Landesbeauftragter
für den Datenschutz
Sachsen-Anhalt

Datenschutzmanagement

Stand: 10.10.2011

Herausgeber:

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt
Leiterstraße 9, 39104 Magdeburg
Postfach 1947, 39009 Magdeburg
Telefon: 0391 81803 0
Fax: 0391 81803 33
Freecall: 0800 9153190 (Festnetz DTAG in Sachsen-Anhalt)
Internet: www.datenschutz.sachsen-anhalt.de
E-Mail: poststelle@lfd.sachsen-anhalt.de

Inhaltsverzeichnis

...

1. Was ist überhaupt Datenschutz? Und was ist Datenschutzmanagement?

Beim Datenschutz stehen die natürlichen Personen, über die Informationen verarbeitet werden, im Mittelpunkt. Rechtlicher Ausgangspunkt ist das Grundrecht auf informationelle Selbstbestimmung. Jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten setzt nach den Vorgaben des Bundesverfassungsgerichts aus dem sog. Volkszählungsurteil vom 15. Dezember 1983 eine Rechtsgrundlage und damit eine Rechtsvorschrift als Erlaubnisnorm oder die Einwilligung des Betroffenen voraus. Für alle öffentlichen Stellen des Landes Sachsen-Anhalt bildet das Gesetz zum Schutz personenbezogener Daten der Bürger **(DSG LSA)** diese Rechtsgrundlage, falls keine Rechtsvorschrift im Landes- oder Bundesrecht als spezialgesetzliche Regelung zum Datenschutz existiert und damit dem DSGLSA vorgeht. (Das Gesetz und die dazu ergangenen Verwaltungsvorschriften können von der Homepage des Landesbeauftragten abgerufen werden.)

1.1 Datenschutz

Datenschutz beschreibt die Daueraufgabe der öffentlichen Stellen, dafür zu sorgen, dass beim Umgang mit personenbezogenen Informationen den verfassungsrechtlichen und gesetzlichen Anforderungen zum Schutz des Persönlichkeitsrechts umfassend Rechnung getragen wird. Der Konzeption und Ausführung konventioneller Verwaltungstätigkeiten und auch der automatisierten Verarbeitung personenbezogener Daten muss der Datenschutz stets immanent sein. Er stellt damit eine gestaltende Querschnittsaufgabe dar.

1.2 Datenschutzmanagement

Mit Datenschutzmanagement werden alle zu organisierenden Prozesse bezeichnet, die erforderlich sind, um die Umsetzung aller datenschutzrechtlichen Anforderungen beim Umgang öffentlicher Stellen mit personenbezogenen Daten präventiv sicher zu stellen. Das gilt für automatisierte und für konventionell aktengestützte Verfahren gleichermaßen.

2. Datenschutzmanagement - Wer ist verantwortlich, wer ist überhaupt zuständig?

Die Pflicht zur Einhaltung datenschutzrechtlicher Vorgaben obliegt der verantwortlichen Stelle insgesamt. Datenschutz ist aber auch Teil jeder Fachaufgabe. Die Einhaltung des Datenschutzes durch organisatorische Vorgaben sicherzustellen, ist als Datenschutzmanagement verantwortliche Aufgabe der Behördenleitung. Von dort werden alle relevanten Prozesse durch ein Datenschutzkonzept initiiert. Die primäre Verantwortlichkeit der Behördenführung leitet sich aus § 14 Abs. 1 Satz 1 DSG LSA ab und gilt auch dann, wenn ein Teil der Datenschutzmanagement-Aufgaben und damit der Verantwortung auf einen Beauftragten für den Datenschutz übertragen worden ist.

Aber auch **jeder Beschäftigte** ist für den Datenschutz verantwortlich. Denn nach § 5 Satz 1 DSG LSA ist den bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Jeder Beschäftigte trägt damit in seinem Aufgabenfeld selbst die volle datenschutzrechtliche Verantwortung.

3. Rechtliche Grundlagen

3.1 Datenschutz als Persönlichkeitsrecht – verfassungsrechtliche Grundlagen

Im Volkszählungsurteil hat das Bundesverfassungsgericht entschieden, dass unter den Bedingungen der modernen Datenverarbeitung der Schutz des einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz umfasst wird. Dieses Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen:

> *Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.*

In Sachsen-Anhalt wird dieses Grundrecht durch Art. 6 Abs. 1 der Verfassung des Landes Sachsen-Anhalt und entsprechend dessen Vorgaben durch bereichsübergreifende (im DSG LSA) und durch bereichsspezifische Regelungen (z.B. in § 84a SchulG; im SOG) garantiert. Art. 6 Abs. 1 lautet:

> *Jeder hat das Recht auf Schutz seiner personenbezogenen Daten. In dieses Recht darf nur durch oder auf Grund eines Gesetzes eingegriffen werden. Dabei sind insbesondere Inhalt, Zweck und Ausmaß der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten zu bestimmen und das Recht auf Auskunft, Löschung und Berichtigung näher zu regeln.*

3.2 Europarechtliche Rahmenvorgaben

Den europarechtlichen Rahmen gibt die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vor. Außerdem werden personenbezogene Daten ausdrücklich in Artikel 8 der Charta der Grundrechte der Europäischen Union als integraler Bestandteil des Vertrages über eine Verfassung für Europa geschützt.

3.3 Bereichsspezifische Regelungen (Beispiele)

Besondere Ausprägung findet der Schutz des informationellen Selbstbestimmungsrechts in sog. bereichsspezifischen Regelungen, wie z.B. für:

- Daten besonderer Art (wie Gesundheitsdaten; § 76 SGB X)
- Personalaktendaten (§ 50 Satz 3 Beamtenstatusgesetz: Personalaktengeheimnis)
- Sozialdaten (§ 35 SGB I: Sozialgeheimnis)
- Steuerdaten (§ 30 Abgabenordnung: Steuergeheimnis)
- Statistikdaten (§ 16 Bundesstatistikgesetz: Statistikgeheimnis)
- Berufsgeheimnisse von Ärzten, Anwälten, Journalisten

3.4 Vertraulichkeit und Integrität informationstechnischer Systeme

Mit einem weiteren Urteil vom 27. Februar 2008 hat das Bundesverfassungsgericht das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** (auch als IT-Grundrecht bezeichnet) formuliert, welches sich ebenfalls aus dem allgemeinen Persönlichkeitsrecht ableitet und inhaltlich den Systemdatenschutz betrifft.

> *Die Nutzung informationstechnischer Systeme ist für die Persönlichkeitsentfaltung vieler Bürger von zentraler Bedeutung, sie begründet gleichzeitig aber auch neuartige Gefährdungen der Persönlichkeit. Dieses Grundrecht schützt vor Eingriffen in Systeme, die allein oder durch Vernetzungen so viele personenbezogene Daten eines Betroffenen enthalten können, dass ein Zugriff Einblicke in wesentliche Teile der Lebensgestaltung einer Person gewähren oder gar ein aussagekräftiges Bild der Persönlichkeit ergeben kann.*

4. Datenschutzrechtliche Grundsätze

4.1 Erlaubnisvorbehalt (Zulässigkeit)

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist gemäß § 4 Abs. 1 DSG LSA nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

4.2 Erforderlichkeit

Öffentliche Stellen dürfen personenbezogene Daten nur erheben, verarbeiten oder nutzen, wenn dies zur Erfüllung ihrer jeweiligen (Fach-)Aufgabe erforderlich ist. Die verantwortliche Stelle muss sowohl örtlich als auch sachlich zuständig sein. Bei der Beurteilung der Erforderlichkeit ist ein strenger Maßstab anzulegen. Nützlichkeit ist nicht ausreichend, die Datenerhebung muss unerlässlich sein.

4.3 Datensparsamkeit und -vermeidung

Die Pflicht zur Datenvermeidung gem. § 1 Abs. 2 Satz 1 DSG LSA ist eine Konkretisierung des Grundsatzes der Verhältnismäßigkeit: Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist so weit wie möglich zu vermeiden. Sie ist auf das für die Aufgabenerledigung erforderliche Minimum zu beschränken (Datensparsamkeit).

4.4 Zweckbindung

Die Verarbeitung oder Nutzung personenbezogener Daten ist grundsätzlich an den Erhebungszweck gebunden. Der Verwendungszweck ist regelmäßig in einer Rechtsvorschrift festgelegt oder aus ihr ableitbar. Für die Annahme eines gemeinsamen Zwecks reicht es regelmäßig nicht aus, dass zwischen verschiedenen Aufgaben Ähnlichkeit besteht oder die Aufgaben in einem zeitlichen, räumlichen oder sachlichen Zusammenhang stehen (vgl. 10.1.1 VV-DSG-LSA). Problematisch wäre auch die Zusammenführung von für unterschiedliche Zwecke gespeicherten Daten zu einem anderen, übergeordneten Zweck im Sinne einer Profilbildung. Diese dürfte lediglich auf der Grundlage einer informierten Einwilligung des Betroffenen zulässig sein.

4.5 Informationelle Gewaltenteilung

Auch innerhalb der verantwortlichen öffentlichen Stelle hat eine aufgabenspezifische Trennung beim Umgang mit personenbezogenen Daten zu erfolgen. Zwar ist die stelleninterne Weitergabe personenbezogener Daten keine Übermittlung, sondern eine Nutzung. Für die Nutzung gelten aber die gleichen Voraussetzungen wie für die Übermittlung (vgl. §§ 10, 11 DSG LSA).

5. Betroffenenrechte

Das Grundrecht auf informationelle Selbstbestimmung gewährt den Betroffenen Rechtsansprüche, um ihr Persönlichkeitsrecht gegenüber den öffentlichen Stellen durchsetzen zu können. Gesetzlich festgelegt sind u.a. folgende wesentliche Betroffenenrechte:

- Recht auf Auskunft (§ 15 DSG LSA)
- Recht auf Löschung (§ 16 Abs. 2 DSG LSA)
- Recht auf Sperrung (§ 16 Abs. 3 und 4 DSG LSA)
- Recht auf Widerruf der Einwilligung (§ 4 Abs. 2 Satz 4 DSG LSA)
- Recht auf Einwendungen gegen Datenverwendung bei besonderen persönlichen Gründen (§ 4 Abs. 4 Satz 1 DSG LSA)

6. Umsetzung des Datenschutzmanagements

Datenschutzmanagement hat die Organisation des Datenschutzes zum Inhalt. Es umfasst alle den eigentlichen Prozess der Erhebung, Verarbeitung oder Nutzung personenbezoge-

ner Daten flankierenden Schritte, die für die Ausführung der datenschutzrechtlichen Vorschriften erforderlich sind. Wesentliche (Teil-) Konzepte, Analysen und Maßnahmen sollten dokumentiert werden. Änderungen etwa im Recht und Auswirkungen auf Verfahren sind zu verfolgen. Aufgrund der Dynamik des Datenschutzes sind Anpassungen auch des Datenschutzmanagements zu prüfen und umzusetzen.

Datenschutzmanagement betrifft die Rechtsanwendung, die Selbstkontrolle, den Einsatz und die Sicherheit der Informations- und Kommunikationstechnik (oft synonym als „**IT-Sicherheit** " bzw. „**Informationssicherheit**" als dem umfassenderen Begriff bezeichnet) und nicht zuletzt die Datenschutzkultur.

Die Umsetzung des Datenschutzmanagements bedarf zunächst einer Konzeptionierung durch die Behördenleitung. Das Datenschutzkonzept beschreibt grundlegend alle wesentlichen Aufgaben und Maßnahmen zur Sicherstellung des Datenschutzes. Ausgangspunkt sind die spezifischen Rahmenbedingungen der verantwortlichen Stelle (wie Dienststellengröße, eingesetzte IT-Technologie, Umfang und Sensibilität der personenbezogenen Daten usw.). Danach sind die personellen und materiellen Ressourcen zur Erledigung von Datenschutzaufgaben festzulegen. Schließlich sind die Maßnahmen vorzugeben, die zur Sicherstellung des Datenschutzes geboten sind (z.B. Allgemeine Dienstanweisung zum Datenschutz, Behördlicher Datenschutzbeauftragter, Verfahrensverzeichnis, Datensicherheitskonzept).

6.1 Dienstanweisung zum Datenschutz

Die Behördenleitung sollte durch eine **Allgemeine Dienstanweisung zum Datenschutz** sicherstellen, dass

- eine einwandfreie Rechtsanwendung gewährleistet ist,
- ein Datensicherheitskonzept über technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten als Bestandteil eines umfassenderen IT-Sicherheits- oder Informationssicherheitskonzepts vorliegt,
- sich jeder Mitarbeiter seiner eigenen (Mit-)Verantwortung bewusst ist (was durch eine regelmäßige Belehrung über das Datengeheimnis unterstützt werden kann),
- Kontroll- und Selbstkontrollmechanismen (z.B. Hinweise auf die unter 6.2 bis 6.6 erläuterten Regelungen) bestehen und greifen sowie
- die Datenschutzkultur (z.B. durch regelmäßige Schulungen) gefördert wird.

Weitere Dienstanweisungen zum Datenschutz können in Teilbereichen erforderlich sein, in denen bereichsspezifische Sonderregelungen gelten.

6.2 Datenverarbeitung im Auftrag

Auch zur Datenverarbeitung im Auftrag („Outsourcing“) empfiehlt sich eine Anweisung der Behördenleitung. Dazu sind insbesondere § 8 DSG LSA und die dazu ergangenen Verwaltungsvorschriften zu beachten. Der öffentlichen Stelle als Auftraggeber obliegt bei der Auswahl des Auftragnehmers eine besondere Sorgfaltspflicht. Der Auftrag ist schriftlich zu erteilen. Zu den erforderlichen Festlegungen des Auftraggebers gehören die Abgrenzung der Verantwortungsbereiche von Auftraggeber und Auftragnehmer, Regelungen des Verfahrens zum Test und zur Freigabe der Programme, Verfahren zur Fortschreibung, Änderung, Löschung und Sperrung sowie die Vorgabe der erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit gemäß § 6 DSG LSA.

Werden personenbezogene Daten im Rahmen einer (teilweise) übertragenen Sachaufgabe erhoben, verarbeitet oder genutzt, so handelt es sich dabei regelmäßig nicht um Datenverarbeitung im Auftrag, sondern um **Funktionsübertragung**. Diese Funktionsübertragung bedarf einer eigenen Rechtsgrundlage.

6.3 Behördlicher Beauftragter für den Datenschutz und seine Aufgaben

Öffentliche Stellen haben, so schreibt es § 14a DSG LSA vor, bei Einsatz automatisierter Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (soweit es sich nicht ausschließlich um Verfahren zur Unterstützung der allgemeinen Bürotätigkeit handelt) einen Beauftragten für den Datenschutz schriftlich einzusetzen. Beauftragte für den Datenschutz sind in ihrer Funktion weisungsfrei und können sich unmittelbar an die Leitung der öffentlichen Stelle wenden. Sie sind im erforderlichen Umfang von ihren sonstigen Aufgaben freizustellen. Das Gesetz gibt zwingend vor, dass - über die formelle Bestellung hinaus - bei der Ausgestaltung der Stelle genügend Kapazitäten vorzuhalten sind, um sämtliche Datenschutzaufgaben sachdienlich und in angemessener Zeit erfüllen zu können. Der Datenschutzbeauftragte ist im Organigramm der Behörde gesondert aufzuführen.

? Wer kann bestellt werden?

! Jeder, der die erforderliche Fachkunde und Zuverlässigkeit besitzt. Die notwendige Fachkunde hängt von den lokalen Gegebenheiten ab (Größe der Stelle, IT-Technik, Sensibilität der Daten). Nachschulungen sind zu ermöglichen. Die objektive Zuverlässigkeit ist bei erheblichen Interessenkonflikten zweifelhaft.

? Welche gesetzlichen Aufgaben hat der Beauftragte für den Datenschutz?

! Der Beauftragte für den Datenschutz

- führt das Verfahrensverzeichnis
- nimmt die Vorabkontrolle vor

- unterstützt seine öffentliche Stelle bei der Ausführung der Vorschriften über den Datenschutz
- macht die Mitarbeiter mit den datenschutzrechtlichen Vorschriften vertraut
- kontrolliert die Einhaltung datenschutzrechtlicher Vorschriften

? Welche Aufgaben und Befugnisse kann man ihm noch übertragen?

! Der Beauftragte für den Datenschutz könnte mitwirken

- bei der Erstellung von Richtlinien, Rundschreiben, Dienstvereinbarungen und weiteren Verlautbarungen zum Umgang mit personenbezogenen Daten,
- bei der Erarbeitung und Anwendung datenschutzgerechter Vordrucke und Merkblätter,
- bei Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsverlangen nach den §§ 15 und 16 DSG LSA, bei der Erstellung von Bürgerinformationen sowie bei allgemeinen Bürgereingaben und Anfragen zum Datenschutz.

! Er kann sich beteiligen

- an der Konzeption und Auswertung von Protokolldateien mit Personenbezug,
- an der Schulung der Mitarbeiter zu Fragen des Datenschutzes und der Datensicherheit.

Ferner kann er regelmäßig oder gelegentlich der Behördenleitung über den Stand des Datenschutzes und der Datensicherheit innerhalb der öffentlichen Stelle berichten.

Darüber hinaus bietet sich eine Zusammenarbeit mit allen anderen Stellen an, die bei der Sicherung des Datenschutzes mitzuwirken haben. Dies können der IT-Sicherheitsbeauftragte der eigenen Behörde, die Datenschutzbeauftragten der Rechts- oder Fachaufsichtsbehörden und anderer öffentlicher Stellen mit gleichen oder verwandten Aufgaben, aber auch die Personalverwaltung und der Personalrat sein. Wünschenswert ist das Entstehen eines (regionalen) „Datenschutznetzwerkes“. (Empfehlungen zum Beauftragten für den Datenschutz finden sich auch auf der Homepage des Landesbeauftragten.)

6.4 Verfahrensverzeichnis

Die verantwortlichen öffentlichen Stellen sind nach § 14 Abs. 3 DSG LSA verpflichtet, über die eingesetzten automatisierten Verfahren, mit deren Hilfe personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ein Verzeichnis zu führen. Die Verwaltungsvorschriften zum DSG LSA enthalten das Muster eines solchen Verzeichnisses und eine ausführliche Ausfüllanleitung (vgl. 14.3 und Anlage 3 VV-DSG-LSA). Die Angaben sind regelmäßig zu überprüfen und ggf. zu aktualisieren.

6.5 Vorabkontrolle

Bestimmte in § 14 Abs. 2 DSG LSA genannte Verfahren (wie z.B. Abrufverfahren nach § 7 Abs. 1 Satz 1 DSG LSA) sind vor ihrer Freigabe oder wesentlichen Änderung von der sie betreibenden Stelle daraufhin zu überprüfen, ob sie datenschutzrechtlich überhaupt zulässig und die nach § 6 Abs. 2 DSG LSA vorgesehenen technischen und organisatorischen Maßnahmen ausreichend sind.

6.6 Unterrichtungspflichten gegenüber dem Landesbeauftragten für den Datenschutz

- vor der Einrichtung automatisierter Abrufverfahren (§ 7 Abs. 3 DSG LSA)

  Gem. § 7 Abs. 3 DSG LSA hat die für die Einrichtung eines Abrufverfahrens verantwortliche Stelle den Landesbeauftragten rechtzeitig vor der Inbetriebnahme über das Verfahren zu unterrichten. Dabei sind ihm die in § 7 Abs. 2 DSG LSA genannten Angaben: Anlass und Zweck des Abrufverfahrens, Dritte, an die übermittelt wird, Art der zu übermittelnden Daten und die nach § 6 DSG LSA erforderlichen technischen und organisatorischen Maßnahmen mitzuteilen.

- über die Erteilung von Aufträgen zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (§ 8 Abs. 6 DSG LSA)

  Nach § 8 Abs. 6 Satz 2 DSG LSA haben öffentliche Stellen dem Datenschutz ganz besonders Rechnung zu tragen, wenn sie andere Stellen mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragen. Vor allem dann, wenn auf den Auftragnehmer die Vorschriften des DSG LSA nicht anwendbar sind, weil er eine nicht-öffentliche Stelle ist, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen des DSG LSA befolgt und sich der Kontrolle durch den Landesbeauftragten entsprechend den §§ 22 bis 24 DSG LSA unterwirft. Der Auftraggeber hat den Landesbeauftragten über die Beauftragung zu unterrichten. Nur so kann der Landesbeauftragte die Vertragsdurchführung beim Auftragnehmer überhaupt kontrollieren.

- über bestimmte automatisierte Verfahren des Landes (§ 14 Abs. 1 DSG LSA)

  Nach § 14 Abs. 1 Satz 2 DSG LSA ist der Landesbeauftragte über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten rechtzeitig zu unterrichten. Diese Unterrichtungspflicht richtet sich hauptsächlich an überregional zuständige Stellen, wie z.B. die Ministerien. Durch entsprechende rechtzeitige Mitteilungen soll der Landesbeauftragte in die Lage versetzt werden, bereits in diesem frühen Planungsstadium so seinem gesetzlichen Kontroll- und Beratungsauftrag nachzukommen, dass datenschutzrechtliche Mängel vor ihrer Etablierung erkannt und möglichst ohne hohe Aufwendungen personeller oder monetärer Art geändert werden könnten.

7. Risiken und Gefährdungen für Datensicherheit und Datenschutz

Wie kann man bestehende Risiken und Gefährdungen für Datensicherheit und Datenschutz bestimmen? Wie kann man Informationssicherheit, Datensicherheit und Datenschutz konzeptionell planen und umsetzen?

Bei der Umsetzung eines Datenschutzmanagements kommt es auf folgende Schritte an:

- Risikoanalyse,
- Schutzbedarfsanalyse,
- Datensicherheitskonzept,
- Maßnahmenprogramm.

Den Ausgangspunkt bildet immer eine Risikoanalyse und -bewertung. Für alle anfallenden Informationen in einem IT-System einer Behörde (u.a. Verschlusssachen, Geschäfts- und Betriebsgeheimnisse, interne dienstliche Vermerke, Weisungen, Schreiben und Erlasse sowie auch personenbezogene Informationen) muss diese Risikoanalyse und -bewertung erfolgen. Zunächst werden, ausgerichtet an den Funktionsanforderungen des betrachteten IT-Systems, die Gefährdungsmöglichkeiten analysiert, also wird die Frage beantwortet, was theoretisch alles passieren könnte. Die Analyse erfolgt quantitativ und qualitativ. Dabei kann u.a. ein wirtschaftlicher Verlust oder ein Ansehensschaden in Zahlen ausgedrückt und/oder ermittelt werden, ob und mit welchem Aufwand z.B. verlorene Datenbestände wiederhergestellt bzw. die Daten neu erhoben werden könnten. Für jede ermittelte Gefährdung wird dann die Ursache identifiziert und die Wahrscheinlichkeit des Auftretens bewertet. Die Ergebnisse dieser Risikoanalyse und -bewertung beeinflussen unmittelbar die Erstellung eines Datensicherheitskonzepts und wirken sich so auch auf die zu treffenden Entscheidungen im Rahmen des Datenschutzmanagements aus. Das Datensicherheitskonzept ist integraler Bestandteil eines umfassenden IT-Sicherheitskonzepts (Informationssicherheitskonzepts) der Behörde.

Eine seit mehreren Jahren in der Praxis bewährte Methode zur Erreichung eines angemessenen IT-Sicherheitsniveaus (Informationssicherheitsniveaus) ist die Vorgehensweise nach IT-Grundschutz des BSI. IT-Grundschutz verfolgt einen ganzheitlichen Ansatz. Infrastrukturelle, organisatorische, personelle und technische Standardsicherheitsmaßnahmen ergeben ein Standardsicherheitsniveau („mittlerer Schutzbedarf“), um u.a. auch personenbezogene Daten zu schützen (siehe Baustein B 1.5 Datenschutz, der auf der Homepage des BfDI abrufbar ist).
Auch bei der automatisierten Verarbeitung personenbezogener Daten können nach einer Risikoanalyse und -bewertung durchaus Maßnahmen für einen mittleren Schutzbedarf ausreichend sein. Bei höheren Risiken oder sensiblen personenbezogenen Daten (vgl. 3.3) sind technische und organisatorische Maßnahmen, die über den mittleren Schutzbedarf hinausgehen („Grundschutz plus X“) und eine Einzelprüfung notwendig.

Das BSI hat hierzu **IT-Grundschutz-Kataloge** entwickelt. Die IT-Grundschutz-Kataloge beinhalten Baustein-, Maßnahmen- und Gefährdungskataloge. Die Vorgehensweise nach

IT-Grundschutz, Ausführungen zum Informationssicherheitsmanagement und zur Risikoanalyse sind in den **IT-Grundschutz-Standards des BSI** zu finden:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 100-4: Notfallmanagement

Bei der Anwendung der IT-Grundschutz-Kataloge durch öffentliche Stellen des Landes Sachsen-Anhalt sind die dort genannten Kontrollziele des Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) mit den Sicherheitszielen des DSG LSA (§ 6 Abs. 2) abzugleichen, weil die datenschutzrechtlichen Kontrollziele des BDSG nur für öffentliche Stellen des Bundes und für private Unternehmen der Wirtschaft gelten. § 6 Abs. 2 DSG LSA greift zwar teilweise die für die IT-Sicherheit (Informationssicherheit) grundlegenden **Sicherheitsziele** wie **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** auf, geht aber mit der Festlegung von weiteren Sicherheitszielen wie **Authentizität**, **Revisionsfähigkeit** und **Transparenz** im Interesse eines wirksamen Schutzes personenbezogener Daten noch darüber hinaus!

Entscheidend ist neben der Erstellung eines Datensicherheitskonzepts im Rahmen eines IT-Sicherheitskonzepts (Informationssicherheitskonzepts) besonders die Umsetzung durch konkrete technische und organisatorische Maßnahmen.

7.1 Schutzziele bei der automatisierten Verarbeitung

Datenschutzmanagement verfolgt bei der automatisierten Verarbeitung personenbezogener Daten, egal ob nun mit Laptop, PC oder Mainframe bzw. autark oder in einem lokalen Netzwerk (LAN), in einem Funknetz (WLAN) oder sogar über das Internet, bestimmte Schutzziele. Diese Schutzziele hat der Gesetzgeber in § 6 DSG LSA festgelegt und das Ergreifen der zum Erreichen dieser Schutzziele erforderlichen Maßnahmen zur Pflicht gemacht. Nach § 6 Abs. 1 Satz 1 DSG LSA haben die öffentlichen Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die nach § 6 Abs. 2 und 3 DSG LSA erforderlich sind, um die Ausführung der Vorschriften des Datenschutzgesetzes zu gewährleisten.

Das DSG LSA verwendet in § 6 nicht unmittelbar den Begriff „**Datensicherheit“**, regelt aber diesem Zweck dienende Maßnahmen, soweit sie für den Datenschutz von Bedeutung sind, also dem Schutz des Persönlichkeitsrechts dienen. Durch geeignete technische und organisatorische Vorkehrungen soll die Erfüllung der Vorschriften des DSG LSA gewährleistet, also der Beeinträchtigung schutzwürdiger Interessen Betroffener bei der Datenverarbeitung entgegengewirkt werden. Die Maßnahmen sind sowohl für automatisierte als

auch für nicht-automatisierte Verfahren zu treffen und umzusetzen. Ziel aller getroffenen technischen und organisatorischen Maßnahmen ist eine störungsfreie und gegen Missbrauch gesicherte Datenverarbeitung. Maßnahmen der Datensicherheit sind für jede Art von Datenverarbeitung unerlässlich; besonders wichtig sind sie in automatisierten Verfahren. Jede Störung oder Verzögerung der Datenverarbeitung kann schwerwiegende Folgen haben.

Welche Schutzziele sind das und wie kann man sie erreichen?

- **Vertraulichkeit** (Daten sollen nur Befugte zur Kenntnis nehmen können)

Erreichen kann man dieses Schutzziel z.B. durch Datenverschlüsselung, gesicherte Datenträgeraufbewahrung, Verbot privater Hard- und Software und sinnvolle Benutzer- bzw. Rechteverwaltung.

- **Integrität** (Daten sollen unversehrt, vollständig und aktuell bleiben)

Erreichen kann man dieses Schutzziel z.B. durch Virenschutz, Plausibilitätsprüfungen, Kontrolle bei der IT-Wartung durch Dritte.

- **Verfügbarkeit** (Daten sollen zeitgerecht zur Verfügung stehen)

Erreichen kann man dieses Schutzziel z.B. durch USV (unterbrechungsfreie Stromversorgung), Backup, ausreichende Datenübertragungsraten im Netzwerk.

- **Authentizität** (Daten sollen ihrem Ursprung zugeordnet werden können)

Erreichen kann man dieses Schutzziel z.B. durch Digitale Signatur, Protokollierung.

- **Revisionsfähigkeit** (wer wann welche Daten in welcher Weise erhoben, verarbeitet oder genutzt hat, soll jederzeit festgestellt werden können)

Erreichen kann man dieses Schutzziel z.B. durch Protokollierung, Protokollauswertung.

- **Transparenz** (Verfahren zur Erhebung, Verarbeitung oder Nutzung von Daten sollen nachvollziehbar und aktuell dokumentiert sein)

Erreichen kann man dieses Schutzziel z.B. durch Vorabkontrolle und Verfahrensfreigabe, nachvollziehbare Dokumentation der eingestellten Softwareparameter und der eigenen Programmierung.

7.2 Nicht-automatisierte Datenverarbeitung

Was ist bei der sogenannten nicht-automatisierten Datenverarbeitung, also dem Umgang mit manuellen Karteien oder herkömmlichen Akten zu beachten?

Der Gesetzgeber hat den öffentlichen Stellen in § 6 Abs. 3 DSG LSA auch für diese Fälle aufgegeben, Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport oder der Vernichtung dieser Daten zu verhindern. Das einfachste Beispiel dafür, wann entsprechende Maßnahmen ergriffen werden müssen, ist der nachtaktive Reinigungsdienst im Verwaltungsgebäude. Es macht deutlich, dass nicht alle Zugangsberechtigten zu den Diensträumen auch zum Zugriff auf Verwaltungsakten berechtigt sind. Die einfachste Maßnahme, die in solchen Fällen ergriffen werden müsste, wäre das konsequente Einschließen der Verwaltungsakten in den Büromöbeln. Die Initiative dafür muss von der Behördenführung ausgehen, die auch für die entsprechenden Voraussetzungen, also abschließbare Schreibtische und Aktenschränke, zu sorgen hat.

8. Datenschutzmanagement im Behördenalltag (Beispiele)

8.1 Organigramm mit den Namen der Beschäftigten

Häufig veröffentlichen Behörden ihren Organisationsplan oder ein Organigramm und nennen zu den einzelnen Ämtern jeweils Amtsleiter oder Amtsleiterin. Aufgrund jüngerer Rechtsprechung kann man mittlerweile die Auffassung vertreten, dass keine Einwilligung zur Veröffentlichung der Namen und dienstlichen Telefonnummern im Internet erforderlich ist. Anders wäre das, wenn auch die Namen von Beschäftigten veröffentlicht würden, die weit unterhalb der Leitungsebene tätig sind oder keinerlei Außenkontakte pflegen. Für diesen Personenkreis wäre stets eine Einwilligung in die Veröffentlichung erforderlich. Das gilt auch für die Mitglieder des Personalrates, Gleichstellungs- und Behindertenbeauftragte. Hier wird eine Einwilligung erforderlich sein, weil der Name dieser Personen für die Öffentlichkeit weniger von Bedeutung ist, als für die Beschäftigten ihrer Behörde selbst.

8.2 Anbieterkennzeichnung

Nach § 5 des Telemediengesetzes (TMG) hat der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung seiner personenbezogener Daten zu unterrichten. Das gilt speziell dann, wenn der Diensteanbieter für die Bereitstellung des Dienstes erhobene personenbezogene Daten, z.B. die

IP-Adresse, für andere Zwecke, also z.B. für die Erstellung von Statistiken, Verbesserung des Internetangebotes etc. verwendet. Dies ist nur zulässig, wenn der Nutzer hierin eingewilligt hat (§ 12 Abs. 2 TMG). Da es sich bei einer Behörde um eine juristische Person des öffentlichen Rechts handelt, ist im Impressum auch der Vertretungsberechtigte, also i. A. der Behördenleiter, anzugeben. Nach § 13 Abs. 5 TMG ist dem Nutzer die Weitervermittlung (Verlinkung) zu einem anderen Diensteanbieter anzuzeigen.

8.3 Videoüberwachung

Bei der Einrichtung und datenschutzrechtlichen Bewertung einer gemeinhin als „Videoüberwachung“ bezeichneten optisch-elektronischen **Beobachtung** öffentlich zugänglicher Bereiche durch eine öffentliche Stelle ist § 30 DSG LSA zu beachten. „Videoüberwachung“ ist dann rechtlich zulässig, wenn sie zur Wahrnehmung des Hausrechts, zum Schutz des Eigentums oder zur Kontrolle von Zugangsberechtigungen erforderlich und verhältnismäßig ist und keine Anhaltpunkte bestehen, dass schutzwürdige Belange von Personen im Aufnahmebereich der Videokameras überwiegen (§ 30 Abs. 1 DSG LSA).

Die Möglichkeit einer Videoüberwachung muss für Betroffene erkennbar sein (§ 30 Abs. 2 DSG LSA). Eine Beobachtung des öffentlichen Raumes außerhalb des Bereiches, für den die öffentliche Stelle das Hausrecht besitzt, ist nur zum Schutz des Eigentums oder Besitzes der öffentlichen Stelle zulässig (§ 30 Abs. 1 Nr. 2 DSG LSA). Darüber hinaus ist eine optisch-elektronische Beobachtung des dem öffentlichen Verkehr gewidmeten Raumes mangels einer gesetzlichen Grundlage unzulässig. Dies gilt es insbesondere bei der Planung und dem Einsatz von Außenvideokameras zu beachten.

Besonders enge Grenzen hat der Gesetzgeber der verantwortlichen Stelle für den Fall gesetzt, dass nicht nur eine Beobachtung von Beschäftigten sowie eventuell Besuchern, Boten, Lieferanten der öffentlichen Stelle in Echtzeit erfolgt, sondern dass diese Videoüberwachungsbilder auch **aufgezeichnet** werden sollen. Dies ist nur dann zulässig, wenn es für die o.g. Zwecke erforderlich oder unvermeidlich ist und die Verhältnismäßigkeit der Maßnahme gegeben ist (§ 30 Abs. 3 DSG LSA). Die gespeicherten Videodaten sind unverzüglich zu löschen, wenn sie zur originären Zweckerfüllung nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen (§ 30 Abs. 4 DSG LSA).

Auch wenn der Einsatz von Videotechnik nicht unter eines der in § 14 Abs. 2 DSG LSA genannten automatisierten Verfahren fällt, die eine gesetzliche Vorabkontrolle erfordern, hält der Landesbeauftragte die rechtzeitige Information und Beteiligung des behördlichen Be-

auftragten für den Datenschutz für erforderlich, um seiner Beratungsfunktion gegenüber der Leitung der öffentlichen Stelle (§ 14a Abs. 4 DSG LSA) nachkommen zu können.

Bereits in seinem VIII. Tätigkeitsbericht (Ziff. 12.4 "Schutzprofil für den Einsatz von Videoüberwachungssystemen") hat der Landesbeauftragte für den Datenschutz darauf hingewiesen, dass es ein Schutzprofil bei korrekter Umsetzung ermöglicht, die Einhaltung von datenschutzrechtlichen Vorgaben beim Einsatz von Videoüberwachungstechnik technisch zu realisieren und zu kontrollieren. Die Anforderungen dieses Schutzprofils sollten bei Ausschreibungen für den Einsatz von Videoüberwachungstechnik Berücksichtigung finden bzw. bereits installierte Anlagen sollten auf Basis der Anforderungen aus dem Schutzprofil überprüft werden.

Unabhängig von der datenschutzrechtlichen Beurteilung ist die Installation von Videotechnik nach § 69 Nr. 2 Landespersonalvertretungsgesetz Sachsen-Anhalt mitbestimmungspflichtig.

8.4 Löschung von Daten

Insbesondere bei Einsatz automatisierter Verfahren ist bereits vor der Einführung darauf zu achten, dass eine „Archivfunktion“ im Programm allein nicht zur Wahrung des Datenschutzes ausreicht, sondern dass entsprechend § 14 Abs. 3 Nr. 7 DSG LSA Regelfristen festgelegt sein müssen, an denen die Löschung der personenbezogenen Daten geprüft wird. Personenbezogene Daten sind regelmäßig zu löschen, wenn sie zur Aufgabenerfüllung (oder Dokumentation der Aufgabenerfüllung) nicht mehr erforderlich sind. An die Stelle einer Löschung tritt die Sperrung der personenbezogenen Daten - insbesondere dann, wenn durch eine Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt werden könnten (vgl. § 16 DSG LSA).

9. Informationsfreiheit

Mit Inkrafttreten des Informationszugangsgesetzes (IZG LSA) zum 1. Oktober 2008 hat jeder nach Maßgabe des IZG LSA einen Anspruch auf Zugang zu amtlichen Informationen gegenüber den Behörden des Landes, der Kommunen und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Sonstige Organe und Einrichtungen des Landes unterfallen dem Gesetz, soweit sie Verwaltungsaufgaben wahrnehmen. Zur effizienten Anwendung des IZG LSA sollte ein zentraler Ansprechpartner geschaffen werden, der die Behördenleitung und die fachlich zuständigen Bearbeiter bei der Interpretation und effektiven Umsetzung des IZG LSA berät. Wegen der Sachnähe zum Datenschutz (vgl. § 5 IZG LSA) sollte diese Aufgabe dem behördlichen Datenschutzbeauftragten übertragen werden.