Kurzgutachten

über das Auditverfahren gemäß § 43 Abs. 2 LDSG

Verarbeitung personenbezogener Daten mit IT-Systemen in der Gemeindeverwaltung Timmendorfer Strand

Kiel, 15. November 2004

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits

Das Unabhängige Landeszentrum für Datenschutz (ULD) und die Gemeinde Timmendorfer Strand haben am 24.05.2004 eine Vereinbarung getroffen, aufgrund der ein **Behördenaudit** bezogen auf das Projekt

- „**Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung der Gemeinde Timmendorfer Strand ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter“** und

- **„Anschluss des internen Netzes der Gemeindeverwaltung an das Internet“**

durchgeführt werden sollte.

Als **Datenschutzziele** wurden von der Leitungsebene der Gemeindeverwaltung

- die technische und organisatorische Umsetzung von Sicherheitsmaßnahmen für die interne automatisierte Datenverarbeitung und für den Anschluss des internen Netzes an das Internet,

- der ausreichende Schutz der automatisiert verarbeiteten Daten vor Angriffen aus dem Internet sowie

- ein hinreichend sicherer Transport der über die Internetdienste „E-Mail“ und „WWW“ versendeten bzw. empfangenen Daten

festgelegt.

Die **Realisierung** der Sicherheitsmaßnahmen umfasste folgende Teilaspekte:

a) Beachtung von Rechtsvorschriften, Richtlinien und sonstigen Arbeitsanweisungen zur Datensicherheit und zur Ordnungsmäßigkeit der Datenverarbeitung,

b) Festlegung der entsprechenden Zuständigkeiten und Verantwortungsabgrenzungen,

c) Ausgestaltung der technischen und organisatorischen Maßnahmen zur Datensicherheit der IT-Systeme,

d) Festlegung der technischen und organisatorischen Maßnahmen bei der Nutzung der Internetdienste,

e) Definition der Maßnahmen zur Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme,

f) Gewährleistung der Vollständigkeit der Dokumentation der Programme und Verfahren.

Mit der Umsetzung der festgelegten Ziele wurde die **IT-Koordination** der Gemeindeverwaltung betraut.

2 Feststellungen zu den sicherheitstechnischen Elementen des Datenschutz-Managementsystems

2.1 Zuständigkeiten und Verantwortlichkeiten

Die **Gesamtverantwortung** für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung trägt der Bürgermeister als Leiter der Daten verarbeitenden Stelle. Für die Einhaltung der **Vorschriften** zum Datenschutz und zur Datensicherheit in den **Fachämtern** sind die Amtsleiter zuständig und verantwortlich.

Die **Überwachung** und **Prüfung** der in den Sicherheitskonzepten festgelegten Sicherheitsmaßnahmen obliegt dem Hauptamtsleiter in Zusammenwirken mit den Fachamtsleitern.

Die Schaffung der Voraussetzungen für den Einsatz und die Überwachung des laufenden Betriebs der IT-Systeme obliegt dem IT-Koordinator und seiner Vertreterin (IT-Koordination). Die durchzuführenden Arbeiten dieser Mitarbeiter werden prinzipiell als **Dienstleistungen** für die **Fachämter** angesehen.

2.2 Datenschutzkonzept

Als Grundlage für die Festlegung der Sicherheitsmaßnahmen wurde zunächst ein **IT-Konzept** erstellt. Zusätzlich wurden in einzelnen Fachbereichen weitere Erhebungen über **Arbeitsabläufe** sowie über **den Hard- und Softwarebestand** vorgenommen.
Auf dieser Basis wurden die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen in einem umfassenden **Datenschutzkonzept** festgelegt. Es gliedert sich in die Bereiche

- Grundlagen und Aufbau,
- allgemeine Datenverarbeitung,
- automatisierte Datenverarbeitung und
- Internetdienste.

Die festgelegten Sicherheitsmaßnahmen gelten als **Mindestanforderungen** für alle Fachämter. Das Datenschutzkonzept wurde der Leitungsebene (Bürgermeister, Amtsleiter) vorgelegt und mit ihr im Rahmen einer Präsentation erörtert.

2.3 Automatisierte Datenverarbeitung

In der Gemeindeverwaltung werden in **allen** Fachbereichen PC eingesetzt, die über das interne Netzwerk mit zentralen Servern verbunden sind. Der Einsatz und der Betrieb der IT-Systeme wird von der **IT-Koordination** sichergestellt. Von ihr wurden für eine sichere und ordnungsgemäße Datenverarbeitung u.a. folgende **Anforderungen** an das Sicherheitsniveau gestellt:

- Gewährleistung einer Datenabschottung durch eine nachvollziehbare Benutzer- und Rechteverwaltung,
- Reduzierung der Funktionalitäten der Arbeitsplatz-PC auf das erforderliche Maß,

- strukturierte zentrale Datenverwaltung,
- sachgerechte Dokumentation aller Einstellungen an Hard- und Software,
- Aufbau einer qualifizierten IT-Koordination,
- Kontrolle und Überwachung durch den Leiter des Hauptamtes.

Die **Konkretisierung** des Sicherheitsniveaus wurde durch die Festlegung einzelner Sicherheitsmaßnahmen im Datenschutzkonzept vorgenommen. So wurden Sicherheitsmaßnahmen z.B. für

- die Arbeitsplatzebene,
- die zentralen Komponenten bzw. der Server,
- das Netzwerk bzw. die Verkabelung,
- die externen Dienstleister,
- die Datenverwaltung,
- die Datensicherung,
- die Fachverfahren sowie
- für die Benutzer- und Rechteverwaltung

festgelegt.

Weiterhin wurde für die IT-Koordination eine **Dienstanweisung** für den Umgang mit den Datenverarbeitungssystemen erstellt. Folgende Inhalte sind von datenschutzrechtlicher Bedeutung:

- Administrative Aktivitäten werden in einer Systemakte protokolliert.
- Für die Installation bzw. Löschung von Software ist die Genehmigung des Hauptamtsleiters einzuholen.

- Die Berechtigung zum Systemzugang hat nur die IT-Koordination.

- Externe Dienstleister erhalten nur im Beisein der IT-Koordination Systemzugang.

- Programme und Verfahren sind entsprechend der Datenschutzverordnung zu dokumentieren.

- Für jedes Verfahren mit personenbezogenen Daten ist eine Verfahrensakte anzulegen.

- Den einzelnen Benutzern sind nur diejenigen Befugnisse zuzuweisen, die für die jeweilige Aufgabenstellung erforderlich sind.

- Fernwartung durch externe Dienstleister wird nur im Einzelfall und auf Veranlassung der IT-Koordination durchgeführt. Dabei werden die Aktivitäten abgestimmt und nachvollziehbar aufbereitet.

- Für die IT-Koordination ist jährlich ein Ausbildungsplan aufzustellen.

Auf den **Arbeitsplatz-PC** und den **Servern** wurden u.a. folgende sicherheitstechnische Maßnahmen ergriffen:

- Deaktivierung der Disketten- und CD-ROM-Laufwerke sowie des USB-Ports mit der Sicherheitssoftware Devicelock.

- Deaktivierung der auf den Arbeitsplatz-PC befindlichen Systemfunktionen über den Einsatz der Gruppenrichtlinien.

- Einrichtung und Abschottung einer nach dem Geschäftsverteilungsplan angelehnten Datenablage für Word- und Exceldateien.

- Ein nach Ämtern strukturiert eingerichtetes Active Directory für die Benutzer- und Gruppenverwaltung.

- Zentrale Verwaltung aller Fachanwendungen und die mit ihnen verarbeiteten Daten auf den Servern.

Die IT-Koordination verfügt darüber hinaus über eine **Testumgebung (Server und Clients)**, in der die umzusetzenden sicherheitstechnischen Maßnahmen zunächst getestet werden können. Des Weiteren nutzt die IT-Koordination die Testumgebung für die Vertiefung ihres sicherheitstechnischen Know-hows.

2.4 Internetkommunikation

Die Einführung neuer Informations- und Kommunikationstechnologien in der Gemeindeverwaltung zielt neben einer Verbesserung des **Bürgerservices** auch auf **Effizienzsteigerungen** durch verbesserte Informationsflüsse ab. Vor diesem Hintergrund kommt zunächst die Nutzung nachstehender Internetdienste in Betracht:

- WWW (Informationsabfrage)
- E-Mail (Nachrichtenaustausch)

2.4.1 Sicherheitskonzept für den Internetanschluss

Von besonderer Bedeutung sind folgende Gegebenheiten:

- Die **Verfügungsgewalt** (Überwachung und Administration) über die eingesetzten Firewall-Komponenten liegt bei der Gemeindeverwaltung.
- Es soll sichergestellt werden, dass **Angriffe auf der physikalischen** Ebene erkannt und abgewehrt werden.
- Eine **Fernadministration** der Firewall-Komponenten ist nicht gestattet.
- Ausgehende E-Mails dürfen **keine** personenbezogenen Daten enthalten.
- **Kopien** ein- und ausgehender E-Mails werden für **Kontrollzwecke** in einem gesonderten Archiv gespeichert.

- Es werden nur die E-Mails an den Arbeitsplatz geleitet, die **virenüberprüft** sind und zugelassene **Attachements** (z.B. TXT, RTF) enthalten.

- Der Zugriff auf die Web-Seiten wird in Bezug auf die sicherheitskritischen Komponenten **Aktive-X, Java und VBScript** gefiltert.

- Web-Seiten werden nach **Text-Zensur-Skripten** geprüft und ggf. für den Aufruf nicht zugelassen.

- Das **„Herunterladen“** ausführbarer Programme und Dateien auf die Arbeitsplatzrechner ist nicht zugelassen.

- Alle Einstellungen auf den Internet-Komponenten werden **nachvollziehbar** dokumentiert.

2.4.2 Überwachung des Internetanschlusses

Für die dauerhafte Gewährleistung der **Einhaltung des Sicherheitsniveaus** sollen die **Internetaktivitäten** in Bezug auf **unerlaubte Aktionen** überwacht werden. Es soll insbesondere sichergestellt werden, dass Angriffe auf das interne Netz der Gemeindeverwaltung **erkannt** und **abgewehrt** werden können. Folgende Sicherheitsmaßnahmen wurden diesbezüglich ergriffen:

- Das **Systemprotokoll der Firewall** protokolliert alle nicht erlaubten Aktivitäten. Es wird täglich von der IT-Koordination ausgewertet.

- Die **ordnungsgemäße Nutzung der Internetdienste** wird in regelmäßigen Abständen von der IT-Koordination nach Auftrag durch den Hauptamtsleiter überwacht.

2.4.3 Dienstanweisung zur Nutzung der Internet-Dienste

In der Dienstanweisung zur Nutzung der Internet-Dienste werden die im Sicherheitskonzept für den Internetanschluss festgelegten Sicherheitsmaß-

nahmen in konkrete **Handlungsanweisungen** für die Mitarbeiter der Gemeindeverwaltung umgesetzt. In ihr werden insbesondere

- die Verantwortlichkeiten für den Betrieb der Internetkomponenten und die Umsetzung der Dienstanweisung,
- die Nutzungsbedingungen für die Internetdienste,
- Regelungen über den Datenschutz und die Datensicherheit,
- der Protokollierungsumfang bei der Nutzung der Internetdienste sowie
- disziplinarische Maßnahmen bei Nichteinhaltung der Anweisungen

beschrieben.

2.5 Landesnetzanschluss

Die Gemeindeverwaltung ist mit ihrem internen Netz an das **Landesnetz** angeschlossen. Sie hat vor dem Übergaberouter eine **Firewall** platziert. Unberechtigte Zugriffe aus dem Landesnetz in das interne Verwaltungsnetz werden somit über entsprechende **Firewallregeln** unterbunden.

2.6 Datenschutz-Management im laufenden Betrieb

Zum Zeitpunkt der Begutachtung lag das Datenschutz-Management bei der IT-Koordination.

Von ihr wurden u.a. folgende Aufgaben durchgeführt:

- Umsetzung und Dokumentation der Datenschutzziele,
- Schulung der Mitarbeiter der Gemeindeverwaltung in Bezug auf den Datenschutz und die Datensicherheit,
- Überwachung der Einhaltung und Umsetzung der im Datenschutzkon-

zept festgelegten Sicherheitsmaßnahmen.

Mit Abschluss des Behördenaudits geht das Datenschutz-Management auf den **Hauptamtsleiter** über. In Zusammenarbeit mit der IT-Koordination **überwacht** er in regelmäßigen Abständen die Verfahrensabläufe in Bezug auf die Einhaltung gesetzlicher Vorschriften. Änderungen an Verfahren werden ihm von der IT-Koordination unverzüglich mitgeteilt, so dass er ggf. rechtzeitig das Unabhängige Landeszentrum für Datenschutz zum Zweck der Durchführung einer Nachprüfung informieren kann.

Mittelfristig wird beabsichtigt, einen **behördlichen Datenschutzbeauftragten** zu bestellen, der dann auch die Aufgaben des Datenschutz-Managements übernimmt.

3 Datenschutzrechtliche Bewertung

Folgende Rechtsvorschriften wurden für die datenschutzrechtliche Bewertung herangezogen:

- **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 u. Protokolle

Die Überprüfung hat ergeben, dass die während der Bestandsaufnahme festgestellten Defizite im Rahmen des Audits systematisch beseitigt wurden.

In sicherheitstechnischer Hinsicht sind nach Abschluss des Audits also **keine Schwachstellen** erkennbar, die die Rechte der betroffenen Bürger und der Mitarbeiter der Gemeindeverwaltung beeinträchtigen könnten.

Das modular aufgebaute Datenschutzkonzept repräsentiert ein **qualitativ hohes Niveau**. Es bildet die Grundlage für ein wirksames Datenschutzmanagement im laufenden Betrieb der automatisierten Verfahren.

Die durch das Audit **„Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung und Anschluss des internen Verwaltungsnetzes an das Internet“** erfassten Verarbeitungsprozesse zeichnen sich insbesondere durch folgende „datenschutzfreundliche“ Aspekte aus:

1. Die auf den Arbeitsplatz-PC enthaltenen Funktionen sind durch den Einsatz der Gruppenrichtlinien auf ein Mindestmaß reduziert.

2. Die Disketten- und CD-ROM-Laufwerke sowie der USB-Port werden über eine Sicherheitssoftware zentral reglementiert.

3. Alle Fachanwendungen und die mit ihnen verarbeiteten Daten werden strukturiert zentral auf den Servern verwaltet.

4. Für den Internet-Anschluss wird ein Firewallsystem eingesetzt, das u.a. eingehende Verbindungen blockiert.

5. Die IT-Systeme und die auf ihnen eingesetzten Fachverfahren sind vorbildlich dokumentiert.

6. Die IT-Koordination verfügt für Test- und Weiterbildungszwecke über eine Testumgebung bestehend aus 3 vernetzten IT-Systemen.

Die Verleihung des Auditzeichens nach § 42 Abs. 3 LDSG ist damit gerechtfertigt.