ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Kurzgutachten über das Auditverfahren gemäß § 43 Abs. 2 LDSG

Personalverwaltungs- und Informationssystem (PVS) der Stadt Norderstedt
Reauditierung hinsichtlich des Audits 04/2003 vom 24. August 2003 und
Neuauditierung zusätzlicher Verfahrensmodule

10.1.2007

1. Gegenstand des Auditverfahrens

Die Einführung eines Personalverwaltungs- und Informationssystems (PVS) war der Gegenstand des Datenschutz-Behördenaudits 4/2003 vom 24. August 2003. Der Betrieb dieses Verfahrens ist Gegenstand der vorliegenden Reauditierung. Sie wird kombiniert mit der Neuauditierung zweier Verfahrensmodule, um die das auditierte PVS erweitert wird. Die Stadt Norderstedt setzt für diese Aufgabe das Produkt KOMMBOSS der Firma GfOP Neumann & Partner mbH ein. In diesem Auditverfahren wird der konkrete Einsatz ausgewählter Module dieses Produktes auditiert. In die Bewertung gehen dabei auch die technisch-organisatorischen Maßnahmen und Einsatzbedingungen bei der Stadt Norderstedt ein. Dies betrifft z. B. die Deaktivierung einzelner Teilmodule bzw. Nichtnutzung von Funktionalitäten des Produktes, die daher nicht Gegenstand der Auditierung sind. Daher sind Rückschlüsse auf die Vereinbarkeit sämtlicher Produktfunktionalitäten mit den Regelungen über Datenschutz und Datensicherheit, wie sie ein Gütesiegel erlaubt, nicht zulässig.

Vor der Beschaffung eines PVS erstellte die Stadt Norderstedt im Jahre 2000 ein "Pflichtenheft zur Einführung eines Personalverwaltungs- und Informationssystems". Dieses enthält eine detaillierte Beschreibung der einzelnen Arbeitsabläufe zur Erfüllung der Personalverwaltungsaufgaben. Gleichzeitig wurde daraus ein Anforderungsprofil für den Einsatz eines automatisierten Verfahrens abgeleitet. Dieses Pflichtenheft wird fortlaufend fortgeschrieben und die daraus resultierenden Anforderungen bei der Implementierung neuer Verfahrensmodule umgesetzt.

Nicht alle Verfahrensmodule des PVS waren Gegenstand der Erstauditierung. Neue Gegenstände der vorliegenden Auditierung sind die Verfahrensmodule „Fortbildung“ und „Dokumentenverwaltung“ sowie Änderungen am bestehenden Verfahren, insbesondere im Bereich der Protokollierung. Auch die zum Zeitpunkt der Erstauditierung formulierten und in der Zwischenzeit erreichten Datenschutzziele sind Gegenstand der Begutachtung.

Grundlage des Datenschutz-Behördenaudits bei der Stadt Norderstedt sind die Anwendungsbestimmungen des ULD zur Durchführung eines Datenschutz-Behördenaudits nach § 43 Abs. 2 Landesdatenschutzgesetz (LDSG) vom 22. März 2001 (Amtsblatt Schl.-H. 13/2001, S. 196).

Mit dem vorliegenden Kurzgutachten fasst das ULD gemäß Ziffer B 8.5 der Anwendungsbestimmungen (im Folgenden HDSA) das Ergebnis seiner Mitwirkung zusammen. Dieses enthält eine Zusammenfassung der Datenschutzerklärung sowie die Bewertung der dort getroffenen Aussagen durch das ULD.

2. Verfahrensunterlagen

Im Rahmen des Reauditierungsverfahrens wurden von der Stadt Norderstedt im Wesentlichen folgende Unterlagen vorgelegt:

a. Datenschutzerklärung der Stadt Norderstedt vom 14.12.2006, enthaltend:
   (1) Bestandsaufnahme,
   (2) Analyse der Restrisiken gemäß Ziffer B 5.2 und Festlegung der Datenschutzziele gemäß Ziffer B 6 HDSA,

(3) Datenschutzmanagementsystem gemäß Ziffer B 7 HDSA,

b. Übersicht über Bildschirmmasken, darin verarbeiteten Daten und die zugehörige Aufgabe im Pflichtenheft für die Module Personalmanagement, Stellenplan, Fortbildung, Dokumentenverwaltung,

c. EDV-Sicherheitskonzept der Stadt Norderstedt vom 1.11.2005,

d. Benutzerhandbuch Kommboss, Version 2.8.3: Module Dokumentenverwaltung, Protokollierung und Fortbildung,

e. Vordruck der Stadt Norderstedt für die Rechtefreigabe im Verfahren Kommboss (Blankovordruck und Beispiel),

f. Übersicht über die Protokollierung von Rechtefreigaben auf Ebene der Datenfelder und Formulare,

g. Vordruck über die Durchführung von Verfahrenstests im Verfahren Kommboss (Blankovordruck und Beispiele),

h. Dienstanweisung für die elektronische Datenverarbeitung der Stadt Norderstedt (DA 10.16) vom 1.11.2005,

i. Dienstvereinbarung zwischen der Stadt Norderstedt und dem Personalrat der Stadt Norderstedt 24.8.2005,

j. Eintrag des Verfahrens *Personal- und Informationssystem KOMMBOSS* in das Verfahrensverzeichnis,

k. Freigabevermerk für das Modul Fortbildung 20.11.2006.

3. Wesentlicher Inhalt der Bestandsaufnahme

3.1. Allgemeines

Die Bestandsaufnahme enthält vor allem

- eine Darstellung der Zwecke des Personalverwaltungs- und Informationssystems sowie der zum Einsatz kommenden Module, die dem Datenschutzaudit unterfallen,
- eine Benennung der wesentlichen datenschutzrechtlichen Vorschriften, die bei der Datenverarbeitung im Rahmen des Personalverwaltungs- und Informationssystems zu beachten sind,
- eine Beschreibung der technischen und organisatorischen Maßnahmen zur Aufrechterhaltung der Datensicherheit sowohl in abstrakter als auch in konkreter Form.

3.2. Zweck des Verfahrens

Die Stadt Norderstedt setzt das Personalverwaltungs- und Informationssystem Kommboss in der Version 2.8.3.4 der Firma GfOP Neumann und Partner mbH ein. Die Freigabe des Systems erfolgte nach erfolgreichem Abschluss des Erstauditverfahrens im August 2003.

Mit Hilfe des Systems werden die Daten der bei der Stadt Norderstedt beschäftigten Mitarbeiterinnen und Mitarbeiter zum Zwecke der Begründung, Durchführung, Beendigung oder Abwicklung der Dienst- und Arbeitsverhältnisse sowie zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zum Zwecke der Personalplanung und des Personaleinsatzes verwaltet. Bei den verarbeiteten Daten handelt es sich um Personaldaten bzw. Personalaktendaten sowie um Organisations- und Stellenplandaten. Über eine Schnittstelle zum Abrechnungssystem PERMIS Abrechung können Daten in das PVS übernommen werden. Darüber hinaus werden Fortbildungsmaßnahmen, zum Teil mit externer Beteiligung, organisiert. Dabei werden auch Daten von Teilnehmern und Dozenten, die nicht der Stadt Norderstedt angehören, verarbeitet.

Das System Kommboss besteht aus verschiedenen Modulen. Folgende Module werden reauditiert:

- Personalmanagement (Personalinformation)
- Stellenplan
- Terminüberwachung
- Datenschnittstelle
- Protokollierung
- Administration

Die Module

- Fortbildung und
- Dokumentenverwaltung

werden erstmalig auditiert.

Mit Hilfe des Moduls Fortbildung werden Fortbildungsveranstaltungen organisiert. Dies umfasst die Verwaltung von Veranstaltungsterminen, Teilnehmerverwaltung, Schriftwechsel mit Teilnehmer und Dozenten (bezogen auf Fortbildungsveranstaltungen), Erstellung von Teilnahmebescheinigungen und Übernahme von Teilnahmebestätigungen in den Personaldatenbestand der Teilnehmer und betrifft sowohl Mitarbeiterinnen und Mitarbeiter der Stadt Norderstedt als auch Teilnehmer aus anderen öffentlichen Verwaltungen; für Teilnehmern aus anderen öffentlichen Verwaltungen erfolgt aber keine Datenübermittlung in die jeweiligen Personaldatenbestände.

Das Modul Dokumentenverwaltung dient der Erstellung von individuellen Schreiben und Serienbriefen, die aus Vorlagen durch Ergänzung mit adressatenindividuellen Daten aus den übrigen Modulen, in erster Linie Personalmanagement und Fortbildung, erstellt werden. Das eingesetzte Programm ermöglicht als Dokumentenmanagementsystem die dauerhafte Speicherung der so erstellten Schreiben in elektronischer Form. Da aber die Personalakten der Stadt Norderstedt derzeit nur in Papierform geführt werden, erfolgt keine dauerhafte Speicherung der Schreiben, sondern nur eine vorübergehende, so lange sich das Dokument in der Be-

arbeitung und Abstimmung befindet. Nach maximal drei Monaten werden die erstellten Dokumente gelöscht. Die so erstellten Schreiben unterliegen denselben Zugriffsbeschränkungen wie die zu Grunde liegenden Personaldaten. Das Modul Dokumentenverwaltung erlaubt auch den Versand der erstellten Schreiben per E-Mail; diese Funktionalität wird nicht genutzt.

Die Software ermöglicht den Einsatz weiterer Module (Personalkostenplanung, Bewerberverwaltung). Diese Module sind nicht Gegenstand des Auditverfahrens.

Die Datenverarbeitung im System Kommboss richtet sich gemäß § 23 LDSG im Wesentlichen nach den Vorschriften der §§ 106 bis 106h des Landesbeamtengesetzes (LBG). Diese datenschutzrechtliche Vorschrift regelt die Datenverarbeitung bei Dienst- und Arbeitsverhältnissen und erweitert den Anwendungsbereich der Vorschriften des Landesbeamtengesetzes auf die Datenverarbeitung aller Beschäftigten bei öffentlichen Stellen.

Eine detaillierte Beschreibung der einzelnen im System verarbeiteten und zu verarbeitenden Daten sowie der hierbei zu beachtenden Rechtsvorschriften lässt sich dem Pflichtenheft entnehmen, das Gegenstand der Erstauditierung war. Dieses Pflichtenheft ist Gegenstand der Bestandsaufnahme.

3.3. Technische und organisatorische Maßnahmen

Die Bestandaufnahme enthält eine Beschreibung der technischen und organisatorischen Maßnahmen, die abstrakt und konkret für die Aufrechterhaltung der Datensicherheit erforderlich sind. Außerdem werden die eingesetzten Hard- und Softwarekomponenten beschrieben.

Ein Zugang zum Verfahren Kommboss ist innerhalb der Personalabteilung möglich. Dort erfolgt auch die Administration des Verfahrens durch ausdrücklich berechtigte Mitarbeiterinnen und Mitarbeiter des Personalamtes.

Die Leitung des Hauptamtes trägt für die Vergabe der Zugriffsrechte die Verantwortung. Sie hat im Rahmen der Erforderlichkeit ebenfalls Zugriff auf das Verfahren. Die technische Umsetzung der vergebenen Zugriffsrechte erfolgt durch die Verfahrensadministration.

Die Organisationsabteilung hat Zugriff auf das Modul Organigramm, das aber nicht Gegenstand des Datenschutzaudits ist.

Eine weitere Zugriffsmöglichkeit auf Verfahrensdaten besteht prinzipiell für die EDV-Abteilung, da von dort der Server des Verfahrens administriert wird (Systemadministration). Zugriffe auf Verfahrensdaten erfolgen aber ausschließlich auf ausdrückliche Weisung des Personalamtes (vgl. Abschnitt II Nr. 5 und Abschnitt III „Zuständigkeiten und Verantwortung“ der Datenschutzerklärung und Abschnitt 6.5.2 der Dienstvereinbarung zwischen der Stadt Norderstedt und dem Personalrat der Stadt Norderstedt).

Eine eventuelle künftige Erweiterung der Zugriffe auf das System durch andere Fachämter oder den Personalrat erfolgt erst nach einer sorgfältigen Prüfung, ob der Zugriff auf die vorhandenen Daten zur Aufgabenerfüllung der jeweiligen Mitarbeiterin bzw. des jeweiligen Mitarbeiters erforderlich ist. Die Erteilung von Zugriffsrechten für einzelne Eingabefelder, die aufgrund von Versionsänderungen in die Module eingefügt werden, erfolgt hingegen direkt durch die Verfahrensadministratoren entsprechend den generellen Festlegungen der Hauptamtsleitung.

Das System kann erst genutzt werden, nachdem sich die Mitarbeiterin oder der Mitarbeiter mit einer spezifischen Benutzerkennung und einem gesonderten Passwort authentifiziert haben. Für die einzelnen Datenfelder der verschiedenen Module werden Zugriffsrechte mitarbeiterbezogen definiert. Da für jedes einzelne Datenfeld die Zugriffsrechte gesondert vergeben werden, wird ein ungeprüfter Zugriff ausgeschlossen. Die Vergabe der Zugriffsrechte wird auf einem eigens hierfür entwickelten Vordruck dokumentiert. Die Rechtefreigabe wird ausschließlich aufgrund konkreter schriftlicher Vorgaben durch die Verfahrensadministration

implementiert, die die Vergabe der Rechte wechselseitig nach dem Vieraugen-Prinzip kontrolliert. Ebenso werden die tatsächlich eingerichteten Rechte durch ein Protokoll des Systems dokumentiert, das, soweit betroffen, den Fachamtsleitungen zur Verfügung steht.

4. Wesentlicher Inhalt der Analyse der Restrisiken und Definition der Datenschutzziele

Die Datenschutzerklärung enthält eine Beschreibung einzelner noch bestehender Restrisiken im Hinblick auf die Einhaltung datenschutzrechtlicher und datensicherheitstechnischer Vorgaben. Des Weiteren werden Ziele zur Erhaltung und Verbesserung bezüglich des Datenschutz- und Datensicherheitsniveaus festgelegt; in diesem Zusammenhang wird ein Zeitraum für deren Umsetzung benannt.

Konkret handelt es sich bei diesen Restrisiken zum einen um in der Software gegenwärtig noch fehlende Funktionen zur automatisierten Löschung von Personaldaten und zur Löschung von Fortbildungsveranstaltungen, die zwar bereits durch den Hersteller programmiert, aber noch nicht freigegeben sind. Die Löschung von Personaldaten erfolgt daher z. Zt. manuell. Zum anderen handelt es sich um Test und Freigabe für das Modul Dokumentenverwaltung. Für diese Datenschutzziele ist ein präziser Zeithorizont vorgegeben.

Es ist zu erwarten, dass die Vorgaben im Rahmen dieses Zeitraumes erfüllt werden, so dass es gerechtfertigt ist, bereits zum gegenwärtigen Zeitpunkt das Vorliegen der für ein erfolgreiches Auditverfahren erforderlichen Voraussetzungen zu bestätigen.

Zwei weitere Maßnahmen zur Abdeckung von Restrisiken, die die Protokollierung von Datenübernahmen aus dem System PERMIS A und die Dokumentation von Zugriffen durch die EDV-Abteilung betreffen, werden bereits umgesetzt.

5. Wesentlicher Inhalt des Datenschutzmanagementsystems

Das Datenschutzmanagementsystem enthält die internen Organisationsregelungen der Stadt Norderstedt im Hinblick auf das Erreichen der in der Bestandsaufnahme genannten Datenschutzziele sowie die Einhaltung der datenschutzrechtlichen Vorgaben.

Die Grundlagen hierfür bilden das "Pflichtenheft zur Einführung eines Personalverwaltungs- und Informationssystems" sowie das "EDV-Sicherheitskonzept der Stadt Norderstedt". Sowohl das Pflichtenheft als auch das Sicherheitskonzept werden laufend an geänderte rechtliche und technische Bedingungen angepasst.

Das Datenschutzmanagementsystem enthält ferner allgemeine Vorgaben, die geeignet sind, eine dauerhafte Aufrechterhaltung des erreichten Datenschutzniveaus zu gewährleisten.

Die Zuständigkeiten und Verantwortlichkeiten im Hinblick auf die Rechtmäßigkeit und Ordnungsmäßigkeit der Datenverarbeitung sind detailliert geregelt. Die Zuständigkeit für das Verfahren obliegt nach der "Dienstanweisung für die elektronische Datenverarbeitung der Stadt Norderstedt (DA 10.16)" dem Hauptamt, Personalabteilung. Die Zuständigkeit für die technische Vergabe der Zugriffsrechte obliegt der Administration. Alle Änderungen im Verfahren bedürfen der förmlichen Freigabe durch die Hauptamtsleitung.

Die Stadt hat mit dem Leiter des Rechnungsprüfungsamtes einen behördlichen Datenschutzbeauftragten im Sinne des § 10 LDSG förmlich bestellt.

Hinsichtlich aller im Pflichtenheft beschriebenen Aufgaben ist ein umfangreiches Test- und Freigabeverfahren durchzuführen. Hierfür wurde eine Vorgehensweise entwickelt, die nachvollziehbar und schlüssig dokumentiert ist und im Zeitraum zwischen Erst- und Reauditierung erfolgreich umgesetzt wurde.

Bezüglich der Einführung der einzelnen Module sind bereits Schulungen der Mitarbeiterinnen und Mitarbeiter erfolgt. Sofern Änderungen vorgenommen werden, finden erneut Schulungen statt, die insbesondere auch Fragen des Datenschutzes und der Datensicherheit behandeln. Diese Schulungen werden dokumentiert.

Bei Aktualisierung der Software wird dafür Sorge getragen, dass Änderungen einer Prüfung im Hinblick auf die Einhaltung der Vorgaben zum Datenschutz und zur Datensicherheit unterzogen werden.

6. Abschließende Bewertung

Die Stadt Norderstedt hat bei der Einführung des Personalverwaltungs- und Informationssystems die geltenden Vorschriften zu Datenschutz und Datensicherheit von vornherein berücksichtigt. Das vor der Beschaffung der Software Kommboss erstellte Pflichtenheft wurde im Rahmen des Auditverfahrens einer ständigen Bearbeitung und Anpassung im Hinblick auf die datenschutzrechtlichen Vorgaben unterzogen. Eine laufende Anpassung an gegebenenfalls geänderte sachliche und rechtliche Anforderungen hat laufend stattgefunden und wird auch in Zukunft stattfinden.

In der Dokumentation zum Verfahren Kommboss wird dargelegt, für welche der im Pflichtenheft genannten Aufgaben die einzelnen in Kommboss gespeicherten Daten zum Einsatz kommen sollen. Da für jedes Datenfeld ein entsprechender Nachweis erbracht wird, ist gewährleistet, dass die vorgesehene Datenspeicherung insgesamt zur rechtmäßigen Erfüllung der im Pflichtenheft nachgewiesenen Personalverwaltungsaufgaben erforderlich ist. Eine Nutzung von Datenfeldern aus dem Standardprogramm, die zur Aufgabenerfüllung der Stadt nicht erforderlich sind, wird dadurch ausgeschlossen, dass dafür keine Zugriffsrechte vergeben werden. Insoweit wird die Einhaltung der datenschutzrechtlichen Vorgaben durch technische Maßnahmen sichergestellt.

Die Einhaltung der Löschungsfristen für die einzelnen Personalaktendaten, insbesondere diejenigen aus § 106 h Abs. 2 LBG, wird durch entsprechende automatisierte Auswertungsmöglichkeiten des Datenbestandes überwacht. Eine automatische Löschfunktion wird zukünftig durch den Hersteller bereitgestellt (vgl. Datenschutzmanagement, Abschnitt II Analyse der Restrisiken, Datenschutzziel 2).

Die Organisationsentscheidung, mit dem Leiter des Rechnungsprüfungsamtes einen behördlichen Datenschutzbeauftragten im Sinne des § 10 LDSG förmlich zu bestellen, ist als wesentliche Verbesserung gegenüber der Erstauditierung ausdrücklich zu begrüßen.

Im Ergebnis ergibt die Begutachtung der von der Stadt Norderstedt vorgelegten Datenschutzerklärung, dass die Stadt Norderstedt bei der Einführung des Personalverwaltungs- und Informationssystems ein gutes datenschutzrechtliches Niveau erreicht hat. Die präzise zeitliche Festlegung der Umsetzung der in der Datenschutzerklärung definierten Datenschutzziele sowie das entwickelte Datenschutzmanagementsystem lassen erwarten, dass im Gültigkeitszeitraum des verliehenen Auditzeichens dieses Niveau gehalten oder sogar noch eine weitere Verbesserung des Datenschutzes erreicht wird.

Die Verleihung des Auditzeichens auf der Grundlage von § 43 Abs. 2 LDSG in Verbindung mit Ziffer B 9 HDSA ist gerechtfertigt.