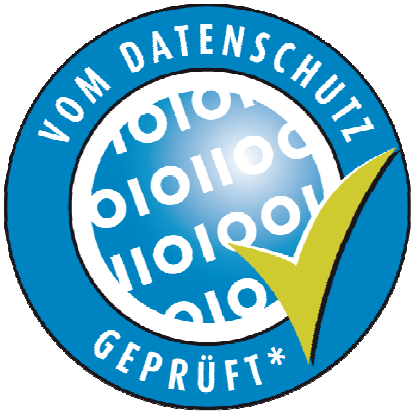


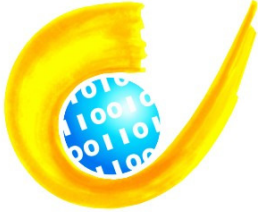
Gutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Amt Viöl

Interne automatisierte Datenverarbeitung

Anbindung des internen Netzes an das Internet



ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Autor: Sven Thomsen
Tel.: 0431-988-1211
Fax: 0431-988-1226
E-Mail: ULD3@datenschutzzentrum.de
Datum: 31.08.2009
Version: 1.0

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits

1.1 Vereinbarung

Grundlage des Datenschutz-Behördenaudits ist der Audit-Vertrag zwischen dem Amt Viöl und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein vom 16. Februar 2009.

Gegenstand des Datenschutz-Behördenaudits ist

- die Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter und
- die Anbindung des internen Netzes der Gemeindeverwaltung an das Internet.

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 im Amt Viöl 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.

Das Voraudit wurde durch Herrn Heiko Behrendt, Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz, durchgeführt.

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

- Überprüfung der Abgrenzung des Auditgegenstands,

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

Die vom Amt Viöl vorgelegte Dokumentation für den Auditgegenstand bildet die Grundlage für die Begutachtung vor Ort.

Das Datenschutz-Behördenaudit wurde durch Herrn Sven Thomsen, Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz, durchgeführt.

1.3 Datenschutzziele

Das Amt Viöl hat in einem Sicherheitskonzept Ziele für den sicheren und datenschutzkonformen Einsatz festgelegt.

Die Ordnungsmäßigkeit der automatisierten Datenverarbeitung im Amt Viöl soll unter Berücksichtigung

- der Integrität (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen oder der Manipulation von Daten),
- der Vertraulichkeit (z. B. Schutz vor unbefugter Kenntnisnahme von Daten) und
- der Verfügbarkeit (z. B. Schutz vor Diebstahl oder Zerstörung)

der zur Aufgabenerfüllung notwendigen personenbezogenen Daten gewährleistet werden.

Das Amt Viöl 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.

2 Feststellung zu den sicherheitstechnischen Elementen des Datenschutzmanagementsystems

2.1 Aufbau- und Ablauforganisation

2.1.1 Verantwortung

Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung trägt der Leitende Verwaltungsbeamte.

2.1.2 Systemadministration

Die Systemadministration wird durch Frau Marion Phillips durchgeführt.

Die Arbeit der Systemadministration ist durch eine Dienstanweisung geregelt.

In der Dienstanweisung werden der Systemadministration die folgenden Aufgaben zugewiesen:

- IT-Projektplanung
- Erstellung von IT-Realisierungskonzepten
- Erarbeitung von Sicherheitsanforderungen
- Erstellung von IT-Dienstanweisungen
- Haushaltsplanung für den EDV-Bereich
- Beratung der Fachämter
- Beschaffung der Hard- und Software und EDV-Verbrauchsmittel
- Installation und Konfiguration der Hard- und Software
- Gewährleistung des Netzbetriebes und Überwachung des Systems
- Gewährleistung der Sicherheits- und Sicherungsanforderungen
- Durchführung der Datensicherung
- Verwaltung der Software und Überwachung der zugelassenen Programme
- Benutzerverwaltung
- Störfallbeseitigung
- Erstellung der erforderlichen Programm- und Verfahrensdokumentation
- Regelung der Durchführung von Schulungen für die Mitarbeiter
- Führung des Geräte- und Inventarverzeichnisses
- Führung des Softwareverzeichnisses

2.1.3 Datenschutzbeauftragte

Die zentralen Datenschutzfunktionen obliegen der EDV-Abteilung. Als behördliche Datenschutzbeauftragte ist Frau Marion Phillips gemäß § 10 LDSG schriftlich bestellt. Die Bestellung erfolgte durch den Leitenden Verwaltungsbeamten.

Frau Phillips verfügt aufgrund langjähriger Tätigkeit als Systemadministratorin über die erforderliche Sachkunde.

Es wurde geprüft, ob bei der Ausführung ihrer Aufgaben als Datenschutzbeauftragte ein Konflikt mit ihrer Tätigkeit als Systemadministratorin besteht. Festgestellt wurde, dass Frau Phillips ausreichende zeitliche Ressourcen von der Leitungsebene zur Verfügung gestellt werden, so dass sie ihre Doppelfunktion ordnungsgemäß ausführen kann. Ferner werden ihre Aufgaben im Rahmen der Umsetzung von Sicherheitsmaßnahmen durch Vorgesetzte kontrolliert. Die enge Anbindung an die Leitungsebene sorgt weiterhin dafür, dass Datenschutzaufgaben vom Leitenden Verwaltungsbeamten unterstützt werden (siehe Tz. 2.1.4 bis 2.1.6).

2.1.4 Regelmäßige und anlassbezogene Kontrollen

Die Überwachung und Prüfung der im Sicherheitskonzept festgelegten Sicherheitsmaßnahmen obliegt gemäß Sicherheitskonzept dem Leitenden Verwaltungsbeamten unter Einbeziehung der Systemadministration. Laut Sicherheitskonzept ist die Personalvertretung zu beteiligen. Die Ergebnisse der Kontrollen sind schriftlich festzuhalten.

2.1.5 Verhalten bei Sicherheitsvorfällen

Bei Verstößen gegen die festgelegten technischen und organisatorischen Sicherheitsmaßnahmen leitet die behördliche Datenschutzbeauftragte zusammen mit dem Leitenden Verwaltungsbeamten eine Überprüfung ein. Die Ergebnisse der Überprüfung werden sollen schriftlich dokumentiert.

2.1.6 Integration von Datenschutz und Datensicherheit

Die behördliche Datenschutzbeauftragte wirkt an der Fortentwicklung der Informations- und Kommunikationstechnologie des Amtes Viöl unmittelbar mit.

2.2 Dokumentation

Das Amt Viöl hat die nach dem LDSG und der DSVO erforderliche Dokumentation der automatisierten Datenverarbeitung modular aufgebaut.

2.2.1 Systemakten

In einer Dienstanweisung ist festgelegt, dass für jedes System eine Systemakte zu führen ist. Aufbau und Inhalt der Systemakten 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.

2.2.2 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.

2.2.3 IT-Konzept

Die Amtsverwaltung 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 festgelegt.

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

2.2.4 Sicherheitskonzept

Im Sicherheitskonzept für die automatisierte Datenverarbeitung des Amts Viöl werden die technischen und organisatorischen Maßnahmen dargestellt, die seitens der Amtsverwaltung getroffen worden sind.

Das Sicherheitskonzept enthält unter anderem Maßnahmen

- zur Schulung der Mitarbeiter,
- zur Gebäudesicherheit,
- zur Aktenführung und Aktenaufbewahrung, insbesondere auch zu Archiv und Aufbewahrungsfristen,
- zum Umgang mit Fremdpersonal, insbesondere Reinigungspersonal,
- zum Umgang mit Publikumsverkehr und
- zur Umsetzung von Betroffenenrechten, insbesondere Auskünfte und Nachweise zur Datenübermittlung.

Das Sicherheitskonzept enthält spezielle Sicherheitsmaßnahmen für Server (vgl. Abschnitt 2.2.10) sowie für Clients (vgl. Abschnitt 2.2.11).

Es werden spezielle Regelungen für die anfallenden Datenbestände, insbesondere zur Datensicherung und zum Umgang mit externen Datenträgern getroffen.

In einem eigenen Abschnitt des Sicherheitskonzepts werden Sicherheitsmaßnahmen zur Anbindung des verwaltungsinternen Netzes an externe Netze, insbesondere dem Kreisnetz Nordfriesland als auch dem Internet, beschrieben.

2.2.5 Dienstanweisungen und Dienstvereinbarungen

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 Juni 2009) wird der Umgang mit den Informations- und Kommunikationssystemen der Amtsverwaltung 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 „Nutzung der Internet-Dienste“ (Stand Juni 2009) hält unter anderem fest, dass Internet-Dienste nur als Informationsmedien in dienstlichen Belangen genutzt werden dürfen. Weitere Details zur Nutzung sind in einer Dienstvereinbarung (s.u) geregelt.
- In der Dienstanweisung „IT-Koordination“ (Stand Juni 2009) werden die Aufgaben und Zuständigkeiten der EDV-Abteilung festgelegt.

Zusätzlich zu den Dienstanweisungen hat die Amtsverwaltung mit dem Personalrat des Amtes Viöl eine „Dienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz“ geschlossen.

In der Dienstvereinbarung ist festgehalten, dass die private Nutzung in geringfügigem Umfang zulässig ist, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für dienstliche Zwecke nicht beeinträchtigt werden und haushaltsrechtliche Grundsätze dem nicht

entgegenstehen.

Privater E-Mail-Verkehr darf laut Dienstvereinbarung nur über Web-Mail-Dienste abgewickelt werden.

Ferner wurde festgelegt, dass die Amtsverwaltung berechtigt ist, die private Internetnutzung der Mitarbeiter zu protokollieren und zu kontrollieren.

Neben weiteren Verhaltensgrundsätzen ist insbesondere das Vorgehen zur Protokollierung und Kontrolle detailliert geregelt.

2.2.6 Büroräume

Die Amtsverwaltung Viöl nutzt das Gebäude Westerende 41, 25884 Viöl.

Im Gebäude sind noch weitere Untermieter untergebracht. Es findet keine gemeinsame Nutzung von Räumen statt. Es ist eine ausreichende räumliche Abschottung vorhanden.

Alle Räume sind verschließbar und mit ausreichendem Ablageplatz in verschließbaren Schränken ausgestattet.

2.2.7 Serverraum

Der Serverraum befindet sich im Erdgeschoss. Das Fenster des Serverraums ist durch ein zusätzliches Gitter gesichert. Zutritt zum Serverraum hat nur die IT-Koordination.

2.2.8 Verwaltungsinternes Netz

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

Zugang zum Netz ist grundsätzlich nur in den Büroräumen möglich, nicht für den Publikumsverkehr zugänglichen Bereich. Eine Ausnahme bilden einzelne Peripheriegeräte (vgl. 2.2.12).

Nicht benötigte Anschlüsse in den Büroräumen sind nicht beschaltet.

2.2.9 Rechnersysteme allgemein

Sämtliche Systeme 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 der verwendete Paketfilter.

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

Jedes System wird regelmäßig mit Patches, Bugfixes und Service Packs versehen. Die Amtsverwaltung betreibt hierzu einen WSUS-Server (Windows Server Update Services der Firma Microsoft), der jedes Rechnersystem mindestens wöchentlich mit Sicherheitsaktualisierungen versieht.

2.2.10 Server

Die Amtsverwaltung betreibt einen zentralen Server.

Das System befindet sich im Serverraum der Gemeindeverwaltung. Der Server hängt an einer unterbrechungsfreien Stromversorgung, die im Falle eines Stromausfalls für ein geordnetes Herunterfahren des Servers sorgt.

Die Ablage von Daten erfolgt ausschließlich auf dem Server. Die Daten des Servers werden auf Datensicherungsbänder in mehreren Generationen gesichert. Die verwendeten Sicherungsbänder werden in einem feuersicheren Tresor aufbewahrt. Lediglich die IT-Koordination hat Zugriff auf die Datensicherungsbänder.

Die Ablage der Daten erfolgt in Übereinstimmung mit dem Berechtigungskonzept in einer strukturierten Dateiablage getrennt nach Fachämtern, Benutzern und Funktionen.

2.2.11 Arbeitsplatz-PCs

Die Arbeitsplatz-PCs werden zentral konfiguriert und administriert.

Jeder Arbeitsplatz-PC wird sowohl bei der Erstinstallation als auch bei der weiteren Pflege der installierten Programme mit getesteten und freigegebenen Programmversionen versehen.

Durch den Einsatz von Gruppenrichtlinien werden:

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

Externe Schnittstellen (Laufwerke, USB oder IEEE1394-Anschlüsse, serielle oder parallele Anschlüsse) werden grundsätzlich gesperrt und nur bei Bedarf nach Genehmigung durch die Amtsleitung freigeschaltet.

2.2.12 Peripheriegeräte

Die Amtsverwaltung setzt für Druckaufträge mit größerem Volumen oder spezieller Nachbearbeitung – Heften, Lochen, Falzen – ein vernetztes Großgerät ein, das zusätzlich die Funktion eines Kopierers übernimmt.

Es werden nur Geräte eingesetzt, die eine gerätebezogene Verschlüsselung der auf der lokalen Festplatte vorhandenen Daten ermöglichen. Alternativ verbleibt die Festplatte im Eigentum der Amtsverwaltung. Das Gerät ist in einem Raum aufgestellt, welches zwar für den Publikumsverkehr

indirekt zugänglich ist, aber unter stetiger Aufsicht steht. Das Gerät bietet die Möglichkeit, für Druckaufträge mit personenbezogenen Daten eine verzögerte Ausgabe nach Eingabe eines PIN-Codes durchzuführen.

2.3 Zugänge zum Internet und zum Kreisnetz

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

Jeglicher Datenverkehr wird nicht nur auf seine Zulässigkeit, sondern auch auf schadhafte Inhalte wie Viren, Würmer und Trojaner geprüft.

Die Amtsverwaltung setzt hierfür eine Kombination aus einem von der Amtsverwaltung verwalteten Paketfilter, der einzelne Verbindungen in externe Netze von Systemen der Gemeindeverwaltung freischaltet, und einem vom Kreis Nordfriesland verwalteten Proxy-Server ein, der die übertragenen Daten auf schadhafte Inhalte kontrolliert.

Die Amtsverwaltung hat zu diesem Zweck mit dem Kreis Nordfriesland einen Vertrag zur Auftragsdatenverarbeitung geschlossen.

2.3.1 Paketfilter

Als zentraler Übergabepunkt ist ein Paketfilter eingerichtet. An zentraler Stelle werden sämtliche Datenverbindungen aus dem internen Netz in externe Netze (Kreisnetz, Internet) kontrolliert.

Der Paketfilter weist sämtliche Verbindungsversuche von externen Netzen in das Netz der Verwaltung ab.

2.3.2 Proxy-Filter

Die Amtsverwaltung nutzt Internet-Dienste über den Proxy-Server des Kreises Nordfriesland. Die Konfiguration des Proxy-Servers inkl. der Filterregeln liegt der Amtsverwaltung vor. Der Aufruf schadhafter Inhalte sowie von Seiten mit unerwünschten Inhalten wird blockiert.

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

Die Überprüfung hat ergeben, dass die 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.

Die durch das Datenschutz-Behördenaudit in der Amtsverwaltung Viöl erfassten Verarbeitungsprozesse zeichnen sich besonders durch folgende „datenschutzfreundliche" Aspekte aus:

- Die in den Fachverfahren der Amtsverwaltung verarbeiteten Bürgerdaten werden durch ausreichende IT-Sicherheitsmaßnahmen geschützt.
- Die Disketten-, CD-ROM-Laufwerde und USB-Speichermedien werden durch den Einsatz von Sicherheitssoftware zentral reglementiert.
- Die Amtsverwaltung hat eine gut strukturierte, systematische und übersichtliche Dokumentation gemäß DSVO erstellt. Diese bietet eine effektive Arbeitsgrundlage für das behördliche Datenschutzmanagementsystem.
- Für den Anschluss den internen Verwaltungsnetzes an das Internet werden Sicherheitskomponenten eingesetzt, die unerwünschte Zugriffe abwehren.
- Die Sicherheitsmechanismen zur zentralen Vergabe von Berechtigungen und der Steuerung der Arbeitsplatzrechner über das Active Directory werden intensiv genutzt.

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

Kiel, 31.08.2009 (Sven Thomsen)