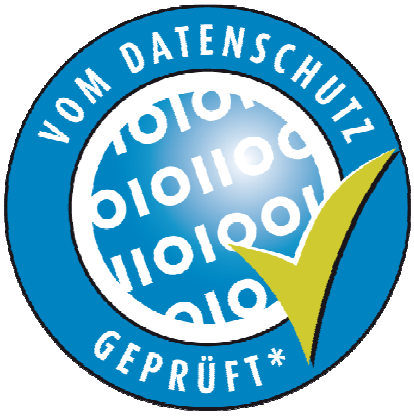

Gutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

IT-Sicherheitsmanagement

der

Kreisverwaltungen Nordfriesland, Schleswig-Flensburg und Nordbits AöR

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Datum : 08.12.2011
Aktenz. : 16.01/10.004
Telefon : 0431 988 1200
Fax : 0431 988 1223
E-Mail : mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutzaudits

Das Unabhängige Landeszentrum für Datenschutz (nachfolgend: ULD) und die Anstalt öffentlichen Rechts Nordbits (nachfolgend: Nordbits AöR) haben vereinbart, dass das ULD die „**Implementierung eines gemeinsamen, organisationsübergreifenden IT-Sicherheitsmanagements der Kreisverwaltungen Nordfriesland, Schleswig-Flensburg und Nordbits AöR**“ in einem Datenschutzbehördenaudit gemäß § 43 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG) überprüft und bewertet.

Der Gegenstand des Audit umfasst das **IT-Sicherheitsmanagementsystem** für Nordbits AöR und die beteiligten Kreisverwaltungen für die durch Nordbits AöR im Auftrag durchgeführte Verarbeitung personenbezogener Daten.

Vom Audit ausdrücklich nicht erfasst ist die korrekte Umsetzung aller in den jeweiligen Fachkonzepten der Nordbits AöR dargestellten fachverfahrensbezogenen Sicherheitsmaßnahmen im Rahmen des IT-Betriebs für die Auftraggeber in der Kreisverwaltung Schleswig-Flensburg und der Kreisverwaltung Nordfriesland.

Das IT-Sicherheitsmanagement wurde bezüglich der Aufbau- und Ablauforganisation sowie der Umsetzung der in der Verantwortung des Sicherheitsmanagements liegenden Prozesse im Rahmen des Datenschutzaudits auf die Konformität mit einzelnen Normen und rechtlichen Grundlagen überprüft. Bestandteil der Überprüfung waren neben einer Bewertung der konzeptionellen Aspekte des IT-Sicherheitsmanagements auch eine stichprobenartige Prüfung einzelner technischer und organisatorischer Maßnahmen vor Ort.

2 Feststellung zu den sicherheitstechnischen Elementen des IT-Sicherheitsmanagementsystems

2.1 Vertragliche Vereinbarungen

Die Nordbits AöR ist ein im Juli 2008 gegründetes gemeinsames Kommunalunternehmen der Kreise Nordfriesland und Schleswig-Flensburg.

Die Kreise Nordfriesland und Schleswig-Flensburg haben mit der Nordbits AöR jeweils einen Vertrag über die Datenverarbeitung im Auftrag gemäß § 17 LDSG geschlossen.

Gegenstand der Verträge ist die ordnungsgemäße Durchführung des technisch-operativen Teils aller Verwaltungsprozesse der Kreisverwaltungen durch die Nordbits AöR.

In den Verträgen sind die Pflichten des Auftragnehmers und des Auftraggebers explizit geregelt. Die datenschutzrechtliche Verantwortung verbleibt in Übereinstimmung mit § 17 Abs. 1 LDSG bei den Auftraggebern. Die Pflicht zur Umsetzung der Betroffenenrechte verbleibt bei den Auftraggebern.

Die Verträge sehen eine strikte Weisungsgebundenheit der Nordbits AöR in Fragen der Datenverarbeitung im Auftrag sowie ein jederzeitiges Kontrollrecht durch die Auftraggeber oder das Unabhängige Landeszentrum für Datenschutz vor. Die Anforderungen gemäß § 17 Abs. 2 und 3 LDSG sind erfüllt.

Die expliziten Regelungen zu Unterauftragsverhältnissen entsprechen den gesetzlichen Vorgaben. Zu den Pflichten des Auftragnehmers gehört die Einrichtung von und Teilnahme an einem gemeinsamen Sicherheitsmanagement des Auftragnehmers und der Auftraggeber. In den Verträgen sind Vorgaben zur Bearbeitung von Sicherheits- und Datenschutzvorfällen fixiert.

Nordbits AöR verpflichtet sich vertraglich, die technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Datenschutz- und Datensicherheitsniveaus gemäß den gesetzlichen Vorgaben und in Anlehnung an die IT-Grundschutzvorgehensweise und die Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) umzusetzen und eine wirksame Umsetzung schriftlich nachzuweisen.

Die vertraglichen Regelungen erfüllen die Anforderungen des § 17 LDSG. Das ULD hat geprüft, dass die Verträge rechtswirksam unterzeichnet wurden. Die Unterzeichnung hat im April 2010 stattgefunden.

2.2 IT-Sicherheitsleitlinie

Die Kreisverwaltungen der Kreise Nordfriesland und Schleswig-Flensburg sowie die Nordbits AöR haben in einer gemeinsamen IT-Sicherheitsleitlinie die Grundzüge des IT-Sicherheits- und Datenschutzmanagements festgelegt.

Die Leitlinie legt den Stellenwert der IT-Sicherheit fest und definiert IT-Sicherheitsziele. Die Sicherheitsziele umfassen die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme. Zu-

sätzlich werden eine Datentrennung nach Auftraggebern, die Revisionsfähigkeit der Datenverarbeitung und der Grundsatz der Schadensminimierung vereinbart. Als Ziel wird das Erreichen eines Sicherheitsniveaus in Anlehnung an die Vorgaben der IT-Grundschutzvorgehensweise des BSI beschrieben. In der Leitlinie werden das gemeinsame Sicherheitsmanagement, eine modulare Sicherheitskonzeption und –dokumentation sowie eine regelmäßige Sicherheitsrevision festgelegt.

Die Leitlinie enthält explizite Aussagen zur Verantwortung für die IT-Sicherheit und den Datenschutz. Die Bekanntgabe sowie die regelmäßige Überarbeitung der Leitlinie ist geregelt. Die Leitlinie wurde im April 2010 durch die Landräte und den technischen Leiter der Nordbits AöR in Kraft gesetzt.

Die Leitlinie entspricht den Anforderungen internationaler und nationaler Standards. Das ULD hat die Umsetzung der Leitlinie in der Kreisverwaltung Schleswig-Flensburg durch eine Kontrolle vor Ort nachvollzogen.

2.3 Aufbau- und Ablauforganisation

Die in der Sicherheitsleitlinie getroffenen Regelungen sind in einem Konzept zum gemeinsamen IT-Sicherheitsmanagement der Kreise Nordfriesland, Schleswig-Flensburg und der Nordbits AöR festgelegt.

Das IT-Sicherheitsmanagement wird durch den technischen Leiter der Nordbits AöR, die IT-Sicherheitsbeauftragte und die Datenschutzbeauftragte der Kreise sowie jeweils einen Vertreter der Kreisverwaltungen gebildet.

Die Aufgaben der Teilnehmerinnen und Teilnehmer des Sicherheitsmanagements sind im Konzept klar festgelegt. Das ULD hat die Regelungen geprüft und keine Rollenkonflikte festgestellt.

Das IT-Sicherheitsmanagement hat zielgruppenspezifische Schulungen zur IT-Sicherheit und zum Datenschutz durchgeführt. Das ULD hat die Schulungsinhalte und die Nachweise zur Durchführung der Schulung stichprobenartig überprüft.

Die IT-Sicherheitsbeauftragte unterrichtet alle Beschäftigten der Kreisverwaltungen und der Nordbits AöR durch Infobriefe zu aktuellen Themen der IT-Sicherheit.

Das IT-Sicherheitsmanagement tagt regelmäßig und dokumentiert die Ergebnisse der Sitzungen schriftlich. Das ULD hat die schriftlichen Nachweise der monatlich stattfindenden Sitzungen stichprobenartig geprüft und stellt eine regelmäßige und zielorientierte Befassung mit Fragen der IT-Sicherheit und des Datenschutzes fest.

2.4 Dokumentation der technischen und organisatorischen Sicherheitsmaßnahmen

Nordbits AöR orientiert sich bei der Auswahl angemessener technischer und organisatorischer Sicherheitsmaßnahmen an dem Grundschutzstandard des BSI.

Das Sicherheitsmanagement wirkt an der Erhebung und Pflege der Maßnahmenbearbeitung

mit. Die technischen und organisatorischen Maßnahmen werden im Grundschutztool des BSI dokumentiert.

Das ULD hat die Sicherheitsmaßnahmendokumentation stichprobenartig überprüft.

2.5 Anlassbezogene Kontrollen

Die IT-Sicherheitsbeauftragte führt anlassbezogene Kontrollen durch.

Die Ergebnisse der Kontrollen werden dem gemeinsamen Sicherheitsmanagement und den zuständigen Fachbereichsleitern der Auftraggeber mitgeteilt.

Die IT-Sicherheitsbeauftragte wirkt beratend und unterstützend an der Behebung erkannter Mängel mit. Die Mängelbearbeitung wird schriftlich dokumentiert. Das ULD hat die Bearbeitung einzelner Mängel stichprobenartig überprüft.

2.6 Regelmäßige Kontrollen

Die IT-Sicherheitsbeauftragte führt in eigener Planung regelmäßige Kontrollen durch. Darüber hinaus begleitet sie andere Kontrollprozesse zum Beispiel im Bereich Brandschutz und ergänzt sie durch eigene Kontrolltätigkeiten.

2.7 Integration von Datenschutz und Datensicherheit in die betrieblichen Prozesse

Das IT-Sicherheitsmanagement hat an den Migrationskonzepten zur Aufnahme des IT-Betriebs der Nordbits AöR mitgewirkt. Zusätzlich ist das IT-Sicherheitsmanagement an der jährlich fortgeschriebenen IT-Planung beteiligt. Alle wesentlichen Änderungen der IT-Infrastruktur werden mit dem IT-Sicherheitsmanagement abgestimmt.

2.8 Bearbeitung von Sicherheits- und Datenschutzvorfällen

Das Sicherheitsvorfallmanagement der Nordbits AöR und die Zusammenarbeit mit den Auftraggebern Schleswig-Flensburg und Nordfriesland ist in einer Rahmendienstanweisung festgelegt.

Die Dienstanweisung legt die Ansprechpartner und das konkrete Vorgehen zur Bearbeitung, Dokumentation und Nachbereitung von Sicherheitsvorfällen fest.

Sicherheitsvorfälle werden durch ein eigens hierfür festgelegtes Sicherheitsvorfallteam bearbeitet. Zu den festen Mitgliedern des Teams gehören die verantwortlichen Datenschutzbeauftragten, die IT-Sicherheitsbeauftragte und der technische Leiter der Nordbits. Das Team kann durch zusätzliche Mitglieder ergänzt werden.

Die schriftliche Nachbereitung von Sicherheitsvorfällen ist zwingend vorgeschrieben. Hierzu werden durch das Sicherheitsmanagement vordefinierte Meldebögen und Merkblätter bereitgestellt.

Das ULD hat die Dokumentation von Sicherheitsvorfällen und die schriftlichen Nachweise zur Bearbeitung der Sicherheitsvorfälle stichprobenartig geprüft.

3 Datenschutzrechtliche Bewertung

3.1 Prüfungsverlauf

Das Audit „**Implementierung eines gemeinsamen organisationsübergreifenden IT-Sicherheitsmanagements der Kreisverwaltungen Nordfriesland, Schleswig-Flensburg und Nordbits AöR**“ wurde vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) durchgeführt.

Zunächst hat das ULD im Rahmen eines Voraudits die Nordbits AöR bei der ordnungsgemäßen Implementierung des IT-Sicherheitsmanagements unterstützt. In mehreren Terminen vor Ort wurden gemeinsam mit dem IT-Sicherheitsmanagement die notwendigen Sicherheitsprozesse besprochen und deren Ausgestaltung festgelegt.

Das Voraudit wurde durch Herrn Heiko Behrendt durchgeführt.

Nach dem Voraudit wurden die für das IT-Sicherheitsmanagement erstellten Konzepte und Nachweise dem ULD zur Durchführung des Datenschutz-Behördenaudits übergeben. Die Überprüfung der Konzeption erfolgte auf Basis eines konsolidierten Dokumentenstands.

Das ULD hat die vorliegenden Dokumente auf die Vereinbarkeit mit den datenschutzrechtlichen Vorgaben gemäß Landesdatenschutzgesetz Schleswig-Holstein (LDSG) und der Datenschutzverordnung (DSVO) sowie auf die Erfüllung der Anforderungen des Grundschutzstandards geprüft.

In einem zweiten Schritt wurde vor Ort die Angemessenheit und Wirksamkeit der ordnungsgemäßen Implementierung der IT-Sicherheitsprozesse für das IT-Sicherheitsmanagement stichprobenartig überprüft. In diesem Zusammenhang wurde festgestellt, dass das gemeinsame IT-Sicherheitsmanagement die Umsetzung der notwendigen Sicherheitsmaßnahmen des IT-Verbundes der Kreise überwacht.

Das Auditverfahren wurde durch Herrn Sven Thomsen durchgeführt.

3.2 Bewertung

Im Auditverfahren wurde festgestellt, dass von der Nordbits und den Kreisverwaltungen Nordfriesland und Schleswig-Flensburg die datenschutzrechtlichen Anforderungen sowie die Vorgaben des Grundschutzstandards für die Implementierung eines gemeinsamen organisationsübergreifenden IT-Sicherheitsmanagements erfüllt werden. Das Sicherheitsmanagement orientiert sich an den Vorgaben des Standards 100-1 des BSI. In Bezug auf die Umsetzung von technischen und organisatorischen Maßnahmen folgt das IT-Sicherheitsmanagementsystem den Vorgaben der IT-Grundschutzvorgehensweise gemäß Standard 100-2 des BSI.

Darüber hinaus wurden bei der Durchführung des Audits folgende Aspekte festgestellt, die im Sinne einer **datenschutzkonformen und –fördernden Gestaltung von Technik und Organisation besonders hervorzuheben** sind:

1. Das IT-Sicherheitsmanagementsystem gewährleistet durch eine regelmäßige und nachhaltige Befassung mit den Themenkreisen Datenschutz und Datensicherheit ein hohes Gesamtsicherheitsniveau.
2. Die Sicherheitsprozesse sind unter Berücksichtigung eines anerkannten Sicherheitsstandards gestaltet.
3. Die technischen und organisatorischen Abläufe des IT-Sicherheitsmanagementsystems sind vollständig und nachvollziehbar beschrieben.
4. Die Datenverarbeitung wird unter den Aspekten der Verfügbarkeit, Vertraulichkeit, Integrität sowie der Ordnungsmäßigkeit in einer geregelten Aufbau- und Ablauforganisation überwacht.
5. Sicherheitsrelevante Ereignisse können über das IT-Sicherheitsvorfallmanagement rechtzeitig erkannt und nachvollziehbar bearbeitet werden.

Die Prüfung hat ergeben, dass die Implementierung des IT-Sicherheitsmanagementsystems keinen Anlass zu datenschutzrechtlichen Beanstandungen gibt. Durch stichprobenartige Kontrollen wurde festgestellt, dass eine konzeptkonforme Umsetzung erfolgt ist.

Kiel, 08. Dezember 2012 gez. Sven Thomsen

(Auditor)