

Gutachten zum Datenschutzaudit

„Zutrittsberechtigungssystem und Videoanlage für das Landeshaus Kiel“

Reauditierung hinsichtlich des Audits 07/2004
vom 23. September 2004 und Neuauditierung der
Videoüberwachungsanlage

28. August 2006

Inhaltsverzeichnis

A.	Gegenstand des Audits	- 4 -
B.	Gegenstand der Begutachtung	- 4 -
C.	Bewertung	- 4 -
I.	Darstellung der Datenschutzziele	- 4 -
1.	Aufbau	- 4 -
a)	Zutritts- und Zufahrtskontrollsystem der Tiefgarage	- 5 -
(i)	Aufbau	- 5 -
(ii)	Nordtor	- 5 -
(iii)	Südtor	- 6 -
(iv)	Funkfernsteuerung	- 6 -
b)	Video-Anlage	- 6 -
(i)	Aufbau der Anlage	- 6 -
(ii)	Kameras	- 7 -
(iii)	Sichtbereiche	- 7 -
(iv)	Bewegungserkennung und Alarmer	- 7 -
(v)	Beobachtungssystem	- 8 -
(vi)	Speicherung der Aufnahmen	- 9 -
(vii)	Abruf und Auswertung gespeicherter Aufnahmen	- 10 -
(viii)	Zugriff auf gespeicherte Bilder	- 10 -
(ix)	Herausgabe gespeicherte Bilder an Dritte	- 11 -
II.	Datenschutzrechtliche Zulässigkeit	- 11 -
1.	Zutritts- und Zufahrtskontrollsystem der Tiefgarage	- 11 -
2.	Video-Anlage	- 11 -
a)	Rechtsgrundlage	- 12 -
b)	Videoüberwachung	- 12 -
c)	Videoaufzeichnung	- 15 -
III.	Technisch-Organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit	- 17 -
1.	Bestandsaufnahme	- 17 -
a)	Hardware	- 17 -
(i)	Videoanlage (neu aufgenommen)	- 17 -
(ii)	Hardware Zutrittskontrolle Tiefgarage	- 17 -
(iii)	Veränderungen an bestehender Hardware	- 18 -
b)	Vernetzung	- 18 -
(i)	Vernetzung der Videoanlage	- 18 -
(ii)	Änderungen und Ergänzungen der Vernetzung	- 18 -
c)	Software	- 19 -
(i)	Software in Zusammenhang mit der Videoanlage	- 19 -
(ii)	Ergänzungen und Veränderungen an bestehender Software des Zutrittberechtigungssystems	- 20 -
d)	Datenbestände und Kommunikation	- 20 -
e)	Regelungen	- 20 -
(i)	Nutzungsrechte	- 20 -
(ii)	Nutzerauthentisierung:	- 21 -
(iii)	Protokolldaten:	- 21 -
(iv)	Datensicherung:	- 21 -
(v)	Arbeitsanweisungen	- 21 -
2.	Verfahrensdokumentation nach § 3 DSVO	- 22 -
a)	Verfahrenszweck nach § 4 DSVO	- 22 -

b)	Verfahrensbeschreibung nach § 5 DSVO	- 22 -
c)	Sicherheitskonzept nach § 6 DSVO	- 22 -
d)	Risikoanalyse	- 23 -
e)	Test und Freigabe	- 23 -
f)	Verfahrensübergreifende Dokumentation und Protokolle nach § 8 DSVO	- 24 -
IV.	Datenschutzmanagementsystem.....	- 24 -
1.	Darstellung des Datenschutzmanagementsystems	- 24 -
2.	Bewertung Datenschutzmanagementsystem	- 25 -
V.	Bewertung	- 26 -

A. Gegenstand des Audits

Gegenstand des Audits sind das Zutrittsberechtigungssystem des Landeshauses, Düsternbrooker Weg 70 und des Gebäudes Karolinenweg 1 in Kiel sowie die Videoüberwachung dieser Gebäude, der zum Landeshaus gehörenden Tiefgarage und des Parkhauses Reventlouallee, Kiel.

Am 23.9.2004 wurde das Zutrittsberechtigungssystem des Landtages Schleswig-Holstein auditiert. Grundlage für diese Auditierung war das Konzept „Landeshaus Kiel, Zutrittsberechtigungssystem“ Dieses Konzept wird laufend fortgeschrieben.

In einer solchen Fortschreibung wurde das Konzept um ein Videoüberwachungssystem ergänzt, das die Außenhülle des Landtagsgebäudes umfasst. Eine weitere Ergänzung betrifft das Zutritts- und Zufahrtskontrollsystem der Tiefgarage sowie die Videoüberwachung der Tiefgarage und des Parkhauses Reventlouallee. Im vorliegenden Auditverfahren werden diese neuen Komponenten erstmalig auditiert und das Zutrittsberechtigungssystem (ZBS) reauditiert. Die Reauditierung umfasst den Echtbetrieb des ZBSs und die Umsetzung der Datenschutzziele, die bei der Erstauditierung des ZBS im Konzeptstadium 2004 aufgestellt worden waren. Beide Auditergebnisse werden zu einem gemeinsamen Audit zusammengefasst.

B. Gegenstand der Begutachtung

- Feinkonzept „Landeshaus Kiel, Zutrittsberechtigungssystem und Videoanlage“, Version 249 vom 15.9.2005
- Dienstanweisung für die mit dem Zutrittsberechtigungssystem des Schleswig-Holsteinischen Landtages befassten Mitarbeiterinnen und Mitarbeiter , 19. April 2006
- Datenschutzmanagementsystem für die Videoanlage im Zutrittsberechtigungssystem (ZBS) des Schleswig-Holsteinischen Landtages, 17.08.2006

C. Bewertung

I. Darstellung der Datenschutzziele

1. Aufbau

Das Zutrittskontrollsystem des Landeshauses und des Gebäudes Karolinenweg ist im Gutachten vom 22.9.2004 ausführlich beschrieben. Dieser Abschnitt beschreibt die inzwischen erfolgten Veränderungen und Ergänzungen.

a) Zutritts- und Zufahrtskontrollsystem der Tiefgarage

(i) Aufbau

Die Tiefgarage ist in das Zutrittskontrollsystem des Landeshauses eingebunden. Dies umfasst sowohl die Türen für das Betreten der Tiefgarage als auch die Tore zum Befahren der Garage. Zu unterscheiden ist dabei zwischen Türen, die vom Freigelände in die Tiefgarage führen und dem Verbindungsgang zwischen Tiefgarage und Landeshaus.

Die Türen vom Freigelände in das Innere der Tiefgarage sind gewöhnliche Türen, die sich von außen erst nach dem Nachweis der Zutrittsberechtigung mit Hilfe einer Chipkarte öffnen lassen. Diese schaltet einen elektro-mechanischen Türöffner frei. Von innen lassen sie sich mechanisch durch Bedienung des Drückers, ohne Nachweis einer Berechtigung, öffnen.

Die Tür im Verbindungsgang zwischen Tiefgarage und Landeshaus ist, ähnlich wie der Zugang am Eingangsportal, als Vereinzelungsanlage ausgelegt. Der Zugang von der Tiefgarage in das Landeshaus ist nur mit der entsprechenden Berechtigung möglich, der Zugang vom Landeshaus in die Tiefgarage erfordert keinen Berechtigungsnachweis.

Die Garageneinfahrten zum Befahren der Tiefgarage werden ebenfalls kontrolliert. Hierbei ist zwischen Nord- und Südtor zu unterscheiden.

(ii) Nordtor

Das Nordtor wird von Dienstfahrzeugen, von Parkberechtigten sowie von Menschen mit Behinderungen genutzt.

Die Einfahrt in die Tiefgarage ist durch zwei Schranken als KFZ-Vereinzelungsanlage ausgelegt. Die zweite Schranke ist mit einem Rolltor gekoppelt, das sich parallel zur Schranke öffnet und schließt. Eine Einfahrt in die Schleuse ist nach erfolgreicher Berechtigungsprüfung durch das ZBS möglich. Eine Gegensprechanlage mit Videoübertragung ist mit der Pförtnerlei verbunden, die die erste Schranke auch manuell öffnen kann.

Die Ausfahrt aus der Tiefgarage ist durch ein Rolltor geschützt. Dieses Rolltor ist mit dem ZBS gekoppelt und erfordert auch bei der Ausfahrt eine Berechtigungsprüfung. Für Problemfälle ist innerhalb der Tiefgarage eine Gegensprechstelle mit der Pförtnerlei verbunden, die das Tor manuell öffnen kann.

Dienstfahrzeuge verfügen neben einer Chipkarte für das ZBS über einen Handfunksender, der eine Öffnung der Schranken bzw. des Tores auch mit Hilfe einer Funkfernsteuerung erlaubt (s. Abschnitt Funkfernsteuerung).

Menschen mit Behinderung können mit Hilfe der Funkfernsteuerung das Ausfahrtstor des Nordtores öffnen, um in die Tiefgarage zu Fuß oder im Rollstuhl zu gelangen oder diese zu verlassen. In diesem Fall sperrt eine Ampelsteuerung die Ausfahrt von Autos aus der Tiefgarage.

(iii) Südtor

Die Garageneinfahrt Süd wird ausschließlich von Dienstfahrzeugen und Radfahrern genutzt. Für Radfahrer steht eine Drehflügeltür mit elektro-mechanischem Antrieb zur Verfügung, die an das ZBS gekoppelt ist und für die Öffnung von außen eine Berechtigungsprüfung erfordert. Von innen kann die Tür von Hand (Klinke) oder mechanisch durch Betätigung eines Schalters geöffnet werden; eine Berechtigungsprüfung beim Verlassen der Tiefgarage erfolgt nicht.

Das Rolltor kann zur Einfahrt von Dienstfahrzeugen mit Hilfe des Handfunksenders geöffnet werden.

(iv) Funkfernsteuerung

Die Funkfernsteuerung verfügt über 6 Kanäle, die von Dienstfahrzeugen und Menschen mit Behinderungen genutzt werden können. Einzelne Kanäle und damit zugeordnete Funktionen für die Öffnung von Toren werden anhand eines Berechtigungsprofils vergeben, das in Abschnitt 15.1.1.6 des Konzepts beschrieben wird. Es können die erste Schranke der Vereinzelungsanlage für die Einfahrt des Nordtors, das Ausfahrtrolltor des Nordtors, die Schranke an der oberirdischen Parkplatzanlage Nord sowie das Tor der Garageneinfahrt Süd gesteuert werden. Zwei weitere Steuerungsmöglichkeiten der Funkfernsteuerung erlauben eine durchgängige Öffnung der Schleuse des Nordtors für eine ungehinderte Einfahrt sowie das Öffnen der Ausfahrt des Nordtores für Menschen mit Behinderungen (siehe Abschnitt Nordtor).

b) Video-Anlage

(i) Aufbau der Anlage

Die Videoanlage besteht aus mehreren Komponenten:

- stationären Farbkameras, ..., einschließlich Beleuchtung
- schwenkbare Kameras ..., die manuell oder automatisch gesteuert werden können
- stationäre Kameras ...
- Bildsprechanlagen ...
- Detektionsverfahren, die Veränderungen auf den Videobildern erkennen und Alarmierungen auslösen, Beleuchtungen aktivieren, Aufzeichnungen starten und die beweglichen Kameras steuern
- Aufzeichnungsanlage für mehrtägige Aufzeichnungen incl. Software zum Auslesen
- Monitore zur Betrachtung von Live-Bildern in der Pförtnerlei
- Steuereinrichtungen zum Schwenken der Kameras
- Monitoren und Steuersoftware zum Abruf gespeicherter Bilder in den Referaten L12 und L13.

Die Bildsprechanlagen innerhalb des Landeshauses (...) sind nicht in die Videoanlage integriert. Die Kameras und ihre Standorte sind in Abschnitt 8.1.1.7 des Konzepts genau bezeichnet, dort ist in einer Übersicht auch angegeben, ob und wie lange eine Aufzeichnung erfolgt.

(ii) Kameras

Außenfassade

Das Kernstück der Videoanlage bilden die stationären und beweglichen Kameras an der Außenfassade des Landeshauses sowie auf ... der Freifläche zwischen Plenarsaal und Hindenburgufer. ...

Ausrichtung und Brennweite der schwenkbaren Kameras können manuell mittels Bedienpulten ... gesteuert werden.

Im Eingangsportal gibt es ... weitere stationäre Kameras. Die ... des Gebäudes Karolinenweg wird ... überwacht.

Innenbereiche

In den Innenbereichen des Landeshauses gibt es Kamerainstallationen ...

Tiefgarage und Parkhaus Reventlouallee

In der Tiefgarage sind ... stationäre Kameras installiert, die Ein- und Ausfahrtsbereiche der Tiefgarage ... sowie die Parkplätze für Frauen und ... überwachen. In der Stele im Einfahrtsbereich, in der das ZBS installiert ist, ist ebenfalls eine Kamera eingebaut. Im Parkhaus Reventlouallee werden die Frauenparkplätze ... überwacht. ...

Weitere Kameras

Weitere Kameras, die an die Videoanlage angeschlossen sind, beobachten das Portal und den Nebeneingang des Gebäudes Karolinenweg ... sowie

(iii) Sichtbereiche

Die Sichtbereiche der stationären Kameras werden durch den Montageort und die Ausrichtung bei der Montage festgelegt. Die Kamerastandorte und die zugehörigen Sichtbereiche sind in einem Konzept dokumentiert.

Der Neigungswinkel der schwenkbaren Kameras ist durch die interne Software begrenzt. So ist es beispielsweise nur möglich, die Fensterfront der Gebäude am Düsternbrooker Weg, die dem Landeshaus gegenüber liegen, in der Totale zu beobachten. Ein Heranzoomen ist nicht möglich. Einzelheiten etwa zur Identifikation einzelner Personen hinter den Fensterscheiben, sind nicht erkennbar...

(iv) Bewegungserkennung und Alarmer

Die stationären Kameras können durch Bildvergleiche eine Veränderung des aktuell aufgenommen Bildes (Bildveränderungen) detektieren. Diese Detektion erfolgt mit Hilfe so

genannter Videosensoren. Es kann konfiguriert werden, ab welchen Grad an Veränderung (Prozent der geänderten Pixel) eine Detektion erfolgen soll (Empfindlichkeit der Detektion).

An der überwiegenden Zahl der stationären Kameras im Außenbereich sind auch Infrarotteleskope vorhanden (...), die eine Änderung der Wärmestrahlung detektieren können.

Eine Detektion einer Bewegung wird wie folgt verarbeitet:

- Sind an den Standorten der stationären Kameras auch schwenkbare Kameras vorhanden (...), so wird die schwenkbare Kamera automatisch auf den Ort der Bewegung gerichtet.
- Werden an den Kameras der Außenfassade gleichzeitig Bewegung und Änderung der Wärmestrahlung detektiert, so wird ein „Alarmbild“ (siehe unten) in der Pförtnerlei aufgeschaltet. „Aufschaltung eines Alarmbildes“ bedeutet, dass das Bild der detektierenden Kamera großformatig auf einem der Monitore in der Pförtnerlei angezeigt wird.
- Werden an den Kameras im Innenbereich des Landeshauses (...) Bewegungen detektiert, so wird ein „Alarmbild“ aufgeschaltet.

Diese Funktion des Aufschaltens eines Alarmbildes ist ... Uhr aktiviert.

(v) Beobachtungssystem

Alle Videoaufnahmen laufen in einem zentralen System zusammen. Zur Beobachtung und Auswertung sind verschiedene Systeme installiert:

- im Bereich der Pförtnerlei und der Polizei-Arbeitsplätze
- im Bereich der Landtagsverwaltung (Referate L 12 und L13)
- zwei Monitore in den Treppenhäusern

Ein weiterer Monitor im Videoschrank ..., in dem die gesamten Videoinformationen zusammenlaufen, dient der Steuerung der Hard- und Software der Videoanlage. Auf ihm können auch Videobilder sichtbar gemacht werden.

Es gibt drei Arten der Betrachtung von Videoaufnahmen:

- Beobachtung von Live-Aufnahmen aller Kameras, Steuerung der schwenkbaren Kameras und Überwachung von Alarmen
- Abruf gespeicherter Videobilder
- Beobachtung einzelner Eingangsbereiche

Jedes Beobachtungs- und Auswertungssystem dient einem anderen Zweck. Im folgenden Abschnitt werden die Systeme und die Beobachtungszwecke beschrieben.

Pförtnerlei

In der Pförtnerlei stehen insgesamt ... Monitore für Pförtner und Polizei zur Verfügung, je .. pro Arbeitsplatz. Diese werden wie folgt eingesetzt:

- ... zur Beobachtung mit den schwenkbaren Kameras, die durch das Bedienpult gesteuert und auf den Monitor geschaltet werden (...)
- ... zur Darstellung einer einstellbaren Reihenfolge von Kamerabildern im Ringverfahren (zeitverzögerter Wechsel), die einen „virtuellen Rundgang“ erlauben,

- ..., die jeweils in Split-Darstellung das aktuelle Alarmbild und ... weitere Kamerabilder in Kleinformat zeigen
- ... zur Nutzung mit der Software ..., die dem Benutzer eine freie Zusammenstellung von Kamerabildern in einer Splitdarstellung oder einen Vollbildmodus erlaubt.

Arbeitsplätze in der Landtagsverwaltung

Die Arbeitsplätze in den Referaten L12 und L13 der Landtagsverwaltung dienen dem Abruf von gespeicherten Aufnahmen sowie der Konfiguration der Anlage. Daneben können alle aktuellen Kamerabilder auf den Arbeitsplätzen sichtbar gemacht werden, zum einen als Vollbild, zum anderen als Split-Bild (gleichzeitige verkleinerte Darstellung mehrere Bilder).
...

Treppenhäuser

Die Monitore in den Treppenhäusern ... zeigen in einer Split-Darstellung ... aktuelle Kamerabilder:

(vi) Speicherung der Aufnahmen

Der überwiegende Teil der Kameras ist an ... Bildrekorder angeschlossen, die die Aufnahmen speichern. Die Bildrekorder arbeiten dabei parallel und zeichnen die Bild auf mehrere Spuren auf. Lediglich die Kameras ... werden nicht aufgezeichnet.

Der Bildrekorder verfügt über eine Funktion, die die Aufzeichnung erst bei der Detektion einer Bewegung, d.h. Änderung des Bildes, startet. Für einen Teil der Kameras (...) ist diese Funktion zumindest zeitweise aktiviert (8.2.2.3).

Eine Speicherung ist wie folgt konfiguriert:

- dauerhafte Speicherung alle Kamerabilder in der Zeit ...
- Speicherung nach „Alarmbildern“ während der übrigen Zeit (bei Erkennung einer Bewegung wird die Aufzeichnung gestartet; sie wird beendet, wenn ... Minuten keine Bewegung mehr erfolgt).

Die Aufnahmen werden in einem so genannten Ringspeicher gespeichert, in dem Aufnahmen mit festgelegtem Alter überschrieben werden. Die Speicherdauer kann kameraindividuell festgelegt werden. Als Speicherzeit ist in den allermeisten Fällen ... Tage konfiguriert; lediglich die Aufnahmen der Kameras im Gebäudeinneren (...) sowie der Kameras im Parkhaus Reventlouallee werden ... Tage gespeichert. Geplant ist, im Rahmen eines Kameraaustausches die Speicherzeit der Kameras an die der übrigen Kameras in den Parkanlagen anzugleichen

Die Qualität der gespeicherten Videosequenzen und ihr Platzbedarf hängen von der Anzahl der Bilder ab, die pro Sekunde aufgezeichnet werden. Das Konzept sieht vor, dass ... Bilder pro Sekunde aufgezeichnet werden. ... Der im Konzept geforderte Wert wird zeitnah umgesetzt.

(vii) Abruf und Auswertung gespeicherter Aufnahmen

Zum Abruf der gespeicherten Aufnahmen dient die Software Diese Software ist in den Arbeitsplätzen in den Referaten L12 und L13 sowie in der Pfortnerei (Pfortner- und Polizeiarbeitsplatz) installiert. Neben dem Abruf gespeicherter Aufnahmen können aktuelle Bilder (Live-Bilder) als Split-Darstellung und im Vollbild betrachtet werden; es ist eine beliebige Auswahl der Kameras und eine beliebige Zusammenstellung der Split-Aufnahmen möglich.

Das Konzept (8.4.3.2) sieht vor, dass auf gespeicherte Aufnahmen grundsätzlich nur nach dem 4-Augen-Prinzip zugegriffen wird. Die erste Person soll aus dem Bereich Pfortnerei, Wachdienst, L12 oder Polizei stammen, die zweite Person aus dem Bereich der Dienststellenleitung o.V.i.A. (oder Vertretung im Amt) sein. Zur Abwehr einer Gefahr darf vom Vier-Augen-Prinzip abgewichen werden. Der Zugriff soll mit Hilfe eines ... hinterlegten Passwortes erfolgen, dessen Benutzung (Datum, Uhrzeit, Anlass, Personen) protokolliert wird. Die Vergabe eines neuen Passwortes nach Benutzung durch die Systemadministration (L13) ist organisatorisch geregelt. Eine entsprechende Dienstanweisung wird im Rahmen des Datenschutzmanagements erstellt (Datenschutzziel Nr. 3).

(viii) Zugriff auf gespeicherte Bilder

Die Software ... erlaubt die Einrichtung von Nutzerkonten und die Konfiguration von Zugriffsrechten. Im Bereich der abgegrenzten Pfortnerei ist die Software so konfiguriert, dass sie nach dem Einschalten der Geräte automatisch einen Standardbenutzer anmeldet (ohne Notwendigkeit einer Passwordeingabe). Für diesen Standardbenutzer ist die Funktion zum Abruf der Aufzeichnungen deaktiviert, so dass ein Abruf durch die Pfortnerei nicht möglich ist.

Nur die Nutzerkonten der Mitarbeiter aus den Referaten L 12 und L13 sind derzeit so konfiguriert, dass Aufzeichnungen abgerufen werden können. Dazu genügt die jeweilige Anmeldung des Benutzers am Benutzerkonto. Die Eingabe eines zweiten Passwortes ist nicht erforderlich; ein Vier-Augen-Prinzips ist technisch nicht eingerichtet.

Ein von den Produktherstellern angebotenes Verfahren, das ein Vier-Augen-Prinzips durch die Notwendigkeit der Eingabe zweier Passworte sicherstellt, bezieht sich nicht auf die Konfiguration der Software ... und die Nutzung dort angebotenen Funktionen (z. B. Ausdruck, Abruf gespeicherte Aufnahmen, Ansehen von Live-Aufnahmen, Kopie von Datenströmen etc.), sondern auf den erstmaligen Anschluss und die Initialisierung von Aufnahmerekordern (diese verfügen über eine eigene Benutzerverwaltung). Es muss bei der Installation konfiguriert werden, ob die Software ... *grundsätzlich* mit einem Aufnahmerekorder kommunizieren kann.

Durch die Aufnahmerekorder wird sowohl der Zugriff auf Live-Bilder als auch auf gespeicherte Aufnahme gesteuert. Bei der Einrichtung und Konfiguration des Anschlusses zwischen ... und Aufnahmerekordern kann nicht zwischen späteren Zugriffen auf Live-Aufnahmen des Rekorders und den Zugriff auf gespeicherte Aufnahmen des Rekorders unterscheiden werden. Daher ist die vom Hersteller angebotene doppelte Passwordeingabe nicht geeignet, den Zugriff auf gespeicherte Aufnahmen gesondert abzusichern.

Geplant ist, durch die Einrichtung von mehreren Administrationskonten und Einstellung von Zugriffsrechten die Software so zu konfigurieren, dass alltägliche Administrationsarbeiten (ohne Abrufmöglichkeit gespeicherter Bilder und ohne die Möglichkeit, sich dieses Recht zu verschaffen) möglich sind, der Sonderfall des Abrufs gespeicherter Aufnahmen und die Änderung von Nutzerrechten aber einem besonderen Nutzerkonto („Superadministrator“) vorbehalten ist. Das Passwort zu diesem Konto soll dann, wie ursprünglich vom Konzept vorgesehen, ... in einem versiegelten Umschlag aufbewahrt werden. Dieser Umschlag soll nur zugänglich sein, wenn zwei Personen zugleich ihn abholen (4-Augen-Regelung), siehe vorheriger Abschnitt.

(ix) Herausgabe gespeicherte Bilder an Dritte

Durch eine im Rahmen des Datenschutzmanagementsystems zu erstellenden Dienst- und Verfahrensanweisung (Datenschutzziel Nr. 4) wird sichergestellt, dass – falls erforderlich – die Herausgabe von gespeicherten Videodaten nur im Falle eines entsprechenden Anspruches und unter Wahrung der Interesse des Hauses erfolgt.

II. Datenschutzrechtliche Zulässigkeit

1. Zutritts- und Zufahrtskontrollsystem der Tiefgarage

Das Zutritts- und Zufahrtskontrollsystem ist sowohl hinsichtlich des Nordtores als auch des Südtores in das generelle Zutrittsberechtigungskonzept des Landeshauses eingebunden worden. Besonderheiten gegenüber dem sonstigen Zutrittsberechtigungskonzept bestehen nicht. Hinsichtlich der verarbeiteten Stammdaten und Bewegungsdaten ergeben sich keine Veränderungen gegenüber dem Gutachten zum Datenschutzaudit vom 23. September 2005. Das Verfahren ist datenschutzrechtlich zulässig.

2. Video-Anlage

Das Feinkonzept setzt sich in Kapitel 8.5 mit den datenschutzrechtlichen Vorgaben hinsichtlich der Video-Anlage auseinander. Insbesondere wird hierbei auf § 20 des Landesdatenschutzgesetzes (LDSG) vom 09. Februar 2000 Bezug genommen. Der Verfasser kommt zu dem Ergebnis, dass die Voraussetzungen sowohl hinsichtlich der Videoüberwachung als auch der Videoaufzeichnung erfüllt sind. Die Videoanlage wird als Werkzeug zur Erhöhung der Sicherheit eingestuft, da von einer realen Bedrohung des Gebäudes und seiner Nutzer auszugehen sei. Außerdem seien die entsprechende Beschilderung, Anweisungen und technischen Maßnahmen umgesetzt worden. Die Speicherdauer der Aufzeichnungen von den Außenkameras von ... Tagen ergebe sich aus.... Eine wechselnde Speicherzeit im Jahresbetrieb in Anpassung an den jeweiligen Feiertagen sei aus ablauftechnischen Gründen nur mit hohem finanziellem Aufwand und dann trotzdem mit Risiken behaftet umsetzbar.

Auf das Allgemeine Verwaltungsgesetz für das Land Schleswig-Holstein (LVwG) wird vom Verfasser nur kurz hinsichtlich §184 LVwG eingegangen, da die Videoüberwachung und – aufzeichnung bereits durch §20 LDSG gedeckt sei. Hinsichtlich des Umgangs mit der Anlage weist der Verfasser darauf hin, dass das Bedienpersonal über die Bedeutung des Datenschutzes belehrt werden müsse. Außerdem dürften entgegen der technisch möglichen

Reichweite der Kameras keine Bereiche außerhalb des Landeshauses eingesehen und aufgenommen werden.

Die dem Feinkonzept auch hinsichtlich der Video-Anlage zu Grunde liegenden datenschutzrechtlichen Erwägungen sind aus Sicht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein grundsätzlich zutreffend. Die Zulässigkeit der Video-Überwachung und –Aufzeichnung ergibt sich aus Sicht des ULD aus folgenden Erwägungen:

a) Rechtsgrundlage

Der Landtag wird nicht direkt vom Anwendungsbereich des LDSG erfasst, da es sich nicht um eine öffentliche Stelle im Sinne des §3 Abs. 1 LDSG handelt. Nach §1 Abs. 2 Satz 1 und 2 Nr. 3 der Datenschutzordnung des Schleswig-Holsteinischen Landtages vom 3. September 1988 gelten die Vorschriften des Landesdatenschutzgesetzes jedoch auch für den Landtag, wenn dieser personenbezogene Daten bei der Wahrnehmung von Verwaltungsaufgaben verarbeitet. Als Verwaltungsaufgabe wird hierbei auch die Ausübung des Hausrechts und der Ordnungsgewalt gemäß Artikel 14 Abs. 3 Satz 2 der Landesverfassung angesehen.

Die speziellen Regelungen des BDSG (insbesondere §6b BDSG) kommen aus dem Rückschluss von §1 Abs. 2 Nr. 2 BDSG nicht zur Anwendung. Insbesondere ist der Landtag keine öffentliche Stelle, die Bundesrecht ausführt.

b) Videoüberwachung

(i) §20 Abs. 1 LDSG

Nach §20 Abs. 1 LDSG dürfen öffentliche Stellen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume beobachten, soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrnehmung eines Hausrechts erforderlich ist und schutzwürdige Belange Betroffener nicht überwiegen. Dabei hat die verantwortliche Stelle stets auch die Grundsätze der Datenvermeidung und Datensparsamkeit zu beachten.

Bei den im Außenbereich des Landtages installierten Kameras handelt es sich um optisch-elektronische Einrichtungen, die der Beobachtung dienen.

Öffentlich zugängliche Räume sind im Sinne von öffentlich zugänglichen Bereichen zu verstehen. Unerheblich ist, ob diese umschlossen oder überdacht sind. Relevant ist vielmehr, ob die Räume entweder dem öffentlichen Verkehr gewidmet sind oder nach dem erkennbaren Willen des Berechtigten von jedermann genutzt oder betreten werden können.¹ Öffentlich zugänglich ist ein Raum, wenn sich seine Zugänglichkeit nach allgemeinen Merkmalen bestimmt, die von jeder Person erfüllt werden kann.²

Das Landeshaus ist so gestaltet, dass insbesondere die beiden Wege links und rechts vom Landeshaus als Verbindung zwischen Kiellinie und Düsternbrooker Weg von jedermann genutzt werden können. Verbotsschilder oder Absperrungen bestehen nicht. Vielmehr will man sich gerade als offenen und bürgernahen Landtag zum Anfassen präsentieren. Damit sind zumindest die befestigten Wege am Landtag sowie die Straße zwischen Landeshaus und Wirtschaftsministerium als öffentlicher Raum anzusehen. Eindeutig gilt dieses natürlich für den Düsternbrooker Weg und die Kiellinie selber. Anders hingegen stellt die Tiefgarage keinen öffentlich zugänglichen Raum dar. Der Zutritt bzw. die Einfahrt ist hier von außen

¹ Vgl. Gola/Schoerus BDSG zum diesbezüglich wortgleichen §6b BDSG (Rn. 8).

² Vgl. Simitis BDSG zum §6b BDSG (Rn. 42).

gesichert, so dass nur berechtigte Personen die Tiefgarage entweder mit Ausweisen oder nach Anmeldung bei der Pförtnerie erreichen können.

Wie sich aus §20 Abs. 1 LDSG ergibt, muss ein zulässiger Beobachtungszweck vorliegen. Die Videoüberwachung ist keine direkte Aufgabe des Landtags. Allerdings könnte sie zur Wahrnehmung des Hausrechts erforderlich sein. Das Hausrecht umfasst die Befugnis, Störer aus einem bestimmten Bereich zu verweisen. Es folgt den Grenzen des sachenrechtlichen Widmungszwecks aus der Zuständigkeit und Verantwortlichkeit etwa einer Verwaltung, für ihre Gebäude zu sorgen. Dabei kann die Videoüberwachung präventiv dazu dienen, Personen davon abzuhalten, Rechtsverstöße zu begehen (Abschreckungswirkung). Auch die repressive Verfolgung von Verstößen gegen das Hausrecht kann ein legitimer Zweck sein.

Zweck der Videoüberwachung des Landeshauses ist der Schutz des Gebäudes und der Menschen und Sachen, die sich hierin befinden. Dies schließt die Sicherung der Funktionsfähigkeit des Landtages mit ein. Dieser Zweck ist grundsätzlich vom Hausrecht umfasst.

Des Weiteren muss die Videoüberwachung erforderlich und somit geeignet zur Erreichung des angestrebten Zwecks und diesbezüglich das mildeste Mittel sein. Die Videoüberwachung des Landeshauses ist durchaus dazu geeignet, eventuelle Störer abzuschrecken. Die Videoanlage ist für jedermann gut zu erkennen. Außerdem weisen an den Wegen angebrachte Schilder zusätzlich auf die Videoüberwachung hin. Auch die nächtliche Videoüberwachung liefert zwar schlechtere, durch die Aktivierung der Beleuchtung ... jedoch verwendbare Bilder, die die Umsetzung des Hausrechts unterstützen. Ein gleich geeignetes, milderer Mittel ist nicht erkennbar. Sollte diese Funktion durch Wachpersonal erfüllt werden, wären hierfür weit mehr Mitarbeiter rund um die Uhr erforderlich. Auch der Einsatz nur von Kameraattrappen dürfte nur kurzfristig eine vergleichbare Abschreckung bewirken, da nicht ausgeschlossen werden kann, dass dies bekannt wird.

Allerdings endet die Beobachtungsgrenze des Hausrechtsinhabers grundsätzlich an der Grenze des Grundstücks.³ Sowohl die Kiellinie als auch der Düsternbrooker Weg einschließlich der dort angrenzenden Wege und Gebäude dürfen nicht von der Videoüberwachung betroffen sein, soweit diese Details erfasst, die einzelne Personen und ihre Handlungen identifizierbar machen. Durch die inzwischen eingerichtete Ausblendung dieser Bereiche wird diesem Anspruch genüge getan. Hinsichtlich des teilweise erfassten Vorbereichs des Wirtschaftsministeriums (Kantine / Mülleimer) existiert entsprechend den Angaben der Landeshausverwaltung eine entsprechende Vereinbarung bzw. Erlaubnis zur Übernahme des Hausrechts.

Und schließlich dürfen schutzwürdige Belange Betroffener nicht überwiegen. Maßstab sind die durch das Recht auf informationelle Selbstbestimmung gestützten Interessen derjenigen, die Objekte der Videoüberwachung sind.⁴ Die Schutzbedürftigkeit ist insbesondere dann hoch, wenn es sich um einen Bereich handelt, in dem sich Menschen typischerweise länger aufhalten und miteinander kommunizieren.

Auf dem Grundstück des Landeshauses werden vor allem die beiden Wege links und rechts des Gebäudes, die den Düsternbrooker Weg mit der Kiellinie verbinden, zeitweise rege von Menschen genutzt. Allerdings handelt es sich hierbei um einfache Verbindungsstrecken, bei denen es nicht üblich ist, dass man sich länger aufhält. Neben dem Landeshaus selber befinden sich hier keine Objekte (wie etwa einer Ausstellung), die zum längeren Verweilen oder Kommunizieren mit anderen Menschen anregen. Außerdem befinden sich in nicht all zu weiter Entfernung sowohl in Höhe Reventloubrücke als auch des Weltwirtschaftsinstituts

³ Vgl. BGH NJW 1995, 1955.

⁴ Simitis BDSG, §6b Rn. 60.

weitere öffentliche Wege, die den Düsternbrooker Weg und die Kiellinie verbinden. Wer möchte, kann somit die Videoüberwachung ohne großen Umweg umgehen. Dem gegenüber steht der oben genannte Schutz des Landeshauses vor Anschlägen, Einbrüchen und Verschandelungen. Die schutzwürdigen Belange der Betroffenen überwiegen dieses Interesse nicht.

(ii) §184 Abs. 3 LVwG

Nach §184 Abs. 3 LVwG dürfen allgemein zugängliche Flächen und Räume von Ordnungsbehörden bzw. Polizei mittels Bildübertragung beobachtet werden, soweit dies zur Abwehr von Gefahren für die Allgemeinheit oder einzelne Personen erforderlich ist. Hinsichtlich des Geländes des Landeshauses selber ist die Videoüberwachung schon durch §20 Abs. 1 LDSG zumindest den Mitarbeitern des Landeshauses gestattet. Hinsichtlich des Gebiets drum herum ist die Erforderlichkeit einer Videoüberwachung zur Gefahrenabwehr fraglich. Es ist nicht ersichtlich, welche weiteren Gefahren insbesondere vom Düsternbrooker Weg und der Kiellinie ausgehen, die nicht durch die Überwachung des Geländes des Landtages begegnet werden kann. Soweit z.B. Demonstrationen über den Düsternbrooker Weg zum Landeshaus erfolgen und hiervon eine Gefahr ausgehen würde, wäre die sowieso vorhandene Präsenz der Polizei selbst zur Gefahrenabwehr besser geeignet. Sofern erforderlich, könnte dann eine einzelfallbezogene Überwachung zur Repression mittels mobiler Kameras erfolgen. Eine ständige Überwachung mittels fest installierter Kameras ist hierfür nicht erforderlich.

(iii) §185 Abs. 1 Nr. 2 a LVwG

Auch §185 Abs. 1 Nr. 2 a LVwG rechtfertigt keine dauerhafte Überwachung des Geländes um den Landtag herum. Vielmehr ist für diese Art der Videoüberwachung nach §186 Abs. 1 Satz 6 LVwG die Anordnung etwa durch die Leiterin oder den Leiter des Landeskriminalamtes oder entsprechend berechnigte Personen erforderlich. Sie gilt dann in der Regel auch nur für Ordnungsbehörden bzw. die Polizei.

(iv) Nicht öffentlich zugänglicher Bereich der Tiefgarage / Parkhaus / Zugänge / Übergänge

§20 Abs. 1 LDSG ist nicht direkt anwendbar auf nicht öffentlich zugängliche Räume wie den Bereich der Garage oder die Schleusen und Übergänge. Für den Bereich der Frauenparkplätze gilt jedoch die Landesverordnung über den Bau und Betrieb von Garagen (GarVO) vom 30. November 1995. §2 Abs. 2 GarVO schreibt vor, dass Frauenparkplätze „in der Nähe der Zufahrt so angeordnet sein [sollen], daß sie von mindestens einer von der Betreiberin oder dem Betreiber zu bestimmenden Person eingesehen oder durch Videokameras und Monitore in ausreichender Zahl überwacht werden können. Zu den Frauenparkplätzen führende Treppenträume müssen ebenfalls eingesehen oder durch Videokameras überwacht werden können.“ Die Videoüberwachung ist für diesen Bereich somit nicht nur zulässig, sondern sogar geboten.

Für Parkbereiche, die nicht direkt die Frauenparkplätze betreffen, und die Schleusen / Übergänge ermöglicht es das Hausrecht grundsätzlich dem Hausherrn, eine Videoüberwachung durchzuführen. Diese hat sich jedoch an den allgemeinen Regelungen zu orientieren, so dass z.B. keine umfassende Mitarbeiterkontrolle erfolgen darf. Im Fall der Tiefgarage des Landeshauses, dem Parkhaus und die Schleusen / Übergänge kommt hinzu, dass hier nicht nur Mitarbeiter des Landeshauses, sondern auch Gäste (ggf. nach Einlass durch den Pförtner) Zutritt haben. Auch die besondere Stellung des Landeshauses als Begegnungsstelle der Vertreter unterschiedlicher Gruppen aus Schleswig-Holstein muss dabei

beachtet werden. Damit werden auch zahlreiche Menschen von der Videoüberwachung erfasst, die nicht in einem Näheverhältnis zum Landeshaus stehen. Somit muss sich die Videoüberwachung innerhalb des Landeshauses ebenfalls an den Grenzen des §20 Abs. 1 LDSG orientieren.

Die Videoüberwachung der Bereiche ist dazu geeignet, als Abschreckung und zur Verfolgung eventueller Verstöße gegen die Hausordnung oder gar Straftaten (Vandalismus, Unfälle, Überfälle) zu dienen. Ein milderer und gleichgut geeignetes Mittel ist nicht erkennbar.

Bei den überwachten Bereichen handelt es sich um keine Räume, die zum längeren Verweilen der Nutzer oder der Kommunikation zwischen den Besuchern dienen. Die Videoüberwachung ist deutlich erkennbar und für Besucher nicht überraschend. Außerhalb des Landeshauses steht zudem etwa an der Kiellinie weiterer Parkraum zur Verfügung, der nicht videoüberwacht wird. Die schutzwürdigen Belange der Betroffenen überwiegen damit die Wahrnehmung des Hausrechts nicht.

(v) Fazit Videoüberwachung

Die Videoüberwachung des Geländes des Landeshauses, Tiefgarage, Parkhaus und der Schleusen bzw. Übergänge ist grundsätzlich im Rahmen des Hausrechts zulässig. Dies gilt jedoch nicht, soweit Bereiche außerhalb dieses Geländes von den Kameras detailliert erfasst werden können. Diesbezüglich ist nach Angaben der Landeshausverwaltung inzwischen durch Ausblendungen sichergestellt worden, dass diese Bereiche entsprechend dem Konzept nicht mehr einzusehen sind. Die Beobachtung einzelner Personen und deren Identifizierung ist danach nicht mehr möglich. Die Videowachung ist daher in dieser Form zulässig.

c) Videoaufzeichnung

Nach §20 Abs. 2 LDSG darf das Bildmaterial gespeichert werden, wenn die Tatsache der Aufzeichnung für die Betroffenen durch geeignete Maßnahmen erkennbar gemacht ist. Dabei sind die Aufzeichnungen spätestens nach sieben Tagen zu löschen, es sei denn, sie dokumentieren Vorkommnisse zu deren Aufklärung die weitere Speicherung erforderlich ist.

Notwendig für die Videoaufzeichnung ist somit zusätzlich zu den Voraussetzungen der Videoüberwachung, dass durch geeignete Maßnahmen, etwa deutlich sichtbare Hinweisschilder, die Transparenz für die Betroffenen gewährleistet wird. Der Betroffene soll sein Verhalten im Sichtbereich einer Kamera darauf einrichten oder der Kamera ausweichen können.

Sowohl die Kameras an der Fassade des Landeshauses wie auch die auf den Stelen und in der Tiefgarage sind deutlich zu erkennen. Hinzu kommen Hinweisschilder jeweils am Anfang und am Ende der beiden Verbindungswege zwischen dem Düsternbrooker Weg und der Kiellinie. Diese Schilder weisen ein Piktogramm auf, das eine herabhängende Kamera darstellt. Außerdem steht dort „zu ihrer und unserer sicherheit: das gelände des landtages wird kamera überwacht.“ Hiermit wird jedoch nur auf die Videoüberwachung hingewiesen. §20 Abs. 2 LDSG fordert jedoch, dass „die Tatsache der Aufzeichnung“ erkennbar gemacht wird. Diesem Erfordernis entsprechen die Schilder nicht ausdrücklich, da hier nur auf die Überwachung hingewiesen wird. Ob jedoch die Transparenz für den Betroffenen gewahrt ist, ergibt sich aus dem Empfängerhorizont. Die meisten Personen dürften nicht zwischen Überwachung und Aufzeichnung differenzieren. Dies deckt sich auch mit der Regelung des §6b BDSG, die ebenfalls nicht so ausdrücklich zwischen Überwachung und Aufzeichnung differenziert und nur eine generelle Hinweispflicht auf die Überwachung verlangt. Vielmehr dürfte der weit überwiegende Teil der Passanten davon ausgehen, dass gerade nachts auch eine Aufzeichnung erfolgt, selbst wenn das Schild nur von einer Überwachung spricht. Damit dürften die Schilder ausreichend sein, auf die Aufzeichnung hinzuweisen.



Abbildung 1: Schild am Zugang Kantine



Abbildung 2: Hinweisschild Höhe Düsternbrooker Weg

Als maximale Aufbewahrungsfrist, sofern keine besonderen Vorkommnisse vorliegen, schreibt §20 Abs. 2 Satz 2 LDSG sieben Tage vor. Die Aufzeichnungsanlage des Landeshauses ist so eingestellt, dass die Daten nach ... Tagen gelöscht bzw. überschrieben werden, so dass diese Voraussetzung erfüllt wird. Auch nach den Grundsätzen von Datensparsamkeit und Datenvermeidung ist diese Frist in Anbetracht von ggf. betroffenen Wochenenden und Feiertagen noch als erforderlich anzunehmen. Hinzu kommt, dass die Einsicht in die Aufzeichnungen besonders gesichert ist.

Die Videoaufzeichnung ist somit in der Konzeptform bzw. Umsetzung rechtmäßig.

III. Technisch-Organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit

1. Bestandsaufnahme

In der folgenden Bestandsaufnahme werden die Ergänzungen und Änderungen des Bestandes im Vergleich zur Erstauditierung dargestellt.

a) Hardware

(i) Videoanlage (neu aufgenommen)

Die verwendete Hardware der Videoanlage besteht aus folgenden Komponenten:

- ... Kameras (Außenkameras, Innenkameras, schwenkbaren Kameras)
- ... Infrarotsensoren
- ... Videosensoren zur Detektion von Bewegungen in Bildern
- ... Kreuzschienen zur Aufschaltung von beliebigen Kamerabildern auf die vorhandenen Monitore
- ... digitale Bildspeicher (Rekorder zur parallelen Aufnahme von Kamerasignalen auf mehreren „Spuren“)
- ... „Quad-Controller“ ...
- ... Monitore, ... PC-Systeme und ... Steuereinrichtungen im Bereich der Pförtnerie und der Polizei zur Beobachtung von Live-Aufnahmen und Steuerung der schwenkbaren Kameras
- ... Monitore und PC-Systeme in den Referaten L12 und L13 zur Steuerung, Konfiguration und zum Abruf gespeicherter Daten.

Videosensoren, Kreuzschienen, Bildspeicher und Quad-Controller sind in einem Schrank ... untergebracht. Dieser Raum ist besonders zugangsgesichert und verfügt über Einbruchmelde- und Brandlöschanlagen. In diesem Schrank ist eine Bedienschublade integriert, um per Bildschirm und Tastatur zur Konfiguration auf die Systeme zugreifen zu können.

Die Typen und Standorte der Kameras sowie deren Blickrichtung und Sichtbereiche sind im Konzept (Abschnitt 8.1.1.7) und in weiteren bauplanerischen Unterlagen dokumentiert. Die übrige Hardware ist in Abschnitt 8.2 des Konzeptes beschrieben.

Die Bildsprechanlagen ... sind nicht in die Videoanlage eingebunden.

(ii) Hardware Zutrittskontrolle Tiefgarage

Die im Bereich der Zutritts-/Zufahrtskontrolle der Tiefgarage verwendete Hardware ist in Abschnitt 15 des Konzeptes beschrieben. Sie stellt zum Teil eigenständige Komponenten (z. B. die Funkfernsteuerung), zum Teil Erweiterungen bestehender Komponenten (z. B. zusätzliche Kartenleser, Tür-Controller und Vernetzungen) dar. Diese Erweiterungen sind in Abschnitt 5 des Konzeptes, das das Zutrittsberechtigungssystem beschreibt, ergänzt worden.

(iii) Veränderungen an bestehender Hardware

Über die oben beschriebenen neuen Komponenten hinaus sind Teile der bestehenden Hardware ergänzt oder verändert worden. Änderungen und Ergänzungen sind im Feinkonzept beschrieben. Sie betreffen eine Änderung der Ansteuerung der Fluchttürterminals (Abschnitt 5.4.7.2), die Einrichtung eines Intrusion Detection Systems (siehe Abschnitt b) (ii)) sowie den Aufbau eines „Primary Domain Controllers“ für eine zentrale Verwaltung von Benutzerkonten von Nutzern der Software des Zugriffsberechtigungssystems (...).

b) Vernetzung

Ein zentraler Bestandteil der Hardware ist die Vernetzung der einzelnen Hardwarekomponenten. Auch in diesem Bereich gab es Veränderungen und Ergänzungen.

(i) Vernetzung der Videoanlage

Die von der Videoanlage übertragenen Daten werden durch unterschiedliche Kabel und Netze übertragenen:

- Für die Datenübertragung zwischen den Aufnahmerecordern und der Software ... und ..., die auf den Arbeitsplätzen in der Pfortnerei und in den Referaten L12 und L13 installiert ist, wird das besonders abgesicherte Netz SecLAN verwendet. Dieses Netz kommt auch für das Zutrittsberechtigungs-system zum Einsatz und wird in Abschnitt 4 des Konzeptes dargestellt.
- Für alle anderen Datenübertragungen, z. B. von den Bildsignalen der Kameras zu den Videosensoren, Aufnahmerecordern, Kreuzschienen und von dort zu den Monitoren in der Pfortnerei, von den Steuersignalen der schwenkbaren Kameras, die in den Kreuzschienen und über Bedienteile ... generiert werden, sowie den Alarmbildern für die Pfortnerei kommen Koaxial-Kabel und serielle Kabel zum Einsatz. Längere Strecken werden z.T. mit Glasfaserleitungen überbrückt,

Alle Leitungen werden ausschließlich für Video- und Steuersignale verwendet und sind nicht in andere Netze eingebunden.

(ii) Änderungen und Ergänzungen der Vernetzung

An der bestehenden Netzkomponente SecLAN (ein abgeschottetes, besonders gesichertes Netzsegment ausschließlich für das Zutrittsberechtigungs-system und die Videoanlage), die bereits für das Zutrittsberechtigungs-system installiert wurde, wurden folgende Änderungen vorgenommen:

Das Intrusion Detection System (eine Hard- und Software zur Erkennung unberechtigten Netzverkehrs), das bislang lediglich konzipiert war, wurde installiert. Zum Einsatz kommt die Software Eine Dokumentation dieser Software ist erfolgt. Es ist aber geplant, sie durch ein anderes IDS, vermutlich ..., zu ersetzen: ...

Die Rechner für Benutzung der Software ... sind mit Hilfe des SecLAN mit den Bildrekordern verbunden.

c) Software

(i) Software in Zusammenhang mit der Videoanlage

Firmware

In den Komponenten der Videoanlage ist zum überwiegenden Teil Firmware installiert, die grundsätzlich weniger anfällig ist für Viren, Trojaner und andere Angriffe, die Sicherheitslücken ausnutzen. Die beiden wesentlichen Komponenten betreffen die Videosensoren und die Bildrekorder. Alle zur Verfügung stehenden und freigegebenen Updates der Firmen ... werden vom Administrator installiert. In der Regel sind das aber keine Sicherheits- sondern Funktionsupdates.

Bei den Videosensoren lassen sich für jede der daran angeschlossenen Kameras Schrifteinblendungen (Datum, Uhrzeit) sowie die Parameter der Bewegungserkennung (Empfindlichkeit, Sensorflächen, perspektivische Erkennung) konfigurieren. Die Konfiguration erfolgt mit Hilfe eines Terminals im Raum

Bei den Bildspeichern lassen sich für jede angeschlossene Kamera die Dauer der Aufzeichnungen (bzw. ob überhaupt aufgezeichnet wird) oder die Aufzeichnungsgeschwindigkeit (Bilder pro Sekunde) konfigurieren. Die Software in den Bildspeichern wird auch angesprochen, wenn aufgezeichnete Bilder abgerufen werden. Konfiguration und Abruf erfolgen mit Hilfe der Software ..., die einen Fernzugriff von den Rechnern in der Pförtnerlei bzw. den Arbeitsplätzen (...) in den Referaten L12 und L13 erlaubt.

Eigenständige Software:

Die ...-Stations laufen unter dem Betriebssystem Die Programme ... und ... des Herstellers ... sind als Anwendungssoftware installiert. Beide Programme ermöglichen umfangreiche Abfragen und Konfigurationen der digitalen Bildspeicher.

... dient dabei als zentrales Steuerungsinstrument der Rekorder. Es lassen sich aktuelle Aufnahmen anzeigen (Auswahl der Kamera) und Split-Darstellungen konfigurieren. Eine entsprechende Berechtigung vorausgesetzt, können auch gespeicherte Bilder abgerufen werden. Die Konfiguration der virtuellen Rundgänge und der Split-Darstellungen in der Pförtnerlei erfolgt ebenfalls mit

Zur Überwachung von Alarmen und zur Verwaltung der Alarmmeldungen, die von den Bildrekordern generiert werden, wird die Software ... eingesetzt. Diese ist zusammen mit der Software ... installiert (d.h. in den Referaten L12 und L13, in der Pförtnerlei auf den Arbeitsplätzen für das Wachpersonal und den Polizeiarbeitsplätzen). Die Software ist so konfiguriert, dass Alarmmeldungen nur in der Pförtnerlei auflaufen.

Betriebssysteme und Sicherheitssoftware

Die in Abschnitt 8.3.4 des Konzeptes beschriebene Härtung der Betriebssysteme und der Einsatz von Virenschaltern ist bei den Rechnern in den Referaten L12 und L13 erfolgt. Die Rechner der Pförtnerlei werden neu aufgesetzt und dann ebenfalls gehärtet und mit einem Virenschutz versehen. Geplant ist die 34./35. KW.

(ii) Ergänzungen und Veränderungen an bestehender Software des Zutrittberechtigungs-systems

Die in Abschnitt 5.3.3.1 des Konzeptes angesprochene Software zum Virenschutz derjenigen PC und Server, auf denen Komponenten des Zugriffsberechtigungs-systems installiert sind, wurde inzwischen ausgewählt und installiert. Es kommt die Software ... zum Einsatz.

d) Datenbestände und Kommunikation

Innerhalb der Videoanlage werden folgende Datenbestände gespeichert:

- Konfigurationsdaten, Zugriffsberechtigungen etc.
- Gespeicherte Aufnahmen der Kameras (in den Bildrekordern)
- Alarmmeldungen.

Nicht betrachtet wird die Weiterverarbeitung gespeicherter Aufnahmen (Ausdruck, Kopie), die aus der Videoanlage für weitere Zwecke abgerufen wurden, beispielsweise zu Ermittlungszwecken. Die Alarmmeldungen umfassen Meldungen über Bildveränderungen (Bewegungsdetektionen) und technische Alarme (z.B. Füllungsgrad von Festplatten). Da sie keine personenbezogenen Daten umfassen, werden sie nicht weiter betrachtet.

Neben Videodaten werden durch die Videoanlage auch Steuersignale verarbeitet, etwa Signale zur selbständigen Ausrichtung der schwenkbaren Kameras, zur Konfiguration der Anzeigen oder zur manuellen Steuerung der Kameras. Die Steuersignale zum Schwenken und Zoomen werden nicht gespeichert.

Eine Übersicht über die Kommunikation zwischen den einzelnen Komponenten kann der folgenden Graphik entnommen werden.

e) Regelungen

(i) Nutzungsrechte

Es gibt drei Arten von Nutzungsrechten für die Videoanlage:

- Administration und Konfiguration (wahrgenommen durch das Referat L 13)
- Live-Beobachtung und Steuerung der schwenkbaren Kameras (Pförtneri, Polizei)
- Situationsbedingte Live-Aufschaltung (z.B. Demonstration) und Live-Abruf gespeicherter Aufnahmen (derzeit wahrgenommen durch Mitarbeiter der Referate L12 und L13).

Es erfolgt durch die Mitarbeiter der Referate L12 und L13 eine zusätzliche strichprobenartige Kontrolle der Mitarbeiter der Pförtneri. Mit Hilfe der Software ..., die auf den Arbeitsplätzen dieser Mitarbeiter installiert ist, können sämtliche Live-Aufnahmen, insbesondere die der schwenkbaren Kameras, dargestellt werden. Ein Abruf gespeicherter Aufnahmen zum Zwecke dieser Kontrolle erfolgt nicht. Entsprechendes ergibt sich aus den gemäß Datenschutzmanagementsystem zu erlassenden Verfahrensanweisungen (Datenschutzziele 2 und 5).

(ii) Nutzerauthentisierung:

Eine Nutzerauthentisierung erfolgt innerhalb der Software ..., die der Live-Beobachtung und ggf. dem Abruf gespeicherter Aufnahmen dient. Für die Mitarbeiter der Referate L12 und L13 sind entsprechende Benutzerkonten vergeben. Die Mitarbeiter der Pförtnerie benutzen den Account eines Standardbenutzers, der automatisch nach dem Start der Software eingeloggt ist. Die Software kann daher nicht zwischen verschiedenen Mitarbeitern der Pförtnerie unterscheiden. Ein Abruf gespeicherter Daten ist dem Standardbenutzer nicht möglich.

Die Nutzerauthentisierung innerhalb der Software ... unterscheidet zwischen Standardbenutzern und administrativen Benutzern. Ein Standardbenutzer, dessen Nutzerkonto die Mitarbeiter der Pförtnerie verwenden, kann lediglich aufgelaufene Alarmlisten löschen.

Die Bedienpulte ... zum Schwenken der Kameras und zum Aufschalten der Kameraaufnahmen auf die Monitore verfügen über keine Benutzerauthentisierung. Jedoch ist der Zutritt ... gesichert, so dass dieses kein Sicherheitsproblem darstellt.

(iii) Protokolldaten:

Als Protokolldaten der Software ... fallen unter anderem Konfigurationsänderungen, Verbindungsaufbau, Ausdruck von Bildern und das Öffnen der Protokolldatei an. Die Kontrolle der administrativen Tätigkeiten anhand der Protokolldaten erfolgt analog zur Kontrolle der Administration des Zutrittskontrollsystems. Das Datenschutzmanagement enthält unter Datenschutzziel 2 die Aufgabe, eine entsprechende Dienst- und Verfahrensanweisung zu erlassen.

(iv) Datensicherung:

Backups sämtlicher Konfigurationsdateien einschließlich der Software ... sind vorhanden. ...

(v) Arbeitsanweisungen

Es liegt die Verfahrensanweisung „Dienstanweisung für die mit dem Zutrittsberechtigungsverfahren des Schleswig-Holsteinischen Landtages befassten Mitarbeiterinnen und Mitarbeiter“, 19. April 2006“ vor. Sie setzt die Vorgaben des Feinkonzeptes für das ZBS (Stand 21.5. 2004), des Gutachtens des ULD zum Datenschutz-Audit 2004, des Datenschutzmanagementsystems aus der Auditierung des Jahres 2004 sowie der IT-Sicherheitsüberprüfung des ZBS (10.12.2004) um.

Zentrale Punkte sind:

- die technische Umsetzung der Rollentrennung von Systemadministration und ZBS-Kartenadministration einschließlich Dokumentation der vergebenen Berechtigungen (Abschnitt 3.3, 3.5, 3.7)
- Regelungen zur Datensicherung, zum Umgang mit Wissen über den Funktionsstatus des ZBS und mit papierbasierten Protokollen (Abschnitte 3.4, 3.6, 3.8)
- Regelungen zur Dokumentation administrativer Tätigkeiten, zu Zutrittsbefugnissen zu Serverräumen, zur Kennwortvergabe für Mitarbeiter ... sowie zur Einschränkung von Benutzerrechten (Abschnitte 3.9-3.12).

2. Verfahrensdokumentation nach § 3 DSGVO

In diesem Abschnitt wird untersucht, ob die gemäß § 3 DSGVO geforderten Dokumentationen vorliegen.

a) Verfahrenszweck nach § 4 DSGVO

Das vorliegende Feinkonzept stellt die Bereiche Zutrittsberechtigungssystem, Videoanlage, Einbruchmeldeanlage, Brandmeldeanlage sowie die interne Vernetzung durch das SecLAN dar. Es beschreibt die technischen und organisatorischen Maßnahmen des Verfahrens und enthält eine rechtliche Bewertung über die Zulässigkeit des Zutrittsberechtigungssystems. Die Zweckbestimmung ist dadurch nachgewiesen.

b) Verfahrensbeschreibung nach § 5 DSGVO

Gemäß § 5 DSGVO Abs. 1 sind automatisierte Verfahren eindeutig von anderen Verfahren abzugrenzen und die eingesetzten Programme und ihre Beziehungen zueinander darzustellen. Dies geschieht überblicksartig in Abschnitt 3 des Feinkonzeptes und detailliert für das Zutrittsberechtigungssystem in den Abschnitten 5 und 15 (für die Tiefgarage). Die Beziehungen zu den Verfahren Einbruch- und Brandmeldeanlage sowie zur Infrastruktur (Vernetzung SecLAN) werden in den Abschnitten 4, 6 und 7 dargestellt. Die Videoanlage wird in Abschnitt 8 beschrieben.

Die detaillierte Dokumentation der Programme einschließlich ihrer Konfiguration gemäß § 5 Abs. 2 DSGVO wird verschiedentlich im Konzept angesprochen (s. Abschnitt 4.7 für das SecLAN, Abschnitt 5.7 für das Zutrittsberechtigungssystem, 8.7 für die Videoanlage). Es umfasst insbesondere eine Dokumentation über die Standorte der gelieferten und installierten Hardware, die Beschaffung von Dokumentationsunterlagen der Hersteller durch den Lieferanten, die Dokumentation über installierte Software und deren Konfigurationsparameter einschließlich Benutzereinrichtung. Laut Konzept sind diese Dokumentationen vom Hersteller bzw. Dienstleister zu liefern. Dies ist zwischenzeitlich erfolgt.

c) Sicherheitskonzept nach § 6 DSGVO

Gemäß § 6 DSGVO ist ein Sicherheitskonzept sowie ggf. eine Risikoanalyse zu erstellen, in der die technischen und organisatorischen Maßnahmen zur Erfüllung der Anforderungen gemäß §§ 5 und 6 LDSG dargestellt sind.

Im vorliegenden Konzept werden die technischen und organisatorischen Maßnahmen für die Videoanlage und das Zutrittsberechtigungssystem an vielen Stellen ausführlich dargestellt. Auf die im Konzept ebenfalls vorhandene Risikodarstellung wird im nächsten Abschnitt eingegangen.

Einige Sicherheitsmaßnahmen haben in der Formulierung des Konzeptes empfehlenden Charakter. Im Rahmen der Erstauditierung 2004 waren noch umzusetzende Empfehlungen als Aufgaben in das Datenschutzmanagement aufgenommen worden.

Dies betraf die folgenden Punkte:

- Installation eines Intrusion Detection System im Netz SecLAN
- Test des Gesamtsystems (ZBS) durch Dataport
- laufende Fortschreibung des IT-Konzepts
- Freigabe des ZBS durch den Landtagspräsidenten
- Erlass einer Dienstanweisung für Karten- und IT-Administratoren
- Integration der von den Fachfirmen zu liefernden (Fach)Dokumentation in eine Gesamtdokumentation
- jährliche stichprobenartige Kontrolle der Administration im Auftrag des Datenschutzgremiums.

Diese Empfehlungen, die sich auf den Konzeptstand 2004 beziehen, sind inzwischen fast vollständig umgesetzt worden:

- ein Instrusion-Detection-System wurde installiert (vgl. Abschnitt III 1 b (ii))
- das Gesamtsystem wurde einem durch dataport im Herbst 2004 einem Sicherheitstest unterzogen
- das IT-Konzept wird fortlaufend fortgeschrieben und ergänzt
- das ZBS wurde durch freigegeben (vgl. Abschnitt III 2 e)
- eine Dienstanweisung für alle Mitarbeiterinnen und Mitarbeitern, die mit dem ZBS befasst sind, wurde am 19.4.2006 erlassen (vgl. Abschnitt III 1 e)
- die von den Fachfirmen zu liefernde Dokumentation wurde in die Gesamtdokumentation integriert.

Für eine stichprobenartige externe Kontrolle das Referat Informations- und Kommunikationsmanagement (Team ParlaNet) im Auftrag des Datenschutzgremiums, die laut Datenschutzmanagement (Stand 2004) jährlich vorgesehen ist, wurde bisher noch kein Auftrag erteilt.

Durch die Videoanlage sind weitere Empfehlungen und noch umzusetzende Maßnahmen hinzugekommen. Im Hinblick auf das Sicherheitskonzept dies in erster Linie der Erlass einer Dienstanweisung für Betrieb und Administration der Videoanlage sowie die Kontrolle der Administration. Dies ist als Datenschutzziel 2 des Datenschutzmanagementsystems vorgesehen.

d) Risikoanalyse

...

e) Test und Freigabe

Die Überprüfung der festgelegten Sicherheitsmaßnahmen war in der Konzeptversion 2004 durch dataport als Gesamtabnahme vorgesehen. Diese ist zwischenzeitlich erfolgt. Eine formelle schriftliche Freigabe durch den Landtagspräsidenten erfolgte am 13. Januar 2005.

Diese Freigabe schließt die Videoanlage nicht ein, da sich diese noch im Test- und Aufbaustadium befindet. Nach Abschluss der Arbeiten wird eine entsprechende Freigabe erfolgen. Test und Freigabe sind als Datenschutzziel 6 des Datenschutzmanagements genannt.

f) Verfahrensübergreifende Dokumentation und Protokolle nach § 8 DSVO

Gemäß § 8 Abs. 1, 2 DSVO sind informationstechnische Geräte und eingesetzte Programme in einem Geräte- und Programmverzeichnis zu erfassen; ersatzweise kann auf ein Inventarverzeichnis zurückgegriffen werden. Das Konzept sieht die Erstellung dieser Dokumentation vor (vgl. Abschnitt b) Verfahrensbeschreibung nach § 5 DSVO).

Ebenso sind eingeräumte Nutzungsrechte und eingeräumte Administrationsrechte zu dokumentieren (§ 8 Abs. 4, 5 DSVO) und administrative Tätigkeiten gemäß § 8 Abs. 5 DSVO zu protokollieren. In Abschnitt c) Sicherheitskonzept nach § 6 DSVO wurde festgestellt, dass die konkrete Umsetzung im Datenschutzmanagement vorzunehmen ist.

Für das Zutrittsberechtigungs-system wurden diese Maßnahmen durchgeführt. Für die Videoüberwachungsanlage erfolgt der Abschluss der Dokumentation nach der Fertigstellung der Videoüberwachungsanlage. Dies ist als Daueraufgaben „Fortschreibung der Bestandsaufnahme und der Datenschutzziele“ und „Dokumentation der Datenschutzziele und der Umsetzung“ in Abschnitt II Nr. 1 und 2 des Datenschutzmanagements festgelegt.

IV. Datenschutzmanagementsystem

1. Darstellung des Datenschutzmanagementsystems

Das Datenschutzmanagementsystem des Zutrittsberechtigungs-systems (Auditierung 2004) wird um ein Datenschutzmanagementsystem der Videoanlage ergänzt. Dieses umfasst drei Bereiche:

- I. Umsetzung aktueller Datenschutzziele
- II. Allgemeine Aufgaben des Datenschutzmanagements
- III. Schulung und Fortbildung der Mitarbeiter.

Die aktuellen Datenschutzziele betreffen die Fertigstellung der Implementierung der Videoüberwachungsanlage und insbesondere organisatorische Regelungen. Im Einzelnen sind dies:

1. Die Gewährleistung einer funktionierenden Videoanlage /-überwachung innerhalb des Zutrittsberechtigungs-systems unter Einhaltung der in dem Konzept vom 15.09.2005 Version 249 festgelegten Bedingungen
2. Analoge Ergänzung/Fortschreibung der Dienstanweisungen für das ZBS vom 19.April 2006 um die Systeme der Videoanlagen bezüglich der Verwaltung, Administration und den Kontrollmaßnahmen
3. Dienstanweisung für den Zugriff auf das Archiv der gespeicherte Aufnahmen gem. Konzept
4. Dienstanweisung/Verfahrensregelung für die Herausgabe von gespeicherten Videoaufnahmen und deren rechtliche Prüfung

5. Erstellung einer Information an die Mitarbeiter in der Pförtnerie bezüglich der durch Dienstanweisung geregelten Aufsicht/Kontrolle über das Schwenk und Zoom-Verhalten
6. Test und Freigabe der Videoanlage innerhalb des ZBS.

Der Regelungsbedarf, der sich aufgrund der Datenschutzziele 2 bis 5 ergibt, wird nicht durch mehrere Dienstanweisungen erfüllt, sondern in eine Ergänzung der bestehenden „Dienstanweisung für die mit dem Zutrittsberechtigungssystem des Schleswig-Holsteinischen Landtages befassten Mitarbeiterinnen und Mitarbeiter“ münden. Die Ergänzung wird die sich aus dem Betrieb des Videoüberwachungssystem ergebenden Auswirkungen, insbesondere den Zugriff auf das Archiv, die Herausgabe gespeicherter Videoaufnahmen und die Kontrolle des Schwenk- und Zoomverhaltens regeln.

Allgemeine Aufgaben des Datenschutzmanagementsystems zur Sicherstellung eines dauerhaft hohen Datenschutzniveaus sind:

7. Fortschreibung der Bestandsaufnahme und der Datenschutzziele
8. Dokumentation der Datenschutzziele und der Umsetzung
9. Bekanntgabe der Ziele und des Stands der Umsetzung an die Mitarbeiter
10. Unterrichtung des Datenschutzgremiums über den Stand der Umsetzung der Datenschutzziele und Unterrichtung des Datenschutzgremiums und des ULD über wesentliche Änderungen des auditierten Verfahrens
11. Sicherstellen der Beachtung von Rechtsänderungen
12. Einrichtung von Abstimmungs- und Kommunikationsverfahren
13. Stichprobenartige Datenschutzkontrolle.

2. Bewertung Datenschutzmanagementsystem

Die im Datenschutzmanagementsystem für das Zutrittsberechtigungssystem (Auditierung 2004) vorgesehenen Maßnahmen wurden weitestgehend umgesetzt (siehe Abschnitte C III 1 e (v) und C III 2 c). Das Datenschutzmanagementsystem für die Videoanlage vom 17.8.2006 ist geeignet, das gegenwärtig bestehende Datenschutzniveau auch für den gesamten Zeitraum der Auditierung aufrechtzuerhalten. Durch die Umsetzung der einzelnen Datenschutzziele werden darüber hinaus weitere Verbesserungen des Datenschutzes und der Datensicherheit erreicht.

Insbesondere wird durch das Datenschutzmanagementsystem sichergestellt, dass die zur datenschutzgerechten Umsetzung des Konzepts in die Praxis zu ergreifenden Maßnahmen getroffen werden. Dies betrifft u.a. den Abschluss der Dokumentation des Verfahrens, deren Ergänzung an einigen Stellen für den praktischen Einsatz des Konzepts erforderlich ist. Ebenso wird durch die Verpflichtung im Datenschutzmanagementsystem, Dienstanweisungen für die am System arbeitenden Mitarbeiter zu erstellen, gewährleistet, dass für den Praxisbetrieb Regelungen getroffen werden, die den datenschutzgerechten Umgang mit dem System durch die Beteiligten sicherstellen. Dies betrifft insbesondere den Abruf gespeicherter Aufnahmen und die Weitergabe an Dritte.

Durch Maßnahmen, die auf Dauer angelegt sind, werden im Datenschutzmanagementsystem Vorkehrungen ergriffen, das bereits erreichte und durch die Verwirklichung der kurzfristigen Ziele noch zu erhöhende Datenschutzniveau auch dauerhaft aufrechtzuerhalten. Hierzu dienen insbesondere die fortlaufende Bestandsaufnahme, die Fortschreibung der Dokumentation sowie die Fortbildung der Administratoren.

Die Mitteilungspflicht gegenüber dem ULD für wesentliche Änderungen des Verfahrens stellt sicher, dass das Verfahren im Einklang mit den in der Datenschutzerklärung enthaltenen Vorgaben durchgeführt wird.

V. Bewertung

Die Bewertung unterscheidet zwischen der Reauditierung des Zutrittsberechtigungs-systems und der Neuauditierung der Videoüberwachungsanlage.

Das Feinkonzept zur Gestaltung des Zutrittsberechtigungs-systems sowie die zur Umsetzung des Feinkonzepts durch die Landtagsverwaltung ergriffenen Maßnahmen erfüllen die rechtlichen Anforderungen des Datenschutzes. Dem Gebot der Datenvermeidung und Datensparsamkeit wird Genüge getan, da auf eine Erhebung von Bewegungsdaten in weitem Maße verzichtet und diese nur für besonders sicherheitsrelevante Zwecke erfolgt. Durch die gegenwärtige technische Umsetzung und die Umsetzung der bei der Erstauditierung vorgesehenen und im Datenschutzmanagementsystem (Stand 2004) festgeschriebenen Maßnahmen, insbesondere der organisatorischen Umsetzung durch eine Dienstanweisung, wird den Anforderungen an die Datensicherheit in vorbildlicher Weise entsprochen. Lediglich die vorgesehene jährliche externe Kontrolle im Auftrag des Datenschutzgremiums ist bisher noch nicht erfolgt.

Im Bereich der Videoüberwachung erfüllen die zur Umsetzung des Feinkonzepts durch die Landtagsverwaltung ergriffenen und weiterhin geplanten Maßnahmen die rechtlichen Anforderungen des Datenschutzes. Insbesondere wird dem Gebot der Datenvermeidung und Datensparsamkeit Genüge getan, da die Speicherdauer der aufgezeichneten Videobilder ... beträgt und zum überwiegenden Teil lediglich Übersichtsaufnahmen gemacht werden. Der Einsichtsbereich der fest installierten Kameras ist im Rahmen des Möglichen auf das Gebäude und die Flächen des Landeshauses beschränkt. Der Sichtbereich der schwenk- und zoombaren Kameras, die in Einzelfall eine großformatige Detailaufnahme ermöglichen, ist ebenfalls auf Gebäude sowie zugehörige Flächen des Landeshauses beschränkt.

Die Reauditierung des Zutrittsberechtigungs-systems und die Verleihung des Datenschutz-Audits gemäß § 43 Abs. 2 LDSG SH für die Videoüberwachungsanlage ist damit gerechtfertigt.