Gutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Gemeinde Stockelsdorf

Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Kiel, 27. September 2017

Auditor: Heiko Behrendt

Az.: 16.01/16.004

E-Mail: mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits

1.1 Vereinbarung

Grundlage des Datenschutz-Behördenaudits ist der Audit-Vertrag zwischen der Gemeinde Stockelsdorf und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

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

Dazu gehören:

- der Betrieb der PCs, Notebooks, Tablets, Smartphones, Server und Netzkomponenten ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter sowie
- die Anbindung des internen Netzes der Gemeinde Stockelsdorf an externe Netze.

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“. Der Gemeinde Stockelsdorf wurde bereits im Jahr 2007 ein Datenschutzaudit-Zertifikat vergeben. Dieses wurde aber nach Ablauf im Jahr 2010 nicht erneuert.

Die Auditierung wurde zur Ergebnissicherung durch ein Voraudit vorbereitet. Im Voraudit wurde überprüft, ob bei der Gemeinde Stockelsdorf die Voraussetzungen für das Datenschutz-Behördenaudit vorliegen. Die Überprüfung umfasste u. a. folgende Aspekte:

- Abgrenzung des Auditgegenstands,
- Festlegung der Datenschutzziele,
- die zum Auditgegenstand gehörende Dokumentation,
- Einrichtung eines Datenschutzmanagementsystems,
- Erstellung der Dokumentation für Datenschutz- und Informationssicherheit auf Grundlage des IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und
- Umsetzung von technischen und organisatorischen Maßnahmen des Grundschutzkatalogs.

Die Durchführung des Datenschutz-Behördenaudits erfolgte auf Basis der Ergebnisse des Voraudits in den folgenden Schritten:

- Überprüfung der Abgrenzung des Auditgegenstands,
- Analyse der Datenschutz- und Informationssicherheitsdokumentation,

- Begutachtung der Wirkungsweise des Datenschutzmanagementsystems und der Erreichung der festgelegten Datenschutzziele,
- Hervorhebung von besonders anerkennenswerten und datenschutzfreundlichen Datenverarbeitungsprozessen,
- stichprobenartige Überprüfung der Umsetzung der festgelegten Sicherheitsmaßnahmen und
- Überprüfung der Einhaltung datenschutzrechtlicher und bereichsspezifischer Vorschriften in Bezug auf den Auditgegenstand.

Die von der Gemeinde Stockelsdorf vorgelegte Dokumentation für den Auditgegenstand bildete die Grundlage für die Begutachtung vor Ort.

2 Feststellungen im Rahmen der Begutachtung

2.1 Datenschutz- und Informationssicherheitsstrategie

In der Leitlinie für Datenschutz und Informationssicherheit hat die Gemeinde Stockelsdorf Leitaussagen zu ihrer **Datenschutz- und Informationssicherheitsstrategie** zusammengefasst, um die festgelegten Datenschutz- und Sicherheitsziele und das angestrebte Datenschutz- und Sicherheitsniveau für alle Mitarbeiter zu dokumentieren. Mit der Datenschutz- und Sicherheitsleitlinie bekennt sich die Leitungsebene zu ihrer Verantwortung für Datenschutz und Informationssicherheit.

Für die Implementierung einer nachvollziehbaren und messbaren Sicherheit der IT orientiert sich die Gemeinde Stockelsdorf an dem international anerkannten Grundschutzstandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Dabei werden die datenschutzrechtlichen Anforderungen für die personenbezogene Datenverarbeitung berücksichtigt.

Es wurden folgende Datenschutz- und Informationssicherheitsziele festgelegt:

- Es werden nur die für die Aufgabenerfüllung benötigten Daten gespeichert und vorgehalten (Datenminimierung),
- die bereichsspezifischen Vorschriften zur ordnungsgemäßen Datenverarbeitung und des Datenschutzes werden eingehalten (Vertraulichkeit),
- die Daten werden nur in der vorgeschriebenen Verfahrensweise verarbeitet (Integrität),
- die von den Nutzern benötigten Daten stehen kontinuierlich im erforderlichen Umfang zur Verfügung (Verfügbarkeit),
- Daten werden nur für den Zweck verarbeitet und ausgewertet, für den sie erhoben wurden (Nichtverkettbarkeit),
- Verfahren werden so gestaltet, dass die Gemeinde in die Datenverarbeitung eingreifen kann und den Betroffenen die Ausübung der ihnen zustehenden Rechte (u. a. Auskunft, Berichtigung, Sperrung und Löschung) wirksam möglich ist, und

- Betroffene und auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen können erkennen, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt (Transparenz).

Darüber hinaus ist in der Leitlinie festgelegt, dass zur Erreichung der Datenschutz- und Informationssicherheitsziele ein behördlicher Datenschutzbeauftragter (DSB) ernannt und ein Datenschutz- und Informationssicherheitsmanagement-Team (DISM-Team) eingerichtet wird.

2.2 Datenschutz- und Informationssicherheitsmanagement-Team (DISM)

Das **DISM-Team** initiiert, steuert und kontrolliert den Datenschutz und Informationssicherheitsprozess in der Gemeinde Stockelsdorf. Es besteht aus folgenden Personen:

- Frau Rahlf-Behrmann, Bürgermeisterin
- Herr Kerbstadt, Hauptamtsleitung
- Herr Büker, Datenschutzbeauftragter
- Herr Schulz, IT-Administration

Das DISM-Team führt regelmäßige oder anlassbezogen Sitzungen durch. Es

- steuert und koordiniert den Informationssicherheitsprozess und stellt den dazugehörigen Informationsfluss sicher,
- initiiert und koordiniert die Erstellung von allgemein notwendigen Datenschutz- und IT-Sicherheitsrichtlinien,
- erstellt und koordiniert datenschutz- und sicherheitsrelevante Konzepte und überwacht deren Umsetzung,
- erstellt und koordiniert weiterführende Konzepte, soweit sie für den Datenschutz und die Informationssicherheit erforderlich sind,
- legt in Zusammenarbeit mit den Verantwortlichen der Ämter die Datenschutz- und Sicherheitsanforderungen / Sicherheitsstufe von Fachverfahren fest (Schutzbedarfsfeststellung) und überprüft diese,
- koordiniert datenschutz- und sicherheitsrelevante Projekte,
- untersucht datenschutz- und sicherheitsrelevante Zwischenfälle,
- kann alle relevanten Verträge und Konzepte oder deren Entwürfe einsehen,
- veranlasst oder erstellt Berichte über Datenschutz- und Sicherheitsvorfälle.

2.3 Behördlicher Datenschutzbeauftragter (DSB)

Als behördlicher Datenschutzbeauftragter wurde Herr Büker gemäß § 10 LDSG schriftlich bestellt. Er ist für die organisatorische Abwicklung und Koordination der Datenschutzmanagementsitzungen, umzusetzender Maßnahmen und eines zugehörigen Berichtswesens einschließlich Managementberichten an die Leitung zuständig. Darüber hinaus werden von ihm in Zusammenarbeit mit der IT-Administration folgende Aufgaben wahrgenommen:

- Führen des Verfahrensverzeichnisses bzw. Führen der Verzeichnisse der Verarbeitungstätigkeiten,
- Organisation des Datenschutzes (Dienstanweisungen und Richtlinien),
- Mitwirkung bei der Planung, Durchführung und Weiterentwicklung von Qualifizierungsmaßnahmen,
- Mitwirkung bei der Planung und Gestaltung der informationstechnischen Infrastruktur,
- Schulung und Beratung der Mitarbeiterinnen und Mitarbeiter in datenschutzrelevanten und praktischen Fragen,
- Bearbeitung von Anfragen Betroffener, insbesondere zur Wahrnehmung von Rechten (Auskunft, Berichtigung, Sperrung, Löschung),
- Kontrolle der Datenverarbeitung der Dienststelle,
- Überprüfung der Einhaltung von technischen und organisatorischen Maßnahmen zur Datensicherheit,
- Kontrolle der Datenverarbeitung bei Auftragnehmern,
- Beteiligung bei der Freigabe von automatisierten Verfahren,
- Untersuchung datenschutz- und sicherheitsrelevanter Vorfälle,
- Ansprechpartner für die Landesbeauftragte für Datenschutz Schleswig-Holstein und
- Sensibilisierungs- und Schulungsmaßnahmen zum Datenschutz und zur Informationssicherheit.

Der Datenschutzbeauftragte wird bei allen Projekten, die relevante Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme beteiligt. Darüber hinaus ist festgelegt, dass der Datenschutzbeauftragte interne Audits durchführt, bei denen stichprobenartig die Umsetzung, Wirksamkeit und Praktikabilität der getroffenen Maßnahmen überprüft werden.

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

Bei der Bearbeitung der vielfältigen „Datenschutzaufgaben“ hat der Datenschutzbeauftragte auch akzeptanzfördernde Strategien zur Umsetzung der festgelegten Ziele entwickelt. So hat er für die Datenminimierung der digitalen Datenbestände der Fachabteilungen ein „Speicherplatzwettbewerb“ durchgeführt. Alle Mitarbeiter wurden aufgefordert, ihre Ablage mit Datenbeständen auf das erforderliche Maß zu reduzieren. Gezählt wurden dabei die Dateienbestände vor und nach Abschluss des Wettbewerbs. Die Fachabteilung mit der größten Reduzierung ihrer Dateibestände erhielt vom Datenschutzbeauftragten einen kleinen „Überraschungspreis“.

Darüber hinaus wurde von ihm ein Informationsblatt für die Löschung und Vernichtung von Daten erstellt. Damit wurden die Mitarbeiter aufgefordert, auch den Aktenbestand in Büros und Archiven auf das für die Aufgabenerfüllung erforderlich Maß zu reduzieren. Der Datenschutzbeauftragte bestellte daraufhin 2 Großcontainer bei einer Spezialfirma für Aktenvernichtung mit der Aufforderung an die Mitarbeiter, den Aktenbestand zu reduzieren. Das Ergebnis war auch hier vorbildlich: Es wurden sehr viele nicht mehr benötige Akten und Ordner mit Daten entsorgt.

Diese Maßnahmen zeigen, dass die Mitarbeiter der Gemeinde Stockelsdorf durch den Datenschutzbeauftragten vorbildlich sensibilisiert wurden. So steigerte er bei den Mitarbeitern das Bewusstsein für Datenschutz und Informationssicherheit und erhöhte damit auch die Akzeptanz für eine ordnungsgemäße und datenminimierende Datenverwaltung.

2.4 IT-Administration

Die zentrale IT-Administration in der Gemeinde Stockelsdorf führt folgende Aufgaben durch:

- Unterstützung der Abteilungen bei der Realisierung des IT- Konzeptes,
- Beschaffung der Hard- und Software,
- Installation der Hard- und Software,
- Hard- und Softwareadministration, soweit diese nicht im Einzelfall den Abteilungen oder externen Dienstleistern übertragen wurden,
- Führung eines Geräte- und Inventarverzeichnisses,
- Unterrichtung der Leitungsebene über festgestellte Mängel und daraufhin getroffene Maßnahmen und
- Durchführung bzw. Koordinierung von Schulungen.

Die systembezogenen Arbeiten werden durch die IT-Administration in einem Ticketsystem dokumentiert. Über automatisierte Vordrucke beauftragen die Fachabteilungen die IT-Administration, Berechtigungen für Mitarbeiter auf der Arbeitsplatzebene zu konfigurieren. Darüber hinaus werden Systemarbeiten durch externe Dienstleister von der IT-Administration überwacht.

Die Ausbildung bzw. Fortbildung der IT-Administration wird stetig fortgeführt. Bei der Auswahl der Schulungen wird darauf geachtet, dass die Seminare aufeinander aufbauen und in regelmäßigen Zeitabständen stattfinden. Des Weiteren stehen der IT-Administration Testsysteme zur Verfügung,

auf denen die erworbenen Kenntnisse ausprobiert und Testinstallationen vorgenommen werden können.

Im Rahmen des Audits wurden von der IT-Administration neue technische Instrumente für die Verbesserung der Informationssicherheit implementiert. Dabei hat sich die IT-Administration besonders dafür eingesetzt, dass ein Inventarisierungstool für die IT-Komponenten sowie ein Ticketsystem für die Dokumentation administrativer Aktivitäten eingesetzt werden.

2.5 Schutzbedarfsfeststellung und Risikoanalyse

Die Gemeinde Stockelsdorf hat mit der Schutzbedarfsfeststellung den Schutzbedarf für ihre Datenverarbeitung festgelegt. Die Festlegung des Schutzbedarfs orientierte sich an möglichen Schäden, die mit einer Beeinträchtigung der Datenverarbeitung und damit der jeweiligen Geschäftsprozesse und der Rechte und Freiheiten betroffener Personen verbunden sind.

Die Durchführung der Schutzbedarfsfeststellung wurde in dem Dokument „Schutzbedarfsfeststellung und Risikoanalyse“ nachvollziehbar anhand folgender Schadensszenarien beschrieben:

- Verstoß gegen Gesetze / Vorschriften / Verträge, insbesondere die Verpflichtung zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts bzw. Verletzung der Grundrechte und Grundfreiheiten natürlicher Personen,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung und
- finanzielle Auswirkungen.

Zusammenfassend wurde der Schutzbedarf für die Datenverarbeitung mit Fachanwendungen in die Schutzkategorie „hoch“ eingestuft. Demzufolge wurde der festgelegte Schutzbedarf auch auf die für die Fachanwendungen eingesetzten IT-Systeme, das Datenkommunikationsnetz sowie die Gebäude- und Rauminfrastruktur übertragen.

Mit einer ergänzenden Risikoanalyse hat die Gemeinde Stockelsdorf bei der Umsetzung der Schutzmaßnahmen für normalen Schutzbedarf überprüft, ob die Gefährdungen für ein hohes Schutzniveau ausreichend eingedämmt sind. Durch die Ergreifung zusätzlicher Schutzmaßnahmen wurden nicht ausreichend eingedämmte Gefährdungen weitergehend reduziert.

Die im Rahmen der ergänzenden Risikobetrachtung festgelegten Schutzmaßnahmen sind im Verinice-Tool mit der Klassifizierung „Z“ hinterlegt und können zu den Standardschutzmaßnahmen mit der Klassifizierung „A“, „B“ und „C“ transparent gemacht werden (vgl. Tz. 2.6).

2.6 Infrastruktur, IT-Systeme, Netz und Anwendungen

Die Gemeinde Stockelsdorf hat zum Schutz ihrer Daten nach der Grundschutzmethode einen sogenannten Informationsverbund festgelegt. Dem Verbund wurden die schützenswerten Objekte – Infrastruktur, IT-Systeme, Netz und Anwendungen – mit den erforderlichen Bausteinen und Schutzmaßnahmen des Grundschutzkatalogs zugeordnet. Dabei wurden für die Gewährleistung der Rechte und Freiheiten betroffener Personen in einem eigenentwickelten Baustein auch Schutzmaßnahmen aus dem „Standarddatenschutzmodell" (SDM) des ULD ergänzt.

Bei der Anwendung der Grundschutzinstrumente wurden nicht alle in den Bausteinen des Grundschutzkatalogs enthaltenen Schutzmaßnahmen umgesetzt, sondern nur diejenigen Schutzmaßnahmen, die eine starke und angemessene Gefährdungseindämmung implizieren. Durch diese Verfahrensweise wurde die Komplexität der Schutzmaßnahmen reduziert, aber nur insoweit, dass keine bedeutsamen Gefährdungen bzw. Risiken für die Datenverarbeitung der Gemeinde Stockelsdorf oder für betroffene Personen eingegangen werden.

2.6.1 Gebäude und Büroräume

Die Gemeinde Stockelsdorf ist in einem Gebäude untergebracht. Es ist eine ausreichende räumliche Abschottung der einzelnen Fachabteilungen vorhanden. Alle Büroräume sind mit einem Schließsystem ausgestattet. Räume mit schützenswerten Informationen verfügen über verschließbare Schränke. Für die Entsorgung sensibler papierener Daten wurden verschließbare Behältnisse in allen Fachabteilungen aufgestellt. Die Leerung der Behältnisse wird von einer Fachfirma durchgeführt. In den Abendstunden überprüft ein Sicherheitsdienst die Außentüren des Gebäudes auf Verschluss.

2.6.2 Serverraum

Die zentralen IT-Komponenten der Gemeinde Stockelsdorf sind in einem verschlossenen Serverraum installiert. Nur die IT-Administration hat Zutritt. Der Serverraum ist mit einer Einbruchs- und Brandmeldeanlage sowie mit einem Klimatisierungssystem ausgestattet.

2.6.3 IT-Komponenten

Die Gemeinde Stockelsdorf verfügt über folgende Hard- und Softwarekomponenten:

Server:

- ESX01 VMWare Host-Server
- ESX02 VMWare Host Server
- DC-Domaincontroller
- VEEAM Datensicherungsserver mit Bandlaufwerk

Virtuelle Server:

- VM1-Bauhofsrv: Terminalserver für die Bauhofmitarbeiter
- VM1-Bauamtsrv: Stellt Programme für das Bauverwaltungsamt bereit
- VM1-Kaemmereisrv: Stellt Programme für die Kämmerei bereit
- VM1-Schulen: Terminalserver für die Schulen (Bereitstellung der Finanzsoftware CIP)
- VM1-Zeit: Server für die Zeiterfassung
- VM2-Exchange: Zentraler Exchange Server (E-Mail Verteilung)
- VM2-Fileserver: Dateiablageserver
- VM2-Sophos: Stellt die Antivirensoftware bereit
- VM2-WSUS: Zentrale Verteilung von Windows Updates
- VM3-HSH: Stellt Programme für das Einwohnermeldeamt bereit
- VM3-Printserver: Druckjobverwaltung über die Software Streamline NX
- VM3-Allrisnet: Stellt die Fachanwendung ALLRIS zur Verfügung
- VM3-VEEAM-Endpoint: Sicherungsserver für Domaincontroller
- VM4-DC: Zweiter Domaincontroller

Netz-, Druck- und Speicherkomponenten:

- NetApp E2700A Storage für ESX01 und ESX02
- Landesnetz Zugangsrouter und Übergaberouter
- Internetzugang DSL-Modem
- Router Telekom für Ethernet Connect Leitung
- 3 USV-Stationen (Unterbrechungsfreie Stromversorgung)
- Hardwarefirewall Sophos UTM 9 Gateway Security
- 1 Plotter (Bauamt)
- 12 Multifunktionsgeräte (Drucker, Kopierer und Scanner)

Arbeitsplätze:

- 49 PC-Arbeitsstationen mit Windows 7 Professional
- 8 Laptops mit Windows 7 Professional
- 10 Apple iPads mit iOS
- 60 Apple iPads mit iOS Gemeindevertreter

- 48 Samsung Galaxy mit Android
- 2 Apple iPhones mit iOS

Software bzw. Fachanwendungen:

- Meso, Einwohnermeldeamt, Standesamt
- DIGANT, Einwohnermeldeamt
- Autista, Standesamt
- GESO, Gewerbeabteilung
- Kirchner ProOpen, Geoinformationssystem
- C.I.P Kommunal, Finanzsoftware
- ALLRIS, Sitzungsdienst
- IKISS, Internetgestaltung - für den Redakteur
- IRIS, Einwohnermeldeamt
- Prosoz/W, Wohngeld
- IDC-Time, Personalabteilung
- BfA-Programm, Rentenanträge
- VKA Überleitungsprogramm TVÖD
- Kirchner ProOpen, gesamter Bauamtsbereich
- ORCA Ava, Ausschreibungsprogramm
- Vectorworks, CAD Software Hochbau
- Nordholz Schuldenverwaltung
- S-Firm Sparkassenprogramm
- Vollkom, Vollstreckung
- KKGW, Beitragsprogramm

Die Überprüfung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren war nicht Gegenstand des Audits.

Standard-, System- und Sicherheitssoftware:

- Microsoft Exchange
- Microsoft SQL
- MS-Office

- Mailsoftware Microsoft Outlook
- Adobe Reader
- Alcatel PIMphony
- Datensicherungsprogramm
- Sophos Anti-Virusprogramm
- Device-Management-Software (geplant)

2.6.4 Systemmanagement

Alle Server, PCs und Notebooks (Clients) werden in einem zentralen Verzeichnisdienst (Active Directory) verwaltet. Die Server und Clients mit Windows-Betriebssystemen sind mit einer Antivirensoftware Sophos ausgestattet. Der Virenscanner wird täglich aktualisiert. Die korrekte Funktion des Virenscanners sowie seine Aktualität werden zentral überwacht. Für die Tablets und Smartphones wird geplant, eine Sicherheitssoftware für die zentrale Administration einzusetzen (siehe Tz. 2.6.5).

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 Gemeinde Stockelsdorf betreibt hierzu einen WSUS-Server (Windows Server Update Services der Firma Microsoft).

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

Die Verwaltung von Daten erfolgt auf einem zentralen Network Attached Storage (NAS). Die Daten des Systems werden über ein Backupsystem auf gesonderten Datensicherungsbändern jeweils täglich, wöchentlich und monatlich gesichert. Die verwendeten Sicherungsbänder werden in einem Tresor aufbewahrt. Die eingesetzten Tagesbänder werden nach einer Woche, die Wochenbänder nach einem Monat und die Monatsbändernach einem Jahr überschrieben.

2.6.5 Arbeitsstationen – PCs, Notebooks und Tablets

Die PCs und Notebooks sind mit dem Betriebssystem Microsoft Windows 7 Professional ausgestattet. Alle PCs und Notebooks der Fachbereiche sind über das Netz mit den Servern verbunden. DVD-Laufwerke und USB-Schnittstellen sind bis auf wenige dienstlich begründete Ausnahmen deaktiviert.

Neben den eingesetzten Fachanwendungen wird bei der Gemeinde Stockelsdorf eine einheitliche Bürokommunikation-Standardsoftware eingesetzt. Auf den Arbeitsstationen wurden die Gruppenrichtlinien von Microsoft aktiviert, so dass z. B. Systemfunktionen für den Mitarbeiter nicht im Zugriff stehen.

Darüber hinaus verfügen einige Mitarbeiter über einen Tablet (iPad), das für dienstliche Zwecke beispielsweise im Rahmen von Gemeindevertretersitzungen genutzt wird. Die Funktionen der Tablets sollen über eine Sicherheitssoftware auf die erforderlichen Funktionen begrenzt werden. Die Nutzung der Internetdienste E-Mail und Web wird über die Firewall reglementiert (siehe Tz. 2.6.6).

2.6.6 Internes Netz, Firewall und Netzübergänge

In der Gemeinde Stockelsdorf wurde eine strukturierte Verkabelung für die Datenverarbeitung implementiert. Sämtliche aktive Netzgeräte (Switches und Router) sind in verschlossenen Serverschränken untergebracht. Nicht benötigte Anschlüsse in den Büroräumen sind nicht beschaltet.

Das Netz der Gemeinde Stockelsdorf ist für die Datenkommunikation mit Dataport über das Landesnetz Schleswig-Holstein angeschlossen. Darüber hinaus sind Außenstellen, wie z. B. der Bauhof über eine Standleitung an das interne Netz angebunden. Die Netzübergabepunkte sind über eine Firewall geschützt. Der Datenverkehr des verwaltungsinternen Netzes mit externen Netzen wird an den Netzübergängen über die Firewall freigeschaltet. Es gilt das Prinzip: „Es ist alles verboten, was nicht ausdrücklich erlaubt ist."

Der Datenverkehr wird nicht nur auf seine Zulässigkeit, sondern bereits von der Firewall auch auf schadhafte Inhalte wie Viren, Würmer und Trojaner geprüft. Die Gemeinde Stockelsdorf setzt hierfür eine Sicherheitssoftware ein, die die übertragenen Daten insbesondere bei der E-Mail- und Web-Kommunikation auf schadhafte Inhalte kontrolliert. Die Firewall ermittelt verdächtige Verhaltensweisen und kann spezielle Malware, wie z. B. Verschlüsselungstrojaner, aufspüren. In Zusammenwirken mit der Antivirensoftware „Endpoint Protection Advanced" werden somit Bedrohungen abgefangen und blockiert (vgl. Tz. 2.6.7).

Zusätzlich hat die Gemeinde Stockelsdorf für politische Amtsträger einen vom internen Netz abgeschotteten Internetzugang eingerichtet, den die Amtsträger über ein verschlüsseltes WLAN mit den ihnen zur Verfügung gestellten Tablets nutzen können. Über eine Vereinbarung zwischen dem Amtsträger und der Gemeinde Stockelsdorf wird jeder Amtsträger auf die Nutzungsmöglichkeiten hingewiesen. Erst nach Unterzeichnung der Vereinbarung vergibt die Gemeinde Stockelsdorf an den Amtsträger die Zugangsdaten für die Nutzung des WLANs.

2.6.7 Virenschutz

Für die Nutzung der Internetdienste E-Mail und Web sowie die Datenkommunikation über Schnittstellen und angeschlossene externe Netze setzt die Gemeinde Stockelsdorf zum Schutz der Daten das Virenschutzprodukt „Endpoint Protection Advanced" von der Firma Sophos ein. Es verfügt über folgende Funktionen:

- Maleware auf Basis von Signaturen abwehren,
- Web-Filterung bei verdächtigen Verhaltensweisen und Aktivitäten von Schad-URLs,

- Schutz gegen Crypto-Ransomware,
- Exploid-Prevention zum Schutz gegen Software-Schwachstellen und
- Web, Application, Device und Data-Control mit Richtlinienumsetzung.

Über einen URL-Filter werden nach Kategorien unerwünschte Webseiten geblockt. Anhänge der E-Mail-Kommunikation werden ebenfalls auf schädigende Inhalte gescannt. Nicht erlaubte Anhänge werden von der E-Mail abgehängt und in einem gesonderten, nur für die IT-Administration im Zugriff stehenden, Ordner gespeichert. Die IT-Administration kann daraufhin auf Nachfrage des Empfängers die Anhänge auf ihre Zulässigkeit überprüfen.

Der Virenschutz ist auf allen PCs, Notebooks und Servern installiert und wird durch neue Virensignaturen täglich aktualisiert.

2.6.8 Mobile-Security-Management

Die Gemeinde Stockelsdorf beabsichtigt, für einen sicheren und datenschutzkonformen Betrieb der von Mitarbeitern und Gemeindevertretern genutzten Smartphones und Tablets eine Sicherheitssoftware einzusetzen. Die Managementsoftware soll auf Systemen der Gemeinde Stockelsdorf installiert werden, so dass über die Software erstellte Sicherheitsrichtlinien auf die mobilen Geräte übertragen werden können. Über die zentral vorgegebenen Sicherheitsrichtlinien lassen sich dann die Zugriffe auf Funktionen der mobilen Geräte und die nutzbaren Apps bzw. Fachanwendungen individuell reglementieren, so dass eine Absicherung der auf den Geräten befindlichen Daten gewährleistet werden kann. Die Gemeinde Stockelsdorf hat bereits für einen sicheren Einsatz der mobilen Geräte eine Sicherheitsrichtlinie festgelegt, die nach der Implementierung der Managementsoftware umgesetzt werden soll:

Übermittlung von Diagnosedaten	Blockieren
Bildschirmaufnahme	Blockieren
Nicht vertrauenswürdige TLS-Zertifikate	Blockieren
Kontoänderung	Blockieren
Aktivieren von Einschränkungen in den Geräteeinstellungen	Blockieren
Verwendung der Option zum Löschen aller Inhalte und Einstellungen auf dem Gerät	Blockieren
Gerätenamensänderung	Blockieren
Änderung der Vertrauenseinstellungen für die Unternehmens-App	Blockieren
Konfigurationsprofiländerungen	Blockieren
Aktivierungssperre (nur überwachter Modus)	Erteilen Sie
Kennwort	Anfordern
Einfache Kennwörter	Blockieren
Erforderlicher Kennworttyp	Alphanum.
Anzahl nicht alphanumerischer Zeichen im Kennwort	1

Mindestlänge für Kennwort	8
Anzahl von Anmeldefehlern, bevor das Gerät zurückgesetzt wird	5
Maximaler Zeitraum der Bildschirmsperre (in Minuten) bis zur Anforderung eines Kennworts	15 Minuten
Maximaler Zeitraum der Inaktivität (in Minuten) bis zur Bildschirmsperrung	15 Minuten
Kennwortablauf (in Tagen)	90
Wiederverwendung vorheriger Kennwörter verhindern	3
Kontrollcenterzugriff bei gesperrtem Gerät	Blockieren
App Store	Blockieren
In-App-Einkäufe	Blockieren
Anzeige von Unternehmensdokumenten in nicht verwalteten Apps	Blockieren
Anzeige nicht unternehmenseigener Dokumente in Unternehmens-Apps	Blockieren
AirDrop als nicht verwaltetes Ziel behandeln	Blockieren
Face Time	Blockieren
Siri	Blockieren
Änderungen an den App-Einstellungen zur Verwendung von Datenverbindungen (nur überwacht)	Blockieren
Privater Hotspot	Blockieren
In iCloud sichern	Blockieren
Dokumentsynchronisierung in iCloud	Blockieren
JavaScript	Blockieren
Popups	Blockieren
…	

Die Einstellungen auf den mobilen Geräten werden in Absprache mit den Fachbereichen und der Bürgermeisterin vorgenommen und dokumentiert. Die vollständige Implementierung der Sicherheitssoftware und der Übertragung der Sicherheitsrichtlinie auf die mobilen Geräte soll bis Ende November 2017 abgeschlossen sein.

2.7 Dokumentation und Nachweise für die Einhaltung datenschutzrechtlicher Vorschriften

Die Gemeinde Stockelsdorf hat für die automatisierte Datenverarbeitung folgende Dokumentation und Nachweise erstellt und im Rahmen der Begutachtung vorgelegt:

- Leitlinie für Datenschutz und Informationssicherheit (siehe Tz. 2.1)
- Datenschutz- und Informationssicherheitsmanagement (siehe Tz. 2.2)
- Schutzbedarfsfeststellung und Risikoanalyse (siehe Tz. 2.5)
- Allgemeines Konzept für die automatisierte Datenverarbeitung (siehe Tz. 2.6)
- Konzept für die Datensicherung
- Report Informationsverbund mit Infrastruktur, Systeme, Netz und Anwendungen
- Report Technische und organisatorische Maßnahmen

- Allgemeine Dienst- und Geschäftsordnung (ADGO)
- Allgemeine Dienstanweisung zur Nutzung der Informations- und Kommunikationstechnologie
- Spezielle Dienstanweisung zur Nutzung der Internet-Dienste
- Spezielle Dienstanweisung für die Administration
- Informationsblatt zur Löschung und Vernichtung von Daten
- Verhaltensregeln bei Auftreten von Schadprogrammen
- Merkblatt über Verhalten bei Sicherheitsvorfällen
- Antrag auf Einrichtung eines Benutzerkontos
- Checkliste für den Basisclient
- Richtlinien für die Benutzung von mobilen Geräten
- Sicherheitseinstellungen für Tablets und Mobiltelefone (siehe Tz. 2.6.8)
- Sicherheitseinstellungen für Firewall und Clients
- Verfahrensakten mit Verfahrensbeschreibungen
- Verträge mit Dienstleistern im Rahmen einer Auftragsdatenverarbeitung

2.7.1 Report „Informationsverbund mit Infrastruktur, Systeme, Netz und Anwendungen“

Der Informationsverbund der Gemeinde Stockelsdorf enthält die Objekte für Infrastruktur, Systeme, Netz und Anwendungen. Die im Rahmen einer Bestandsaufnahme erhobenen Objekte wurden mit der Software „Verinice“ erfasst und können über den Report dargestellt werden.

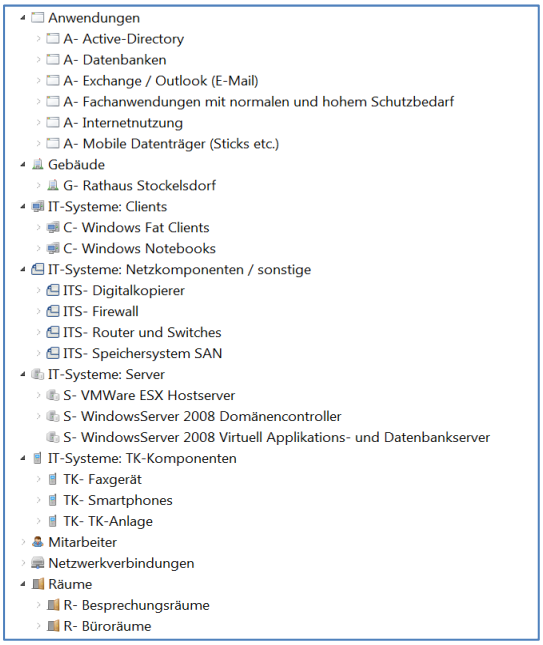

Abb.: Ausschnitt Informationsverbund Stockelsdorf

2.7.2 Report „Technische und organisatorische Maßnahmen“

Der Report „Technische und organisatorische Maßnahmen“ enthält die technischen und organisatorischen Maßnahmen, die für die Informationssicherheit und den Datenschutz festgelegt wurden. Der Report listet bausteinbezogen alle Schutzmaßnahmen mit einer Beschreibung über den Umsetzungstand auf. Der in der Abbildung dargestellte Auszug enthält Schutzmaßnahmen für das Datenschutz- und Informationssicherheitsmanagement sowie Schutzmaßnahmen aus datenschutzrechtlicher Perspektive für die eingesetzten Fachanwendungen.

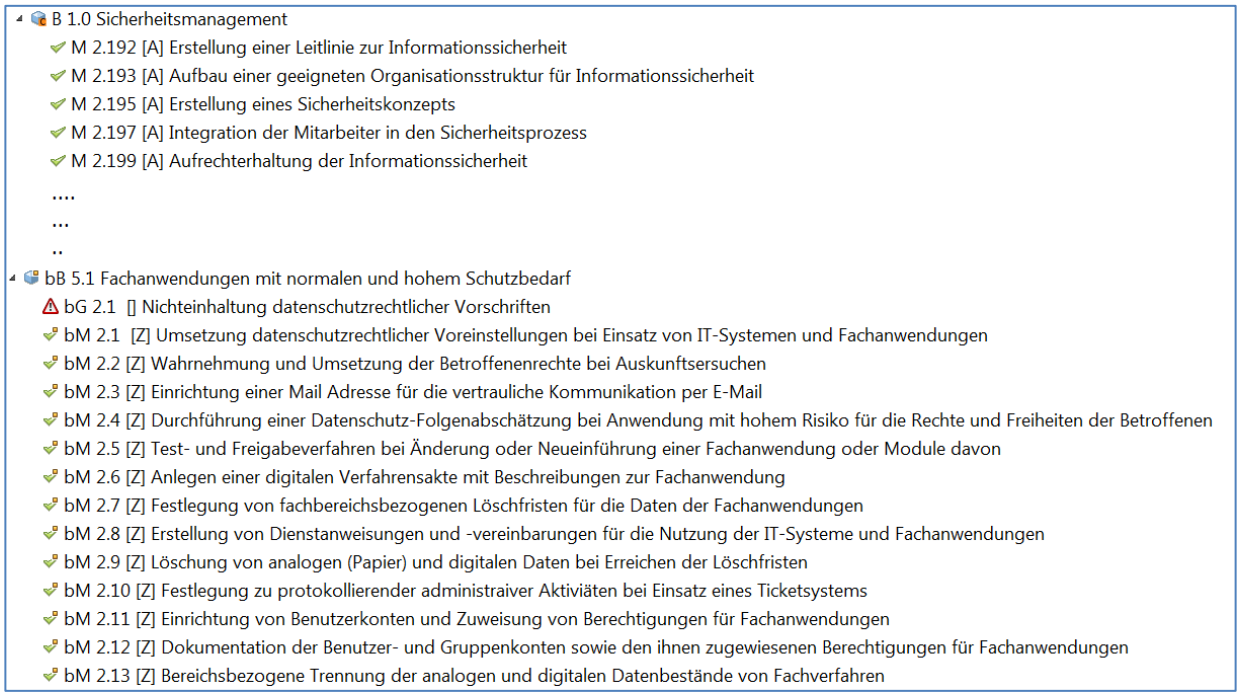

Abb.: Ausschnitt technische und organisatorische Maßnahmen

2.7.3 Verfahrensakten mit Verfahrensbeschreibungen

In den überprüften Verfahrensakten befinden sich Informationen über die Einführung und den Betrieb des Verfahrens. In digitaler Form wird die „Verfahrensakte“ mit folgender Gliederung geführt:

- Allgemeiner Schriftverkehr
- Verfahrensbeschreibung
- Verzeichnis von Verarbeitungstätigkeiten
- Risikoanalyse
- Test und Freigabe
- Berechtigungskonzept
- Verträge mit Dienstleistern
- Handbücher

- Protokolle und Kontrollen
- Updates
- Hardware

Dokumente, die nicht digitalisiert vorliegen, werden in einer entsprechenden papierenen Verfahrensakte geführt.

2.7.4 IT-Konzept

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

Neben Vorgaben für die IT-Systeme und Netzinfrastruktur sind im IT-Konzept die Aufgaben der IT-Administration festgelegt. Das IT-Konzept dokumentiert zusammen mit der Systemdokumentation und den Verfahrensakten den Ist-Stand der Informations- und Kommunikationsinfrastruktur der Gemeinde Stockelsdorf.

2.7.5 Dienstanweisungen und Richtlinien

Die festgelegten technischen und organisatorischen Maßnahmen wurden zum Teil in Handlungsanweisungen im Rahmen von Dienstanweisungen und/oder Richtlinien mitarbeiterbezogen übertragen. Die Allgemeine Dienstanweisung zur Nutzung der Informations- und Kommunikationstechnologie beinhaltet z. B. folgende Regelungen:

- Zugriffsrechte auf Daten und Datenträger besitzen nur dazu berechtigte Personen. Diese und der zeitliche Umfang werden durch die Leitung des zuständigen Fachamtes festgelegt.
- Die von der Leitung des Fachamtes vergebenen Berechtigungen werden der EDV-Abteilung auf dem Dienstweg schriftlich mitgeteilt und von dieser umgesetzt und protokolliert.
- Bei der erstmaligen Anmeldung hat jeder Benutzer sein Windows-Anmeldepasswort selbst festzulegen. Das Passwort muss mindestens 8 Zeichen lang sein und ein Sonderzeichen und eine Zahl enthalten.
- Bei servergestützten Anwendungen wird dem Benutzer auf der Grundlage eines Berechtigungskonzeptes für die vorgesehene Funktion vor der erstmaligen Nutzung von der EDV-Abteilung eine Benutzerkennung und ein Initialpasswort eingerichtet und persönlich mitgeteilt.
- Beim erstmaligen Anmelden an einer Server-Anwendung ist das Initialpasswort durch ein persönliches Passwort zu ersetzen. Es darf keine Rückschlüsse auf seinen Besitzer zulassen und ist vertraulich zu behandeln.
- Die vom Benutzer verwendeten Passwörter für die Systemanmeldung und die Anmeldung an Fachanwendungen sind von ihm nicht an Dritte weiterzugeben.

- Besteht der Verdacht, dass Unbefugte Kenntnisse von einem Passwort erhalten haben, ist unverzüglich ein neues Passwort einzurichten. Darüber hinaus ist das Passwort in unregelmäßigen Zeitabständen - spätestens jedoch nach 3 Monaten - zu ändern, sofern das System nicht automatisch dazu auffordert.
- Jeder Benutzer hat sicherzustellen, dass von seinem Arbeitsplatz-PC kein unbefugter Zugriff auf das Netzwerk erfolgen kann. Beim Verlassen des Arbeitsplatzes (auch kurzzeitig) ist der Bildschirm auf die Anmeldungsmaske zu stellen. Bei Dienstende sind die aktivierten Programme ordnungsgemäß zu beenden und - soweit keine andere dienstliche Regelung besteht - der PC auszuschalten.
- Zu Räumen, in denen Geräte installiert sind, dürfen nur Berechtigte Zugang haben. Außenstehende Personen (so auch das Wartungspersonal der Lieferfirmen) dürfen sich nur in Begleitung eines Beauftragten der Dienststelle in diesen Räumen aufhalten.
- Unbesetzte Räume sind abzuschließen. Die Schließanlagentransponder sind so aufzubewahren, dass sie nicht von Unbefugten benutzt werden können.
- Diejenigen Personen, die zur Eingabe, zur Veränderung oder zur Löschung von personenbezogenen Daten in automatisierten Verfahren berechtigt sind, sind im Einzelnen festzulegen. Die Autorisierung der berechtigten Personen erfolgt durch Zuweisung eines Berechtigungscodes (i. d. R. Benutzerkennung und Passwort). Sie soll sich lediglich auf die für die Aufgabenerfüllung erforderlichen Anwendungen erstrecken. Die Berechtigungen innerhalb der Anwendungen sind ebenfalls auf das notwendige Maß zu beschränken.
- Bei der Verarbeitung von personenbezogenen Daten ist zu verhindern, dass Unbefugte Einblick in die laufende Datenverarbeitung haben (Sichtschutz).
- Personenbezogene Daten auf Standalone-PCs oder portablen Geräten sind zu verschlüsseln.
- Nach Abschluss der Arbeiten sind alle Ausdrucke aus dem Drucker zu entfernen. Das Abholen von Ausdrucken von den zentralen Netzwerkdruckern ist nur mittels eines registrierten Transponders möglich.
- Maschinell lesbare Datenträger mit personenbezogenen Daten sind im verschließbaren Schreibtisch oder Schrank bzw. in einem Tresor aufzubewahren. Es ist sicherzustellen, dass nur berechtigte Personen Zugriff auf diese Datenträger haben.
- Grundsätzlich ist die Benutzung von Wechselmedienlaufwerken untersagt. Daher sind Laufwerke sowie das Anschließen von USB-Sticks und Speicherkarten deaktiviert. Für den Transport von Daten sind nur die von der EDV freigegebenen verschlüsselten USB-Sticks zu verwenden.
- Die Freischaltung der Laufwerke ist nur in begründeten Fällen möglich und ist vom zuständigen Fachamtsleiter bei der EDV-Abteilung schriftlich zu beantragen.
- Die Speicherung der Daten erfolgt grundsätzlich zentral auf dem für den Benutzer vorgesehenen Serververzeichnis. Für die Pflege der vom Benutzer angelegten Unterverzeichnisse ist dieser selbst verantwortlich.
- Es gilt der Grundsatz der Datensparsamkeit. Nicht mehr benötigte Datensätze sind zeitnah aus dem Serververzeichnis zu löschen.

- Daten aus Fachanwendungen sind ebenfalls zentral auf den Servern zu speichern.
- Die Speicherung von dienstlichen Daten auf Cloud-Speichern (z. B. Google Drive, Apple iCloud, Dropbox) ist grundsätzlich untersagt. Auf allen eingesetzten Geräten ist sicherzustellen, dass Daten nicht mit Cloudspeichern automatisch synchronisiert werden.

2.7.6 Auftragsdatenverarbeitung mit Dienstleistern

Die Gemeinde Stockelsdorf hat im Rahmen einer Auftragsdatenverarbeitung u. a. folgende Dienstleister vertraglich beauftragt:

- **Reisswolf-Papierentsorgung**

Die Gemeinde Stockelsdorf entsorgt über Sicherheitsbehälter Papierabfälle und ausgesonderte digitale Datenträger über die Firma Reisswolf GmbH. Die Firma sichert eine Vernichtung im Rahmen der DIN 66399 mit der Schutzklasse 2 zu.

- **C3 Computer Communication Consulting und L & M Business IT GmbH**

Die Firmen C3 und L & M sind u. a. damit beauftragt, die IT-Administration in den Bereichen Netz und Wartung der Server zu unterstützen. Erforderliche Dienstleistungen werden von der Gemeinde Stockelsdorf anlassbezogen beauftragt und kontrolliert.

- **CC e-gov GmbH**

Die Firma CC e-gov GmbH erbringt „Versersharing“ bzw. Providerdienstleistungen im Zusammenhang mit der Software „ALLRIS“, einem Ratsinformationssystem. Mit der Software werden insbesondere den Gemeindevertretern Tagesordnungen und Sitzungsprotokolle der Gemeinde Stockelsdorf bereitgestellt.

- **Dataport**

Von Dataport werden einzelne Fachverfahren, z. B. „Autista“ (Standesamtfachverfahren), gehostet. Der Zugriff erfolgt über das Landesnetz Schleswig-Holstein.

3 Datenschutzrechtliche Bewertung

Die automatisierte Verarbeitung personenbezogener Daten erfordert technische und organisatorische Maßnahmen, die 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 in konkrete Datensicherungsmaßnahmen umgesetzt werden und ihre Einhaltung durch das Datenschutz- und Informationssicherheitsmanagement kontrolliert wird. Dabei sind z. B. 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, Wartung

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 festgelegten Schutzmaßnahmen für Datenschutz und Informationssicherheit angemessen sind und umgesetzt werden.

Der behördliche Datenschutzbeauftragte verfügt über die erforderliche Sachkunde und Zuverlässigkeit. Er führt die ihm übertragenen Aufgaben sehr motiviert durch und sorgt bei den Mitarbeitern für Akzeptanz für die einzuhaltenden Schutzmaßnahmen.

Das Datenschutz- und Informationssicherheitsmanagement nimmt seine Aufgaben im erforderlichen Maße wahr und steuert die Datenschutz- und Informationssicherheitsprozesse.

Für die Auftragsdatenverarbeitungen mit Dienstleistern wurden Verträge erstellt, die den Datenschutzvorgaben entsprechen.

Die im Rahmen des Datenschutz-Behördenaudits bei der Gemeinde Stockelsdorf erfassten Verarbeitungsprozesse zeichnen sich besonders durch folgende datenschutzfreundliche Aspekte aus:

- Die mit den Fachverfahren der Gemeindeverwaltung verarbeiteten Bürgerdaten werden durch Datenschutz- und Informationssicherheitsmaßnahmen geschützt. Durch die Anwendung der Grundschutzinstrumente lassen sich Schutzmaßnahmen zu den schützenswerten Bereichen – Gebäude, Räume, Clients, Server, Router, Firewall, Fachanwendungen, etc. – direkt zuordnen, so dass Datenschutz und Informationssicherheit besonders gut umgesetzt werden.
- Die IT-Administration setzt für eine effektive Verwaltung der IT-Komponenten Systemmanagementsoftware ein. Darüber hinaus werden von der Gemeinde Stockelsdorf einheitliche IT-Systeme am Arbeitsplatz eingesetzt, so dass damit eine Standardisierung der Arbeitsumgebung sichergestellt wird. Ferner lassen sich Sicherheitsfunktionen zentral und einheitlich administrieren. CD-ROM-Laufwerke und Schnittstellen für USB-Speichermedien sind grundsätzlich deaktiviert.
- Für den Anschluss des internen Verwaltungsnetzes an das Internet werden Sicherheitskomponenten eingesetzt, die unerwünschte Zugriffe abwehren. Smartphones und Tablets sollen durch Einsatz einer Sicherheitssoftware reglementiert und auf Systemen der Gemeinde Stockelsdorf zentral verwaltet werden.
- Das Datenschutz- und Informationssicherheitsmanagement führt in regelmäßigen Abständen Sitzungen durch, in denen Datenschutz- und Informationssicherheitsaspekte bearbeitet werden. Darüber hinaus wurden organisatorische Abläufe für die Behandlung von auftretenden Datenschutz- und Sicherheitsvorfällen festgelegt.

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

Kiel, 27. September 2017 Heiko Behrendt