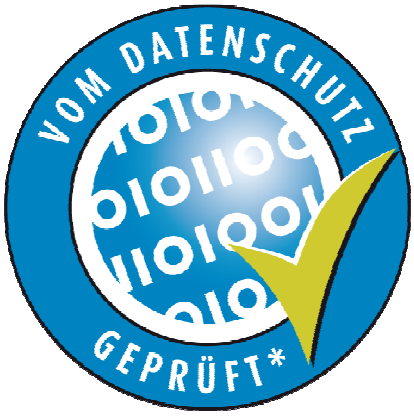

Kurzgutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Gemeinde Stockelsdorf:

Allgemeine Datenverarbeitung

Anbindung des internen Netzes an das Internet

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datum:	02.10.2007
Aktenzeichen:	16.01/05.005
Telefon:	0431/988-1211
Fax	0431/988-1223
E-Mail:	mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Audits

1.1 Vereinbarung

Grundlage dieses Datenschutz-Audits ist der Audit-Vertrag zwischen der Gemeindeverwaltung Stockelsdorf und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein vom 05.07.2005.

Gegenstand des Datenschutz-Audits ist

- die Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung der Gemeindeverwaltung Stockelsdorf 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 Datenschutzziele

Die Gemeindeverwaltung Stockelsdorf hat die folgenden Datenschutzziele festgelegt:

- Beachten der Rechtmäßigkeit und Ordnungsmäßigkeit der Datenverarbeitung
- Wahrung des Rechts der Bürgerinnen und Bürger auf informationelle Selbstbestimmung
- Beachten der Grundsätze der Ordnungsmäßigkeit des Verwaltungshandelns
- Beachten von wirtschaftlichen oder haushaltsrechtlichen Obliegenheiten
- Datensparsame Durchführung der Datenverarbeitung
- Sicherstellen der Verfügbarkeit der verwendeten Systeme und Programme
- Aufrechterhalten der Integrität der Systeme und insbesondere der gespeicherten personenbezogenen Daten
- Gewährleisten der Vertraulichkeit der in der Gemeindeverwaltung Stockelsdorf verarbeiteten Daten

Diese Ziele sind durch die Leiterin der Daten verarbeitenden Stelle im Rahmen einer internen Datenschutzerklärung festgelegt worden.

Die Datenschutzziele bilden die Grundlage des allgemeinen Sicherheitskonzepts für die automatisierte Datenverarbeitung der Gemeindeverwaltung.

2 Feststellung zu den sicherheitstechnischen Elementen des Datenschutz-Managementsystems

2.1 Aufbau und Ablauforganisation

2.1.1 Allgemeine Geschäftsverteilung

Die Gemeindeverwaltung Stockelsdorf gliedert sich in vier Ämter:

- Hauptamt
- Ordnungsamt
- Bauamt
- Kämmereiamt

Der Bürgermeisterin direkt unterstellt sind die Gleichstellungsbeauftragte und ein Mitarbeiter des Hauptamtes in seiner Funktion als behördlicher Datenschutzbeauftragter.

2.1.2 Systemadministration

Die Systemadministration wird durch Herrn Gert Schulz, Mitarbeiter des Hauptamtes, durchgeführt. Er wird in Fragen des Datenschutzes, der Datensicherheit und Einzelfragen der ordnungsgemäßen Datenverarbeitung durch den behördlichen Datenschutzbeauftragten beraten.

Die Arbeit der Systemadministration ist zusätzlich durch eine spezielle Dienstanweisung geregelt.

Herr Schulz ist vom ULD geprüfter Systemadministrator mit Datenschutzzertifikat.

2.1.3 Datenschutzbeauftragter

Als behördlicher Datenschutzbeauftragter gemäß § 10 LDSG ist Herr Nils Theisen schriftlich bestellt. Die Bestellung erfolgte durch die Bürgermeisterin am 02.07.2007.

Herr Theisen hat sich die erforderliche Sachkunde durch mehrere Kurse an der Datenschutzakademie erworben und ist bereits für die Prüfung zum Systemadministrator mit Datenschutzzertifikat Ende des Jahres 2007 angemeldet.

Herr Theisen arbeitet in seiner Funktion als Datenschutzbeauftragter weisungsfrei und ist der Bürgermeisterin direkt unterstellt.

Herr Theisen ist mit einem Stellenanteil von 30% für seine Tätigkeit als behördlicher Datenschutzbeauftragter freigestellt. Ihm stehen die notwendigen Mittel zur Ausübung seiner Tätigkeit zur Verfügung.

Der behördliche Datenschutzbeauftragte übernimmt in Abwesenheit des Systemadministra-

tors vertretungsweise dessen Aufgaben, ist aber nicht mit regelmäßigen Aufgaben in der Systemadministration betraut. Ein Konflikt im Sinne des § 10 Abs. 2 LDSG besteht nicht.

2.1.4 Regelmäßige Kontrollen

Im Sicherheitskonzept für die allgemeine Datenverarbeitung ist festgelegt, dass der behördliche Datenschutzbeauftragte die Angemessenheit und Wirksamkeit der getroffenen zumindest einmal jährlich überprüft.

Die Gemeindeverwaltung gliedert ihre Dokumentation gemäß DSVO in Verfahrens- und Systemakten. Im Rahmen einer jährlichen Fortschreibung werden die Systemakten und Verfahrensakten durch den behördlichen Datenschutzbeauftragten auf Vollständigkeit und Aktualität geprüft.

Die Ergebnisse der regelmäßigen Kontrollen werden in den jeweiligen System- und Verfahrensakten dokumentiert und der Bürgermeisterin zur Kenntnis gegeben.

2.1.5 Anlassbezogene Kontrollen

Ergeben sich durch Berichterstattung in der Fachpresse, aufgrund von Meldungen der Softwarehersteller oder aus anderen Publikationen Hinweise, dass die Gemeindeverwaltung Stockelsdorf ihre Sicherheitskonzeption neu prüfen muss, so führt der Datenschutzbeauftragte in Zusammenarbeit mit der Administration eine entsprechende Prüfung durch.

Die Ergebnisse dieser Kontrolle werden durch den Datenschutzbeauftragten dokumentiert und der Bürgermeisterin zur Kenntnis gegeben.

2.1.6 Verhalten bei Sicherheitsvorfällen

Die Gemeindeverwaltung hat im Sicherheitskonzept festgelegt, welche Kriterien auf einen Sicherheitsvorfall schließen lassen und wie ein möglicher Sicherheitsvorfall zu bearbeiten ist.

Die Bearbeitung erfolgt in zwei Schritten. Im ersten Schritt wird die Behebung des Sicherheitsvorfalls durch Sofortmaßnahmen durchgeführt. Sämtliche getroffenen Maßnahmen werden dokumentiert. Im zweiten Schritt wird der Sicherheitsvorfall nachbereitet und eine abschließende Dokumentation des Vorfalls erstellt.

Die Dokumentation wird der Bürgermeisterin zur Kenntnis gegeben.

2.1.7 Integration von Datenschutz und Datensicherheit in das Verwaltungshandeln

Der Datenschutzbeauftragte wird bei jeder Beschaffung von Informations- und Kommunikationstechnologie beteiligt. Es ist festgelegt, dass bei der Planung und Änderung von Verfahren zur Verarbeitung personenbezogener Daten der behördliche Datenschutzbeauftragte zu

beteiligen ist.

2.2 Dokumentation

Die Gemeindeverwaltung Stockelsdorf wählt für die Dokumentation der automatisierten Datenverarbeitung gemäß DSVO einen strukturierten Ansatz.

In einem „Stammordner“ werden sämtliche allgemeinen, verfahrens- und systemübergreifenden Aspekte der Datenverarbeitung zusammengefasst. Der Stammordner dient gleichzeitig als Verfahrensverzeichnis gemäß §7 Abs. 1 LDSG.

Darüber hinaus werden im Stammordner große Teile der verfahrensübergreifenden Dokumentation und Protokolle gemäß § 8 DSVO geführt. Die system- oder verfahrensspezifischen Teile sind dann in einzelnen System- oder Verfahrensakten aufgeführt.

Grundsätzlich werden möglichst viele Aspekte der Verarbeitung personenbezogener Daten im allgemeinen Sicherheits- und IT-Konzepten zusammengefasst. Sollte darüber hinaus für einzelne Fachverfahren oder Systeme zusätzlicher Bedarf an Regelungen und Maßnahmen entstehen, so werden diese speziellen Maßnahmen in speziellen Konzepten in der jeweiligen System- oder Verfahrensakte aufgenommen.

2.2.1 Systemakten

Für die Führung der Systemakten ist der Systemadministrator verantwortlich.

Die Gemeindeveraltung hat für jedes Client- und Serversystem eine Systemakte eingeführt. In den Systemakten werden neben der Bezeichnung des jeweiligen Systems, dem Standort des Systems und der Einbindung in das Netzwerk zusätzlich sämtliche auf dem System installierten Programme dokumentiert.

Für jedes System wird eine Dokumentation der administrativen Tätigkeiten im Sinne des § 8 Abs. 5 DSVO in der jeweiligen Systemakte geführt.

2.2.2 Verfahrensakten

Die Pflege der Verfahrensakten erfolgt durch die jeweiligen durch die Bürgermeisterin benannten Fachverfahrensverantwortlichen. Zum Zeitpunkt der Auditierung liegt diese Verantwortung bei der jeweiligen Fachamtsleitung.

In den Verfahrensakten ist neben allgemeinen Informationen zum Verfahren stets ein Berechtigungskonzept für das jeweilige Fachverfahren im Sinne einer Dokumentation der vergebenen Rechte gemäß § 8 Abs. 4 DSVO enthalten.

Die Verfahrensakten dokumentieren darüber hinaus die gemäß § 7 DSVO durchgeführten Test- und Freigabeverfahren für das jeweilige Fachverfahren.

2.2.3 Allgemeines IT-Konzept

Die Gemeindeverwaltung hat die technischen und organisatorischen Vorgaben für die allgemeine Verarbeitung personenbezogener Daten in einem informationstechnischen Konzept gemäß § 4 DSVO zusammengefasst.

Neben Vorgaben für die Server-, Client- und Netzwerkinfrastruktur sind im IT-Konzept die Obliegenheiten der Fachverfahrensverantwortlichen, der Systemadministration sowie des Datenschutzbeauftragten festgelegt.

2.2.4 Allgemeines Sicherheitskonzept

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

Das Sicherheitskonzept enthält Maßnahmen zu:

- Räumen und Gebäuden,
- dem verwaltungsinternen Netzwerk,
- den Übergängen aus dem verwaltungsinternen Netzwerk in das Internet oder das Landesnetz,
- Servern und Clients,
- mobilen Geräten und
- Peripheriegeräten.

Zusätzlich sind die sicherheitsrelevanten Regelungen bezüglich der Administration der Systeme, Maßnahmen zur Notfallvorsorge und dem Verhalten bei Sicherheitsvorfällen enthalten.

Das Sicherheitskonzept beschreibt darüber hinaus die regelmäßigen und anlassbezogenen Kontrolltätigkeiten des behördlichen Datenschutzbeauftragten.

2.2.5 Dienstanweisungen

Die im allgemeinen IT-Konzept und dem allgemeinen Sicherheitskonzept festgelegten technischen und organisatorischen Vorgaben sowie die Sicherheitsmaßnahmen werden durch mehrere Dienstanweisungen in geltende Anweisungen an die Beschäftigten der Gemeindeverwaltung umgesetzt. Die folgenden Dienstanweisungen sind zum Zeitpunkt des Audits in Kraft:

- In der allgemeinen Geschäftsanweisung sind Regelungen zum Verschluss von Fenstern und Türen sowie der korrekten Durchführung der aktenbasierten Datenverarbeitung enthalten.
- Die allgemeine Dienstanweisung zur Nutzung der Informations- und Kommunikationstechnologie stellt die Rahmenbedingungen für die ordnungsgemäße, automati-

sierte Datenverarbeitung her.

- In der speziellen Dienstanweisung zur Nutzung der Internet-Dienste ist zunächst geregelt, dass die Internet-Dienste ausschließlich für die dienstliche Nutzung zur Verfügung gestellt werden, eine private Nutzung ist ausdrücklich verboten. Es ist geregelt, wie die Kontrolle dieses Verbots unter Beteiligung des Datenschutzbeauftragten und unter Wahrung der Rechte der Personalvertretung durchgeführt wird.
- In der speziellen Dienstanweisung für die Administration werden die Aufgaben der Administration festgelegt. Explizit geregelt ist, dass die Überwachung der Mitarbeiter bezüglich der Einhaltung der in der EDV-Dienstanweisung für Benutzer aufgeführten Regelungen nur anlassbezogen und auf gesonderte Anweisung vom Fachamtsleiter im Beisein der Systemverwaltung und des Datenschutzbeauftragten durchgeführt wird. Die Beteiligungsrechte des Personalrats seien hierbei zu beachten.

2.3 Allgemeine Datenverarbeitung

2.3.1 Büroräume

Die Gemeindeverwaltung Stockelsdorf teilt sich auf drei Standorte auf:

- das Rathaus, Ahrensböker Straße 7, 23517 Stockelsdorf
- die Kämmerei, Ahrensböker Straße 7, 23517 Stockelsdorf
- der Bauhof, Wilhelm-Maybach-Straße 3, 23617 Stockelsdorf

In allen Gebäuden befinden sich Büroräume, in den eine automatisierte Datenverarbeitung personenbezogener Daten stattfindet.

Alle Räume sind verschließbar. Durch die allgemeine Geschäftsanweisung ist sichergestellt, dass Türen und Fenster nach Dienstschluss verschlossen zu halten sind. Die Räume im Erdgeschoss des Rathauses werden durch einen Alarmanlage überwacht.

2.3.2 Serverraum

Der Serverraum befindet sich im Erdgeschoss des Rathauses. Das Fenster des Serverraums ist durch ein zusätzliches Gitter gesichert. Der Serverraum verfügt über eine vom Rest des Hauses unabhängige Alarmanlage mit direkter Benachrichtigung eines Wach-Unternehmens.

Der Serverraum ist mit einer Klimaanlage und für den IT-Bereich zugelassenen Feuerlöschern ausgestattet. Ferner ist der Serverraum mit einem Funkbrandmelder ausgestattet. Dieser ist mit einem zweiten Brandmelder im zweiten Stock des Rathauses verbunden.

Zutritt zum Serverraum haben nur der behördliche Datenschutzbeauftragte, der Systemadministrator, der Leiter des Hauptamtes und die Bürgermeisterin.

2.3.3 Netzwerk

Das Netzwerk der Gemeindeverwaltung ist als strukturierte Verkabelung ausgeführt. Sämtlichen aktiven Netzwerkgeräte (Switches und Router) sind im Serverraum untergebracht.

Zugang zum Netzwerk ist grundsätzlich nur in den Büroräumen möglich, nicht im für den Publikumsverkehr zugänglichen Bereich. Eine Ausnahme bilden einzelne Peripheriegeräte (vgl. 2.3.7). Nicht benötigte Anschlüsse in den Büroräumen sind nicht beschaltet.

Die Kämmerei ist über eine Glasfaserleitung im Eigentum der Gemeindeverwaltung direkt an das verwaltungsinterne Netz angebunden.

Der Bauhof ist über eine VPN-Verbindung mit dem Rathaus verbunden.

2.3.4 Rechnersysteme allgemein

Sämtliche Systeme werden in einem zentralen Verzeichnisdienst (Active Directory von Microsoft) verwaltet. Ausnahmen bilden lediglich eigenständige, vernetzte Peripheriesysteme wie Netzwerkdrucker 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 Gemeindeverwaltung betreibt hierzu einen WSUS-Server (Windows Server Update Services der Firma Microsoft), der jedes Rechnersystem mindestens wöchentlich mit Sicherheitsaktualisierungen versieht.

Zur Durchführung von Funktionstests und für die Vorbereitung der Test und Freigabe gemäß § 7 DSVO verfügt die Gemeindeverwaltung über vom übrigen Verwaltungsnetz isolierte Testsysteme.

2.3.5 Server

Sämtliche Server befinden sich im Serverraum der Gemeindeverwaltung. Jeder 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 den Servern. Die Daten jedes Servers werden auf Bandlaufwerke in mehreren Generationen gesichert. Die verwendeten Sicherungsbänder werden in einem feuersicheren Tresor aufbewahrt. Lediglich die Administration hat Zugriff auf die Datensicherungsbänder. Für jedes System sind ein Sicherungsplan und eine Anleitung zur Wiederherstellung in der jeweiligen Systemakte hinterlegt.

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

der für die Mitarbeiter zur Verfügung stehenden Datenablage ist fachamtsbezogen eingeschränkt.

2.3.6 Client

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 über Mechanismen zur automatisierten Softwareverteilung (Installation von Programmen über MSI-Pakete via Gruppenrichtlinien) 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.

Bei mobilen Geräten werden die Datenträger, die zur Verarbeitung personenbezogener Daten genutzt werden, komplett verschlüsselt. Die hierfür verwendeten Passworte werden von der Systemadministration erzeugt und in der Systemakte hinterlegt.

2.3.7 Peripherie

Die Gemeindeverwaltung setzt für Druckaufträge mit größerem Volumen oder spezieller Nachbearbeitung – Heften, Lochen, Falzen – vernetzte Großgeräte ein, die zusätzlich die Funktion eines Kopierers übernehmen.

Es werden nur Geräte eingesetzt, die eine gerätebezogene Verschlüsselung der auf der lokalen Festplatte vorhandenen Daten ermöglichen. Alternativ verbleibt die Festplatte im Eigentum der Gemeindeverwaltung Stockelsdorf. Die Geräte werden in Räumen aufgestellt, die nicht für den Publikumsverkehr direkt zugänglich sind oder verfügen über eine Sperre des Bedienfeldes. Die Geräte bieten die Möglichkeit, für Druckaufträge mit personenbezogenen Daten eine verzögerte Ausgabe nach Eingabe eines PIN-Codes durchzuführen.

2.4 Internetanschluss

2.4.1 Zugang

Jeglicher Datenverkehr des verwaltungsinternen Netzes mit externen Netzwerken wird explizit an den Netzübergängen freigeschaltet. 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 Gemeindeverwaltung setzt hierfür eine Kombination aus einem Paketfilter, der einzelne Verbindungen in das Internet von Systemen der Gemeindeverwaltung freischaltet, und einem Proxyserver ein, der die übertragenen Daten auf schadhafte Inhalte kontrolliert.

2.4.2 Paketfilter

Als zentraler Übergabepunkt ist ein Paketfilter auf Linux-Basis installiert.

Der Paketfilter lässt ausschließlich vom Proxyserver initiierte Verbindungen auf Dienste im Internet zu und zwar ausschließlich:

- Domain Name Service (dns) zur Namensauflösung von Rechnern im Internet,
- Hypertext Transfer Protocol (http) und dessen verschlüsselte Variante (https) zur dienstlichen Informationsrecherche im Internet,
- File Transfer Protocol (ftp) zur Dateiübertragung aus dem Internet

Aus dem verwaltungsinternen Netz ist auf Netzwerkebene grundsätzlich kein direkter Zugriff auf das Internet möglich. Eine Ausnahme stellt hier der Zugriff auf das Verfahren Elster dar.

Der Paketfilter wird durch einen externen Dienstleister über eine dedizierte ISDN-Einwahl ferngewartet. Die Einwahl ist erst nach dem Einstecken des ISDN-Kabels durch den Systemadministrator möglich. Nach Beendigung der Fernwartung wird das Kabel wieder abgezogen.

Der Paketfilter ruft die an die Gemeindeverwaltung adressierten E-Mails über POP3 von einem Dienstleister ab und leitet sie an den Proxyserver weiter. Er nimmt E-Mails des Proxyservers entgegen und leitet diese an den Dienstleister weiter.

2.4.3 Proxyserver für E-Mail und WWW

Der Paketfilter leitet E-Mails an den Proxyserver für E-Mail weiter. Auf dem Proxyserver werden die E-Mails auf schadhafte Inhalte und unerwünschte Mail geprüft.

Der http-Verkehr wird durch den Proxyserver auf schadhafte Inhalte überprüft. Zusätzlich prüft der Proxyserver gegen eine Negativliste von Internetangeboten, die dem Verbot der

privaten Nutzung widersprechen.

2.5 Landesnetzanschluss

Die Gemeindeverwaltung ist an das Landesnetz Schleswig-Holstein angeschlossen. Sämtliche verfügbaren Sicherheitsmaßnahmen werden umgesetzt. Hierzu zählen die Prüfung des Berichtswesens, der Zugang zum webbasierten Auskunftssystem LNWebView und die Nutzung des Überwachungsprogramms „LNRC – Landesnetz Router Control“.

3 Datenschutzrechtliche Bewertung

3.1 Rechtsvorschriften

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 Datenschutz-Management 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

Datenschutzverordnung (DSVO)

- § 3 Verfahrensdokumentation
- § 4 Verfahrenszweck
- § 5 Verfahrensbeschreibung
- § 6 Sicherheitskonzept
- § 7 Test und Freigabe
- § 8 Verfahrensübergreifende Dokumentation und Protokolle

Die folgenden Bedingungen müssen somit den Datenschutzzielen der Gemeindeverwaltung folgend eingehalten werden:

- Es sind die Vorschriften über Berufs- und besondere Amtsgeheimnisse unter Berück-

sichtigung der bereichsspezifischen Gesetze zu beachten (z.B. § 30 AO, § 35 SGB I, § 38 LMG, § 203 StGB).

- Die Daten verarbeitende Stelle hat den Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten (§ 4 Abs. 1 LDSG).
- Unbefugten ist der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren (§ 5 Abs. 1 Nr. 1 LDSG).
- Es ist zu verhindern, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können (§ 5 Abs. 1 Nr. 2 LDSG).
- Die sicherheitstechnischen Anforderungen an die automatisierte Datenverarbeitung sind in einem Sicherheitskonzept festzulegen und umzusetzen (§ 5 Abs. 3 LDSG i.V.m. § 6 DSVO).
- Die Verarbeitung personenbezogener Daten wird erst ermöglicht, nachdem systemseitig die Berechtigung der Benutzer festgestellt worden ist (§ 6 Abs. 1 LDSG).
- Die Befugnisse zur Systemadministration sind eindeutig festgelegt (§ 6 Abs. 2 LDSG i.V.m. § 8 Abs. 4 u. 5 DSVO).
- Die Arbeiten der Systemadministratoren werden protokolliert und kontrolliert (§ 6 Abs. 2 LDSG).
- Die Hardware und die Software sind in einem Geräte- bzw. Softwareverzeichnis erfasst (§ 8 Abs. 1 u. 2 DSVO).
- Es ist zu dokumentieren, welchen Personen welche Zugriffsbefugnisse auf Datenbestände gewährt wurden (§ 8 Abs. 4 DSVO).
- Automatisierte Verfahren sind vor ihrem erstmaligen Einsatz und nach Änderungen zu testen und durch die Bürgermeisterin oder dem Bürgermeister als Daten verarbeitenden Stelle oder von ihr / ihm befugte(n) Person(en) freizugeben (§ 5 Abs. 2 LDSG i.V.m. § 7 DSVO).
- Die automatisierten Verfahren sind so zu dokumentieren, dass sie für sachkundige Personen in angemessener Zeit nachvollziehbar sind und als Grundlage für die Überwachung der automatisierten Datenverarbeitung herangezogen werden können (§ 6 Abs. 5 i.V.m. § 3 DSVO).
- Die ordnungsgemäße Anwendung der Datenverarbeitung ist zu überwachen (§ 6 Abs. 5 LDSG).

3.2 Zusammenfassende Bewertung

Die Überprüfung hat ergeben, dass die im Sicherheitskonzept festgeschriebenen Maßnahmen angemessen sind und vollständig umgesetzt werden.

Die durch dieses Audit erfassten Verarbeitungsprozesse zeichnen sich insbesondere durch folgende „datenschutzfreundliche“ Aspekte aus:

- Die Gemeindeverwaltung hat eine gut strukturierte, systematische und übersichtliche Dokumentation gemäß DSVO erstellt. Diese bietet eine effektive Arbeitsgrundlage für das behördliche Datenschutzmanagementsystem.
- Die Sicherheitsmechanismen zur zentralen Vergabe von Berechtigungen und der Steuerung der Arbeitsplatzrechner über das Active Directory werden intensiv genutzt.
- Sämtlicher Datenverkehr mit dem Internet wird sowohl auf Inhalts- als auch auf Netzwerkebene kontrolliert. Die dabei anfallenden Protokolldaten werden nach einem geregelten Verfahren unter Beteiligung des behördlichen Datenschutzbeauftragten ausgewertet.

Des Weiteren ist positiv hervorzuheben ist, dass der Administrator bei der Datenschutzakademie das Datenschutzzertifikat für Systemadministratoren erworben hat und der behördliche Datenschutzbeauftragte diese Prüfung Ende des Jahres 2007 ablegen wird.

Die Prüfung hat ergeben, dass Konzepte und Anwendung des Datenschutz-Managementsystems keinen Anlass zu datenschutzrechtlichen Beanstandungen geben.

Kiel, 28.09.2007 (Angelika Martin)