Gutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Gemeinde Oststeinbek

Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Kiel, 24. Mai 2018

Auditor: Heiko Behrendt

Az.: 16.01/17.001

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 Oststeinbek und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

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

Dazu gehören:

- der Betrieb der PCs, Notebooks, Server und Netzkomponenten ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter sowie
- die Anbindung des internen Netzes der Gemeindeverwaltung Oststeinbek an das Internet sowie
- die netztechnische Anbindung der Außenstellen „Kindertagesstätte“, „Bauhof“, „Jugendzentrum“ und „Jugendberatung“ an das interne Netz der Gemeindeverwaltung.

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 bei der Gemeindeverwaltung Oststeinbek 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 Grundschutzkompendiums.

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 Gemeindeverwaltung Oststeinbek 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 Gemeindeverwaltung Oststeinbek Leitaussagen zu ihrer **Datenschutz- und Informationssicherheitsstrategie** zusammengefasst, um die festgelegten Datenschutz- und Sicherheitsziele und das angestrebte Datenschutz- und Sicherheitsniveau für alle Mitarbeiterinnen und 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 Informationstechnik orientiert sich die Gemeindeverwaltung Oststeinbek 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, Zweckbindung),

- Verfahren werden so gestaltet, dass die Gemeindeverwaltung 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).

Für die Umsetzung des Datenschutzes und der Informationssicherheit hat sich die Gemeindeverwaltung Oststeinbek mit der Leitlinie folgende Anforderungen auferlegt:

- Schaffung von organisatorischen Rahmenbedingungen zur nachhaltigen Umsetzung der Datenschutz- und Grundschutzanforderungen.
- Einführung einheitlicher und übergreifender technischer Sicherheitsstandards für die IT-Komponenten einschließlich der Definition von Verantwortlichkeiten und Befugnissen.
- Herstellung des Bewusstseins bei den Mitarbeiterinnen und Mitarbeitern für den sicheren Umgang mit vertraulichen Daten.
- Regelmäßige Durchführung von Schulungen und Unterweisungen der Mitarbeiterinnen und Mitarbeiter in den Bereichen Datenschutz und Informationssicherheit.
- Erstellung einer Sicherheitskonzeption, die den Einsatz und den Betrieb der IT-Komponenten, die Datenverarbeitung sowie die umgesetzten Sicherheitsmaßnahmen beschreibt.
- Einrichtung von Kontrollmechanismen zur Überprüfung der Umsetzung der Datenschutz- und Informationssicherheitsziele bzw. der Sicherheitskonzeption.

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

2.2 Datenschutz- und Informationssicherheitsmanagement-Team (DISM)

In dem Dokument „Datenschutz- und Informationssicherheitsmanagement“ wurden Festlegungen über die Zusammensetzung und Zuständigkeiten des DISM getroffen. Das **DISM-Team** initiiert, steuert und kontrolliert den Datenschutz- und Informationssicherheitsprozess in der Gemeindeverwaltung Oststeinbek. Es besteht aus folgenden Personen:

- Frau Raza, Fachbereichsleitung Finanzen und zentrale Dienste, Büroleitung

- Frau Braune, behördliche Datenschutzbeauftragte, Vorsitz im DISM-Team
- Herr Liszok, IT-Service und Administration, stellvertretender Vorsitz im DISM-Team
- Frau Trekel, IT-Service und Administration
- Frau Laatz, Sachgebiet Personal und zentrale Dienste, als Stellvertreterin für die datenschutz- und datensicherheitsrelevanten Aufgaben im nichttechnischen Bereich
- ein Mitglied des Personalrats

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

- steuert und koordiniert den Datenschutz- und Informationssicherheitsprozess und stellt den dazugehörigen Informationsfluss sicher,
- initiiert und koordiniert die Erstellung von allgemein notwendigen IT-Sicherheitsrichtlinien,
- erstellt und koordiniert 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 Fachbereiche die 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,
- berichtet der Dienststellenleitung und
- veranlasst oder erstellt Berichte über Datenschutz- und Sicherheitsvorfälle.

Das DISM-Team wird bei allen Projekten, die Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme beteiligt. Dazu gehören z. B. die Einführung neuer Verfahren, die Beschaffung von IT-Systemen oder die Gestaltung von IT-gestützten Geschäftsprozessen.

2.3 Behördliche Datenschutzbeauftragte (DSB)

Als behördliche Datenschutzbeauftragter wurde Frau Braune gemäß § 10 LDSG schriftlich bestellt. Sie führt den Vorsitz im DISM-Team und ist für die organisatorische Abwicklung und Koordination der Sitzungen, umzusetzender Maßnahmen und einem zugehörigen Berichtswesen einschließlich Managementberichten an die Dienststellenleitung zuständig.

Zu den weiteren Aufgaben der Datenschutzbeauftragten gehört es,

- die Leitungsebene bei der Erstellung der Datenschutz- und Informationssicherheitsleitlinie zu unterstützen,
- die Erstellung des Sicherheitskonzepts und anderer und Sicherheitsrichtlinien zu koordinieren,
- datenschutz- und sicherheitsrelevante Zwischenfälle zu untersuchen sowie
- Sensibilisierungs- und Schulungsmaßnahmen zum Datenschutz und zur Informationssicherheit zu initiieren und zu steuern.

Die Datenschutzbeauftragte wird bei allen größeren Projekten, die Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme beteiligt.

2.4 Interne Audits

Im Rahmen von Audits wird das DISM-Team zukünftig die Umsetzung, Wirksamkeit und Praktikabilität der im Sicherheitskonzept getroffenen Sicherheitsmaßnahmen überprüfen. Die Audits sollen stichprobenartig durchgeführt werden. Ein zu erstellender Auditbericht soll folgende Gliederung enthalten:

- Prüfungsumfang,
- Datum und Prüfdauer,
- beteiligte Personen,
- Ergebnis der Prüfung und
- ggf. hieraus abzuleitende Maßnahmen.

2.5 Behandlung von Datenschutz- und Sicherheitsvorfällen

Für das Melden von Datenschutz- und Sicherheitsvorfällen wurde eine Richtlinie für die Mitarbeiterinnen und Mitarbeiter erstellt. Entsprechende Sensibilisierungsmaßnahmen für die Mitarbeiterinnen und Mitarbeiter wurden von der behördlichen Datenschutzbeauftragten durchgeführt. Vorfälle sollen den Mitgliedern des DISM-Teams sofort gemeldet werden.

Das DISM-Team

- überprüft die Bearbeitung der gemeldeten Datenschutz- bzw. Sicherheitsvorfälle und der getroffenen Maßnahmen zur Schadensbeseitigung,
- veranlasst präventive Maßnahmen zur Risikominimierung (z. B. die Überarbeitung des Sicherheitskonzeptes),
- berichtet dem Bürgermeister.

2.6 IT-Administration

Die zentrale IT-Administration in der Gemeindeverwaltung Oststeinbek führt folgende Aufgaben durch:

- Festlegen von IT-Standards durch den Fachbereich Finanzen und zentrale Dienste im Abstimmung mit den übrigen Fachbereichen,
- Unterstützung der Fachbereiche bei der Realisierung des IT-Konzeptes,
- Beschaffung der Hard- und Software für die Kernverwaltung und die Außenstellen,
- Installation der Hard- und Software, soweit nicht Dataport oder anderen externen Dienstleistern übertragen,
- Hard- und Softwareadministration soweit diese nicht im Einzelfall dem zuständigen Fachbereich oder externen Dienstleistern übertragen wurde,
- Führen der technischen Dokumentation,
- Ermittlung von datenschutz- und datensicherheitsrelevanten Problemstellungen im IT-Bereich in Zusammenarbeit mit der DSB,
- Unterrichtung der Fachbereichsleitung und ggf. der Dienstellenleitung über festgestellte Mängel und daraufhin getroffene Maßnahmen,
- Erstellen der Dokumentationen für alle eingesetzten Verfahren in Zusammenarbeit mit den Fachbereichen und der DSB,
- Systemadministration der Server und der Arbeitsstationen,
- Einweisen der Mitarbeiterinnen und Mitarbeiter ,
- Benutzerverwaltung, soweit nicht im Fachverfahren implementiert (Active Directory),
- Durchführung der Datensicherung,
- Überwachung des Systemverhaltens,
- Fehlerbehandlung.

Über automatisierte Vordrucke beauftragen die Fachabteilungen die IT-Administration, Berechtigungen für Mitarbeiterinnen und 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.

2.7 Schutzbedarfsfeststellung und Risikoanalyse

Die Gemeindeverwaltung Oststeinbek 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 Gemeindeverwaltung Oststeinbek bei der Umsetzung der Schutzmaßnahmen überprüft, ob die Gefährdungen für ein hohes Schutzniveau ausreichend eingedämmt sind.

2.8 Infrastruktur, IT-Systeme, Netz und Anwendungen

Die Gemeindeverwaltung Oststeinbek 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 Grundschutzkompendiums zugeordnet. Dabei wurden für die Gewährleistung der Rechte und Freiheiten betroffener Personen in dem Datenschutzbaustein auch Schutzmaßnahmen aus dem „Standard-Datenschutzmodell" (SDM) des ULD ergänzt.

Bei der Anwendung der Grundschutz-Instrumente wurde die **Basisabsicherung des modernisierten Grundschutzes** umgesetzt. Durch diese Verfahrensweise wurde die Komplexität der Schutzmaßnahmen reduziert, aber nur insoweit, dass keine bedeutsamen Gefährdungen bzw. Risiken für die Datenverarbeitung der Gemeindeverwaltung Oststeinbek oder für betroffene Personen eingegangen werden.

2.8.1 Gebäude und Büroräume

Die Gemeindeverwaltung Oststeinbek ist in einem Gebäude untergebracht. Es ist eine ausreichende räumliche Abschottung der einzelnen Fachabteilungen vorhanden. Darüber hinaus bestehen Außenstellen mit den Bereichen „Kindertagesstätte“, „Bauhof“, „Jugendzentrum“ und „Jugendberatung“. Die Büroräume im Haupthaus und in den Außenstellen sind mit einem Schließsystem ausgestattet. Räume mit schützenswerten Informationen verfügen über verschließbare Schränke. Für die Entsorgung sensibler papierener Daten stehen verschließbare Behältnisse bereit. Die Leerung der Behältnisse wird von einer Fachfirma durchgeführt.

2.8.2 Serverraum

Die zentralen IT-Komponenten der Gemeindeverwaltung Oststeinbek sind in einem verschlossenen Serverraum installiert. Nur die IT-Administration hat Zutritt. Der Serverraum ist mit einem Klimatisierungssystem ausgestattet.

2.8.3 IT-Komponenten

Die Gemeindeverwaltung Oststeinbek verfügt über folgende Hard- und Softwarekomponenten:

Server:

2 Lenovo x3650M5 Server als **Hostsysteme für virtuelle Maschinen** auf Basis Hyper-V

2 QNAP TS-853U-RP NAS Systeme als Datensicherung mit jeweils 12 TB im RAID 5

1 IBM MT 7837 Server als Hostsysteme für virtuelle Maschinen auf Basis Hyper-V

Clients:

65 Arbeitsstationen mit Windows 7. Diese werden vollständig im 2. Quartal 2018 durch neue Arbeitsstationen mit Windows 10 ausgetauscht.

3 Notebooks mit Windows 10

3 Terra PAD 1061 mit Windows 10

Firewall, Router und Switches:

2 Firewalls

2 Cisco 800 Series

4 Netgear GS724TS (Stack)

1 Netgear GS724TS

2 3COM Baseline Switch 2952-SFP Plus

1 HP ProCurve Switch 2610-24

Zentrale und lokale Drucker:

4 TASKalfa

1 HP LaserJet P2055dm

2 Epson MFP EP2000

USB-Sticks:

10 Kingston DataTraveler DTSE9G2

Auf den **Hostsystemen** werden folgende **virtuelle Maschinen** betrieben:

OSTGM-DC01 (Windows Server 2016) Domänencontroller:

- DNS Server
- Active Directory

OSTGM-FS01 (Windows Server 2016) Anwendungsserver:

- Windows Update Server (WSUS)
- Dokumentenmanagement RegisafeIQ
- Regisafe Webpublisher
- Microsoft Office Professional Plus 2016

OSTGM-EX01 (Windows Server 2016) Anwendungsserver:

- Exchange-Server 2016 für die Postfachbereitstellung

OSTGM-DB01 (Windows Server 2016) Datenbankserver:

- MS SQL Server 2017

OSTGM-DB1 (Windows Server 2008 R2) Anwendungsserver:

- Cip-Archiv

OSTGM-AS01 (Windows Server 2016) Anwendungsserver:

- Infoma newsystem

- Anwenkom SVP Schuldnervollstreckungsprogramm

OSTGM-AS02 (Windows Server 2012 R2) Anwendungsserver:

- HSH Meso, Iris, Mia
- ProsozW
- Geve 4
- Kelio Zeiterfassung

OSTGM-VS01 (Windows Server 2016) Systemmanagementserver:

- Sophos Enterprise Console zur Verwaltung der Sophos Endpoint Protection
- Sophos Mobile Control als Verwaltungskonsole für mobile Geräte (MDM)

OSTGM-BS01 (Windows Server 2016) Backupserver:

- Backupserver für die Datensicherung auf die NAS-Systeme
- Veeam Backup & Replication

2.8.4 Systemmanagement

Für die zwei Hyper-V-Hosts wurde ein Hyper-V-Cluster gebildet. Hierdurch ist es möglich, die virtuellen Maschinen im laufenden Betrieb von einem Host auf einen anderen „umziehen" zu lassen. Dadurch ist die Wartung einzelner Hosts möglich bzw. im Falle des Ausfalls eines Hosts können sämtliche Server weiter betrieben werden. Die Zentralrechner sowie die Netzwerkkomponenten sind mit unterbrechungsfreien Stromversorgungen (USV) ausgestattet, um Datenverlust bei Stromausfall vorzubeugen.

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

Die Verwaltung von Daten erfolgt auf zwei in verschiedenen Brandabschnitten installierten Speichersystemen (Network Attached Storage). Die Systeme verfügen über mehrere Festplatten mit einem Raid 5 Level. Die Datensicherung erfolgt täglich auf beiden Speichersystemen. Gesichert werden von allen virtuellen Servern Anwendungs- und Betriebssystemsoftware, Datenbanken sowie System-, Anwendungs- und Benutzerdaten. Die Datensicherung wird maximal 28 Tage vorgehalten.

2.8.5 Arbeitsstationen – PCs, Notebooks und Tablets

Die PCs und Notebooks sind einheitlich mit dem Betriebssystem Windows 7 ausgestattet. Alle PCs und Notebooks der Fachbereiche sind über das Netz mit den Servern verbunden. DVD-Laufwerke und USB-Schnittstellen werden mit Umstellung auf das Betriebssystem Microsoft Windows 10 Professional bis auf wenige dienstlich begründete Ausnahmen deaktiviert.

Neben den eingesetzten Fachanwendungen wird bei der Gemeindeverwaltung Oststeinbek 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 Mitarbeiter im Bauhof über einen Tablet (iPad), das für dienstliche Aufgaben im Bereich der Unterhaltung von Wegen und Plätzen genutzt wird. Die Funktionen der Tablets sollen noch über eine bereits installierte Sicherheitssoftware auf die erforderlichen Funktionen begrenzt werden.

Die Nutzung der Internetdienste E-Mail und Web wird über die Firewall reglementiert (siehe Tz. 2.8.6).

2.8.6 Internes Netz, Firewall und Netzübergänge, Außenstellen

In der Gemeindeverwaltung Oststeinbek 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 Gemeindeverwaltung Oststeinbek ist für die Datenkommunikation mit Dataport über eine Firewall an das Landesnetz Schleswig-Holstein angeschlossen. Darüber hinaus sollen auch die Außenstellen über eine Firewall und eine VPN-Verbindung an das interne Netz angebunden werden. Die dafür benötigten Sicherheitsprodukte sind bereits angeschafft.

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 Gemeindeverwaltung Oststeinbek 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 einer Antivirensoftware werden somit Bedrohungen abgefangen und blockiert (vgl. Tz. 2.8.7).

2.8.7 Virenschutz

Für die Nutzung der Internetdienste E-Mail und Web sowie die Datenkommunikation über Schnittstellen und angeschlossene externe Netze setzt die Gemeindeverwaltung Oststeinbek zum Schutz der Daten eine Virenschutzsoftware ein. Es verfügt über folgende Funktionen:

- Abwehr von Malware auf Basis von Signaturen,
- Web-Filterung bei verdächtigen Verhaltensweisen und Aktivitäten von Schad-URLs,
- Exploit-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 bereits vom Provider Dataport 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 Bereich gespeichert. Die IT-Administration kann daraufhin die Anhänge auf ihre Zulässigkeit überprüfen.

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

2.9 Dokumentation und Nachweise für die Einhaltung datenschutzrechtlicher Vorschriften

Die Gemeindeverwaltung Oststeinbek 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. 2.7)
- IT-Konzept der Gemeinde Oststeinbek (siehe Tz. 2.8)
- Konzept für die Datensicherung
- Schulungskonzept zum Datenschutz und zur Informationssicherheit
- Report Informationsverbund mit Infrastruktur, Systeme, Netz und Anwendungen
- Report Technische und organisatorische Maßnahmen
- Report „Gruppenrichtlinien“ über Sicherheitseinstellungen auf dem Client
- Dienstanweisung der Gemeinde Oststeinbek zur Benutzung von informationstechnischen Systemen (IT-Systemen) sowie zur ordnungsgemäßen Verarbeitung von Informationen
- Dienstvereinbarung der Gemeinde Oststeinbek zur Nutzung von Internet- und E-Maildiensten am Arbeitsplatz

- Dienstanweisung für die Nutzung des Dokumentenmanagementsystems „REGISAFE“
- Richtlinie zum Verhalten bei Datenschutz- und Informationssicherheitsvorfällen
- Checkliste über den Einsatz mobiler Endgeräte
- Verfahrensakten mit Verfahrensbeschreibungen
- Verträge mit Dienstleistern im Rahmen einer Auftragsdatenverarbeitung

Für die Dokumentation wurde folgende Struktur angelegt:

Abb. 1: Ablagestruktur Datenschutz- und Informationssicherheit

2.9.1 Report „Informationsverbund mit Infrastruktur, Systeme, Netz und Anwendungen“ und Report „Modellierung der Grundschutzbausteine“

Der Informationsverbund der Gemeindeverwaltung Oststeinbek 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.

Den Objekten wurden nach den Vorgaben des IT-Grundschutzstandards alle erforderlichen Prozess- und Systembausteine mit den umzusetzenden Anforderungen zugeordnet. Diese können ebenfalls über den Report „Modellierung der Grundschutzbausteine“ dokumentiert werden.

- Gemeinde Oststeinbek
  - Geschäftsprozesse
    - Bauhof, Tiefbau
    - Bewirtschaften und Unterhaltung
    - Bildung und Kultur
    - Bürgerservice
    - Finanzen
    - Planen, Bauen, Umwelt
    - Soziales und Senioren
    - Stabsstelle Controlling
    - Stabsstelle Recht
    - Zentrale Dienste
  - Anwendungen (mod.)
    - Active-Directory
    - Datenablage Regisafe, Word / Excell
    - Datenbank MySQL
    - E-Mail
    - Fachanwendungen
    - Internet-Web
    - Office
  - IT-Systeme
    - Clients
    - Drucker und Kopierer
    - Mobile
    - Server
    - Speichersystem QNAP NAS
  - ICS-Systeme

Abb. 2: Ausschnitt Informationsverbund Oststeinbek

- Prozess-Bausteine
  - CON
    - CON.1 Kryptokonzept
    - CON.2 Datenschutz
    - CON.3 Datensicherungskonzept
    - CON.4 Auswahl und Einsatz von Standardsoftware
    - CON.5 Entwicklung und Einsatz von Allgemeinen Anwendungen
    - CON.6 Löschen und Vernichten
    - CON.7 Informationssicherheit auf Auslandsreisen
  - DER
    - DER.1 Detektion von sicherheitsrelevanten Ereignissen
    - DER.2.1 Behandlung von Sicherheitsvorfällen
    - DER.2.2 Vorsorge für die IT-Forensik
    - DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
    - DER.3.1 Audits und Revisionen
  - ISMS
    - ISMS.1 Sicherheitsmanagement
  - OPS
  - ORP
- System-Bausteine
  - APP
  - INF
    - INF.1 Allgemeines Gebäude
    - INF.2 Rechenzentrum sowie Serverraum
    - INF.3 Elektrotechnische Verkabelung
    - INF.4 IT-Verkabelung
    - INF.7 Büroarbeitsplatz
    - INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume

Abb. 3: Ausschnitt Prozess- und Systembausteine

2.9.2 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
- Test und Freigabe
- Berechtigungskonzept
- Handbücher
- Protokolle und Kontrollen
- Updates
- Hardware

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

2.9.3 IT-Konzept

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

Neben den Vorgaben für die IT-Systeme und der 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 Gemeindeverwaltung Oststeinbek.

2.9.4 Dienstanweisungen und Richtlinien

Die festgelegten technischen und organisatorischen Maßnahmen wurden zum Teil in Handlungsanweisungen im Rahmen von Dienstanweisungen und/oder Richtlinien mitarbeiterbezogen übertragen.

Die Dienstanweisung der Gemeinde Oststeinbek zur Benutzung von informationstechnischen Systemen (IT-Systemen) sowie zur ordnungsgemäßen Verarbeitung von Informationen beinhaltet z. B. folgende Regelungen:

- Vor dem erstmaligen IT-Einsatz ist eine ausreichende Schulung der Benutzer unter Berücksichtigung der datenschutzrechtlichen Anforderungen zu gewährleisten.
- Es darf nur dokumentierte, für den jeweiligen Arbeitsplatz freigegebene und aktuell gültige Software eingesetzt werden.
- Das Einspielen und die Nutzung von nicht ordnungsgemäß lizenzierter oder privat beschaffter Software sind nicht zulässig.
- Änderungen und Erweiterungen an der Hardware dürfen nur von der Systemadministration vorgenommen werden.
- Personenbezogene Daten dürfen nur im zugelassenen Rahmen verarbeitet werden.
- Die Installation der System- und Anwendungssoftware und jede Veränderung ist von der Systemadministration durchzuführen.
- Alle Daten, die mithilfe von Office-Anwendungen verarbeitet werden, sind zentral in den dafür vorgesehenen Ablagen in REGISAFE zu speichern. Einzelheiten hierzu ergeben sich aus der „Dienstanweisung für die Nutzung des Dokumentenmanagementsystems REGISAFE". Speicherungen von Arbeitskopien auf den lokalen Festplatten sind nur in absoluten Ausnahmefällen (z. B. bei Störungen im Netzwerkbetrieb) zulässig.
- Bei Dienstende sind aktivierte Programme ordnungsgemäß zu beenden und das jeweilige Gerät ist auszuschalten.
- Drucker sind so aufzustellen bzw. einzurichten, dass nur Berechtigte Zugang haben. Der vom Arbeitsplatz aus gestartete Druck mit personenbezogenen Daten auf Zentraldruckern darf nur nach Authentifizierung (Eingabe PIN) am Drucker erfolgen. Nach Abschluss der Arbeiten sind alle Ausdrucke aus dem Drucker zu entfernen.
- „Musterschreiben" sind ohne personenbezogenen Inhalt zu speichern.
- Papiergut mit personenbezogenem Inhalt muss datenschutzgerecht entsorgt werden. Die Entsorgung hat entweder mittels eines der im Rathaus sowie in den Außenstellen vorhandenen Papierschredder oder über den im Erdgeschoss des Rathauses befindlichen Datenvernichtungscontainer zu erfolgen. Eine Entsorgung über den Papierkorb ist unzulässig.
- Personenbezogene Daten in Akten sind zu löschen, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Maßgeblich sind hier die bereichsspezifischen Aufbewahrungsfristen.
- Besucher dürfen sich nur in Anwesenheit eines Mitarbeiters im Büro aufhalten.
- Unbesetzte Diensträume mit IT-Systemen, Datenträgern sowie Schriftstücken mit personenbezogenen Daten sind abzuschließen, Datenträger und Schriftstücke mit personenbezogenen Daten sind bei Abwesenheit in verschlossenen Schränken aufzubewahren (Clean Desk Prinzip). Die Schlüssel sind so aufzubewahren, dass sie nicht von Unbefugten benutzt werden können. Fenster in Büroräumen sind nach Dienstschluss geschlossen zu halten.
- Bei der Verarbeitung von personenbezogenen Daten ist zu verhindern, dass Unbefugte Einblick in die laufende Datenverarbeitung haben. Bei Stellen mit Kundenverkehr muss der Moni-

tor so aufgestellt oder präpariert werden, dass Unbefugte diesen nicht einsehen können.

- Die Benutzer der IT-Systeme dürfen nur Zugang zu Daten und Programmen haben, die für die Aufgabenerledigung nach der Arbeitsplatzbeschreibung erforderlich sind. Die Zugangsberechtigungen sind den Verfahrensakten der jeweiligen Verfahren zu entnehmen.
- Alle für den Arbeitsplatz eingerichteten, servergestützten Anwenderfunktionen dürfen nur nach Eingabe einer Benutzerkennung, gekoppelt mit nachfolgender Passworteingabe, aktiviert werden.
- Beim erstmaligen Anmelden an einer Server-Anwendung ist das Initialpasswort durch ein persönliches Passwort zu ersetzen.
- Das Passwort muss mindestens 8 Zeichen lang sein und immer aus einer Kombination von Buchstaben und Ziffern und/oder Sonderzeichen bestehen sowie Groß- und Kleinschreibung beinhalten. Es darf keine Rückschlüsse auf seinen Besitzer zulassen und ist vertraulich zu behandeln. Das Passwort soll in unregelmäßigen Abständen geändert werden. Nach 90 Tagen fordert das System automatisch zur Änderung auf. Die letzten fünf Passwörter dürfen nicht wieder verwendet werden.
- Sofern schützenswerte Informationen verarbeitet werden und Dritte Zugang zum Arbeitsplatz-PC oder mobilen Endgerät haben können, sind Bildschirmschoner passwortgeschützt mit einer maximalen Einschaltzeit von zehn Minuten einzustellen. Grundsätzlich muss bei vorübergehender Nichtnutzung der Geräte die Bildschirmdunkelschaltung mit Passwortaktivierung manuell eingeschaltet und so das betreffende Gerät gesperrt werden (Tastenkombination Strg+ALT+Entf, anschließend Enter oder Windows-Taste +L).
- Sämtliche schriftliche Unterlagen, aus denen Rückschlüsse auf Zugangsmöglichkeiten zum System (z. B. Benutzerkennung, Passwort) gezogen werden können, sind für Unbefugte unzugänglich aufzubewahren.
- Eine Speicherung privater Dokumente auf dem Server, der Festplatte des PCs, auf mobilen Endgeräten und auf externen Speichern, z. B. USB-Stick, ist nicht zulässig.
- Es darf keine private Software installiert und eingesetzt werden.
- Die dienstliche Nutzung privater Daten und die private Nutzung dienstlicher Daten sind nicht zulässig.

2.9.5 Auftragsdatenverarbeitung mit Dienstleistern

Die Gemeindeverwaltung Oststeinbek hat im Rahmen einer Auftragsdatenverarbeitung u. a. folgende Dienstleister vertraglich beauftragt:

- **Papierentsorgung**

Die Gemeindeverwaltung Oststeinbek entsorgt über Sicherheitsbehälter Papierabfälle und ausgesonderte digitale Datenträger über die Firma Meinhardt Recycling GmbH. Die Firma sichert eine

Vernichtung im Rahmen der DIN 66399 mit der Schutzklasse 2und der Sicherheitsstufe P3 zu.

- **Netzwerkstatt**

Die Firma Netzwerkstatt erbringt „Servershare“ bzw. Providerdienstleistungen im Zusammenhang mit der Software „EDITH“, einem Ratsinformationssystem. Mit der Software werden insbesondere den Gemeindevertretern Tagesordnungen und Sitzungsprotokolle der Gemeindeverwaltung Oststeinbek bereitgestellt.

- **Dataport**

Von Dataport werden einzelne Fachverfahren, z. B. „Autista“ (Standesamtsfachverfahren), gehostet. Darüber hinaus wurde Dataport als Provider für die Nutzung der Internetdienste E-Mail und Web beauftragt. Die Kommunikation erfolgt über das Landesnetz Schleswig-Holstein.

Mit den Dienstleistern wurde Kontakt aufgenommen, um die Verträge an die Anforderungen der Datenschutz-Grundverordnung anzupassen.

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.

Die behördliche Datenschutzbeauftragte verfügt über die erforderliche Sachkunde und Zuverlässigkeit. Sie führt die ihr übertragenen Aufgaben sehr motiviert durch und sorgt bei den Mitarbeiterinnen und Mitarbeitern für Akzeptanz für die einzuhaltenden Schutzmaßnahmen.

Die IT-Administration sorgt dafür, dass die Anforderungen des IT-Grundschutzstandards technisch realisiert werden können, und setzt dafür die erforderlichen Sicherheitsprodukte ein.

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

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

- 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 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.
- Es werden von der Gemeindeverwaltung Oststeinbek einheitliche IT-Systeme am Arbeitsplatz eingesetzt, so dass damit eine Standardisierung der Arbeitsumgebung sichergestellt wird.
- Für den Anschluss des internen Verwaltungsnetzes an das Internet werden Sicherheitskomponenten eingesetzt, die unerwünschte Zugriffe abwehren. Mobile Systeme können durch Einsatz einer Sicherheitssoftware reglementiert und auf Systemen der Gemeindeverwaltung Oststeinbek zentral verwaltet werden.

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

Kiel, 24. Mai 2018 Heiko Behrendt