

Aus Sicherheitsgründen wird nur die Kurzfassung des Gutachtens veröffentlicht.

Gutachten zum Datenschutzaudit "Zutrittsberechtigungssystem für das Landeshaus Kiel"

Inhaltsverzeichnis:

| | |
|---|----|
| I. Gegenstand des Audits..... | 3 |
| II. Gegenstand der Begutachtung..... | 3 |
| III. Bewertung | 3 |
| 1. Darstellung der Datenschutzziele..... | 3 |
| 2. Umsetzung der Ziele durch das Feinkonzept und weitere Umsetzungsmaßnahmen der Landtagsverwaltung..... | 4 |
| a) Aufbau des Zutrittskontrollsystems..... | 5 |
| b) Erhebung und Speicherung der Daten..... | 7 |
| aa) Stammdaten..... | 7 |
| bb) Bewegungsdaten..... | 8 |
| c) Löschung der Daten..... | 9 |
| aa) Stammdaten..... | 9 |
| bb) Bewegungsdaten..... | 9 |
| d) Auswertung der Daten..... | 10 |
| e) Übermittlung der Daten..... | 10 |
| f) Sonderfragen..... | 10 |
| aa) Bezahlungsfunktion auf der Karte..... | 10 |
| bb) Besucherkarten..... | 10 |
| 3. Datenschutzrechtliche Zulässigkeit des Verfahrens..... | 11 |
| a) Stammdaten:..... | 11 |
| b) Bewegungsdaten..... | 13 |
| aa) IT-Räume..... | 13 |
| bb) Option: Speicherung der Zutrittsverweigerungen in allen Bereichen | 14 |
| cc) Datenerhebung mit Kenntnis des Betroffenen..... | 14 |
| c) Sonderfälle..... | 15 |
| aa) Besucherkarten..... | 15 |
| bb) Bezahlungsfunktion | 15 |
| 4. Technisch-organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit..... | 15 |
| a) Bestandsaufnahme..... | 15 |
| aa) Hardware..... | 15 |
| bb) Vernetzung..... | 17 |
| cc) Software..... | 18 |
| dd) Datenbestände und Kommunikation | 19 |
| ee) Regelungen..... | 22 |
| b) Verfahrensdokumentation nach § 3 DSVO..... | 24 |
| aa) Verfahrenszweck nach § 4 DSVO..... | 25 |
| bb) Verfahrensbeschreibung nach § 5 DSVO..... | 25 |

| | |
|---|----|
| cc) Sicherheitskonzept nach § 6 DSVO..... | 25 |
| dd) Risikoanalyse..... | 26 |
| ee) Test und Freigabe nach § 7 DSVO..... | 27 |
| ff) Verfahrensübergreifende Dokumentation und Protokolle nach § 8 DSVO..... | 27 |
| 5. Datenschutzmanagementsystem..... | 28 |
| a) Wesentlicher Inhalt..... | 28 |
| b) Bewertung..... | 29 |
| 6. Gesamtbewertung..... | 29 |

I. Gegenstand des Audits

Gegenstand des Audits ist ein automatisiertes Zutrittsberechtigungssystem, durch das der Zutritt in das Landeshaus im Düsternbrooker Weg 70, in das Bürogebäude im Karolinenweg 1 sowie in bestimmte Bereiche innerhalb dieser Gebäude mittels Chipkarte geregelt wird.

Ziel des Zutrittsberechtigungssystems ist es, den Zutritt zum Landeshaus und zum Bürogebäude Karolinenweg nur berechtigten Personen zu gewähren. Vorgesehen sind dazu Personenschleusen und die Sperrung verschiedener Bereiche mittels Chipkarten gesteuerter Türen.

Das Zutrittsberechtigungssystem befindet sich gegenwärtig in der Planungsphase. Einzelne Bestandteile des Systems befinden sich derzeit im Probetrieb. Nach erfolgter Testphase im Echtbetrieb durch ein unabhängiges Unternehmen ist eine Freigabe bis spätestens Ende Oktober vorgesehen.

II. Gegenstand der Begutachtung

- Feinkonzept für das Zutrittsberechtigungssystem, erstellt von der Firma NetUSE AG, Version 146, 21. Mai 2004

- Hinweise der Landtagsverwaltung für die Benutzung der persönlichen Chipkarte (vom September 2004), für den Zugang zum Restaurationsbetrieb Nordhof (vom 7. November 2003), zur Schleusennutzung im Landeshaus (vom 24. November 2003) und zum Schleusenbetrieb zum Nordhof, zur Nutzung der Niedergangstür vom Erdgeschoss zum Nordtor (vom 20. Februar 2004) sowie Ergänzende Hinweise für die Benutzung der persönlichen Chipkarte (vom 20. September 2004).

- Datenschutzmanagementsystem für das Zutrittsberechtigungssystem des Schleswig-Holsteinischen Landtags, Stand: 16. September 2004

III. Bewertung

1. Darstellung der Datenschutzziele

Ziel des Zutrittsberechtigungskonzepts ist die Gewährleistung der Sicherheit im Gebäude des Landeshauses sowie in dem Bürogebäude Karolinenweg durch die Beschränkung des Zutritts auf berechnete Personen. Um die Zutrittsberechtigung zu ermitteln und im Bedarfsfall zu kontrollieren, ist eine personenbezogene Erfassung sämtlicher ständiger Benutzer der geschützten Räumlichkeiten erforderlich. Im Feinkonzept für das Zutrittsberechtigungssystem wird das Spannungsverhältnis zwischen den sicherheitstechnischen Anforderungen auf der einen und den Datenschutzrechten der Betroffenen auf der anderen Seite zum Ausdruck gebracht. Es sollen personenbezogene Daten nur dann verarbeitet werden, wenn dies zur Gewährleistung der Sicherheit in den geschützten Gebäuden erforderlich ist. Dem entsprechend werden im Feinkonzept folgende Zwecke der Datenverarbeitung festgelegt:

- Ermöglichung des Zugangs zum Landeshaus und einzelner Gebäudeteile für berechnete

Personen,

- Abweisung von unberechtigten Personen,
- Nachvollziehbarkeit des Zutritts für besonders geschützte Bereiche und
- Feststellung des Missbrauchs von ausgegebenen Karten.

Um den Datenschutzrechten der Kartenbenutzer Rechnung zu tragen, sind im Feinkonzept folgende Datenschutzziele festgelegt:

- Alle erfassten Daten dürfen nur zu dem Zweck verwendet werden, zu welchem sie erfasst worden sind.
- Es werden nur die personenbezogenen Daten erfasst, die zur Erfüllung des Zweckes benötigt werden.
- Soweit erlaubte Nutzungen im IT-Bereich protokolliert werden, sind auch diese Daten nach einem definierten Zeitraum zu löschen. Eine Nutzung dieser Daten ist alleinig zum Zweck der Sicherstellung und Prüfung der Datensicherheit erlaubt.
- Die erfassten personenbezogenen Daten werden nur so lange gespeichert, wie dies zur Erfüllung des Zweckes notwendig ist. [...]
- Es soll sichergestellt werden, dass die personenbezogenen Daten nur den Personen zugänglich gemacht werden, die für die Bearbeitung zuständig sind.

2. Umsetzung der Ziele durch das Feinkonzept und weitere Umsetzungsmaßnahmen der Landtagsverwaltung

Die Sicherheitsziele werden durch ein System umgesetzt, das den Zugang zu bestimmten Bereichen innerhalb des Landeshauses und des Gebäudes Karolinenweg durch gesicherte Türanlagen beschränkt. Diese Türanlagen, die teilweise mit Vereinzelungsschleusen versehen sind (am Eingang zum Landeshaus, Zutritt Tiefgarage und Übergang vom Kantinenbereich), können mittels einer Chipkarte durch die berechtigten Benutzer geöffnet werden. Beim Betätigen des Türöffners mittels der Chipkarte des Benutzers wird dessen Berechtigung überprüft und im Anschluss der Zugang gewährt bzw. verweigert. Diese Funktionalität wird durch ein System gewährleistet, das wie folgt aufgebaut ist:

a) Aufbau des Zutrittskontrollsystems

Das Landeshaus ist durch Türen zu einzelnen Räumen sowie durch Zwischentüren in den Fluren in einzelne Segmente eingeteilt. Einige dieser Türen sind mit einem Türkontrollsystem ausgestattet, das Türen erst nach einer Berechtigungsüberprüfung öffnet. Dies betrifft in erster Linie Türen in den Fluren, Türen zu IT-Räumen, Türen zum Plenarsaal sowie Eingangstüren im Bereich des Haupteinganges, des Einganges von der Kantine (Nordportal) sowie in der Tiefgarage. Die Eingangstüren sind als Vereinzelungsschleusen ausgebildet und bestehen aus je zwei Türen, von denen jeweils nur eine geöffnet ist. Der durch die beiden Türen begrenzte Raum kann prinzipiell nur von einer Person betreten werden.

Diese Berechtigungsüberprüfung wird mit Hilfe von Chipkarten vorgenommen. Dazu sind die Türen mit einem Chipkartenleser versehen. Durch Vorlage einer Chipkarte, deren Berechtigungsprofil die Öffnung der fraglichen Tür erlaubt, öffnet sich die Tür automatisch bzw. wird ein Schließmechanismus freigegeben.

Die Berechtigungsprüfung und die Öffnung der Türen geschieht im Zusammenspiel zwischen elektro-mechanischen Türöffnern, Kartenlesegeräten, sog. Tür-Controllern, die Daten der Kartenleser auswerten und die elektro-mechanischen Türöffner ansteuern sowie einem Server, in dem zentral die Berechtigungen verwaltet werden. [...]

Die zentrale Einheit für die Steuerung der Türöffnungen sind [...]Nummern, die über eine Zutrittsberechtigung entscheiden. Jeder Chipkarte ist eindeutig eine [...]Nummer zugeordnet. Bei der Vorlage einer Chipkarte an einem Kartenleser wird diese [...]Nummer ausgelesen.

Auf dem zentralen Server zur Verwaltung der Zugriffsberechtigungen [...] sind zu jeder ausgegebenen Chipkarte die Stammdaten des Inhabers sowie sein Berechtigungsprofil gespeichert.[...]

- 6 - durch Kürzung abweichend vom Inhaltsverzeichnis

Die Definition der Zutrittsberechtigungen, die Zusammenstellung der benutzerindividuellen Zutrittsrechte und deren Zuordnung zu einer Karte wird mit Hilfe eines zentralen Servers vorgenommen, der als sog. [...]Server bezeichnet wird (verwendete Software: [...]). Die Software umfasst auch eine Datenbank ([...]), in der die vergebenen Berechtigungen gespeichert werden. Auf diesen Server kann von verschiedenen, eindeutig definierten Arbeitsplätzen zugegriffen werden.

Die in der Datenbank des [...]Server hinterlegten Zugriffsrechte werden an sog. „Tür-Controller“ übertragen und dort gespeichert. Diese Tür-Controller sind sowohl mit Kartenlesern als auch elektro-mechanischen Türöffnern verbunden. Wird eine Karte vorgelegt, so wird vom Kartenleser die Nummer der Karte ausgelesen und an den Tür-Controller übertragen. Dieser entscheidet anhand der gespeicherten Zugriffsrechte, ob die Tür geöffnet werden darf, und steuert gegebenenfalls den elektro-mechanischen Türöffner. Darüber hinaus kann er Informationen über die Nummer der vorgelegten Karte, den Kartenleser sowie die Uhrzeit protokollieren. Art und Umfang der zu protokollierenden Daten werden zentral mit Hilfe des [...]Servers festgelegt und als „Protokollierungsauftrag“ an die Tür-Controller übermittelt. Wurde festgestellt, dass ein zu protokollierendes Ereignis stattgefunden hat (z. B. erfolgreicher oder erfolgloser Versuch einer Türöffnung), so wird zunächst ein Protokolldatensatz im Tür-Controller generiert. Dieser Protokolldatensatz wird in regelmäßigen Zeitabständen vom [...]Servers abgefragt. Dort werden die Protokolldaten gespeichert. Mit Hilfe eines Berechtigungskonzeptes kann festgelegt werden, welcher Benutzer welche Protokolleinträge sehen kann.

Zur Umsetzung der in III. 1 genannten Datenschutzziele, die sich im Wesentlichen an einem strengen Erforderlichkeitsprinzip und einer strengen Zweckbindung orientieren, ist im Feinkonzept folgendes Verfahren zur Verarbeitung der Benutzerdaten vorgesehen:

b) Erhebung und Speicherung der Daten

Für das Zutrittsberechtigungssystem sind zwei verschiedene Arten von Benutzerdaten zu unterscheiden. Zum einen werden im System die so genannten Stammdaten der Benutzer verarbeitet. Hierbei handelt es sich um Identifikationsdaten sowie um die jeweiligen Zutrittsberechtigungen der einzelnen Benutzer. Zum anderen fallen bei der Benutzung des Systems Bewegungsdaten der Nutzer an, sobald diese ihre Karte an den gesicherten Türen benutzen.

aa) Stammdaten

Stammdaten werden für jeden Benutzer erhoben und im System gespeichert, der über eine so genannte persönliche Chipkarte verfügt. Die Chipkarte wird an folgende Personengruppen ausgegeben, die sich regelmäßig im Landeshaus bzw. im Karolinenweg aufhalten:

- der Schleswig-Holsteinische Landtag mit seinen Abgeordneten
- die Mitarbeiter der Fraktionen und des SSW im Landtag
- die Landtagsverwaltung
- die Ministerpräsidentin und Teile der Staatskanzlei
- die Bürgerbeauftragte für soziale Angelegenheiten
- der Beauftragte für Flüchtlings-, Asyl- und Zuwanderungsfragen
- Journalisten der Landespressekonferenz

Für diese Benutzergruppen werden die Stammdaten derjenigen Mitarbeiter, die eine Chipkarte für den Zutritt zum Landeshaus / Gebäude Karolinenweg erhalten sollen, durch die jeweiligen Stellen an die Landtagsverwaltung gemeldet. [...] Die Stammdaten werden [...] auf dem [...]Server gespeichert. Zusätzlich wird durch den Kartenadministrator ein Foto des Benutzers gefertigt und ebenfalls auf dem [...]Server gespeichert. Im Einzelnen handelt es sich um folgende Stammdaten:

[...]

- Name des Karteninhabers
- Passfoto des Karteninhabers
- Organisationseinheit
- Gültigkeit der Karte
- Karte gesperrt
- Funktion
- Ausweisart
- laufende Nummer

Die für die Eingabe dieser Daten im System verfügbare Eingabemaske enthält nur Felder für die Eingabe dieser Daten. Weitere Eingabefelder sind nicht vorhanden.

[...] Die Chipkarten werden durch die Landtagsverwaltung ausgestellt. Bei der Aushändigung der Chipkarte erhält jeder Nutzer ein Hinweisblatt zum Umgang mit der Chipkarte. Das Hinweisblatt enthält Informationen zur Verarbeitung dieser Stamm- sowie der Bewegungsdaten.

bb) Bewegungsdaten

Bei Benutzung der Chipkarte an den Kartenlesegeräten der gesicherten Türen wird die Nummer der verwendeten Karte durch die Tür-Controller erfasst und mit der dort gespeicherten Berechtigung abgeglichen. Anschließend wird bei bestätigter Berechtigung der Zutritt gewährt, anderenfalls wird er verweigert.

Grundsätzlich werden nach dem Konzept die hierbei anfallenden Daten (Kartenummer, Ort und Zeitpunkt des Einsatzes der Karte, Zugang gewährt oder verweigert) nicht gespeichert. Eine Ausnahme erfolgt ausschließlich für den Bereich der IT-Räume. [...] Angesichts des besonderen Sicherheitsbedarfs sollen nach dem Konzept sämtliche berechnete Zugänge zu diesem Bereich gespeichert werden. Die Protokollierung beschränkt sich auf den Zutritt zu den IT-Räumen und die Verweigerung des Zutritts, der Austritt wird nicht protokolliert.[...] Der Zugriff auf die Zutrittsprotokolle ist auf den IT- und den Karten-Administrator beschränktX

Zusätzliche Option:

Zusätzlich zu der Protokollierung im Bereich der IT-Räume ist im Feinkonzept eine Lösung vorgesehen, nach der sämtliche verweigerten Zutritte in allen Bereichen gespeichert werden sollen. Zweck dieser Speicherung ist die automatisierte Erkennung von missbräuchlichen Kartennutzungen. [...] In einem solchen Fall soll durch das System ein Alarm in der Pförtnerie ausgelöst werden.

[...]

Nach dem gegenwärtigen Stand der Planungen soll die Alarmfunktion bis auf Weiteres nicht realisiert werden. Da nach Ansicht der Landtagsverwaltung aus diesem Grund auch die Protokollierung der Zutrittsverweigerungen nicht erforderlich ist, soll diese ebenfalls unterbleiben. Die Einrichtung einer Alarmfunktion und damit die Protokollierung der Zutrittsverweigerungen wird jedoch weiterhin durch die Landtagsverwaltung geprüft und eventuell zukünftig nachgerüstet.

c) Löschung der Daten

aa) Stammdaten

Die Stammdaten werden für die Dauer der Gültigkeit der Karte gespeichert.[...]

[...]

bb) Bewegungsdaten

Die an den Zugängen zu den IT-Räumen erhobenen Bewegungsdaten werden für die Dauer eines definierten Zeitraumes im Protokolldatenbestand des [...]Server gespeichert.-Spätestens nach Ablauf dieser Frist werden die Daten gelöscht.

d) Auswertung der Daten

[...] Zugriff auf diese Daten haben nur der IT- und der Karten-Administrator. Diesen Personen ist auch die Zuordnung der Kartenummer zu den Daten des Benutzers möglich. Eine zulässige Auswertung des Protokolls ist nach dem Feinkonzept nur für den Zweck der Sicherstellung und Prüfung der Datenintegrität vorgesehen.

e) Übermittlung der Daten

Nach dem Datenschutzmanagementsystem ist vorgesehen, Stammdaten der Karteninhaber in bestimmten Fällen an andere Stellen zu übermitteln. Dabei handelt es sich um folgende Fälle:

Diejenigen Stellen, deren Mitarbeiter über eine persönliche Chipkarte verfügen (d.h. z.B. die Staatskanzlei, die Bürgerbeauftragte für soziale Angelegenheiten) erhalten in Abständen eine Übersicht über die von ihnen gemeldeten Karteninhaber. Durch dieses Verfahren soll kontrolliert werden, ob die von einer Stelle gemeldeten Karteninhaber noch dort beschäftigt sind und weiterhin mit den vergebenen Zutrittsberechtigungen ausgestattet sein sollen.

Darüber hinaus ist vorgesehen, denjenigen Stellen, die sich in Bereichen des Landeshauses befinden, die nur bestimmten Personenkreisen zugänglich sind, auf Nachfrage eine Übersicht über die Personen zur Verfügung zu stellen, die über eine Zutrittsberechtigung zu dem jeweiligen Bereich verfügen.[...]

f) Sonderfragen

aa) Bezahlungsfunktion auf der Karte

Nach Angabe in den Hinweisen der Landtagsverwaltung für die Benutzung der persönlichen Chipkarte ist die Chipkarte mit einer Bezahlungsfunktion für den Kantinenbetrieb im Landeshaus ausgestattet. Die Daten des Zahlungsverkehrs werden nach den Angaben in den Hinweisen der Landtagsverwaltung ausschließlich durch den Kantinenbetreiber verarbeitet. Es erfolgt keine Zusammenführung der mittels der Chipkarte erhobenen Daten.

bb) Besucherkarten

(1) Tagesbesucher

Tagesbesucher können in der Pförtnerie gegen Hinterlegung ihres Personalausweises eine Besucherkarte erhalten. Auf den vorgefertigten Besucherkarten sind eine Kartenummer sowie die Zutrittsberechtigungen gespeichert. Weitere Daten enthalten die Besucherkarten nicht. In der Pförtnerie wird bei der Ausgabe der Karten nicht vermerkt, an welchen Benutzer welche Karte ausgegeben wird. Eine Zuordnung der Karte zu der Person des Benutzers kann bei Abgabe der Karte vorgenommen werden, da der Pförtner hierbei die entlehene Besucherkarte entgegennimmt und den zugehörigen Personalausweis dem Besucher aushändigt.

(2) Kantinengäste

Vorgefertigte Karten können ebenfalls für den Zugang zur Kantine erworben werden. Diese Karten berechtigen den Nutzer, über das Nordtor in die Kantine zu gelangen. Die Karten können in der Kantine an einem Automaten erworben werden. Vor Erwerb der Karte soll sich der Benutzer in der Pförtnerie melden. Dort werden jedoch keine Angaben über den Kartenbenutzer erhoben. Die "Kantinenkarte" enthält eine Kartenummer und die Zutrittsberechtigung für den Eingang Nordtor. Weitere Angaben über den Benutzer enthält die Karte nicht. Wie die persönliche Chipkarte für die Prüfung der Zutrittsberechtigung ist auch die "Kantinenkarte" mit einer Bezahlungsfunktion für den Kantinenbetrieb ausgestattet.

3. Datenschutzrechtliche Zulässigkeit des Verfahrens

Das Feinkonzept setzt sich umfangreich mit den datenschutzrechtlichen Vorgaben für die Gestaltung eines Zutrittsberechtigungs-systems und der Zulässigkeit der geplanten Maßnahme auseinander. Dabei kommen die Verfasser zu dem Ergebnis, dass die Einführung des Zutrittsberechtigungs-systems unter Erhebung und weiterer Verwendung der Stammdaten der Kartennutzer auf der Grundlage des Hausrechts des Landtagspräsidenten zulässig ist. Eine Protokollierung der einzelnen Kartennutzungen ist nach den Ausführungen im Feinkonzept

für unberechtigte Nutzungen ebenfalls vom Hausrecht des Landtagspräsidenten erfasst. In besonders schützenswerten Bereichen kann auch die Protokollierung der berechtigten Nutzungen geboten sein. Dies wird für den Bereich der IT-Räume angenommen, da sich aus dem Datenschutzrecht die Pflicht ergebe, durch technisch-organisatorische Maßnahmen den Schutz von personenbezogenen Daten - die innerhalb der IT-Räume zugänglich sein können - zu gewährleisten, vgl. §§ 5, 6 Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH).

Die dem Feinkonzept zu Grunde liegenden datenschutzrechtlichen Erwägungen sind aus Sicht des Unabhängigen Landeszentrums für Datenschutz zutreffend. Die Zulässigkeit der Erhebung und Verwendung der Stamm- und Bewegungsdaten beurteilt sich aus Sicht des ULD folgendermaßen:

a) Stammdaten:

Die oben aufgeführten Stammdaten der Kartennutzer werden nach Angaben des Feinkonzepts durch die personalbearbeitenden Stellen an die Landtagsverwaltung übermittelt. Durch die Landtagsverwaltung werden die Stammdaten in das System eingegeben und die entsprechenden Karten mit den entsprechenden Angaben erstellt.

Gemäß § 1 Abs. 2 Ziff. 3 Datenschutzordnung des Landtags (DSO LT) ist für das Zutrittsberechtigungssystem das LDSG SH anwendbar. Es handelt sich dabei um ein System zur Wahrnehmung des Hausrechts.

Soweit es sich bei der Meldung von Mitarbeitern, die mit einer persönlichen Chipkarte ausgestattet werden sollen, um eine Übermittlung von personenbezogenen Daten handelt, ist diese gemäß § 14 i.V.m. § 11 Abs. 1 Nr. 3 LDSG SH zulässig. Die Landtagsverwaltung als empfangende und weiter verarbeitende Stelle benötigt diese Angaben zur rechtmäßigen Erfüllung ihrer eigenen Aufgaben.

Als Rechtsgrundlage für die Verarbeitung der Stammdaten im Rahmen des Zutrittsberechtigungssystems kommt § 11 Abs. 1 Ziff. 3 LDSG SH in Betracht. Danach ist die Verarbeitung personenbezogener Daten zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben der Daten verarbeitenden Stelle erforderlich ist. Zu den Aufgaben bzw. Befugnissen des Landtagspräsidenten gehört gemäß Art. 14 Abs. 3 der Landesverfassung die Geschäftsführung, zu der Satz 2 ausdrücklich die Ausübung der Ordnungsgewalt im Landtag und des Hausrechts in den Räumen des Landtags zählt.

Das öffentliche Hausrecht ist das einem Hoheitsträger zustehende Bestimmungsrecht über Zutritt und Verweilen von Personen in einem räumlich geschützten Herrschaftsbereich sowie die damit zusammen hängenden Befugnisse¹. Kernaufgabe bei der Wahrnehmung des Hausrechts ist die Verweigerung des Zutritts zu den Räumen des Landtags für Unbefugte. Dies setzt voraus, dass die Personen, die die Räume des Landtags betreten, bekannt sind bzw. ihre Zugehörigkeit zur Gruppe der Befugten oder Unbefugten bekannt ist. Somit erfordert die Zuordnung der Zutritt ersuchenden Personen zu einer dieser beiden Gruppen Kenntnisse über die Person. Um eine Kontrolle zu ermöglichen, ob es sich bei dem Karteninhaber tatsächlich um die Person handelt, deren Zutrittsberechtigung durch Ausstellung einer Karte bestätigt wurde, ist es erforderlich, die Stammdaten der Person wie Name, Organisationseinheit etc. sowie zusätzlich ein Passfoto zum Abgleich der Identität der Person mit dem Karteninhaber auf der Karte zu speichern. Die Erhebung und Speicherung der Stammdaten der

¹ VG Frankfurt am Main, NJW 1998, S. 1424; VGH Kassel, NJW 1990, S. 1250.

Karteninhaber ist somit zulässig.

Ebenfalls zulässig ist die vorgesehene Übermittlung der Stammdaten an die Stellen, die die Karteninhaber an die Landtagsverwaltung melden. Rechtsgrundlage für die Übermittlung der Daten ist § 14 Abs. 1 i.V.m. § 11 Abs. 1 Ziff. 3 LDSG SH. Zur Ausübung des Hausrechts ist nicht nur die einmalige Erfassung der Benutzer, sondern auch eine fortlaufende Aktualisierung des Nutzerbestands erforderlich. Um den Zweck des Zutrittsberechtigungssystems zu erreichen, ist eine regelmäßige Überprüfung der Karteninhaber im Hinblick darauf notwendig, ob die Grundlage für deren Zutrittsberechtigung weiterhin besteht.

Auch die vorgesehene Übermittlung der Stammdaten an die im Landeshaus befindlichen Stellen ist gemäß § 14 Abs. 1 i.V.m. § 11 Abs. 1 Ziff. 3 LDSG SH zulässig. Bezüglich der IT-Räume fällt diese Auskunft der Ausübung des Hausrechts des Landtagspräsidenten sowie dessen Verantwortlichkeit für die Gewährleistung der Datensicherheit. Für den Bereich der Ministerpräsidentin und der Staatskanzlei ist deren eigenes Hausrecht an den von ihnen belegten Bereichen maßgeblich. Zur Ausübung dieses Hausrechts ist die Kenntnis sämtlicher zutrittsberechtigter Personen erforderlich. Gleiches gilt für den Küchenbereich, der von einem Pächter betrieben wird. Die Übermittlung der zutrittsberechtigten Personen an den Pächter, der eine nicht öffentliche Stelle im Sinne des LDSG SH ist, ist auf Grundlage des § 15 Abs. 1 Ziff. 1 LDSG SH zulässig, da dieser aufgrund seines Hausrechts ein berechtigtes Interesse an den zu übermittelnden Daten hat. Durch die Übermittlung werden schutzwürdige Belange der Betroffenen nicht beeinträchtigt.

Gemäß § 1 Abs. 2 Nr. 3 DSO LT i.V.m. § 28 Abs. 2 Nr. 2 LDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist. Gibt ein Karteninhaber seine Karte zurück, werden die Stammdaten umgehend durch die Landtagsverwaltung gelöscht. Wird eine Karte durch den Inhaber als verloren oder gestohlen gemeldet, so erfolgt eine Sperrung der Karte. Die Stammdaten werden für einen definierten Zeitraum gespeichert und nach Ablauf dieser Frist gelöscht. Diese Speicherfrist erscheint aus Gründen der Beobachtung der weiteren Nutzung der Karte durch Unbefugte angemessen.

Verliert die Karte nach Zeitablauf ihre Gültigkeit, wird sie aber vom Karteninhaber nicht zurückgegeben und nicht verlängert, so werden die Stammdaten für einen definierten Zeitraum gespeichert und dann gelöscht. In diesem Fall erscheint eine derart lange Aufbewahrungsfrist angemessen. Grund dafür ist die bestehende Möglichkeit einer weiteren Verlängerung der Karte, für die dann auf die noch gespeicherten Stammdaten zurückgegriffen werden kann. Erst im Fall der Rückgabe der Karte bringt der Karteninhaber unzweifelhaft zum Ausdruck, dass er an einer weiteren Nutzung der Karte nicht interessiert ist. Unterlässt er dies, besteht Grund für die Vermutung, dass eine Verlängerung der Gültigkeit zukünftig beantragt wird. Die Speicherung in dem definierten Zeitraum stellt keine unverhältnismäßige Verletzung der Interessen des Betroffenen dar, da dieser jederzeit durch Rückgabe seiner Karte die Möglichkeit hat, die sofortige Löschung seiner Stammdaten zu veranlassen.

b) Bewegungsdaten

Bei der Nutzung der Karte an den Türen zu den entsprechend gesicherten Bereichen des Landtags fallen Bewegungsdaten an. Nach dem Feinkonzept soll die Protokollierung der Zugänge nur im IT-Bereich erfolgen (a). Als zusätzliche Variante kommt eine Speicherung der verweigerten Zutritte in allen Bereichen des Zutrittsberechtigungssystems in Betracht, die nach dem Konzept als Option vorgesehen ist (b).

aa) IT-Räume

Eine Speicherung der Zutrittsbewilligung soll nach dem Konzept nur an den Zugängen zu den IT-Räumen erfolgen. Hier wird die Tatsache der Zutrittsbewilligung sowie Datum und Uhrzeit [...] gespeichert. Ebenso werden abgewiesene Zutrittsversuche gespeichert. [...] Beim Verlassen der Räume erfolgt keine Kontrolle der Zutrittsberechtigung und somit keine Protokollierung des Verlassens.

Die Speicherung und Nutzung dieser Bewegungsdaten durch die Landtagsverwaltung ist zum Zweck der Sicherheitskontrolle der IT-Einrichtungen zulässig. Nach der Landesverfassung ist dem Landtagspräsidenten die Aufgabe der Ausübung der Ordnungsgewalt im Landtag zugewiesen. In diesem Rahmen hat er die Sicherheit besonders schützenswerter Einrichtungen sowie die Sicherheit der durch den Landtag verarbeiteten personenbezogenen Daten zu gewährleisten. Dabei ist er gemäß § 11 Abs. 2 der Datenschutzordnung des Landtags an die §§ 5 und 6 LDSG SH gebunden. § 5 Abs. 1 Nr. 3 LDSG SH sieht ausdrücklich vor, dass durch technische oder organisatorische Maßnahmen zu gewährleisten ist, dass die Daten verarbeitende Person sowie der Zeitpunkt und Umfang der Datenverarbeitung festgestellt werden kann. Die Protokollierung der Zutritte zu den IT-Räumen ist eine Maßnahme, um zu dokumentieren, welche Person zu welchem Zeitpunkt einen bestimmten Raum betreten hat. Das hierüber erstellte Protokoll der Bewegungsdaten dient zumindest als Anhaltspunkt zur Ermittlung der Aufenthalte bestimmter berechtigter Personen in den IT-Räumen.

Auch die Bewegungsdaten sind zu löschen, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Die Landtagsverwaltung hat eine Löschung nach Ablauf eines definierten Zeitraumes vorgesehen, da dieser Zeitraum von der Landtagsverwaltung als ausreichend, aber auch erforderlich erachtet wird, um eventuelle Missbräuche innerhalb der IT-Räume festzustellen, für deren Aufklärung die Protokoll Daten als Anhaltspunkte benötigt werden können.

bb) Option: Speicherung der Zutrittsverweigerungen in allen Bereichen

Nach dem Feinkonzept ist als Option vorgesehen, in allen Bereichen sämtliche Zutrittsverweigerungen zu speichern. Die Protokollierung hat nach dem Konzept den Zweck, einen Missbrauch der Karte festzustellen und durch Auslösung eines Alarms Maßnahmen zur Unterbindung des weiteren Kartenmissbrauchs zu ermöglichen. [...]

[...]

Die Speicherung der Zutrittsverweigerung kann zur Wahrung des Hausrechts als erforderlich angesehen werden. Es liegt im berechtigten Interesse des Landtagspräsidenten, eine missbräuchliche Nutzung der Karte zu ermitteln und diese zu unterbinden sowie die Karte zu sperren und weitere Maßnahmen gegen den Kartennutzer zu ergreifen.

[...]

cc) Datenerhebung mit Kenntnis des Betroffenen

§ 13 Abs. 1 Satz 1 LDSG SH sieht vor, dass personenbezogene Daten nur mit Kenntnis des Betroffenen zu erheben sind. Über die Vorschrift des § 1 Abs. 2 Ziff. 3 der Datenschutzordnung des Landtages gilt dieses Gebot auch für das Zutrittsberechtigungssystem. In der Praxis bedeutet dies, dass das Zutrittsberechtigungssystem, welches mit kontaktlosen Chipkarten arbeitet, sicherstellen muss, dass Daten der Benutzer nur durch eine aktive Handlung der Benutzer erhoben werden. Benutzerdaten dürfen mit anderen Worten durch die Kartenlesegeräte nicht bereits dann erhoben werden, wenn ein Karteninhaber an einem Lesegerät in einem bestimmten Abstand vorbeigeht, ohne dabei eine Öffnung der Tür veranlassen zu wollen und ohne die hierfür erforderliche Mitwirkung zu tätigen. Diese Anforderung ist durch die Gestaltung der Kartenlesegeräte vorliegend erfüllt. Typische Maximalreichweiten der Kartenleser werden im Konzept und der Gerätespezifikation mit 5-10 cm angegeben. In der Praxis ist es notwendig, die Karte direkt an den Kartenleser anzupressen.

c) Sonderfälle

aa) Besucherkarten

Besucherkarten werden wie oben beschrieben als vorgefertigte Karten durch die Pförtnerie oder durch einen Automaten im Kantinenbereich ausgegeben.

Bei der Ausgabe der so genannten "Kantinenkarten" werden keinerlei personenbezogene Daten der Benutzer erhoben. Eine Zuordnung der Kartenummer zu dem jeweiligen Kartennutzer ist somit nicht möglich. Somit erfolgt die Ausgabe und die Nutzung der Karte anonym und unterliegt keinen datenschutzrechtlichen Beschränkungen.

Anders verhält es sich bei den Tagesbesuchern, die eine Chipkarte gegen Abgabe ihres Personalausweises in der Pförtnerie erhalten. Bei Rückgabe der Chipkarte gegen Rückgabe des Personalausweises wird in der Pförtnerie ein Personenbezug der Karte hergestellt. Eine Speicherung dieses Personenbezugs ist jedoch nicht vorgesehen.

Die Erhebung der Personalausweisdaten durch die Pförtnerie ist als Maßnahme der Einlasskontrolle im Rahmen der Ausübung des Hausrechts des Landtagspräsidenten zulässig. Eine Erhebung und Speicherung der Bewegungsdaten der Besucher erfolgt nur im Bereich der IT-Räume, dort werden auch die abgewiesenen Zutrittsversuche protokolliert. Diese Maßnahme ist im Rahmen der Ausübung des Hausrechts des Landtagspräsidenten zulässig.

Im Fall der Realisierung der Zusatzoption erfolgt ebenfalls eine Erhebung und Speicherung der Bewegungsdaten (Protokollierung der Zutrittsverweigerungen an sämtlichen Türen). Diese Maßnahme liegt ebenfalls im rechtmäßigen Rahmen der Ausübung des Hausrechts des Landtagspräsidenten und ist auf dieser Rechtsgrundlage zulässig.

bb) Bezahlfunktion

Die Chipkarten enthalten neben der Zutrittsberechtigung auch eine Bezahlfunktion, mittels

derer die Karte im Kantinenbetrieb zur bargeldlosen Zahlung verwendet werden kann. Für die unterschiedlichen Funktionen bestehen jeweils unterschiedliche Verantwortungen. Für die Datenverarbeitung zum Zweck des Zutrittsberechtigungs-systems ist die Landtagsverwaltung verantwortliche Stelle; die Abrechnung des Zahlungsverkehrs unterliegt der Verantwortung des Kantinenbetreibers, der mit der Landtagsverwaltung nicht identisch ist. Aus datenschutzrechtlicher Sicht ist eine strikte Trennung der Datenverarbeitung dieser Bereiche geboten, die nach den Angaben im Feinkonzept realisiert ist.

4. Technisch-organisatorische Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit

a) Bestandsaufnahme

aa) Hardware

Die zu verwendende Hardware ist in Abschnitt 5.2 des Konzeptes beschrieben. Sie besteht aus folgenden wesentlichen Teilen:

Zutrittssicherung:

[...]

bb) Vernetzung

Ein zentraler Bestandteil der Hardware ist die Vernetzung der einzelnen Hardwarekomponenten. Diese enthält auch Software-Komponenten, wird hier aber wegen der Bedeutung der Vernetzung als reine Infrastrukturmaßnahme behandelt. Diese Vernetzung zerfällt in zwei Teile. [...]

Interne Vernetzung (SecLAN)

[...]

Intrusion Detection System

[...]

Dokumentation

[...]

Vernetzung der Peripheriegeräte

[...]

cc) Software

Die verwendete Software ist in Abschnitt 5.3 des Konzeptes beschrieben. [...]

Betriebssystem:

[...]

Systemhärtung

[...]

Weitere Software:

[...]

Virenschutz

[...]

dd) Datenbestände und Kommunikation

In den einzelnen Hardware-Bauteilen sind unterschiedliche Datenbestände gespeichert bzw. werden unterschiedliche Daten übermittelt. Die zwischen den einzelnen Bestandteilen übermittelten Daten sind in Abschnitt 5.4 beschrieben. Im Einzelnen sind dies:

Karten:

[...]

Die Karten verfügen über mehrere Speicherbereiche, die nur mit Hilfe kryptographischer Schlüssel zugänglich sind. [...]

Kommunikation zwischen Karten und Kartenlesegerät:

[...]

In der Realisierung wird ein Verfahren eingesetzt, in dem sich Kartenleser und Karte gegenseitig authentisieren. Durch eine Challenge-Response-Verfahren werden zufallsabhängige Authentisierungsdaten verwendet, die sich bei jeder Anwendung ändern. Konkret wird überprüft, ob der Kommunikationspartner auf eine zufällig gewählte („Challenge“) eine richtige Antwort („Response“) nennen kann. Durch dieses Verfahren kann sichergestellt werden, dass eine Aufzeichnung der Authentisierungsdaten kein zweites Mal verwendet werden kann.

[...]

Die Kommunikation zwischen Kartenleser und Karten erfolgt kontaktlos. Typische Maximalreichweiten werden im Konzept mit 5-10 cm angegeben. In der Praxis ist es notwendig, die Karte direkt an den Kartenleser anzupressen.

Kartenlesegerät:

Die Kartenlesegeräte selbst speichern keine Daten.

Kommunikationsabläufe

[...]

[...]

[...]

[...]

[...]

ee) Regelungen

Nutzungsrechte

[...]

Nutzerauthentisierung

[...]

Protokolldaten

[...]

Datensicherung

[...]

b) Verfahrensdokumentation nach § 3 DSVO

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

aa) Verfahrenszweck nach § 4 DSVO

Das vorliegenden Feinkonzept stellt die Bereiche Zutrittsberechtigungssystem, Einbruch-Meldeanlage, 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.

bb) Verfahrensbeschreibung nach § 5 DSVO

Gemäß § 5 DSVO 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 Abschnitt 5. Die Beziehungen zu den Verfahren Einbruch- und Brandmeldeanlage sowie zur Infrastruktur (Vernetzung SecLAN) werden in den Abschnitten 4, 6 und 7 dargestellt.

Die detaillierte Dokumentation der Programme einschließlich ihrer Konfiguration gemäß § 5 Abs. 2 DSVO wird verschiedentlich im Konzept angesprochen (s. Abschnitt 4.7 für das SecLAN, Abschnitt 5.7 für das Zutrittsberechtigungssystem). 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.

cc) Sicherheitskonzept nach § 6 DSVO

Gemäß § 6 DSVO ist ein Sicherheitskonzept sowie ggf. eine Risikoanalyse zu erstellen, in dem 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 an vielen Stellen ausführlich dargestellt. [...]

Zutrittsberechtigungssystem:

[...]

dd) Risikoanalyse

Eine Risikoanalyse des Verfahrens Zutrittsberechtigungssystem ist in Abschnitt 5.8 des Konzeptes enthalten. Entstehende Risiken werden nach zwei Arten unterschieden: Zum einen gibt es Risiken, die mit den Risiken herkömmlicher Zutrittskontrollverfahren durch mechanische Schlösser vergleichbar sind (Verlust, Diebstahl und Kopie von Schlüsseln bzw. Karten). Zum anderen gibt es Risiken, die durch das neue Zutrittsberechtigungssystem erst geschaffen werden. Im Konzept werden im Abschnitt 5.8.2 die Risiken der Datenspionage, des Systemausfalls, der Bedienfehler, der Sabotage und der Softwarefehler beleuchtet. Von entscheidender Bedeutung für datenschutzrechtliche Fragen ist die Analyse im Bereich der „Datenspionage“, wo die Risiken einer unbefugten Kenntnisaufnahme von Stammdaten und von Bewegungsdaten untersucht werden. Unterschieden wird dabei nach Zugriffen durch Unbefugte (Außentäter) und Zugriffen durch die Administration, die unzulässigerweise ihre Zugriffsberechtigungen erweitert bzw. unzulässigerweise eine nicht geplante Erhebung von Bewegungsdaten durch eine Umkonfiguration veranlasst.

[...]

[...]

Die Analyse unterscheidet weiter nach potentiellen Angreifertypen. Untersucht werden Angriffe durch Einbrecher, psychisch verwirrte Einzeltäter, Insider, politisch motivierte Terroristen mit geringen Fähigkeiten, politisch motivierte Terroristen mit hohen Fähigkeiten, Geheimdienste sowie Hacker.

[...]

ee) Test und Freigabe nach § 7 DSVO

Die Überprüfung der festgelegten Sicherheitsmaßnahmen ist im Konzept durch dataport als Gesamtmaßnahme vorgesehen. Dies betrifft Einzelaspekte wie beispielsweise die Härtung von Betriebssystemen (Abschnitt 5.3.3) oder den Test der Systemwiederherstellung im Fehlerfall (5.6.3.2). Die Tests sind zu protokollieren. Erst nach dem Test kann eine formelle Freigabe erfolgen, die schriftlich zu erteilen ist.

ff) 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 bb) 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 cc) Sicherheitskonzept nach § 6 DSVO wurde festgestellt, dass die konkrete Umsetzung im Datenschutzmanagement vorzunehmen ist.

5. Datenschutzmanagementsystem

Zur Umsetzung der Datenschutzziele hat die Landtagsverwaltung gemäß Tz. B 7 der Anwendungsbestimmungen des ULD für die Durchführung von Datenschutzaudits ein Datenschutzmanagementsystem eingerichtet.

a) Wesentlicher Inhalt

Das Datenschutzmanagementsystem legt die zur Erfüllung dieser Ziele erforderlichen Aufgaben sowie die Zuständigkeiten innerhalb der Landtagsverwaltung für deren Durchführung fest. Insgesamt sind die im Datenschutzmanagementsystem beschriebenen Maßnahmen darauf angelegt, für den gesamten Zeitraum der Auditierung das bislang erreichte Datenschutzniveau aufrechtzuerhalten und in Teilen weiter zu verbessern.

Nach den Festlegungen im Datenschutzmanagementsystem liegt die Gesamtverantwortlichkeit für die Erfüllung der Datenschutzziele und die Einhaltung der datenschutzrechtlichen Vorgaben bei der Leitung der Abteilung Zentrale Angelegenheiten und Service. Die Zuständigkeiten für die bauliche Einrichtung und Technik sowie die Benutzerverwaltung liegen im Referat Liegenschaften, Innerer Dienst und für die IT-Technik im Referat Informations- und KommunikationsmanagementX

Das Datenschutzmanagementsystem sieht den Erlass einer Dienstanweisung für den Karten- und den IT-Administrator vor, die mit dem Zutrittsberechtigungssystem befasst sind. Des Weiteren soll ein Intrusion Detection System eingerichtet werden, um die Sicherheit des Netzwerks durch Kontrolle auf bekannte Angriffssignaturen und verdächtige Aktivitäten zu erhöhen.

Ein Test des Systems soll nach Festlegung im Datenschutzmanagementsystem durch dataport durchgeführt werden und eine Freigabe durch den Landtagspräsidenten bis Ende Oktober 2004 erfolgen.

Das Datenschutzmanagementsystem sieht weiterhin eine fortlaufende Fortschreibung der Dokumentation vor. Sämtliche Änderungen und Ergänzungen im IT-Konzept sollen fortgeschrieben werden und es sollen die noch abzugebenden Dokumentationen der beauftragten Fachplaner und Fachfirmen in die Gesamtdokumentation integriert werden.

Ferner werden im Datenschutzmanagementsystem dauerhafte Maßnahmen wie die Fortbildung der Administratoren, eine fortlaufende Bestandsaufnahme und die Meldung von wesentlichen Änderungen an das Datenschutzgremium und das ULD festgelegt.

Das Datenschutzmanagementsystem sieht des Weiteren eine regelmäßige stichprobenartige externe Kontrolle im Auftrag des Datenschutzgremiums vor. [...]

b) Bewertung

Die im Datenschutzmanagementsystem festgelegten Maßnahmen sind insgesamt 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 insbesondere die Dokumentation des Verfahrens, deren Ergänzung an einigen Stellen für den praktischen Einsatz des Konzepts erforderlich ist (siehe oben Tz. III 4). Ebenso wird durch die Verpflichtung im Datenschutzmanagementsystem, eine Dienstanweisung 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.

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.

6. Gesamtbewertung

Das Feinkonzept zur Gestaltung des Zutrittsberechtigungssystems sowie die zur Umsetzung des Feinkonzepts durch die Landtagsverwaltung ergriffenen und weiterhin geplanten Maßnahmen erfüllen die rechtlichen Anforderungen des Datenschutzes. Insbesondere wird dem Gebot der Datenvermeidung und Datensparsamkeit Genüge getan, da auf eine Erhebung von Bewegungsdaten in weitem Maße verzichtet und diese nur für besonders sicherheitsrelevante Zwecke eingesetzt wird. Durch die gegenwärtige technische Umsetzung und die zusätzlich vorgesehenen und im Datenschutzmanagementsystem festgeschriebenen Maßnahmen wird den Anforderungen an die Datensicherheit in vorbildlicher Weise entsprochen. Die Verleihung des Datenschutz-Audits gemäß § 43 Abs. 2 LDSG SH ist damit gerechtfertigt.

-