# Gutachten

## zur Reauditierung

## im Rahmen des Auditverfahrens gemäß § 43 Abs. 2 LDSG

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

**Auditor: Heiko Behrendt**

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstraße 98

24103 Kiel

Kiel, 18. November 2013

Auditor: Heiko Behrendt

Az.: 16.01/02.008

E-Mail: mail@datenschutzzentrum.de

# Inhaltsverzeichnis

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

Der Stadtverwaltung Bad Schwartau wurde am 16. Juni 2004 vom Unabhängigen Landeszentrum für Datenschutz (ULD) nach Durchführung eines Datenschutzaudits zu

- der „Sicherheit und Ordnungsmäßigkeit der internen automatisierten Datenverarbeitung der Stadt Bad Schwartau ohne Berücksichtigung der Rechtmäßigkeit der Datenverarbeitung in den einzelnen Fachverfahren der Fachämter“ und
- dem „Anschluss des internen Netzes der Stadtverwaltung an das Internet“

ein Datenschutzauditzeichen für drei Jahre verliehen.

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

In den Jahren 2007 und 2010 fanden erfolgreiche Reauditierungen statt, in denen überprüft wurde, ob die Kriterien für die Verleihung des Datenschutzauditzeichens weiterhin Bestand hatten. Die entsprechenden Gutachten sind auf der o. a. ULD-Webseite abrufbar.

Die Stadtverwaltung Bad Schwartau hat im Juni 2013 mit Ablauf des Zeitraums von drei Jahren, für die das Datenschutzauditzeichen verliehen wurde, eine erneute Reauditierung beantragt. Das ULD hat eine stichprobenartige Begutachtung des Gegenstands des Datenschutzaudits durchgeführt. Ein Schwerpunkt wurde diesbezüglich auf die Einhaltung der mit dem Datenschutzaudit zu erreichenden Datenschutzziele (siehe Gutachten über das Datenschutzaudit von 2004) und der im Datenschutzkonzept festgelegten und mittlerweile fortgeschriebenen Sicherheitsmaßnahmen gelegt. Die Ergebnisse dieser Überprüfung werden im Folgenden dargestellt.

# 2 Fortentwicklung des Datenschutzmanagementsystems

Im Rahmen des Datenschutzmanagementsystems wurden folgende technische und organisatorische Aspekte fortentwickelt:

- Die Verfahrensverantwortlichen der Ämter überwachen zur Einhaltung der gesetzlichen Vorschriften die Verfahrensabläufe.
- Der behördliche Datenschutzbeauftragte überprüft in regelmäßigen Abständen die im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen. Folgende Aufgaben wurden u. a. von ihm durchgeführt:
  - Verwaltung und Abgabe der Freigabeerklärung für automatisierte Verfahren nach § 5 Abs. 2 Landesdatenschutzgesetz (LDSG).
  - Überprüfung der Zugriffsberechtigungskonfiguration der einzelnen Mitarbeiterinnen und Mitarbeiter auf vorhandene Softwareprogramme.
  - Stichprobenartige Überprüfung der Zugriffsberechtigten auf Missbrauch im Bereich der Kurzauskünfte des Einwohnermeldewesens.
  - Überprüfung der Vernichtung alter bzw. erledigter Fälle nach den Aufbewahrungsfristen der KGSt in den Bereichen Wohngeldwesen, Überwachung ruhender Verkehr und Vollstreckungswesen der Finanzbuchhaltung.
  - Jährlicher Bericht über den Datenschutz im Schlussbericht über die Prüfung des Jahresabschlusses der Stadt Bad Schwartau.
  - Beratung der Fachabteilungen in datenschutzrechtlichen Angelegenheiten.
  - Teilnahme an Sitzungen des Arbeitskreises IT-Prüfungen.
  - Begleitende Tätigkeit bei der Erstellung einer Vereinbarung zur Auftragsdatenverarbeitung.
- Die in der für Standardsoftware zentralen Ablage befindlichen Datenbestände werden nach Erreichung der festgelegten Löschungsfristen gelöscht.
- Das Konzept für den Einsatz von Terminal-Server wurde vollständig umgesetzt. In allen Fachbereichen werden mit wenigen begründeten Ausnahmen Thin-Clients eingesetzt.
- Für die Benutzer- und Gruppenkontenverwaltung sowie für das Rechtemanagement wird eine Sicherheitssoftware zur Dokumentation und Nachvollziehbarkeit der Einstellungen eingeführt.
- Mit dem Einsatz der Gruppenrichtlinien werden auf den Thin-Clients nur diejenigen Funktionen und Anwendungen zur Verfügung gestellt, die für die dienstlichen Aufgaben erforderlich sind.
- Die Schnittstellen der Thin-Clients werden unter Einsatz einer Sicherheitssoftware gesperrt.
- Für den Betrieb der Fachverfahren wurden veraltete IT-Systeme durch drei Host-Systeme für den Einsatz der Servervirtualisierung erneuert. Darüber hinaus wurden leis-

tungsfähigere, redundant installierte Backup-Server angeschafft sowie ein Firewallsystem auf den neusten Stand gebracht.

- Im Rahmen der Ablösung physikalischer Server wurden folgende virtuelle Systeme eingerichtet:
  - Windows Server 2003, Exchange-Server für die Postfachbereitstellung
  - Windows Server 2003, Domänencontroller, Lizenzserver, Active Directory
  - Windows Server 2008, Domänencontroller, Lizenzserver, Active Directory
  - Windows Server 2003, Citrix Presentation Server, Applikationsserver für Fachanwendungen
  - Windows Server 2003, Server zur Steuerung der Infomonitore EG
  - Windows Server 2003, Active Directory, DNS
  - Windows Server 2003, Printserver für Druck-, Kopier-, Scan- und Faxsysteme
  - Windows Server 2003, Mailgateway, Virenscan für E-Mails, Spamfilter
  - Windows Server 2003, Systemanalysetool, Device-Lock-Console
  - Windows Server 2003, Applikations-Server, Fileserver
  - Windows Server 2003, Citrix-Presentation Server, Applikationsserver für Internet-Explorer, Outlook, Intranet
  - Windows Server 2008, Citrix XenApp, Applikationsserver für Internet-Explorer, Outlook, Intranet
  - Windows Server 2003, Verwaltungskonsole für Thin-Clients
- Ein Backup-Server wurde in einem gesonderten Raum in einem Schutzschrank installiert.
- Das Datenschutzkonzept und das IT-Konzept wurden im Jahr 2013 aktualisiert.
- Die technische Dokumentation der Datenverarbeitung wurde aktualisiert. Für den Backup-Server, den Xen-Server und für die Firewall wurden gesonderte Dokumente erstellt.
- Die Daten der Fachanwendungen werden zentral und strukturiert verwaltet.
- Die Nutzung der Internetdienste ist in einer gesonderten Dienstanweisung geregelt.
- Bei der Versendung von E-Mail dürfen personenbezogene Inhalte grundsätzlich nur in verschlüsselter Form versendet werden.
- Der Zugriff auf WWW wird durch Filtermechanismen auf der Firewall beschränkt. Der Download von ausführbaren Programmen ist nur im Bereich der IT-Koordination erlaubt.
- Mit dem Einsatz der TK-Anlage werden keine Abrechnungsdaten mehr gespeichert. Die Administration wird durch die IT-Koordination durchgeführt. Der Remotezugang für die externe Administration durch einen Dienstleister ist gesperrt und wird nur nach Bedarf freigeschaltet.
- Die Digitalkopierer wurden erneuert. Ein Ausdruck ist erst nach Eingabe einer PIN mög-

lich. Die Daten auf der Festplatte werden vor Abholung der Systeme physikalisch gelöscht.

- In dem Zeitraum seit der letzten Reauditierung im Jahr 2010 gingen keine Beschwerden von Betroffenen ein, denen nachgegangen hätte werden müssen.

# 3 Bewertung

Die Feststellungen im Rahmen der Begutachtung haben ergeben, dass die von der Stadtverwaltung Bad Schwartau getroffenen technischen und organisatorischen Sicherheitsmaßnahmen den datenschutzrechtlichen Vorschriften entsprechen.

Der Sicherheitsstandard hat sich mit der Erneuerung zentraler IT-Systeme und den Einsatz von Sicherheitssoftware positiv fortentwickelt, so dass die Stadtverwaltung die Einhaltung der Anforderungen von Datenschutz und Datensicherheit in Bezug auf den Auditgegenstand fortlaufend gewährleistet.

Folgende aus Datenschutzsicht herausragende Aspekte sind besonders zu erwähnen:

- Der Bürgermeister, der Büroleiter, die Mitarbeiter der IT-Koordination sowie der behördliche Datenschutzbeauftragte sorgen dafür, dass die im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen dauerhaft umgesetzt werden. Sie unterstützen den IT-Sicherheitsprozess vorbildlich.
- Wesentliche zentrale IT-Komponenten wurden erneuert, so dass insbesondere technische Sicherheitsmaßnahmen nach dem Stand der Technik umgesetzt werden.
- Die IT-Systeme für die Datensicherung wurden redundant in unterschiedlichen Räumen eingerichtet.
- Sicherheitssoftware für die Nachvollziehbarkeit der Benutzer- und Gruppenkontenverwaltung sowie den ihnen zugewiesenen Berechtigungen wird eingesetzt.

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

Kiel, 18. November 2013 Auditor: gez. Heiko Behrendt