Kurzgutachten

über das Auditverfahren gemäß § 43 Abs. 2 LDSG

Verarbeitung personenbezogener Daten mit IT-Systemen in der Gemeindeverwaltung Ratekau

Kiel, 1. Dezember 2006

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits

Das Unabhängige Landeszentrum für Datenschutz (ULD) und die Gemeinde Ratekau haben am 10.04.2006 eine Vereinbarung getroffen, aufgrund der ein **Behördenaudit** bezogen auf das Projekt

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

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

durchgeführt werden soll.

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 von Daten der über die Internetdienste „E-Mail“ und „WWW“

festgelegt.

Die **Realisierung** der Sicherheitsmaßnahmen umfasste daher 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 eingesetzten Programme und Verfahren.

Mit der Umsetzung der festgelegten Ziele wurden der **IT-Koordinator** und die **behördliche Datenschutzbeauftragte** der Gemeindeverwaltung betraut.

2 Feststellungen zu den sicherheitstechnischen Elementen des Datenschutz-Managementsystems

2.1 Zuständigkeiten und Verantwortlichkeiten

Die **Verantwortung** 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 jeweiligen Amtsleiter zuständig und verantwortlich.

Die **Überwachung** und **Prüfung** der im Sicherheitskonzept festgelegten Sicherheitsmaßnahmen obliegt dem Hauptamtsleiter in Zusammenwirken mit den Fachamtsleitern und der nach § 10 LDSG bestellten **behördlichen Datenschutzbeauftragten**.

Die Schaffung der Voraussetzungen für den Einsatz und die Überwachung des laufenden Betriebs der IT-Systeme obliegt dem **IT-Koordinator** und seinem **Vertreter** (IT-Koordination). Der IT-Koordinator hat sich bei der Datenschutzakademie im Bereich der technischen Datensicherheit

besonders qualifiziert. Ihm wurde von der Datenschutzakademie das **Datenschutzzertifikat für Systemadministratoren** verliehen.

2.2 Sicherheitskonzept

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

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

Die festgelegten Sicherheitsmaßnahmen gelten als **Mindestanforderungen** für alle Fachämter.

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 werden von dem **IT-Koordinator** sichergestellt. Für eine sichere und ordnungsgemäße Datenverarbeitung wurden von der behördlichen Datenschutzbeauftragten in Zusammenarbeit mit dem Leiter des Hauptamtes folgende **Anforderungen** 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 Sicherheitskonzept 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:

- Die Berechtigung zum Systemzugang hat nur die IT-Koordination.
- Administrative Aktivitäten werden in einer Systemakte protokolliert.
- Für die Installation bzw. Löschung von Software ist die Genehmigung

des Hauptamtsleiters einzuholen.

- 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 an den Geschäftsverteilungsplan angelehnten Datenablage für Word- und Exceldateien.

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

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

Der IT-Koordinator 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

Für die Internetkommunikation wurden entsprechende Sicherheitsmaßnahmen in dem **Sicherheitskonzept** für den Internetanschluss festgelegt. Sie gliedern sich in die Bereiche

- allgemeine Sicherheitsmaßnahmen,
- Sicherheitsmaßnahmen auf der physikalischen Ebene sowie
- Internetdienst bezogene Sicherheitsmaßnahmen.

Von besonderer Bedeutung sind folgende Vorkehrungen:

- Eine unmittelbare Verbindung des internen Netzes der Gemeinde mit dem Internet besteht nicht. Das interne Netz der Gemeinde ist an das **Landesnetz** angeschlossen, so dass die Nutzung der Internetdienste über den **Firewall** von Dataport realisiert wird. Unerlaubte Zugriffe aus dem Internet werden auf der Netzebene bereits an der Firewall von Dataport erkannt und abgewehrt.

- Die **Fernadministration** der Schnittstelle (Übergaberouter) zwischen internem Netz der Gemeinde und dem Landesnetz bzw. dem Internet wird über ein auf dem Administrator-PC der Gemeinde installiertes **Revisionstool** erkannt. Die **Konfiguration** des Übergaberouters lässt sich für **Kontrollzwecke** ebenfalls über das Tool auslesen.

- Ausgehende nicht verschlüsselte E-Mails dürfen **keine** vorgangspersonenbezogenen Daten enthalten. E-Mails mit **vorgangspersonenbezogene Daten** können über einen PC im Bürgerbüro **verschlüsselt** versendet werden.

- **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.

- Beim Zugriff auf die Web-Seiten werden 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.

In der Dienstanweisung zur Nutzung der Internetdienste werden die im Sicherheitskonzept für den Internetanschluss festgelegten Sicherheitsmaßnahmen 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. Für den Anschluss ist von der Firma T-Systems Enterprise Service GmbH ein Zugangsrouter und von dem Dienstleister Dataport des Finanzministerium als Betreiber des Landesnetzes ein Übergaberouter installiert worden. In einem **Nutzervertrag** werden die Rechte und Pflichten der Gemeindeverwaltung und dem Finanzministerium bzw. dem von ihr beauftragten Dienstleister Dataport sowie die für das Landesnetz ergriffenen Sicherheitsmaßnahmen beschrieben.

Für die **Überwachung** des Anschlusses ist ein bei Dataport installiertes **Berichtswesen** eingerichtet, das die Gemeindeverwaltung über die Konfiguration des Übergaberouters sowie über jede darauf ausgeführte Veränderungen umfassend informiert. Darüber hinaus wurde der Gemeinde ein **Revisionstool** zur Verfügung gestellt, mit dem die Einstellungen des Übergaberouters jederzeit ausgelesen werden können. Sobald Dataport an der Konfiguration des Übergaberouters (mit oder ohne Kenntnis) der Gemeinde **Veränderungen** durchführt, wird der Administrator über das Revisionstool automatisiert über den Zugriff auf den Übergaberouter informiert, so dass von ihm eine **Überprüfung** der administrativen Aktivitäten erfolgen kann.

2.6 Dokumentation der automatisierten Datenverarbeitung

Es lagen als **Dokumentation** folgende Unterlagen vor:

- IT-Konzept,
- Sicherheitskonzept,
- Dienstanweisung für Administratoren,
- Dienstanweisung für Benutzer für den Umgang mit Datenverarbeitungssystemen,

- Dienstanweisung für die Nutzung der Internetdienste,
- Systemdokumentation des Landesnetzesanschlusses,
- Sicherheitseinstellungen für die Nutzung von Web und E-Mail,
- Systemakten für die im Einsatz befindlichen Server,
- Verfahrensakten der eingesetzten Fachverfahren.

Die Dokumentation entspricht den Anforderungen der **Datenschutzverordnung**.

2.7 Datenschutz-Management im laufenden Betrieb

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

Von ihr wurden u.a. folgende Aufgaben durchgeführt:

- Umsetzung und Dokumentation der Datenschutzziele,
- Schulung der Mitarbeiter der Gemeindeverwaltung über Anforderungen und Maßnahmen des Datenschutzes und der Datensicherheit,
- Überwachung der Einhaltung und Umsetzung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen.

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

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 und Protokolle

Die Überprüfung hat ergeben, dass die im **Sicherheitskonzept** festgeschriebenen Maßnahmen vollständig umgesetzt worden sind.

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 die Absicherung des Internet-Anschlusses werden Sicherheitskomponenten (Revisionstool, Web- und Mail-Marshal) eingesetzt, die unerwünschte Zugriffe abwehren.

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

6. Die IT-Koordination verfügt für Test- und Weiterbildungszwecke über eine Testumgebung.

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