LD72 –16.01/02.008 Kiel, 19. Juni 2007

# Gutachten

**im Rahmen der Rezertifizierung**

**über das Auditverfahren gemäß § 43 Abs. 2 LDSG**

# Verarbeitung personenbezogener Daten mit IT-Systemen in der Stadtverwaltung Bad Schwartau

## Inhaltsverzeichnis

# 1 Rezertifizierung des Datenschutz-Audits

Der Stadtverwaltung Bad Schwartau wurde am 16. Juni 2004 vom Unabhängigen Landeszentrum für Datenschutz (ULD) das Datenschutz-Audit für

- **die „Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung der Stadt Bad Schwartau ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter“** und

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

verliehen.

Der auditierte Gegenstand sowie die Feststellungen zum Datenschutz-Management-System werden in dem öffentlichen **Kurzgutachten** (www.datenschutzzentrum.de/audit/register.htm) sowie in dem nichtöffentlichen **Langgutachten** vom 16. Juni 2004 dargestellt.

Die Stadtverwaltung hat mit Ablauf des Verleihungszeitraums des Datenschutz-Audits zum 16. Juni 2007 eine Verlängerung des Zertifikates für weitere 3 Jahre beim ULD beantragt. Das ULD hat am 11. Juni 2007 eine eintägige stichprobenartige Begutachtung der Einhaltung der mit dem Datenschutz-Audit erreichten Datenschutzziele und im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen durchgeführt.

# 2 Fortentwicklung der sicherheitstechnischen Elemente des Datenschutz-Managementsystems

- Das Datenschutz-Management wird in Zusammenarbeit des **behördlichen Datenschutzbeauftragten** und definierter Mitarbeitern der IT-Koordination durchgeführt.

- Das Datenschutz-Management **überwacht** in regelmäßigen Abständen die Verfahrensabläufe die Einhaltung der gesetzlichen Vorschriften.

- Die Stelle des behördlichen Datenschutzbeauftragten wurde neu besetzt und im Bereich des **Rechnungsprüfungsamtes** angesiedelt.

- Die **Überwachung** und **Prüfung** der im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen obliegt dem Datenschutzbeauftragten.

- Änderungen an Verfahren werden **getestet** und schriftlich durch die zuständigen Verantwortlichen **freigegeben**.

- Die IT-Koordination informiert den behördlichen Datenschutzbeauftragten über **sicherheitstechnische Veränderungen** der IT-Komponenten.

- Der behördliche Datenschutzbeauftragte erwirbt zusätzliches **Know-how**.

- Der **IT-Sicherheitsprozess** wird von dem behördlichen Datenschutzbeauftragten begleitet.

- Der behördliche Datenschutzbeauftragte hat **Sicherheitschecks**, insbesondere der papierenen Datenverarbeitung durchgeführt. Weitere Sicherheitschecks sind für den automatisierten Bereich in der Planung.

- Die IT-Koordination hat sich zu Fragen und Lösungen der IT-Sicherheit **fortgebildet**.

- Das IT-Konzept und das Datenschutzkonzept wurden im Oktober 2006 **aktualisiert**.

- Die **Dokumentation** der eingesetzten IT-Komponenten wurde fortlaufend vervollständigt und in die Bereiche

  - Fachverfahren,
  - Server,
  - Inventar,
  - Allgemeines,
  - Internet und
  - Lizenzen

  strukturiert. Darüber hinaus existiert eine übersichtliche **automatisierte Ablage**, in der die Dokumente für den IT-Einsatz der Stadtverwaltung

verwaltet werden.

- Veraltete Clients werden im Bürgerbüro und in der Bauverwaltung durch so genannte **Thin-Clients** ausgetauscht.

- Die **Firewallkomponente** wurde durch eine leistungsfähigere Variante ersetzt.

- Zur Datensicherung wird ein separater **Datensicherungsserver** eingesetzt.

- Die **Server** wurden durch neuere Systeme ersetzt. Die eingesetzten **Betriebssysteme** wurden auf den neusten Stand gebracht.

- Die **Datenabschottung** wird technisch durch eine nachvollziehbare Benutzer- und Rechteverwaltung gewährleistet.

- Die **Fachanwendungen** auf dem Arbeitsplatz-PC (Thin-Client) sind auf das erforderliche **Maß** begrenzt.

- Die Daten der **Fachanwendungen** werden **zentral** und **strukturiert** verwaltet.

- **Kopien** ein- und ausgehender E-Mails werden für sicherheitstechnische **Kontrollzwecke** in einem gesonderten Archiv gespeichert.

- Es werden nur E-Mails an den Arbeitsplatz geleitet, die auf **Viren überprüft** sind.

- Webseiten aus dem **Internet** werden nur nach Genehmigung der Leitungsebene über eine so genannte **whitelist** frei geschaltet.

- Das **„Herunterladen“** ausführbarer Programme und Dateien ist auf den Arbeitsplätzen nicht zugelassen.

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

- Die **ordnungsgemäße Nutzung der Internetdienste** wird in regelmäßi-

gen Abständen von dem behördlichen Datenschutzbeauftragten überwacht.

- Das lokale Verwaltungsnetz der Stadtverwaltung ist über eine Firewall an das **Landesnetz** angeschlossen worden.

- Im Serverraum wurden eine **Rauchmeldeanlage** und eine neue Klimaanlage installiert.

## 3 Datenschutzrechtliche Bewertung

Die Feststellungen im Rahmen der Begutachtung haben ergeben, dass die von der Stadtverwaltung getroffenen technischen und aufbau- und ablauforganisatorischen **Sicherheitsmaßnahmen** den datenschutzrechtlichen Vorschriften (LDSG und DSVO) entsprechen.

Der **Sicherheitsstandard** hat sich innerhalb der 3 Jahre positiv fortentwickelt, so dass die Stadtverwaltung die Einhaltung von Datenschutz und Datensicherheit in Bezug auf den Auditgegenstand **fortlaufend** gewährleistet.

Die von der Stadtverwaltung festgelegten **Datenschutzziele** werden von der Leitungsebene der Stadtverwaltung weiterhin verfolgt.

Folgende „datenschutzfreundliche Aspekte“ sind besonders herauszustellen:

1. Für den Einsatz der IT-Systeme ist eine umfassende gut strukturierte **Dokumentation** verfügbar. Sie wird ergänzt durch eine automatisiert geführte Ablage.

2. Die Leitungsebene (Bürgermeister und Büroleiter), die Mitarbeiter der IT-Koordination sowie der behördliche Datenschutzbeauftragte verfolgen die festgelegten **Datenschutzziele** engagiert und nachhaltig. Sie unterstützen den **IT-Sicherheitsprozess vorbildlich**.

3. Der Einsatz von **Thin-Clients** im Rahmen des **Terminal-Server-Konzeptes** sowie die restriktiv abgesicherte Nutzung der Internetdienste werden weiterhin verfolgt.

**Die Verleihung des Auditzeichens nach § 43 Abs. 2 LDSG ist für weitere 3 Jahre gerechtfertigt.**

Kiel, 19. Juni 2007 (Gutachter)

Behrendt