Gutachten

Auditverfahren gemäß § 43 Abs. 2 LDSG

Informationssicherheits-Managementsystem für das Data Center Steuern

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Datum : 28.10.2010
Aktenz. : 16.01/10.005
Telefon : 0431 988 1200
Fax : 0431 988 1223
E-Mail : mail@datenschutzzentrum.de

Inhaltsverzeichnis

1 Gegenstand des Datenschutzaudits

Das Unabhängige Landeszentrum für Datenschutz (ULD) und Dataport haben vereinbart, dass das ULD die **Konzeption** für das „**Informationssicherheits-Managementsystem für das Data Center Steuern**“ in einem Datenschutzbehördenaudit gemäß § 43 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG) überprüft und bewertet.

Der Gegenstand des Audit umfasst das Konzept des **Informationssicherheits-Managementsystems** für das Data Center Steuern und das durch Dataport im Auftrag erstellte **Sicherheitskonzept für das Data Center Steuern**.

Vom Audit ausdrücklich nicht erfasst ist die korrekte Umsetzung der steuerrechtlichen Vorgaben in die im Data Center Steuern ablaufenden Verfahren. Diese liegen in der Verantwortung der zuständigen Steuerbehörden und nicht bei Dataport.

Ebenso nicht erfasst ist die korrekte Umsetzung aller in der Konzeption des Informationssicherheits-Managementsystems oder in dem Sicherheitskonzept des Data Center Steuern beschriebenen Maßnahmen. Es handelt sich um ein Konzeptaudit.

Die einzelnen Dokumente der Konzeption wurden inhaltlich im Rahmen des Datenschutzaudits auf die Konformität mit einzelnen Normen und rechtlichen Grundlagen überprüft. Die Wirksamkeit einzelner Maßnahmen wurde direkt vor Ort evaluiert, um bereits im Rahmen dieses Konzeptaudits Aussagen über die Umsetzbarkeit des Konzeptes zu erhalten.

2 Feststellung zu den sicherheitstechnischen Elementen des Informationssicherheits-Managementsystems

2.1 Vertragliche Vereinbarungen

Die Länder Bremen, Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein haben mit der Anstalt öffentlichen Rechts Dataport Verträge über die Erbringung von IT-Dienstleistungen für die Steuerverwaltung des jeweiligen Landes im Zusammenhang mit dem Betrieb des Data Center Steuern geschlossen. Der Beitritt des Landes Niedersachsen zum Data Center Steuern erfolgte nach der Konsolidierung der Konzeptunterlagen des Data Center Steuern und ist durch entsprechende Änderungsverträge und Ergänzungen berücksichtigt.

Die Grundlage der vertraglichen Vereinbarungen der jeweiligen Länder bildet ein Standardvertrag gemäß EVB-IT[1]. Dieser Vertrag wird durch Anlagen ergänzt, in denen dann spezifische Regelungen aufgenommen sind.

Der Vertrag enthält Regelungen, die gemäß § 17 LDSG für eine Datenverarbeitung im Auftrag notwendig sind. Es sind insbesondere Regelungen zu

- der Leistungsart und dem Leistungsumfang,
- den Rechten und Mitwirkungspflichten der Auftraggeber,
- den Rechten und Pflichten des Auftragnehmers,
- der Aufbau- und Ablauforganisation der Datenverarbeitung,
- dem Regelbetrieb sowie
- dem Sicherheitsmanagementsystem

schriftlich festgehalten.

Diese Regelungen sind in einzelne Servicescheine gegliedert, die die konkreten Vorgaben und Vereinbarungen zum sicheren Betrieb der steuerlichen Fachverfahren und zum Sicherheits- und Datenschutzmanagement enthalten. Unter anderem gibt es Servicescheine mit detaillierten Regelungen zu:

- „RZ-Infrastruktur“: Bereitstellung, Administration und Aktualisierung der zentralen HW- und SW-Ressourcen in baulich verstärkten, klimatisierten, versorgungs- und zutrittsgesicherten Räumen
- „Batch-Produktion“ und „Dialogbereitstellung“: Bereitstellung, Betrieb und Steuerung von Anwendungen und die anwendungsspezifische Bereitstellung und Haltung der

[1] Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik, herausgegeben durch den CIO des Bundes unter http://www.cio.bund.de/cln_102/DE/IT-Angebot/IT-Beschaffung/EVB-IT_BVB/

Daten

- „Test und Entwicklungsumgebung“: Bereitstellung und Betrieb eines Systems für die Verfahrensbetreuung (Testproduktion) und für die Entwicklung (Entwicklungsumgebung)
- „Nachverarbeitung“: Bereitstellung, Betrieb und Steuerung von Nachverarbeitungssystemen
- „IT-Sicherheit“: Sicherheitsmaßnahmen sowie Kontrollmechanismen für die Erbringung der in den Servicescheinen beschriebenen Dienstleistungen und
- „Service Desk / User Help Desk“: Bereitstellung eines einheitlichen Ansprechpartners bei Dataport für das Erfassen, Nachverfolgen, Berichten von Fehlermeldungen.

Neben den gesetzlichen und vertraglichen Grundlagen sind auf Seiten der Auftraggeberländer Regelwerke für IT-unterstützte Geschäftsprozesse in der jeweiligen Steuerverwaltung vorhanden, die durch das Sicherheitsmanagement und Datenschutzmanagement der jeweiligen Auftraggeber und des Auftragnehmers Dataport regelmäßig auf Vereinbarkeit mit den bestehenden vertraglichen Regelungen überprüft werden sollen.

Dataport verfügt über ein übergreifendes Sicherheitsmanagement und Datenschutzmanagement mit einem Regelwerk aus Sicherheitsleit- und -richtlinien (vgl. Abschnitte 2.10 und 2.11).

Die Vergabe von Unteraufträgen ist in Übereinstimmung mit den Vorgaben des § 17 LDSG geregelt: Auftraggeber und Auftragnehmer legen gemeinsam fest, welche Leistungen für eine Unterauftragsvergabe grundsätzlich in Betracht kommen. Werden Unteraufträge vergeben, so hat Dataport vertraglich sicherzustellen, dass die vereinbarten Regelungen, insbesondere die Kontrollmöglichkeiten durch die Auftraggeber beziehungsweise deren jeweils zuständigen Aufsichtsbehörden, auch gegenüber Subunternehmern gelten. Dataport ist verpflichtet, den Auftraggebern bestehende Unterauftragsverhältnisse anzuzeigen.

Zusätzlich ist im Vertrag festgelegt, dass Dataport alle mit der Leistungserbringung betrauten Mitarbeiterinnen und Mitarbeiter nach Maßgabe des Gesetzes über die förmliche Verpflichtung nicht beamteter Personen (Verpflichtungsgesetz) und den in Schleswig-Holstein hierzu erlassenen jeweils gültigen Ausführungsbestimmungen zur Verschwiegenheit in allen dienstlichen Angelegenheiten verpflichtet. Zusätzlich sichert Dataport zu, dass die einschlägigen rechtlichen Vorschriften der §§ 30 ff. der Abgabenordnung, der Steuerdatenabruf-Verordnung, der Steuerdaten-Übermittlungsverordnung, der Buchungsordnung für die Finanzämter, der Landeshaushaltsordnung und des Landesdatenschutzgesetzes in den jeweils geltenden Fassungen den mit der Verarbeitung von Steuerdaten betrauten Mitarbeitern bekannt sind.

Die vertraglichen Regelungen erfüllen die Anforderungen des § 17 LDSG.

2.2 Aufbau- und Ablauforganisation

Betrieb und Weiterentwicklung des Data Center Steuern sind bei Dataport in einer eigenen Organisationseinheit zusammengefasst. Durch Dataport-interne Vereinbarungen sind weitere Organisationseinheiten bei Dataport an der Leistungserbringung beteiligt.

Dataport hat die für den Betrieb des Data Center Steuern geltenden Regelungen und Vorgaben in einem Betriebskonzept zusammengefasst. Das Betriebskonzept enthält unter anderem grundlegende Aussagen

- zur RZ-Infrastruktur in Mecklenburg-Vorpommern,
- zur Standort- und Objektsicherheit, insbesondere zu den baulich-technischen Maßnahmen gegen unbefugten Zutritt, zum vorbeugenden Brandschutz, zur Klimatisierung und zur unterbrechungsfreien Stromversorgung,
- zu den eingesetzten IT-Systemen,
- zum Management des Produktionsbetriebes,
- zur Betriebsorganisation und
- zur Notfallvorsorge.

Die im Betriebskonzept getroffenen Regelungen in Verbindung mit dem Geschäftsverteilungsplan bei Dataport und den konkreten Aufgabenzuweisungen vor Ort ermöglichen es den Auftraggebern, die Anforderungen des § 3 Abs. 2 Punkt 5 DSVO i.V.m § 17 LDSG zu erfüllen.

2.3 Dokumentation des IT-Einsatzes im Data Center Steuern

Dataport pflegt eine Liste der für die Diensterbringung im Data Center Steuern genutzten IT-Systeme. Die Liste enthält unter anderem eine eindeutige Bezeichnung und den Standort des IT-Systems. Die Anforderungen des § 3 Abs. 2 Punkt 2 DSVO sind erfüllt.

Die Installations- und Konfigurationsdokumentation der Systeme und verwendeten Programme wurde vom ULD vor Ort stichprobenartig überprüft. Sie folgt den Vorgaben des Sicherheitskonzepts und den Dataport-internen Leitlinien zur Dokumentation. Die Anforderungen des § 3 Abs. 2 Punkt 3 DSVO sind erfüllt.

In der Dokumentation des Data Center Steuern werden mehrere Netzwerkpläne gepflegt, die sich im Detaillierungsgrad unterscheiden. Die Anforderungen des § 3 Abs. 2 Punkt 4 DSVO sind erfüllt.

Dataport hat für den Betrieb des Data Center Steuern ein dediziertes Betriebskonzept erstellt (vgl. Abschnitt 2.2). Die Anforderungen des § 3 Abs. 2 Punkt 5 DSVO sind erfüllt.

Für die Dokumentation administrativer Tätigkeiten soll die Administration über eine dedizierte Administrationsumgebung mit revisionssicherer Protokollierung (vgl. Abschnitt 2.7) durchgeführt werden. Die hierfür festgelegten technischen und organisatorischen Maßnahmen sind geeignet, die Anforderungen des § 3 Abs. 2 Punkt 6 DSVO zu erfüllen.

Die Dokumentation ist für sachkundige Personen in angemessener Zeit nachvollziehbar. Die Übereinstimmung der Dokumentation mit der konkreten Datenverarbeitung vor Ort wurde vom ULD stichprobenartig überprüft.

Die Dokumentation ist geeignet, die von den Auftraggebern als Daten verarbeitende Stellen im Sinne des LDSG zu führende Verfahrensdokumentation in großen Teilen zu ergänzen.

2.4 Sicherheitskonzept für das Data Center Steuern

Im EVB-IT-Vertrag ist in der Anlage „Serviceschein IT-Sicherheit“ vereinbart, dass Dataport in Abstimmung mit den Auftraggebern ein Konzept zur Wahrung des Steuergeheimnisses, des Datenschutzes und der IT-Sicherheit (kurz: Sicherheitskonzept) erstellt. In dem Konzept sollen die einzelnen organisatorischen, technischen, infrastrukturellen und personellen Maßnahmen sowie das verbleibende Restrisiko beschrieben werden. Änderungen an dem Konzept dürfen nur in Abstimmung mit den Auftraggebern erfolgen.

Dieses Konzept ist in zwei Teile gegliedert: Teil A und Teil B.

Der Teil A enthält allgemeine Vorgaben für die IT-Sicherheitskonzepte und umfasst

- Regelungen zur Vorgehensweise nach den IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie
- eine allgemeine Analyse des Schutzbedarfs und der Sicherheitsanforderungen bei der Auftragsdatenverarbeitung für die Steuerverwaltungen unter anderem in Schleswig-Holstein.

Der Teil B enthält die IT-Sicherheitskonzepte mit spezifischen Ausführungen

- zum Auditgegenstand,
- zur Risikoanalyse,
- zu an den Risiken orientierten technischen und organisatorischen Maßnahmen und
- zu den Restrisiken und deren Übernahme durch die Auftraggeber.

Einige der für das Auditverfahren wesentlichen Teile der Sicherheitskonzeption und des Datenschutzmanagements werden in den folgenden Abschnitten erläutert.

Das im Auftrag erstellte Sicherheitskonzept ist mit Ausnahme der vom Auftraggeber zu verantwortenden Bestandteile der konkreten steuerlichen Datenverarbeitung als Nachweis im Sinne des § 4 Abs. 7 DSVO i.V.m. § 17 LDSG geeignet.

2.5 Sicherheitskonzeption auf Infrastrukturebene

Dataport betreibt das Data Center Steuern an verschiedenen Standorten in Mecklenburg-Vorpommern.

Für die Sicherheit der Räume und Gebäude sind detaillierte Vorgaben und Nachweise vorhanden. Diese enthalten unter anderem Aussagen

- zum Zutritt zu Räumen für technische Infrastruktur,

- zum Zugriff auf Rechnersysteme, Netzwerkkomponenten und Speichersysteme,
- zur Klimatisierung und Brandschutz und
- zur Videoüberwachung der Gebäude.

Die Gefährdungsanalyse und Maßnahmenauswahl folgt dem Vorgehen gemäß BSI-Grundschutz. Die Vorgaben zur Umsetzung sind zusätzlich zu der Dokumentation gemäß Grundschutz-Vorgehensweise in automatisierter Form im GSTOOL in umfassenden und nachvollziehbaren Dokumenten festgehalten.

Die in den Konzepten durchgeführte Risikobetrachtung und Maßnahmenauswahl entspricht den Vorgaben des § 4 Abs. 1 bis 3 DSVO.

Das ULD hat die korrekte Umsetzung der Maßnahmen zur Raum- und Gebäudesicherheit stichprobenartig vor Ort überprüft.

2.6 Sicherheitskonzeption auf Systemebene

Die IT-Systeme des IT-Verbundes umfassen:

- Großrechnersysteme BS2000 und die den Systemen jeweils zugeordnete Speicherperipherie,
- IT-Systeme der mittleren Datentechnik und weitere allgemeine Serversysteme der Steuerdatenverarbeitung, Server mit den Betriebssystemen SuSE Linux und Microsoft Windows Server,
- Einrichtungen zur leitungs- und nicht leitungsgebundenen Datenübertragung sowie aktive Netzwerkkomponenten zur Verkehrslenkung und Netzsegmentierung (Firewalls, Router, Switches) und
- Arbeitsplatzrechner für Zwecke des Operatings und der Administration der Großrechnersysteme, der mittleren Datentechnik und der Netzwerkeinrichtungen.

Dataport hält für die Auftraggeber virtualisierte Test-, Entwicklungs- und Produktionsumgebungen bereit. Die Kapazitäten dieser Umgebungen sind so ausgelegt, dass die Anforderungen aller Auftraggeber bei Bedarf auch an einem Standort abgedeckt werden können. Hierfür werden bei Ausfall eines Standorts die Kapazitäten der Test- und Entwicklungssysteme mitgenutzt. Im Notfall stehen dann für Test- und Entwicklung keine Ressourcen zur Verfügung. Dieses Vorgehen im Notfall ist mit den Vorgaben des LDSG und der DSVO vereinbar.

Dataport betreibt die Systeme nach den Vorgaben der Auftraggeber. Im Rahmen des bundesweiten Entwicklungsverbunds für steuerliche Fachverfahren sind für die Konfiguration detaillierte Vorgaben erarbeitet worden.

Das ULD hat die korrekte Umsetzung der Vorgaben stichprobenartig überprüft.

Dataport betreibt diejenigen Systeme, für die die Auftraggeber keine konkreten Vorgaben gemacht haben oder die als administrative und operative Nebensysteme zur Erbringung der vertraglich vereinbarten Dienstleistungen genutzt werden, gemäß organisationsweit einheitlich geltenden Regelungen. Diese Regelungen sind in spezifischen Leitlinien für einzelne

Systeme schriftlich festgelegt.

Das ULD hat die Angemessenheit der Leitlinien und die wirksame Umsetzung stichprobenartig überprüft.

2.7 Sicherstellung und Kontrolle der Systemadministration

Administrative Änderungen an den Datenverarbeitungssystemen des Data Center Steuern sollen nur über eine hierfür bereitgestellte Administrationsumgebung erfolgen können. Der administrative Zugang zu den einzelnen Komponenten und Programmen des Data Center Steuern soll über Terminalserver kanalisiert werden, um eine revisionssichere Protokollierung und durchgängige Nachvollziehbarkeit administrativer Tätigkeiten sicherzustellen.

Der Zugriff auf die Administrationsumgebung soll durch eine 2-Faktor-Authentifizierung abgesichert werden. Diese umfasst zum einen den Username/Passwort-geschützten-Anmeldezugriff auf das System, zum anderen eine hardwarebasierte Lösung („Besitz und Wissen“)

Die Administration der Administrationsplattform soll durch eine eigene Organisationseinheit bei Dataport erfolgen, die wiederum keinen administrativen Zugriff auf die Systeme und Verfahren des Data Center Steuern erhält. Dieses soll verhindern, dass die Administratoren der Steuerverfahren sich selbst oder anderen zusätzliche administrative Zugriffsmöglichkeiten unter Umgehung der revisionssicheren Protokollierung ermöglichen können.

Die Bediensteten des Data Center Steuern werden nach Maßgabe erteilter Aufträge im Rahmen der ihnen übertragenen Aufgaben einzelnen administrativen Rollen mit spezifischen administrativen Berechtigungen zugeordnet. Unter anderem sind die folgenden Rollen eingerichtet:

- Systemadministration,
- Verfahrensadministration,
- System-Berechtigungsadministration und
- Verfahrens-Berechtigungsadministration.

Jede administrative Tätigkeit darf nur aufgrund eines Kundenauftrags erfolgen. Jede Tätigkeit muss gemäß Konzept von der Auftragserteilung bis zur -erledigung revisionssicher nachgewiesen werden. Hierzu müssen unter anderem über die Administrationsumgebung und durch Einsatz eines Ticketsystems administrative Tätigkeiten personenbezogen protokolliert und dokumentiert werden.

Für das Erstellen und das Verwenden der administrativen Protokolldaten sind die Zwecke datensparsam und konkret festgelegt:

- Sicherstellen der Betriebsbereitschaft von IT-Systemen und Diensten,
- Sicherstellen der Revisionsfähigkeit der Datenverarbeitung im Auftrag und
- Nachweisen der ordnungsgemäßen Auftragserfüllung durch die Administratoren.

Eine Protokollierung zu anderen Zwecken, insbesondere denen der automatisierten Verhaltens- und Leistungskontrolle, wird ausgeschlossen.

Die Protokolldaten müssen im Data Center Steuern für die Dauer von 180 Tagen / 6 Monaten gespeichert und danach gelöscht werden. Eine längerfristige Aufbewahrung bedarf eines hinsichtlich Zweck und Speicherart konkretisierten schriftlichen Auftrages durch eine berechtigte Person. Das Datenschutz- und Sicherheitsmanagement ist hierbei zu beteiligen.

Eine personenbezogene Auswertung der Protokolle darf nur durch dazu berechtigte Personen erfolgen. Die berechtigten Personen sind schriftlich festgelegt.

Die Protokollierung und Kontrolle administrativer Tätigkeiten ist geeignet, die Anforderungen des § 3 Abs. 2 Punkt 6 DSVO i.V.m. § 6 Abs. 2 LDSG zu erfüllen.

2.8 Sicherheitskonzeption auf Anwendungsebene

Im Data Center Steuern werden unter anderem die folgenden Anwendungen betrieben:

- die zentralen IT-Fachverfahren des EOSS-Verbundes zur Festsetzung und Erhebung der Veranlagungs-, Anmelde- und Einzelsteuern,
- die auf den assoziierten Servern eingesetzten Transaktionsmonitore für den Batch- und Dialogbetrieb auf der zentralen BS2000-IT-Systemplattform, Verfahren zur Verwaltung von Nutzern und Berechtigungen,
- IT-Fachverfahren des KONSENS-Verbundes (BIENE, ELFE, Elster, GINSTER) sowie
- Tools für Zwecke des Change- und Release Managements (OPTIK / PROGDOK / ESM).

Die IT-Fachverfahren für die Steuerverwaltungen im EOSS-Verbund werden weit überwiegend von der EOSS-Anwendungsentwicklung, die KONSENS-Produkte von den entwickelnden Ländern bereitgestellt. Aspekte der Verfahrenssicherheit und -integrität sind nicht Bestandteil des Informationssicherheits-Managementsystems bei Dataport. Diese Aspekte liegen in der Verantwortung der Auftraggeber und der von den Auftraggebern organisierten Entwicklungs-Partnerschaften.

Das ULD hat die Prozesse zum Change- und Releasemanagement stichprobenartig vor Ort geprüft.

Die im Rahmen des Change- und Releasemanagement anfallenden Protokolldaten und die seitens Dataport geführte Dokumentation sind geeignet, die Anforderungen des § 3 Abs. 2 Punkt 6 DSVO i.V.m. § 6 Abs.2 LDSG zu erfüllen.

2.9 Sicherheitsmanagement und Datenschutzmanagement für das Data Center Steuern

Für das Sicherheitsmanagement und Datenschutzmanagement des Data Center Steuern hat Dataport ein dediziertes Konzept erstellt. In diesem Konzept sind

- die Verantwortungsbereiche und Zuständigkeiten Dataports und der Auftraggeber,

- Rollen und Aufgaben im Sicherheitsmanagement bei Dataport und den Auftragnehmern sowie
- Schnittstellen, Kommunikationsbeziehungen und Eskalationswege bei Sicherheitsvorfällen

beschrieben und festgelegt.

Das Sicherheitsmanagement ist für die Überwachung einer ordnungsgemäßen und sicheren Datenverarbeitung verantwortlich. Die Aufgaben des Sicherheitsmanagements sind aufbau- und ablauforganisatorisch klar zugewiesen. Die für Datenschutz zuständigen Vertreter der Auftraggeber und bei Dataport sind Mitglieder des Sicherheitsmanagements für das Data Center Steuern.

Im Konzept sind regelmäßige Sitzungen einer gemeinsamen Arbeitsgruppe festgeschrieben. Die Durchführung von Audits und die Mitwirkung bei Planungen von IT-Revisionen sind festgelegt. Das Sicherheitsmanagement erstellt eine abgestimmte Jahresplanung für die durchzuführenden Kontrollen.

Das Sicherheitsmanagement führt bei Sicherheitskonflikten (andauernde Abweichungen zwischen der im Sicherheitskonzept und der Sicherheitsdokumentation beschriebenen Vorgehensweise und den tatsächlichen Abläufen im Regelbetrieb) eine gemeinsame Abstimmung herbei und erarbeitet Vorgaben für das Beheben dieser Konflikte.

Sicherheitsvorfälle (Ereignisse, die im Widerspruch zu den dokumentierten Sicherheitszielen und Sicherheitsgrundsätzen stehen, oder Ereignisse, durch die nach Einschätzung der Mitarbeiterinnen und Mitarbeiter Belange der IT-Sicherheit berührt werden) werden durch das Sicherheitsmanagement bearbeitet.

2.10 Übergreifendes Datenschutzmanagement bei Dataport

Dataport hat das interne, übergreifende Datenschutzmanagement in einer Datenschutz-Leitlinie und in einem IT-Sicherheits- und Datenschutz-Managementhandbuch beschrieben.

Die Leitlinie und das Managementhandbuch sind Bestandteil der Dokumentation und Konzeption des Data Center Steuern und werden in den spezifischen Dokumenten referenziert.

Gemäß § 10 LDSG bestellter Datenschutzbeauftrager ist Herr Ulrich Meyer.

Das ULD hat die auf den Auditgegenstand anwendbaren Regelungen stichprobenartig überprüft.

2.11 Übergreifendes Sicherheitsmanagement bei Dataport

Das übergreifende Sicherheitsmanagement ist Bestandteil des Auditverfahrens „Dataport Informationssicherheits-Managementsystem (ISMS)“ (Audit 17/2007). Das Kurzgutachten ist auf den Webseiten des ULDs abrufbar[2].

[2] https://www.datenschutzzentrum.de/audit/kurzgutachten/a0717/a0617.pdf

3 Datenschutzrechtliche Bewertung

3.1 Prüfungsverlauf

Das Konzeptaudit „**Informationssicherheits-Managementsystems für das Data Center Steuern**“ wurde vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) über mehrere Phasen durchgeführt.

In der ersten Phase (Voraudit) hat das ULD Dataport durch die Prüfung und Bewertung einzelner Dokumente und Konzepte unterstützt. In mehreren Terminen vor Ort wurden gemeinsam mit Dataport die notwendigen Regelungen und Nachweise besprochen und deren Ausgestaltung festgelegt.

Das Voraudit wurde durch Herrn Dr. Martin Meints, zu der Zeit Mitarbeiter im Projektreferat des ULD, durchgeführt. Dr. Meints hat nach Abschluss des Voraudits seine Tätigkeit im ULD beendet und ist zu Dataport gewechselt. Er hat dort die Rolle des Sicherheitsbeauftragten übernommen. Das ULD hat nach dem Wechsel von Dr. Martin Meints das Vorgehen im Audit auf mögliche Interessenskonflikte und Einflüsse auf die Unabhängigkeit des Auditverfahrens überprüft. Nach intensiver Prüfung der vorliegenden Ergebnisprotokolle und des Schriftverkehrs mit Dataport kommt das ULD zu dem Schluss, dass im Rahmen des Voraudits keine Beeinträchtigung der Unabhängigkeit des ULD vorliegt.

Nach dem Voraudit wurden die Konzepte und Nachweise dem ULD zur Durchführung des Datenschutz-Behördenaudits übergeben. Die Überprüfung der Konzeption erfolgt 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) geprüft.

Das ULD weist darauf hin, dass durch dieses Datenschutzaudit die Vereinbarkeit mit Gesetzen und Regelungen anderer Bundesländer, insbesondere der anderen Auftraggeber des Data Center Steuern, nicht geprüft wurde und in diesem Auditverfahren auch keine Aussagen hierzu getroffen werden.

Nach der Dokumentenprüfung hat das ULD in einem Termin vor Ort die Angemessenheit und Wirksamkeit einer Auswahl der in den vorliegenden Dokumenten dargestellten Sicherheitsmaßnahmen stichprobenartig überprüft. Das ULD hat sich durch diese Prüfungen vergewissert, dass die im Konzept dargestellten Maßnahmen von Dataport auch umgesetzt werden können.

Das ULD weist darauf hin, dass mit diesem Auditverfahren die konzeptkonforme Umsetzung nicht nachgewiesen wird. Das ULD geht jedoch auf Basis der vor Ort durchgeführten Stichproben davon aus, dass Dataport in der Lage ist, eine konzeptkonforme Umsetzung zeitnah herbeizuführen.

Das Auditverfahren wurde durch Herrn Sven Thomsen, Leiter des technischen Referats im ULD, durchgeführt.

3.2 Rechtliche Anforderungen

Das **Landesdatenschutzgesetz** sowie die **Datenschutzverordnung** finden neben den bereichsspezifischen Vorschriften Anwendung sowohl bei den Auftraggebern in Schleswig-Holstein als auch bei Dataport.

Die automatisierte Verarbeitung personenbezogener Daten erfordert technische und organisatorische Maßnahmen, die die Datensicherheit bzw. die Ordnungsmäßigkeit der Datenverarbeitung gewährleisten. Ein angemessenes IT-Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgaben sind im Informationssicherheits-Managementsystem für das Data Center Steuern zusammengefasst.

Dabei sind insbesondere folgende Rechtsvorschriften zu beachten:

Landesdatenschutzgesetz (LDSG)

§ 4 Datenvermeidung und Datensparsamkeit

§ 5 Allgemeine Maßnahmen zur Datensicherheit

§ 6 Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

§ 7 Verfahrensverzeichnis, Meldung

§ 8 Gemeinsame Verfahren und Abrufverfahren

§ 17 Verarbeitung personenbezogener Daten im Auftrag, Wartung

Datenschutzverordnung (DSVO)

§ 3 Verfahrensdokumentation

§ 4 Dokumentation der Sicherheitsmaßnahmen

§ 5 Dokumentation des Tests und der Freigabe

Darüber hinaus sind interne Regelungen über die personelle und organisatorische Gestaltung der Datensicherheit zu treffen. Es muss gewährleistet sein, dass die datenschutzrechtlichen Anweisungen auch tatsächlich in konkrete Datensicherungsmaßnahmen umgesetzt werden und ihre Einhaltung durch das Informationssicherheits-Managementsystem kontrolliert wird.

Nach Art. 33 IV Grundgesetz (GG) ist die Ausübung hoheitsrechtlicher Befugnisse i.d.R. Angehörigen des öffentlichen Dienstes zu übertragen, die in einem öffentlichen Dienst- und Treueverhältnis stehen. Zu diesem Personenkreis gehören Amtsträger, d.h. insbesondere Beamte i.S.d. § 11 Abs. 1 Nr. 2 Strafgesetzbuch (StGB), und für den öffentlichen Dienst be-

sonders Verpflichtete i.S.d. § 11 Abs. 1 Nr. 4 StGB. Die Verpflichtung erfolgt in einem förmlichen Akt auf Grundlage des Gesetzes über die förmliche Verpflichtung nicht beamteter Personen (Verpflichtungsgesetz) i.d.F. des Änderungsgesetzes vom 15. August 1974, Bundesgesetzblatt I S. 1942.

Nach Art. 108 Abs. 2 GG kann der Aufbau der Landesfinanzverwaltung durch Bundesgesetz geregelt werden. Dies ist durch das Finanzverwaltungsgesetz (FVG) geschehen. Der Aufbau, Aufgaben und Zuständigkeiten der Landesfinanzverwaltung ergeben sich aus § 2 ff. FVG. Nach § 20 Abs. 2 FVG können die Länder dabei technische Hilfstätigkeiten durch automatische Einrichtungen eines anderen Bundeslandes oder anderer Verwaltungsträger verrichten lassen.

Dataport als Anstalt des öffentlichen Rechts erfüllt die Voraussetzungen eines solchen anderen Verwaltungsträgers. Gem. § 3 Abs. 2 S.1 des Staatsvertrages zur Änderung des Staatsvertrages zwischen dem Land Schleswig-Holstein und der Freien und Hansestadt Hamburg über die Errichtung von Dataport als rechtsfähige Anstalt öffentlichen Rechts erbringt Dataport IuK-Dienstleistungen für die Bundesländer Schleswig-Holstein, Hamburg, Mecklenburg-Vorpommern, Bremen und zukünftig auch Niedersachsen. Es handelt sich sowohl beim eigentlichen Betrieb der Großrechner und anhängiger Systeme als auch bei der Erstellung der hierfür notwendigen Sicherheitskonzepte und der Durchführung des Sicherheitsmanagements um Hilfstätigkeiten gemäß § 20 Abs. 2 FVG.

3.3 Zusammenfassende Bewertung

Im Auditverfahren für das Konzept „**Informationssicherheits-Managementsystem für das Data Center Steuern**“ wurde festgestellt, dass Dataport über eine rechts- und normenkonforme Konzeption verfügt, die die Kernelemente des Informationssicherheits-Managementsystems aufbau- und ablauforganisatorisch beschreibt und praxistauglich umgesetzt werden kann. Dataport ist beauftragt, wesentliche Teile des Sicherheitsmanagements und des Datenschutzmanagements für das Data Center Steuern durchzuführen.

Das Datenschutz- und Sicherheitsmanagement orientiert sich an internationalen Standards. Insbesondere folgt das Informationssicherheits-Managementsystem den Vorgaben des Standards 100-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI). Auf Ebene der technischen und organisatorischen Maßnahmen folgt das Informationssicherheits-Managementsystem mit den Vorgaben der IT-Grundschutz-Vorgehensweise gemäß Standard 100-2 des BSI und den Grundschutz-Katalogen.

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 Informationsicherheits-Managementsystem des Data Center Steuern gewährleistet durch eine dauerhafte Befassung mit den Themenkreisen Datenschutz und Datensicherheit ein hohes Gesamtsicherheitsniveau.
2. Das Informationsicherheits-Managementsystem und die Sicherheitskonzeption bietet

den Auftraggebern des Data Center Steuern eine belastbare Grundlage für eine eigene Sicherheitskonzeption und eigene interne sowie externe Prüf- und Auditverfahren.

3. Die Datenverarbeitung wird unter den Aspekten der Verfügbarkeit, Vertraulichkeit, Integrität sowie der Ordnungsmäßigkeit in einer geregelten Aufbau- und Ablauforganisation überwacht.
4. Die Sicherheitsprozesse sind unter Berücksichtigung eines national anerkannten Sicherheitsstandards gestaltet.
5. Sicherheitsrelevante Ereignisse können über das IT-Sicherheitsvorfallmanagement rechtzeitig erkannt werden.
6. Die technischen und organisatorischen Abläufe des Informationssicherheits-Managementsystems sind vollständig und nachvollziehbar beschrieben.

Die Prüfung hat ergeben, dass die zum Konzept gehörenden Dokumente des Informationssicherheits-Managementsystems keinen Anlass zu datenschutzrechtlichen Beanstandungen geben. Durch stichprobenartige Kontrollen wurde festgestellt, dass eine konzeptkonforme Umsetzung bereits größtenteils erfolgt ist.

Kiel, 28. Oktober 2010

(Auditor: Sven Thomsen)