Kiel, 19. Dezember 2006

Kurzgutachten

über das Auditverfahren gemäß § 43 Abs. 2 LDSG

Verarbeitung personenbezogener Daten mit IT-Systemen in der Stadtverwaltung Pinneberg

Inhaltsverzeichnis

1 Gegenstand des Datenschutz-Behördenaudits

Gegenstand des Datenschutz-Audits

sind

(1) die Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung der Stadtverwaltung Pinneberg, ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter

und

(2) die Anbindung des internen Netzes der Stadtverwaltung an das Internet.

Als **Datenschutzziele** wurden von der Leitungsebene der Stadtverwaltung

- die Gewährleistung der Recht– und Ordnungsmäßigkeit des IT-Einsatzes,
- das Sicherstellen der Verfügbarkeit der Systeme,
- das Sicherstellen der Integrität der Software und der Daten,
- das Sicherstellen der Vertraulichkeit von Daten,
- die technische und organisatorische Umsetzung von Sicherheitsmaßnahmen für die interne, automatisierte Datenverarbeitung,
- die sichere Verbindung des Verwaltungsnetzes mit anderen Netzen, Schutz vor Angriffen aus anderen Netzen und
- der sichere Transport der über die Internetdienste E-Mail und WWW versendeten bzw. empfangenen Daten

festgelegt.

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

- Beachtung von Rechtsvorschriften, Richtlinien, Dienst- und Arbeitsvereinbarungen,
- Festlegung der entsprechenden Zuständigkeiten und Verantwortungsabgrenzungen,
- Ausgestaltung der technischen und organisatorischen Maßnahmen zur Datensicherung der IT-Systeme,
- Festlegung der technischen und organisatorischen Maßnahmen bei der Nutzung der Internetdienste,

- Definition der Maßnahmen zur Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme,
- Gewährleistung der Vollständigkeit der Dokumentation der eingesetzten Programme und Verfahren.

Mit der Umsetzung der festgelegten Ziele wurden der Leiter des IT-Bereichs und der behördliche Datenschutzbeauftragte betraut.

2. Feststellungen zu den sicherheitstechnischen Elementen des Datenschutz-Managementsystems

2.1 Zuständigkeiten und Verantwortlichkeiten

Die Verantwortung für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung liegt beim Bürgermeister als Leiter der Daten verarbeitenden Stelle. Für die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit in den Fachbereichen sind die jeweiligen Bereichsleiter zuständig und verantwortlich.

Die Überwachung und Prüfung der im Sicherheitskonzept festgelegten Sicherheitsmaßnahmen obliegt den Fachbereichsleitern und dem nach § 10 LDSG bestellten behördlichen Datenschutzbeauftragten.

Die Schaffung von Voraussetzungen für den Einsatz und die Überwachung des laufenden Betriebs der IT-Systeme obliegt dem Leiter des IT-Bereichs und seinem Vertreter.

Für jedes Verfahren zur Verarbeitung personenbezogener Daten ist ein Verfahrensverantwortlicher benannt. Die Pflichten eines Verfahrensverantwortlichen sind im IT-Konzept festgelegt.

2.2 Sicherheitskonzept

Das IT-Konzept erfasst die grundsätzliche Basis-IT-Architektur der Stadt sowie die organisatorischen und technischen Vorgaben für die Nutzung sämtlicher Informations- und Kommunikationstechnologie innerhalb der Stadtverwaltung Pinneberg. Es enthält außerdem konzeptionelle Vorgaben für die weitere Entwicklung sämtlicher Informations- und Kommunikationstechnik.

Das auf dem IT-Konzept aufsetzende Sicherheitskonzept stellt umfassend die beim Einsatz von Informations- und Kommunikationstechnologie getroffenen Sicherheitsmaßnahmen dar. Zu jeder Maßnahme werden das Ziel, etwaige aktuell vorhandene Mängel bei der Umsetzung der Maßnahme, notwendige Maßnahmen zur Zielerreichung und die jeweilige Zuständigkeit für die Maßnahme tabellarisch erfasst. Es dokumentiert somit nicht nur die zu treffenden Sicherheitsmaßnahmen, sondern gleichzeitig auch den Umsetzungsstand der Sicherheitsmaßnahmen und zeigt gegebenenfalls Handlungsbedarf auf. Das Sicherheitskonzept wird stetig fortgeschrieben. Das Sicherheitskonzept wird darüber hinaus alle zwei Jahre auf Vollständigkeit und Korrektheit überprüft.

2.3 Automatisierte Datenverarbeitung

Die Stadt Pinneberg betreibt eine Client-Server-Infrastruktur. Auf sämtlichen Serversystemen ist den Vorgaben des IT-Konzepts folgend Windows 2003 SP1 installiert. Auf allen 183 vernetzten Clients ist Windows XP Service Pack 2 installiert.

Die Clients sind nach Stand der Technik abgesichert. So wird beispielsweise durch BIOS-Passworte der Zugriff auf elementare Systemeinstellungen verhindert. Durch den Einsatz zusätzlicher Software sind sämtliche externen Schnittstellen deaktiviert und werden nur in begründeten Ausnahmefällen freigeschaltet. Sämtliche Clients sind mit einem zentral verwalteten Viren-Schutz versehen. Die Nutzer können nicht administrativ eingreifen.

Eine interaktive Anmeldung auf den derzeit 10 Serversystemen ist nur der Gruppe der Administratoren – dem Leiter des IT-Bereichs und seinem Stellvertreter – gestattet. Die IT-Abteilung nutzt die vorhandenen Mittel der Betriebssysteme zur automatisierten Protokollierung der administrativen Zugriffe auf die Systeme. Die Protokolle werden anlassbezogen gemäß des in der Dienstanweisung „IT-Administration“ vorgesehenen Verfahrens ausgewertet. Die IT-Abteilung ist bemüht, sämtliche Fachverfahren möglichst serverzentriert zu betreiben. Fachverfahren werden weitestmöglich in einer kontrollierten Ablaufumgebung auf Terminalservern bereitgestellt. Die Konzepte für den Einsatz dieser Systeme wurden geprüft und passen sich gut in die bestehende Sicherheitsarchitektur ein.

Anwendungen, die zum Datenabruf oder -austausch mit anderen Netzwerken genutzt werden, werden auf Servern in einem eigenen Netzwerksegment betrieben. Ein Großteil der IuK-Infrastruktur sowie die Regelung der Zugriffsrechte wird über einen Verzeichnisdienst, in diesem Falle das ActiveDirectory von Microsoft, zentral verwaltet.

Sämtliche Serversysteme sind in einem mustergültig aufgebauten und abgesicherten Serverraum aufgestellt. Der Zutritt zu diesem und anderen administrativen Räumen ist nur Mitarbeitern des IT-Bereichs möglich.

Vom zentralen Serverraum aus werden dezentrale Technikräume auf den Etagen des Haupthauses versorgt. Die Technikräume enthalten die Etagenverteilung im Sinne einer strukturierten Verkabelung.

Die externen Liegenschaften der Stadtverwaltung werden über VPN-Verbindungen oder Direktleitungen angebunden. Die Terminierung der VPN-Verbindungen erfolgt auf einem Firewallsystem.

2.4 Kommunikation mit anderen Netzwerken

Die Stadt Pinneberg betreibt ein durch den IT-Bereich administriertes und kontrolliertes Firewallsystem. Ein Zugang zu anderen Netzen ist nur über dieses Firewallsystem möglich.

Die IT-Abteilung hat einen zentralen Übergabepunkt in andere Netze aufgebaut. Sämtlicher Datenverkehr der das Verwaltungsnetz verlässt oder im Verwaltungsnetz mündet wird durch das zentrale Firewallsystem kontrolliert.

Die Stadt Pinneberg nutzt für den Zugang zum Internet Dienstleistungen von dataport (E-Mail und Web). dataport markiert unverlangt zugesandte Mails (Spam), unterdrückt diese jedoch nicht. Nutzer haben die Möglichkeit, durch eigene Filter eine eigene Vorgehensweise je nach Spam-Aufkommen zu entwickeln. Pinneberg filtert Mails mit schadhaften Inhalten oder nicht erlaubten Anhängen.

Für den Zugriff auf Informationen im WWW stellt die Stadt Pinneberg im Firewallsystem einen Proxy-Server bereit, der Anfragen aus dem Verwaltungsnetz über die bereits vom ULD zertifizierte Firewall dataports in das Internet weiterleitet. Sämtliche Anfragen werden auf dem Proxy-System auf schadhafte Inhalte (Viren, Würmer, Trojaner) gescannt. Darüber hinaus wird

über Negativlisten und Wortfilter der Zugriff auf unerwünschte Inhalte unterbunden.

Die Stadtverwaltung nutzt das bereits vom ULD auditierte Landesnetz für die landesweite Kommunikation mit öffentlichen Stellen und dem Zugang zum Internet. Der IT-Bereich setzt sämtliche empfohlenen Sicherheitsmaßnahmen um:

- Das Programm zur Kontrolle des Landesnetzrouters (LNRC) wird eingesetzt,
- das Berichtswesen wird genutzt,
- der IT-Bereich nutzt den Zugang zum Tool LN-Webview.

2.5 Dokumentation

Es liegen als Dokumentation vor:

- IT-Konzept,
- Sicherheitskonzept inkl. Risikoanalyse,
- Restrisikoanalysen,
- Dienstanweisungen,
  - E-Mail,
  - WWW,
  - Betrieb von IT-Systemen,
  - IT-Administration
- Systemakten,
- Verfahrensakten der eingesetzten Fachverfahren,
- Systemdokumentation des Landesnetzanschlusses,
- Inventarliste der eingesetzten Hard- und Software.

Die Dokumentation entspricht den Anforderungen der DSVO.

2.6 Datenschutzmanagement

Zum Zeitpunkt der Begutachtung lag das Datenschutz-Management sowohl beim IT-Bereich als auch dem behördlichen Datenschutzbeauftragten. Von diesem Management wurden u.a. die folgenden Aufgaben durchgeführt:

- Dokumentation und Umsetzung der Datenschutzziele,
- Überwachung der Einhaltung und Umsetzung der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen.

Mit Abschluss dieses Audits geht das Datenschutz-Management auf den neuen, nach § 10 LDSG ordentlich bestellten behördlichen Datenschutzbeauftragten über. In Zusammenarbeit mit dem IT-Bereich überwacht dieser regelmäßig die Verfahrensabläufe auf Einhaltung der gesetzlichen und dienstlich vereinbarten Vorschriften. Änderungen an Verfahren werden über den IT-Bereich dem behördlichen Datenschutzbeauftragten unverzüglich mitgeteilt, so dass dieser rechtzeitig das ULD zum Zweck der Durchführung einer Nachprüfung informieren kann. Als vorbildlich ist die Regelung zur Einführung und wesentlichen Änderung neuer Verfahren hervorzuheben.

3. Datenschutzrechtliche Bewertung

Die Überprüfungen haben ergeben, dass die im Sicherheitskonzept festgeschriebenen Maßnahmen, mit Ausnahme von baulichen Unzulänglichkeiten, vollständig umgesetzt worden sind.

Die Stadtverwaltung verfügt darüberhinaus über weitere Dokumentationen auf einem qualitativ hohen Niveau. Die Umsetzung der Vorgaben des IT-Konzepts wird durch aussagekräftige und klar formulierte Dienstanweisungen unterstützt.

Die durch das vorliegende Audit erfassten Verarbeitungsprozesse zeichnen sich insbesondere durch folgende datenschutzfreundliche Aspekte aus:

- Der technische Aufbau und Betrieb des Serverraumes ist vorbildlich. Einzig der Durchzug eines Fernwärmerohres ist bautechnisch problematisch für den Fall, dass dieses Rohr schadhaft werden könnte. Es wurde im Sicherheitskonzept darauf hingewiesen.
- Alle Fachanwendungen und die mit ihnen verarbeiteten Daten werden strukturiert zentral auf den Servern verwaltet. Die Abschottung der Fachanwendungen untereinander ist gewährleistet. Die Zugriffe auf die Anwendungen sind durch eine transparente Zugriffsregelung gewährleistet.
- Die IT-Systeme sowie die auf ihnen eingesetzten Fachverfahren sind gut dokumentiert. Für jedes Fachverfahren ist ein Fachverfahrensverantwortlicher benannt. Die jeweiligen Pflichten des IT-Bereichs und der Fachverfahrensverantwortlichen sind im IT-Konzept nachvollziehbar und eingängig festgelegt.
- Für die Absicherung und Kontrolle des Anschlusses an externe Netze werden Sicherheitskomponenten (LNRC-Tool, Berichtswesen, eigenes Firewallsystem, WebMarshal, zentraler Virenscan auf dem Mail-

server) eingesetzt, die unerwünschte Zugriffe abwehren und den Transport schadhafter Inhalte verhindern.

- Die auf den Arbeitsplatz-PC enthaltenen Funktionen sind durch den Einsatz von Gruppenrichtlinien auf ein Mindestmaß reduziert. Der Zugriff auf externe Schnittstellen wird über eine Sicherheitssoftware zentral reglementiert.
- Der IT-Bereich verfügt für Test- und Weiterbildungszwecke über eine Testumgebung. In dieser Testumgebung werden darüber hinaus administrative Änderungen an Fachverfahren durch den Fachverfahrensverantwortlichen vor dem Einsatz in der Produktivumgebung getestet und freigegeben.
- Zur Einführung und Weiterentwicklung von Fachverfahren ist ein Prozess definiert, der für eine umfassende Berücksichtigung möglicher Anforderungen aus den Bereichen Datenschutz und Datensicherheit sorgt.
- Die Auswertung von Protokollen ist geregelt. Die Revisionstools zur Überwachung des Landesnetzzugangs befinden sich im Einsatz.

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