschutz hinausgehende Maßnahmen getroffen. Das Vorgehen zur Risikoanalyse und Maßnahmenauswahl entspricht dem vorgegeben Vorgehen und ist mit den Anforderungen des § 4 DSVO vereinbar.

2.3.2 Sicherstellung und Kontrolle des ordnungsgemäßen Betriebs

Administrative Änderungen an den informationstechnischen Systemen sind nur einzelnen, explizit berechtigten Mitarbeiterinnen und Mitarbeitern möglich.

Die Unfallkasse Nord hat für die Durchführung der administrativen Tätigkeiten an den vom Auditgegenstand erfassten Systemen konkrete technische und organisatorische Maßnahmen getroffen.

Die durch die Unfallkasse Nord getroffenen Maßnahmen zur Dokumentation von Änderungen an informationstechnischen Geräten, Programmen und Verfahren erfüllen die Anforderungen des § 3 Abs. 2 Punkt 6 der DSVO.

Änderungen werden zunächst auf Testsystemen durchgeführt. Die Durchführung der Tests wird schriftlich dokumentiert. Änderungen werden nach Abstimmung mit dem IT-Sicherheitsbeauftragten freigegeben. Die Anforderungen des § 5 DSVO sind erfüllt.

2.3.3 Räume und Gebäude

Die Unfallkasse Nord ist auf Gebäudekomplexe in Hamburg und Kiel verteilt. Die Serversysteme und Netzkomponenten sind in Serverräumen im Standort Hamburg untergebracht.

Zutritt und Zugriff zu den Räumen und den für die Datenverarbeitung genutzten informationstechnischen Systemen haben nur einzelne, explizit befugte Mitarbeiterinnen und Mitarbeiter. Die Unfallkasse Nord hat konkrete Regelungen zur Begleitung von Fremdpersonal getroffen. Zugriffsberechtigungen werden nach einem einheitlichen Verfahren zur Beantragung und Bewilligung bearbeitet und dokumentiert.

Die Räume sind mit einer Anlage zur Branderkennung ausgestattet. Im Brandfall erfolgt eine automatisierte Alarmierung des Wachdienstes. Die Räume sind klimatisiert. Sämtliche Serversysteme und zentralen Netzwerkkomponenten sind mit einer unterbrechungsfreien Stromversorgung abgesichert.

Das ULD hat die korrekte Umsetzung der Maßnahmen zur Raum- und Gebäudesicherheit stichprobenartig vor Ort überprüft.

2.3.4 Netzwerk und Server

Das interne Netz der Unfallkasse Nord ist als strukturierte Verkabelung ausgeführt. Sämtliche aktive Netzgeräte (Switches und Router) sind in verschlossenen Serverschränken untergebracht.

Zugang zum Netz ist grundsätzlich nur in den Büroräumen möglich, nicht für den Publikumsverkehr zugänglichen Bereich. Nicht benötigte Anschlüsse in den Büroräumen sind nicht beschaltet.

Sämtliche Systeme werden in einem zentralen Verzeichnisdienst verwaltet. Ausnahmen bilden lediglich eigenständige, vernetzte Peripheriesysteme wie Netzdrucker und die eingesetzten aktiven Netzkomponenten.

Jedes Rechnersystem ist mit einem Virenscanner ausgestattet. Der Virenscanner wird zumindest täglich aktualisiert. Die korrekte Funktion des Virenscanners sowie seine Aktualität werden zentral überwacht.

Jedes System wird regelmäßig mit Patches, Bugfixes und Service Packs versehen. Die Unfallkasse sorgt durch eine automatisierte Lösung und angemessene Prozesse zur Bewertung und Freigabe von Aktualisierungen dafür, dass jedes Rechnersystem zeitnah mit Sicherheitsaktualisierungen versehen wird.

2.3.5 Endgeräte

Die den Mitarbeiterinnen und Mitarbeitern der Unfallkasse Nord zur Verfügung stehenden Arbeitsplatz-PCs werden zentral konfiguriert und administriert. Jeder Arbeitsplatz-PC wird sowohl bei der Erstinstallation als auch bei der weiteren Pflege der installierten Programme mit getesteten und freigegebenen Programmversionen versehen.

Durch den Einsatz von Gruppenrichtlinien werden die zur Verfügung stehenden Funktionen auf das für die Aufgabenerfüllung notwendige Maß reduziert und administrative Eingriffsmöglichkeiten durch Beschäftigte verhindert und Eingriffe protokolliert.

Daten auf mobilen Endgeräten werden verschlüsselt.

3 Datenschutzrechtliche Bewertung

3.1 Prüfungsverlauf

Das Auditverfahren wurde vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) über mehrere Phasen durchgeführt.

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

Die Auditierung wurde zur Ergebnissicherung durch ein Voraudit vorbereitet. Im Voraudit wurde überprüft, ob bei der Unfallkasse Nord die Voraussetzungen für das Datenschutz-Behördenaudit vorliegen.

In dieser ersten Phase hat das ULD die Unfallkasse Nord durch die Prüfung und Bewertung einzelner Dokumente und Konzepte unterstützt. In mehreren Terminen vor Ort wurden gemeinsam mit der Unfallkasse Nord die notwendigen Regelungen und Nachweise besprochen und deren Ausgestaltung festgelegt.

Die Durchführung des Voraudits erfolgte in den nachfolgend genannten Schritten:

- Abgrenzung des Auditgegenstands,
- Festlegung der Datenschutzziele,
- Sammlung der zum Auditgegenstand gehörenden Dokumentation,
- Bestandsaufnahme der technischen und organisatorischen Abläufe,
- Erstellung eines Ergebnisberichts mit Projektplan,
- Mängelbeseitigung,
- Einrichtung eines Datenschutzmanagementsystems,
- Erstellung des Datenschutzkonzepts,
- Aufbereitung der für das Datenschutz-Behördenaudit erforderlichen Dokumentation sowie
- abschließende Überprüfung der Erfüllung aller im Voraudit festgelegten und durchzuführenden Aufgaben.

Das Voraudit wurde durch Frau Anke Nöbel, Mitarbeiterin des Unabhängigen Landeszentrums für Datenschutz, durchgeführt.

Nach dem Voraudit wurden die Konzepte und Nachweise dem ULD zur Durchführung des Datenschutz-Behördenaudits übergeben. Die Überprüfung der Konzeption erfolgte auf Basis eines konsolidierten Dokumentenstands.

Das ULD hat die vorliegenden Dokumente auf die Vereinbarkeit mit den datenschutzrechtlichen Vorgaben gemäß Landesdatenschutzgesetz Schleswig-Holstein (LDSG) und der Datenschutzverordnung (DSVO) geprüft.

Die Durchführung des Datenschutz-Behördenaudits erfolgt auf Basis der Ergebnisse des Voraudits 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.

Nach der Dokumentenprüfung hat das ULD in einem Termin vor Ort die Angemessenheit und Wirksamkeit einer Auswahl der in den vorliegenden Dokumenten und Nachweisen dargestellten Sicherheitsmaßnahmen stichprobenartig überprüft. Das ULD hat sich durch diese Prüfungen vergewissert, dass die im Konzept dargestellten Maßnahmen seitens der Unfallkasse Nord angemessen und wirksam umgesetzt werden. Hierzu wird ergänzend auf das Gutachten „Personalverwaltung, Rehabilitation und Leistung, Regress, Schnittstelle Prävention – Arbeitsschutz“ verwiesen.

Das Auditverfahren wurde durch Herrn Henry Krasemann und Herrn Sven Thomsen durchgeführt.

3.2 Rechtliche Anforderungen

Die Unfallkasse Nord ist die gesetzliche Unfallversicherung für den öffentlichen Dienst in Schleswig-Holstein und Hamburg. Aufgabe der Unfallkasse ist es, nach Maßgabe des Siebten Buches Sozialgesetzbuch (SGV VII) Arbeitsunfälle und Berufskrankheiten zu verhüten und nach Eintritt von Arbeitsunfällen oder Berufskrankheiten Versicherte oder Hinterbliebene zu unterstützen und zu entschädigen.

Die Unfallkasse Nord ist eine rechtsfähige landesunmittelbare Körperschaft des öffentlichen Rechts mit Selbstverwaltung.

Rechtsstellung, Organisation, Aufgaben und weitere Regelungen sind in der Satzung der Unfallkasse Nord festgelegt.

Die fachliche Aufsicht über die Unfallkasse Nord führt zum Zeitpunkt des Auditverfahrens das Ministerium für Soziales, Gesundheit, Familie und Gleichstellung.

Die Unfallkasse Nord unterliegt bei der Verarbeitung personenbezogener Daten dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG) und der Datenschutzverordnung (DSVO).

Die automatisierte Verarbeitung personenbezogener Daten erfordert technische und organisatorische Maßnahmen, die die Datensicherheit bzw. die Ordnungsmäßigkeit der Datenverarbeitung gewährleisten. Des Weiteren sind interne Regelungen zu treffen, die insbesondere personelle und organisatorische Aspekte mit einbeziehen. Es muss zudem gewährleistet sein, dass die daten-

schutzrechtlichen Anweisungen auch tatsächlich in konkrete Datensicherungsmaßnahmen umgesetzt werden und ihre Einhaltung durch das Datenschutzmanagement kontrolliert wird. Dabei sind insbesondere folgende Rechtsvorschriften zu beachten:

Landesdatenschutzgesetz (LDSG)

- § 4 Datenvermeidung und Datensparsamkeit
- § 5 Allgemeine Maßnahmen zur Datensicherheit
- § 6 Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren
- § 7 Verfahrensverzeichnis, Meldung
- § 9 Vorabkontrolle
- § 10 Behördliche Datenschutzbeauftragte
- § 17 Verarbeitung personenbezogener Daten im Auftrag

Datenschutzverordnung (DSVO)

- § 3 Verfahrensdokumentation
- § 4 Dokumentation der Sicherheitsmaßnahmen
- § 5 Dokumentation des Tests und der Freigabe

Zusätzlich sind bereichspezifische rechtliche Regelungen regelmäßig daraufhin zu prüfen, ob detaillierte Vorgaben zu Aufbewahrungsfristen, Dokumentationsvorgaben oder Löschfristen bestehen oder sich geändert haben.

Die Überprüfung hat ergeben, dass die schriftlich festgelegten Maßnahmen angemessen sind und vollständig umgesetzt werden. Hierzu wird ergänzend auf das Gutachten „Personalverwaltung, Rehabilitation und Leistung, Regress, Schnittstelle Prävention – Arbeitsschutz“ verwiesen.

3.3 Zusammenfassende Bewertung

Im Auditverfahren wurde festgestellt, dass die Unfallkasse Nord über angemessene und wirksame Sicherheits- und Datenschutzmaßnahmen für die allgemeine Datenverarbeitung verfügt.

Das Datenschutz- und Sicherheitsmanagement orientiert sich an internationalen Standards. Insbesondere folgt das Informationssicherheits-Managementsystem den Vorgaben des Standards 100-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI). Auf Ebene der technischen und organisatorischen Maßnahmen folgt das Informationssicherheits-Managementsystem mit den Vorgaben der IT-Grundschutz-Vorgehensweise gemäß Standard 100-2 des BSI und den Grundschutz-Katalogen.

Darüber hinaus wurden bei der Durchführung des Audits folgende Aspekte festgestellt, die im Sinne einer **datenschutzkonformen und –fördernden Gestaltung von Technik und Organisation** besonders hervorzuheben sind:

1. Datenschutzbeauftragter und IT-Sicherheitsbeauftragter arbeiten in und mit einem Managementsystem für den Datenschutz und die Informationssicherheit, welches durch regelmäßige und anlassbezogene Kontrollen ein hohes Maß an Datenschutz sicherstellt. Definierte Prozesse zur Bearbeitung von Datenschutz- und Sicherheitsvorfällen sowie eine funktionierende Einbindung in IT-Projekte bereits in der Planungsphase sind geeignet, das hohe Niveau zu halten.
2. Die Sicherheitsprozesse sind unter Berücksichtigung eines national anerkannten Sicherheitsstandards gestaltet. Das Datenschutzmanagement orientiert sich eng an den Vorgaben zur Ordnungsmäßigkeit der Datenverarbeitung der Datenschutzverordnung (DSVO).
3. Die technischen und organisatorischen Abläufe des Datenschutz- und Informationssicherheits-Managementsystems sind vollständig und nachvollziehbar beschrieben.

Die Prüfung hat ergeben, dass das Datenschutz- und Informationssicherheits-Managementsystem sowie die technischen und organisatorische Umsetzung keinen Anlass zu datenschutzrechtlichen Beanstandungen geben. Der Auditgegenstand wird ordnungsgemäß betrieben. Die Verarbeitung personenbezogener Daten ist rechtmäßig.

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

Kiel, 20.03.2013

(Henry Krasemann, Auditor Recht) (Sven Thomsen, Auditor Technik)