Gutachten

(öffentlich)

Auditverfahren gemäß § 43 Abs. 2 LDSG

Gemeindeverwaltung Ratekau

Interne automatisierte Datenverarbeitung

Anbindung des internen Netzes an externe Netze

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Kiel, 7. Oktober 2014

Auditoren: Heiko Behrendt, Henry Krasemann

Az.: 16.01/06.002

E-Mail: mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits

1.1 Vereinbarung

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

Gegenstand des Datenschutz-Behördenaudits ist **die Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung der Gemeindeverwaltung Ratekau**.

Dazu gehören:

- der Betrieb der Arbeitsplatz-PCs, Server und Netzkomponenten ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter,
- die Anbindung des internen Netzes der Gemeindeverwaltung an externe Netze (Internet, Landesnetz und Kindergärten),
- die eingesetzten Arbeitsplatz-PCs im kommunalen Kinderhaus mit den Kindergärten der Standorte Ratekau, Sereetz und Pansdorf.

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 Auditierung wurde zur Ergebnissicherung durch ein Voraudit vorbereitet. Im Voraudit wurde überprüft, ob in der Gemeindeverwaltung Ratekau die Voraussetzungen für das Datenschutz-Behördenaudit vorliegen. 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.

Die Durchführung des Datenschutz-Behördenaudits erfolgte 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.

Die von der Gemeindeverwaltung Ratekau vorgelegte Dokumentation für den Auditgegenstand bildete die Grundlage für die Begutachtung vor Ort.

1.3 Datenschutzziele

Die Gemeindeverwaltung Ratekau hat in einem Sicherheitskonzept Ziele für den sicheren und datenschutzkonformen Einsatz festgelegt. Die Ordnungsmäßigkeit der automatisierten Datenverarbeitung in der Gemeindeverwaltung Ratekau soll unter Berücksichtigung

- der Vertraulichkeit (z. B. Schutz vor unbefugter Kenntnisnahme von Daten),
- der Integrität (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen oder der Manipulation von Daten),
- der Verfügbarkeit (z. B. Schutz vor Diebstahl oder Zerstörung),
- der Transparenz (z. B. Schutz vor einer unstrukturierten Datenverarbeitung),
- der Nicht-Verkettbarkeit (z. B. Schutz vor unbefugter Datennutzung) und
- der Intervenierbarkeit (z. B. Schutz vor Verweigerung der Ausübung von Betroffenenrechten)

der zur Aufgabenerfüllung notwendigen personenbezogenen Daten gewährleistet werden.

Die Gemeindeverwaltung Ratekau 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. Die festgelegten Sicherheitsmaßnahmen gelten als Mindestanforderung für alle Bereiche der Gemeindeverwaltung.

2 Feststellungen im Rahmen der Begutachtung

2.1 Datenschutz- und IT-Sicherheitsmanagement

Die Gemeindeverwaltung Ratekau hat für die ordnungsgemäße Datenverarbeitung ein Datenschutz- und IT-Sicherheitsmanagement mit folgenden Funktionsträgern eingerichtet:

- Datenschutzbeauftragte Frau Schönrock
- Hauptamtsleitung Frau Böhm
- Personalrat Frau Krause
- Administration Herr Georgi-Scholl
- Administration Herr Riek

Als behördliche Datenschutzbeauftragte ist Frau Schönrock gemäß § 10 LDSG schriftlich bestellt. Ihr wurden u. a. folgende Aufgaben übertragen:

- Unterstützung bei der Erstellung des Sicherheitskonzepts und anderer Sicherheitsrichtlinien,
- Untersuchung sicherheitsrelevanter Zwischenfälle,
- Durchführung von Sensibilisierung- und Schulungsmaßnahmen,
- Koordinierung der Sitzungen für das Datenschutz- und IT-Sicherheitsmanagement,
- Steuerung und Koordinierung des IT-Sicherheitsprozesses,
- Festlegung und Überprüfung von Sicherheitsanforderungen.

Darüber hinaus ist festgelegt, dass die Datenschutzbeauftragte interne Audits durchführt, bei denen stichprobenartig die Umsetzung, Wirksamkeit und Praktikabilität der im Sicherheitskonzept getroffenen Maßnahmen überprüft werden.

Im Rahmen des Datenschutz- und IT-Sicherheitsmanagements hat die Gemeindeverwaltung Ratekau für die Behandlung von Sicherheitsvorfällen Zuständigkeiten und Organisationsabläufe festgelegt. Die Mitarbeiterinnen und Mitarbeiter können einen identifizierten Sicherheitsvorfall den zuständigen Personen anzeigen, so dass nach Mitteilung der Vorfall sofort bearbeitet werden kann. Die Ergebnisse der Überprüfung werden schriftlich dokumentiert.

Der Bürgermeister wird über die Tätigkeiten des Datenschutz- und IT-Sicherheitsmanagements in regelmäßigen Abständen von der Datenschutzbeauftragten und/oder der Hauptamtsleiterin informiert.

2.2 Infrastruktur, IT-Systeme, Netz und Anwendungen

2.2.1 Büroräume

Die Gemeindeverwaltung Ratekau nutzt das Gebäude Bäderstraße 19, 23626 Ratekau. Es ist eine ausreichende räumliche Abschottung vorhanden. Alle Räume sind verschließbar und mit ausreichendem Ablageplatz in verschließbaren Schränken ausgestattet.

2.2.2 Serverraum

Die Gemeindeverwaltung Ratekau verfügt über 2 Serverräume. Zutritt zu den Räumen haben nur befugte Personen. Die Serverräume sind mit einer Brandmeldeanlage und einer Klimatisierung ausgestattet.

2.2.3 IT-Komponenten

Folgende IT-Komponenten werden eingesetzt:

- Citrix Verwaltungsserver
- Domaincontroller mit Windows Server 2008 R2
- Datenbankserver mit Microsoft SQL 2008 R2
- Groupware mit Exchange Server 2013
- Applikations-Terminalserver mit Windows Server 2008 R2
- Systemmanagementserver (Virenschutz)
- Windows Server Update Service (WSUS)
- Igel UMS, Verwaltungsserver
- Printserver
- Loginventory für Hard- und Software Inventarisierung
- USV Stationen
- Firewall
- Switches
- Igel Thin-Client mit Terminalserver-Anbindung
- PCs mit Windows 7
- Testrechner mit Windows 2008 R2 Hyper-V

2.2.4 Systemmanagement

Alle Server und Clients werden in einem zentralen Verzeichnisdienst (Active Directory von Microsoft) verwaltet. Ausnahmen bilden lediglich eigenständige, vernetzte Peripheriesysteme wie Netzdrucker und die eingesetzten aktiven Netzkomponenten wie Switches, Router und die Firewall.

Die Server und Clients mit Windows-Betriebssystemen sind mit einer Antivirensoftware ausgestattet. Der Virenscanner wird täglich aktualisiert. Die korrekte Funktion des Virenscanners sowie seine Aktualität werden zentral überwacht.

Die Fachanwendungen werden auf Terminalserver betrieben. Für die mit den Fachanwendungen verwalteten Daten wird ein gesonderter Datenbankserver eingesetzt.

Die auf den Servern und Clients installierten Windows-Betriebssysteme werden regelmäßig mit Patches, Bugfixes und Service Packs versehen. Die Gemeindeverwaltung betreibt hierzu einen WSUS-Server (Windows Server Update Services der Firma Microsoft).

Die einzelnen Server werden in einer Virtualisierungsplattform Citrix XenServer auf einem redundant ausgelegten Hostsystem betrieben. Die physischen Systeme und Netzwerkkomponenten sind an einer unterbrechungsfreien Stromversorgung angeschlossen.

Die Verwaltung von Daten erfolgt ausschließlich auf einem zentralen Network Attached Storage (NAS). Die Daten des Systems werden auf einem Backupsystem und auf einer gesonderten Datensicherungsfestplatte gesichert. Die verwendeten Sicherungsbänder werden in einem feuersicheren Tresor aufbewahrt. Nur befugte Personen haben Zugriff auf die Datensicherungsmedien.

Für den Test von z. B. Fachanwendungen, Systemmanagementsoftware und Patches verfügt die IT-Administration über einen Testserver.

2.2.5 Arbeitsplatz-PCs

Als Arbeitsplatz-PCs werden überwiegend Thin-Clients eingesetzt. Sie werden zentral konfiguriert und administriert. Auf den Thin-Clients werden keine Daten verwaltet.

Durch den Einsatz von Gruppenrichtlinien und der für Thin-Clients eingesetzten Management Suite werden

- die zur Verfügung stehenden Anwendungen und Funktionen auf das für die Aufgabenerfüllung notwendige Maß reduziert und
- administrative Eingriffsmöglichkeiten durch Beschäftigte verhindert.

Externe Schnittstellen (Laufwerke, USB, serielle oder parallele Anschlüsse) werden grundsätzlich gesperrt und nur bei Bedarf nach Genehmigung durch die Leitungsebene freigeschaltet.

2.2.6 Zentrale Multifunktionsgeräte

Die Gemeindeverwaltung setzt für Kopier- und Druckaufträge zwei vernetzte Multifunktionsgeräte ein. Die Systeme verfügen über die Funktion, Druckaufträge nur nach Eingabe eines PIN-Codes auszugeben, und sind entsprechend konfiguriert. Im Falle eines Austausches der Multifunktionsge-

räte durch die zuständige Wartungsfirma Heinrich Hünicke GmbH & Co. KG verbleibt die Festplatte zukünftig im Hause. Die Administration löscht die Daten auf der Festplatte physikalisch mit einer entsprechenden Software.

2.2.7 Internes Netz

Das interne Netz der Gemeindeverwaltung ist als strukturierte Verkabelung ausgeführt. Sämtliche aktive Netzgeräte (Switches und Router) sind in verschlossenen Serverschränken untergebracht. Zugang zum Netz ist mit Ausnahme eines im Hausflur aufgestellten zentralen Multifunktionsgeräts grundsätzlich nur in den Büroräumen möglich. Nicht benötigte Anschlüsse in den Büroräumen sind nicht beschaltet.

2.2.8 Firewall und Netzübergänge

Das interne Netz der Gemeindeverwaltung ist an das Landesnetz, an das Internet sowie mit den Kindergärten an den Standorten Ratekau, Sereetz und Pansdorf verbunden. Als zentraler Übergabepunkt ist eine Firewall eingerichtet, die sämtliche Datenverbindungen aus dem internen Netz in die angeschlossenen Netze kontrolliert.

Zugänge zum Internet erfolgen über die externen Dienstleister Dataport und Kabel Deutschland.

Der gesamte Datenverkehr des verwaltungsinternen Netzes mit externen Netzen wird an den Netzübergängen freigeschaltet. Es gilt das Prinzip: „Es ist alles verboten, was nicht ausdrücklich erlaubt ist."

Der Datenverkehr wird nicht nur auf seine Zulässigkeit, sondern auch auf schadhafte Inhalte wie Viren, Würmer und Trojaner geprüft. Die Gemeindeverwaltung setzt hierfür eine Sicherheitssoftware ein, die die übertragenen Daten auf schadhafte Inhalte kontrolliert.

2.2.9 Kindergärten Ratekau, Sereetz und Pansdorf[1]

Die Kindergärten an den Standorten Ratekau, Sereetz und Pansdorf sind mit ihrer Datenverarbeitung jeweils über einen DSL-Anschluss an dem internen Netz der Gemeindeverwaltung Ratekau angeschlossen. Die Datenkommunikation zwischen Kindergärten und Gemeindeverwaltung erfolgt durch Einsatz einer Sicherheitssoftware (VPN) verschlüsselt. Damit erhalten die Kindergärten die Möglichkeit, ihre Daten auf gesicherten zentralen Komponenten der Gemeindeverwaltung zu speichern. Die Kindergärten setzen jeweils einen Thin-Client ein, über den die erforderlichen Fachanwendungen und Daten auf Systemen der Gemeindeverwaltung aufgerufen werden können.

[1] In Bezug auf die Datenverarbeitung der Kindergärten wurde ausschließlich die sichere netztechnische Anbindung mittels Thin-Clients begutachtet.

2.2.10 Zentrale Datenablage

Für die mit MS-Office verwalteten Datenbestände wird von den Mitarbeitern und Mitarbeiterinnen eine fachbereichs- und mitarbeiterbezogene Datenablage genutzt. In dieser werden u. a. Word- und Excel-Dokumente gespeichert.

2.3 Dokumentation

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

2.3.1 Systemakten

In einer Dienstanweisung ist festgelegt, dass für zentrale Systemkomponenten eine Systemakte zu führen ist. Aufbau und Inhalt der Systemakte sind größtenteils vorgegeben und standardisiert. Sie enthalten

- stichwortartig alle von der IT-Koordination ausgeführten Installations- und Konfigurationsarbeiten,
- einen Nachweis über die Durchführung der Datensicherungen,
- eine Übersicht über zugewiesene Zugriffsrechte,
- die Konfiguration des Systems und die ausgeführten Einstellungen an der Software sowie
- ein Datenträger-, Programm- und Verfahrensbestandsverzeichnis.

2.3.2 Verfahrensakten

In den Verfahrensakten befinden sich Informationen über das Verfahrensverzeichnis gemäß § 7 LDSG sowie eine Dokumentation über die vergebenen Berechtigungen.

Darüber hinaus werden für das jeweilige Fachverfahren die Test- und Freigabeaktivitäten dokumentiert.

2.3.3 IT-Konzept

Die Gemeindeverwaltung hat die technischen und organisatorischen Vorgaben für die Verarbeitung personenbezogener Daten in einem informationstechnischen Konzept zusammengefasst.

Neben Vorgaben für die Server-, Client- und Netzinfrastruktur sind im IT-Konzept die Aufgaben, Rechte und Obliegenheiten der Systemadministration und der Datenschutzbeauftragten festgelegt.

Das IT-Konzept dokumentiert zusammen mit den System- und Verfahrensakten den Ist-Stand der Informations- und Kommunikationsinfrastruktur der Gemeindeverwaltung Ratekau.

2.3.4 Sicherheitskonzept

Im Sicherheitskonzept für die automatisierte Datenverarbeitung der Gemeindeverwaltung Ratekau werden die technischen und organisatorischen Maßnahmen dargestellt, die seitens der Gemeindeverwaltung getroffen worden sind.

Das Sicherheitskonzept enthält unter anderem Maßnahmen für

- Organisation und Personal,
- IT-Systeme,
- Anwendungen,
- Datensicherung und Datenträger,
- Schulung,
- Kontrolle und Nachvollziehbarkeit sowie für
- externe Dienstleiser und Besucher.

Das Sicherheitskonzept enthält darüber hinaus eine Übersicht der den festgelegten Sicherheitsmaßnahmen zugrunde gelegten Gefährdungen sowie eine Restrisikobetrachtung.

2.3.5 Datenschutz- und IT-Sicherheitsmanagement

Die Einrichtung eines Datenschutz- und IT-Sicherheitsmanagements wurde in einem gesonderten Dokument festgelegt (siehe auch Tz. 2.1). Es wurden u. a. folgende Aspekte dokumentiert:

- Funktion des Datenschutz- und IT-Sicherheitsmanagements
- Verantwortliche und Ansprechpartner/innen
- Aufgaben der Datenschutzbeauftragten
- Durchführung von Audits
- Behandlung von Sicherheitsvorfällen
- Überwachung des Datenschutz- und IT-Sicherheitsmanagements

2.3.6 Dienstanweisungen

Die im IT-Konzept und im Sicherheitskonzept festgelegten technischen und organisatorischen Regelungen wurden in Handlungsanweisungen im Rahmen von Dienstanweisungen mitarbeiterbezogen übertragen. Die folgenden Dienstanweisungen sind zum Zeitpunkt des Audits in Kraft:

- In der Dienstanweisung „Nutzung der IT-Systeme“ (Stand 2014) wird der Umgang mit den Informations- und Kommunikationssystemen der Gemeindeverwaltung geregelt. Insbesondere ist festgelegt, dass die Informations- und Kommunikationssysteme nur nach vorheriger Freigabe und ausschließlich zu dienstlichen Zwecken genutzt werden dürfen. Der Einsatz privater Hardware ist untersagt.

- Die Dienstanweisung „Internet“ (Stand 2014) hält unter anderem fest, dass Internet-Dienste nur als Informationsmedien in dienstlichen Belangen genutzt werden dürfen.
- In der Dienstanweisung „Administrationsebene“ (Stand 2014) werden die Aufgaben und Zuständigkeiten der IT-Administration festgelegt.

2.3.7 Auftragsdatenverarbeitung mit Dienstleister

2.3.7.1 ZVO Entsorgung GmbH

Die ZWO Entsorgung GmbH wurde mit der Akten- und Datenträgervernichtung beauftragt. Der Auftragnehmer sichert eine Vernichtung im Rahmen der DIN 15713 von 2009 zu und bringt hierzu Prüfprotokolle bei. Im Rahmen der Überprüfung wurde eine Prüfbescheinigung vorgelegt, dass die Zerkleinerungsstufe 6 der DIN 15713 erreicht wird, so dass eine Reproduktion nur mit erhöhtem Aufwand möglich ist.

2.3.7.2 Tenzing – Dr. Müller & Partner GmbH

Die Firma Tenzing ist damit beauftragt, Projektunterstützung in der IT wie z. B. Redesign des Netzes, Wartung der Infrastruktur / Server und Fernwartungsunterstützung zu leisten. Erforderliche Dienstleistungen werden von der Gemeindeverwaltung Ratekau anlassbezogen bei der Firma Tenzing beauftragt.

2.3.7.3 CC e-gov GmbH

Die Firma CC e-gov GmbH erbringt „Sersharing“ bzw. Providerdienstleistungen im Zusammenhang mit der Software „Allris“, einem Ratsinformationssystem. So werden u. a. Tagesordnungen und Sitzungsprotokolle der Gemeindevertretung über die Webseite der Gemeindeverwaltung bereitgestellt.

3 Datenschutzrechtliche Bewertung

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 datenschutzrechtlichen 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

Datenschutzverordnung (DSVO)

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

Zusätzlich sind bereichsspezifische 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 im Sicherheitskonzept festgeschriebenen Maßnahmen angemessen sind und vollständig umgesetzt werden.

Die behördliche Datenschutzbeauftragte verfügt über die erforderliche Sachkunde und Zuverlässigkeit. Ihre Bestellung steht in keinem Konflikt mit anderen dienstlichen Aufgaben.

Das Datenschutz- und IT-Sicherheitsmanagement nimmt seine Aufgaben im erforderlichen Maße wahr und sorgt für eine nachhaltige Bearbeitung.

Für die Auftragsdatenverarbeitung mit den Dienstleistern wurden Verträge vorgelegt, die den gesetzlichen Anforderungen nach § 11 BDSG bzw. § 17 LDSG entsprechen. In Zusatzvereinbarungen wurden insbesondere die von den Dienstleistern umzusetzenden technischen und organisatorischen Maßnahmen festgelegt und vereinbart.

Die durch das Datenschutz-Behördenaudit in der Gemeindeverwaltung Ratekau erfassten Verarbeitungsprozesse zeichnen sich besonders durch folgende „datenschutzfreundliche“ Aspekte aus:

- Die mit den Fachverfahren der Gemeindeverwaltung verarbeiteten Bürgerdaten werden durch ausreichende IT-Sicherheitsmaßnahmen geschützt.
- An den Arbeitsplätzen werden sogenannte Thin-Clients eingesetzt, über die ein besonderer Schutz der Datenverarbeitung am Arbeitsplatz gewährleistet wird. So können Datenbestände nicht mehr lokal, sondern nur zentral gespeichert werden. Ferner lassen sich Sicherheitsfunktionen zentral und einheitlich administrieren. CD-ROM-Laufwerke und Schnittstellen für USB-Speichermedien sind auf den Thin-Clients grundsätzlich deaktiviert.
- Die Gemeindeverwaltung hat eine gut strukturierte, systematische und übersichtliche Dokumentation gemäß DSVO erstellt. Diese bietet eine effektive Arbeitsgrundlage für das Datenschutz- und IT-Sicherheitsmanagement.
- Für den Anschluss des internen Verwaltungsnetzes an das Internet werden Sicherheitskomponenten eingesetzt, die unerwünschte Zugriffe abwehren.
- Die Sicherheitsmechanismen zur zentralen Vergabe von Berechtigungen und der Steuerung der Arbeitsplatzrechner werden intensiv genutzt.
- Das Datenschutz- und IT-Sicherheitsmanagement führt in regelmäßigen Abständen Sitzungen durch, in denen Datenschutz- und IT-Sicherheitsaspekte bearbeitet werden. Darüber hinaus wurden organisatorische Abläufe für die Behandlung von auftretenden Sicherheitsvorfällen festgelegt.

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

Kiel, 7. Oktober 2014 gez. Heiko Behrendt gez. Henry Krasemann