LD72 –16.01/02.008 Kiel, 28. Juni 2010

Gutachten

zur Reauditierung

im Rahmen des Auditverfahrens gemäß § 43 Abs. 2 LDSG

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

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.

Im Juni 2007 fand eine erfolgreiche Reauditierung statt, d.h. es wurde überprüft, ob die Kriterien für die Verleihung des Datenschutzauditzeichens weiterhin Bestand hatten. Das Gutachten vom 16. Juni 2007 ist auf der o.a. ULD-Webseite abrufbar.

Die Stadtverwaltung Bad Schwartau hat im Juni 2010 mit Ablauf des Zeitraums von drei Jahren, für die das Datenschutzauditzeichen verliehen wurde, eine erneute Reauditierung beantragt.

Ein Gutachter des ULD hat am 3. Juni 2010 eine eintägige 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 2007) und der im Datenschutzkonzept festgelegten und mittlerweile fortgeschriebenen Sicherheitsmaßnahmen gelegt. Die Ergebnisse dieser Überprüfung werden im Folgenden dargestellt.

2 Fortentwicklung der sicherheitstechnischen Elemente des Datenschutzmanagementsystems

Seit der Reauditierung im Jahr 2007 wurden im Rahmen des Datenschutzmanagementsystems folgende technische und organisatorische Aspekte fortentwickelt:

- Das Datenschutzmanagement überwacht zur Einhaltung der gesetzlichen Vorschriften die Verfahrensabläufe.

- Der behördliche Datenschutzbeauftragte überprüft in regelmäßigen Abständen die im Datenschutzkonzept festgelegten Sicherheitsmaßnahmen.

- In 2010 wurden auf Veranlassung des behördlichen Datenschutzbeauftragten in einzelnen Fachabteilungen nicht mehr benötigte Akten ausgesondert und vernichtet.

- Die Ablage für Dokumente wurde neu strukturiert. Die darin befindlichen Datenbestände wurden auf ein Mindestmaß reduziert.

- Die IT-Koordination hat das Terminal-Server-Client-Konzept beinahe vollständig umgesetzt. In allen Fachbereichen wurden, soweit möglich, die Fat-Clients durch Thin-Clients ersetzt.

- 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.

- Während die älteren Thin-Client-Geräte nicht über eine USB-Schnittstelle verfügen, ist für die neueren Modelle, die seit 2009 zum Einsatz kommen, geplant, die USB-Schnittstelle unter Einsatz einer Sicherheitssoftware so zu reglementieren, dass nur dienstliche Geräte/Komponenten beim Anschluss unterstützt werden.

- Der veraltete SQL-Server und die Terminal-Server wurden durch neue Systeme ersetzt. Die eingesetzten Betriebssysteme wurden auf den neuesten Stand gebracht. Dies umfasst insbesondere die aus Datensicherheitssicht notwendigen Updates und Patches.

- Die Drucker am Arbeitsplatz werden aus wirtschaftlichen Gründen soweit

möglich reduziert. An vielen Arbeitsplätzen ist bereits das Drucken vom Client nur auf den abgesicherten zentralen Multifunktionsdruckern möglich. Der Druckjob wird vom Client zunächst an den Printserver geschickt und dort zwischengespeichert, bis der/die jeweilige Mitarbeiter(in) seinen/ihren Ausdruck am zentralen Drucker aktiviert. Über einen personalisierten Transponder findet am Multifunktionsgerät die Authentifizierung der entsprechenden Person statt, so dass nur die zugehörigen an den Printserver gesendeten Ausdrucke aktiviert werden. Die Druckberechtigungen werden am Printserver verwaltet.

- Das IT-Konzept wurde im Dezember 2009 aktualisiert.

- Die technische Dokumentation der Datenverarbeitung wurde weiter verbessert. Sie befindet sich in einem vorbildlichen Zustand.

- Zugriffsberechtigungen werden über die jeweilige Amtsleitung über ein spezielles Formular beantragt. Der behördliche Datenschutzbeauftragte wird in den Prozess der Berechtigungsvergabe eingebunden.

- Die Daten der Fachanwendungen werden zentral und strukturiert verwaltet.

- Die Nutzung der Internetdienste ist in einer gesonderten Dienstanweisung geregelt.

- Kopien ein- und ausgehender E-Mails werden für sicherheitstechnische Kontrollzwecke für 3 Monate in einem gesonderten Archiv gespeichert und anschließend automatisiert gelöscht. Bei etwaigen Zugriffen wird streng auf die Zweckbindung geachtet.

- Webseiten aus dem Internet werden nur nach Genehmigung der Leitungsebene über eine so genannte „Whitelist“ frei geschaltet.

- Das „Herunterladen“ ausführbarer Programme und Dateien wird auf den Arbeitsplätzen durch Sicherheitseinstellungen in der Citrix-Terminal-Server-Umgebung technisch unterbunden.

3 Datenschutzrechtliche Bewertung

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

Der Sicherheitsstandard hat sich 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 aus Datenschutzsicht herausragende Aspekte sind besonders zu erwähnen:

1. Der Bürgermeister, der Büroleiter, die Mitarbeiter der IT-Koordination sowie der behördliche Datenschutzbeauftragte verfolgen die festgelegten Datenschutzziele engagiert und nachhaltig. Sie unterstützen den IT-Sicherheitsprozess vorbildlich.

2. In die Fortentwicklung des Terminal-Server-Konzeptes wurde ein zentrales Druckmanagement aufgenommen. Dieses zeichnet sich besonders durch ein transponderunterstütztes Zugriffsrechtesystem aus, so dass die Mitarbeiterinnen und Mitarbeiter nur ihre in Auftrag gegebenen Ausdrucke vor Ort am zentralen Drucker aktivieren können.

3. Für die automatisierte Datenverarbeitung besteht eine gut strukturierte und aktuelle Dokumentation. IT-Konzept, Sicherheitskonzept sowie Verfahrensakten werden in lobenswerter Weise geführt.

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

Kiel, 28. Juni 2010 Behrendt (Gutachter)