

Datenschutz bei Dokumentenmanagementsystemen

- Orientierungshilfe -

Die Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen“ ist von einer Arbeitsgruppe des Arbeitskreises eGovernment der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet worden.

Die Federführung der Arbeitsgruppe lag beim Landesbeauftragten für den Datenschutz Hessen; weitere Mitglieder der Arbeitsgruppe waren Mitarbeiterinnen und Mitarbeiter des Berliner Beauftragten für Datenschutz und Informationsfreiheit, des Landesbeauftragten für den Datenschutz Niedersachsen, des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, des Landesbeauftragten für den Datenschutz Rheinland-Pfalz, des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein sowie des Bundesbeauftragten für den Datenschutz.

Der Text der Orientierungshilfe ist nach Beschlussfassung im Arbeitskreis eGovernment von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Sitzung am 16./17. März 2006 in Magdeburg zustimmend zur Kenntnis genommen worden.

Kontaktadresse: poststelle@datenschutz.hessen.de

Inhaltsverzeichnis

- 1 Einleitung**
- 2 Dokumentenmanagementsystem – Was verbirgt sich dahinter?**
 - 2.1 DMS im engeren und weiteren Sinn
 - 2.2 Ziele eines DMS
 - 2.3 Funktionen eines DMS
 - 2.4 Elektronische Akte - Hybridakte – Papierakte
 - 2.5 Zweckbindung der Protokolldaten und der Verfahrensdaten im DMS
 - 2.6 Ausblick
- 3 Datenhaltungsmodelle**
 - 3.1 Dezentrale Modelle
 - 3.2 Zentrale Modelle
 - 3.3 Verteilte Datenhaltung
 - 3.4. Dezentrale Datenhaltung mit zentraler Komponente
- 4 Organisatorische Rahmenbedingungen**
 - 4.1 Vorabkontrolle
 - 4.2 Projektinitialisierung
 - 4.3 Ist-Analyse, Aufbau- und Ablauforganisation
 - 4.4 Analyse des Schutzbedarfs der Dokumente
 - 4.5 Organisationskonzept
 - 4.6 Domea 2.1
 - 4.7 Datenschutz- und Datensicherheitskonzept, Rollen- und Rechtekonzept
 - 4.8 Organisatorische Regelungen
 - 4.8.1 Dienstvereinbarung
 - 4.8.2 Dienstanweisung
- 5 Rechtsrahmen und datenschutzrechtliche Einordnung**
 - 5.1 Aufgabenstellung und Rechtsrahmen beim Einsatz von DMS
 - 5.2 Anforderungen an elektronische Dokumente
 - 5.3 Bewältigung der Medienbrüche
 - 5.3.1 Rechtliche Probleme beim vollständigen Übergang auf elektronische Dokumente
 - 5.3.2 Übertragung von elektronischen Dokumenten mit Beweisfunktion in Papierform
 - 5.4 Kein vollständiger Übergang auf elektronische Aktenführung
 - 5.5 Datenschutzrechtliche Anforderungen an ein DMS
 - 5.5.1 Vorabkontrolle
 - 5.5.2 Notwendige Festlegungen zur datenschutzgerechten Gestaltung
 - 5.6 Akteneinsicht und Informationszugang bei Verwendung von DMS
- 6 Sicherheitsziele und -maßnahmen bei der Behandlung von Dokumenten**
- 7 Anforderungen an das Signieren in einem Dokumentenmanagementsystem**
 - 7.1 Public-Key-Infrastructure (PKI)
 - 7.2 Spezielle Problemfelder des Dokumentenmanagementsystems

8 Technische Maßnahmen gegen unbefugte Kenntnisnahme

- 8.1 Dokumentenkategorien nach Schutzbedarf
- 8.2 Rollenkonzept /Berechtigungskonzept / Zugriffe
- 8.3 Verschlüsselung in DMS

9 Übernahme eingehender Post in das Dokumentenmanagementsystem

- 9.1 Vorbereitung der in Papierform eingehenden Post
- 9.2 Scannen
- 9.3 Behandlung der in elektronischer Form eingehenden Post
- 9.4 Umwandlung der Grafikdateien in Textdateien (OCR Erkennung)
- 9.5 Metadateneingabe

10 Workflow-Management

- 10.1 Festlegung der Arbeitsabläufe
- 10.2 Sicherstellung des Bearbeitungsweges
- 10.3 Verhaltens- und Leistungskontrolle
- 10.4 Weitere spezifische Problemfelder

11 Recherche

- 11.1 Datenschutzrisiken
- 11.2 Problemlösung
- 11.3 Fazit

Glossar

Checkliste

Wichtige Linkadressen

1 Einleitung

Der Einsatz eines Dokumentenmanagementsystems (DMS) ist eine der wichtigsten Herausforderungen, der sich heute öffentliche Verwaltungen stellen müssen. Unterstützt durch die Entwicklungen beim eGovernment und zur Digitalisierung der Verwaltung, wie z.B. mit der Einführung der elektronischen Akte, bieten eine Vielzahl von Herstellern DMS auf dem Markt an. Neben der Beschleunigung der Verwaltungsvorgänge ist ein wesentliches Ziel dieser neuen Technologie, Informationen jeder Art, die in der Verwaltung vorhanden sind, erschließbar zu machen.

Bisher datenschutzrechtlich zu beurteilende IT-Verfahren waren in aller Regel Fachverfahren, die Teilinformationen einer Akte bzw. eines Vorgangs und Verarbeitungsschritte enthielten. Die Ergebnisse waren oft nur mit Zusatzinformationen für Nichtfachleute verständlich. In DMS dagegen werden nicht nur Daten, sondern in sich **aussagefähige Dokumente** vorgehalten. Das birgt ein höheres Risiko gegenüber konventionellen Verfahren, weil kein Zusatzwissen oder Insiderkenntnisse erforderlich sind, um Informationen verstehen und ggf. verwerten zu können. In DMS werden Informationen fachübergreifend vorgehalten. Damit bringt der Einsatz von DMS neben wirtschaftlichen Vorteilen auch neue Risiken für das Grundrecht auf informationelle Selbstbestimmung. Mit ihm können in automatisierter Weise aus einer Datensammlung durch vielfältige Datenverknüpfungen und –kombinationen sowie durch die Erstellung von Hypothesen und deren Überprüfung bisher völlig unbekannte Informationen gewonnen werden. Insbesondere die gezielte Zusammenführung von personenbezogenen Daten aus unterschiedlichen Datenquellen und ihre Auswertung erfolgen überwiegend ohne Kenntnis der Betroffenen. Diese Entwicklung schafft neue Gefahren für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die besonderen Datenschutzrisiken ergeben sich insbesondere, wenn die Papierakte (weitgehend) durch eine elektronische Akte ersetzt wird, deren Dokumente in einem DMS vorgehalten werden. In diesem Fall führen die Such- und Auswertungsfunktionen eines DMS, besonders dann, wenn eine Volltextrecherche zugelassen ist, zu bisher nicht oder nicht in dem Umfang gegebenen Aussagen zu einer Person. Ohne Aufwand könnten dann Daten von mit der Verwaltung in Kontakt stehenden Bürgerinnen und Bürgern aus verschiedenen Lebens- bzw. Verwaltungsbereichen zusammengeführt werden, ohne dass Zusatzwissen erforderlich wäre. Solange nur einzelne Informationen elektronisch gespeichert sind, Schriftverkehr von Bürgerinnen und Bürgern mit der Verwaltung sich aber in gesonderten Papierakten befindet, ist eine umfassende Recherche zu einer bestimmten Person nur mit erheblichem Aufwand möglich. Mit Einführung der elektronischen Akte in einem DMS kann dies quasi per Knopfdruck geschehen. Damit wächst auch die Gefahr, dass Entscheidungen automatisiert vorgegeben werden, was datenschutzrechtlich unzulässig wäre. Zudem besteht das Risiko, dass es für Bürgerinnen und Bürger noch schwerer wird, zu durchschauen, wer aus der Verwaltung Zugang zu ihren Daten hat.

Dokumentenmanagementsysteme können aber auch zur Ausforschung und zur Verhaltens- und Leistungskontrolle von Mitarbeiterinnen und Mitarbeitern genutzt werden. Werden deren sämtliche Bearbeitungsschritte elektronisch abgebildet, entstehen eine Fülle zusätzlicher Protokoll- und Verfahrensdaten, die mitarbeiterbezogen ausgewertet werden können. Damit können ohne weiteres permanente Verhaltens- und Leistungskontrollen der Beschäftigten erfolgen. Es müssen deshalb Anforderungen für datenschutzgerechte und –freundliche Lösungen formuliert werden.

Da Beschäftigte in der Administration grundsätzlich die Möglichkeit haben, lesend auf jedes Dokument zuzugreifen, könnten sie mit Einführung einer elektronischen Akte in einem DMS künftig jedes Dokument der Verwaltung zur Kenntnis nehmen, wenn nicht zusätzliche Sicherheitsmechanismen – wie etwa Verschlüsselung – eingerichtet werden. Gleiches gilt für die prinzipielle Möglichkeit, Dokumente zu manipulieren oder zu löschen. Dies kann sowohl absichtlich als auch aus Versehen erfolgen. Werden vertrauliche Dokumente offenbart, stehen Beschäftigte in

der Administration immer auch unter Verdacht. Zu ihrem eigenen Schutz sollten deshalb Vorkehrungen getroffen werden, die ihnen den Zugang zu solchen Unterlagen verwehren.

Diese Orientierungshilfe stellt die datenschutzrechtlichen und -technischen Anforderungen, die zu beachtenden Sicherheitsaspekte und die Architektur des DMS als Basiskomponente des eGovernment vor.

Sie will dazu beitragen, dass bei dem Einsatz eines DMS die Anforderungen von Datenschutz und Datensicherheit im Blick bleiben, und praktische Hinweise dafür geben, wie diese Anforderungen in datenschutzgerechte und datenschutzfreundliche Anwendungen umgesetzt werden können. Um die Lesbarkeit zu erhöhen, sind die wichtigsten Begriffe in einem Glossar am Ende der Orientierungshilfe erläutert.

Die Orientierungshilfe gliedert sich wie folgt:

Im **Kapitel 2** sind **Ziele und Funktionen** eines DMS, die **Auswirkungen** auf die Form der Aktenführung und die notwendigen **organisatorischen Veränderungen** beschrieben. Es wird ferner ein Ausblick auf die Einsatzfelder **Wissensmanagement** und weitere in diesem Zusammenhang in der Verwaltung zu erwartende und datenschutzgerecht zu bewältigende Veränderungen gegeben.

Im **Kapitel 3** werden **Datenhaltungsmodelle** eines DMS beschrieben.

Im **Kapitel 4** finden sich die **organisatorischen** und im **Kapitel 5** die **rechtlichen Rahmenbedingungen** für den Einsatz eines DMS.

In den **Kapiteln 6 bis 8** werden die **technisch-organisatorischen Anforderungen** wie Sicherheitsziele, Anforderungen an das Signieren und die Behandlung von Dokumenten dargestellt.

Die **Kapitel 9 bis 11** befassen sich mit den konkreten Schritten der **Übernahme von Dokumenten in das DMS**, des **Workflows** und der **Recherche**.

Als Anhang zur Orientierungshilfe finden Sie eine „**Check-Liste**“, in der die Maßnahmen und Vorkehrungen zur Gewährleistung einer datenschutzgerechten und sicheren DMS-Anwendung mit Verweis auf die jeweiligen Fundstellen in der Orientierungshilfe zusammengestellt sind.

Wir möchten mit dieser Orientierungshilfe alle diejenigen erreichen, die in den Verwaltungen an zentraler Stelle als Behördenleitung, in der Organisation, in der Verfahrensentwicklung, als IT-Verantwortliche, als Datenschutzbeauftragte oder als Personalvertretung den Weg in ein DMS vorbereiten oder schon umsetzen.

2 Dokumentenmanagementsystem – Was verbirgt sich dahinter?

2.1 DMS im engeren und weiteren Sinn

Unter dem klassischen DMS im engeren Sinn sind solche Lösungen zu verstehen, die ursprünglich aus der Notwendigkeit entstanden sind, Instrumente und Verfahren für die Verwaltung der enorm wachsenden Dokumentenbestände zur Verfügung zu stellen. Hierzu zählt man dynamische Ablagesysteme zur Verwaltung der Dokumente im Lebenszyklus vor der Langzeitaufbewahrung. Wesentliche Eigenschaften sind visualisierte Ordnungsstrukturen sowie Metadatenverwaltung zur Indizierung und Suchtechnologien. So gekennzeichnete Dokumente sind über mehr Informationsfelder recherchierbar, als sie ein Dateisystem zur Verfügung stellt. Beim DMS stehen beliebige Felder zur Verfügung wie beispielsweise Aktenzeichen, Eingangsdatum, Bearbeiter etc.

Unter einem DMS im weiteren Sinn werden verschiedene Systemkategorien und deren Zusammenspiel verstanden wie Dokumentenmanagement im engeren Sinn, Bürokommunikation Scannen, Vorgangssteuerung (Workflow) und elektronische Aufbewahrung bis zum Übergang in Archivsysteme. Diese unterschiedlichen Komponenten sind in starkem Maße voneinander abhängig, der Einsatz einer Komponente ist im Allgemeinen nicht ohne den Zugriff auf andere Komponenten sinnvoll. Alle Module haben gemeinsam, dass unterschiedliche Arten von Dokumenten - gescannte Papieroriginale als Scann-Datei, Faxeingänge, Dateien aus Büroanwendungen, eMails, Multimediaobjekte, usw. - datenbankgestützt verwaltet werden. Der Einsatz von Datenbanken erlaubt die Handhabung großer Informationsmengen und einen direkten Zugriff auf einzelne Dokumente und Dokumentengruppen. In diesem Zusammenhang ist zum Beispiel der Bereich Erfassung, Darstellung und Ausgabe von gescannten Dokumenten (Imaging) unter dem Gesichtspunkt zu betrachten, dass es sich hierbei nur um eine spezielle Art von Dokumenten handelt.

DMS haben einen externen und einen internen Anknüpfungspunkt. Schwerpunkt der Betrachtung ist im Regelfall die Frage, wie die Behörde intern zusammenarbeitet. In diesem Zusammenhang müssen die über Jahrzehnte gewachsenen Aufbau- und Ablaufstrukturen der Behörden überdacht, Verwaltungsverfahren analysiert und auf ein Zusammenwirken mit vor- und nachgelagerten Prozessen überprüft werden. Diesen binnenorientierten Veränderungen und insbesondere den hierzu erforderlichen organisatorischen Rahmenbedingungen kommt in diesem Zusammenhang eine entscheidende Bedeutung zu (Näheres s. Ziff. 4).

Mit einem DMS werden Dokumente über den gesamten Lebenszyklus in der Verwaltung bis zur Aussonderung bzw. der Übergabe an die nach den Archivgesetzen des Bundes und der Länder zuständigen öffentlichen Archive verwaltet. Dieser Lebenszyklus kann teilweise Zeiträume von 30 und mehr Jahren umfassen. In dieser Orientierungshilfe konnten die Probleme solcher langen Speicherzeiträume nicht abschließend behandelt werden; zum Teil sind Lösungen dazu noch in der Entwicklung. In diesem Zusammenhang wird auf die Projekte "ArchiSig" (www.archisig.de) und „ArchiSafe“ (www.archisafe.de) verwiesen, die sich mit der sicheren und beweiskräftigen Langzeitarchivierung digital erzeugter und signierter Daten über 30 Jahre und mehr befassen.

Was ist ein Dokumentenmanagementsystem?

Ein Dokumentenmanagementsystem verwaltet elektronisch und nicht-elektronisch erzeugte Dokumente über deren gesamten Lebenszyklus hinweg. Das DMS organisiert dabei Entwurf und Erstellung, Weitergabe und Verteilung, Auffinden, Ablage und Übergabe an ein Archiv oder Löschung der Dokumente sowie Auswertung und Zuordnung von Informationen aus den Dokumenten.

Das DMS soll dabei u. a. die Integration von Dokumenten unterschiedlicher Herkunft und Abbildung von Geschäftsprozessen der Verwaltung abdecken.

2.2 Ziele eines DMS

Mit der Einführung eines DMS sollen u.a. folgende Ziele verwirklicht werden:

- Einführung einer vollständig elektronisch geführten Akte
- Ablösung der konventionellen Registraturhilfsmittel (Karteikarten, Einsenderkarteien, Tagebücher, Adresslisten usw.)
- einfacher und aktueller recherchierbarer Bearbeitungsstand
- Reduzierung von Medienbrüchen durch Bearbeitung in einem DMS oder durch Schaffung von automatisierten Schnittstellen – z.B. über eine Schnittstelle zu den Office-Produkten
- Ermöglichung aller nötigen Auswertungen – unter Berücksichtigung der jeweiligen Zugriffsrechte (zentrale oder dezentrale Recherche)
- Einfache Bereitstellung allgemein zugänglicher Informationen
- Wissensmanagement

Dadurch entstehen die folgenden unmittelbaren Vorteile:

- Die Schnelligkeit der Bearbeitung wird gesteigert, da Transportzeiten entfallen, Dokumente mittels Workflow direkt zu den entsprechenden Bearbeitern geführt werden und paralleles Bearbeiten von mehreren Beteiligten möglich wird.
- Der aktuelle Bearbeitungsstand eines Dokumentes kann jederzeit nachvollzogen werden (für andere Personen als die Sachbearbeiterin oder den Sachbearbeiter allerdings nur im Rahmen des rechtlich Zulässigen, siehe auch Ziffern 2.5, 4.8, 4.8.1, 5.5.2).
- Informationen sind ständig verfügbar. Das aufwändige Suchen in Papier-Archiven entfällt.
- Zeit- und Personalressourcen für Aktentransport entfallen.
- Die Vorhaltung von Räumen für umfangreiche Papierablage entfällt.
- Vervielfältigungsaufwand für allgemein zur Verfügung gestellte Informationen kann vermieden werden.

2.3 Funktionen eines DMS

Die Qualität eines Dokumentenmanagements wird bestimmt durch die Zugriffszeit auf eine gesuchte Information, durch die Vollständigkeit des Dokumentenpools und durch die möglichst präzise Zuordnung der Dokumente zu der gesuchten Information. Dokumentenmanagement bedeutet aber noch mehr. So verändern sich etwa Projektdokumente beständig, bis sie ihren endgültigen Zustand erreicht haben. Im DMS können verschiedene Versionen des Dokuments aufbewahrt werden, damit man nachvollziehen kann, was sich verändert hat. Außerdem muss gewährleistet werden, dass nicht zwei oder mehrere Personen gleichzeitig an einem Dokument arbeiten und ihre Arbeitsergebnisse im schlimmsten Fall gegenseitig vernichten. Diesen Anforderungen versuchen Dokumentenmanagementsysteme gerecht zu werden. Sie archivieren die unterschiedlichen Versionen der Dokumente, überwachen den Zugriff, indizieren die Dokumente und strukturieren die Dokumentenverwaltung. Fortgeschrittene Versionen eines DMS verfügen über Funktionen wie beispielsweise die automatische Nachrichtenfunktion bei Veränderung des Dokumentes oder die Möglichkeit, verschiedene Versionen eines Dokumentes miteinander zu vergleichen und ihre Unterschiede hervorzuheben.

2.4 Elektronische Akte – Hybridakte – Papierakte

Das DMS markiert den Übergang von der Papierakte zur elektronischen Akte. Aus technischer Sicht stellt die elektronische Akte ein Bestandsverzeichnis von Objekten dar. Die Aktenbestandteile können aus Gründen der Datenhaltung oder Bearbeitung dezentral auf verschiedenen Servern abgelegt sein. Es besteht nur die Struktur der Akte mit ihren Metadaten, in der Verweise auf die eigentlichen Dokumente und ihren Inhalt enthalten sind. Erst wenn die Sachbearbeiterin

oder der Sachbearbeiter ein bestimmtes Dokument bearbeiten möchten, wird dieses am Bildschirm zur Anzeige gebracht. Die Vorteile einer rein elektronischen Akte sind:

- Schnellstmöglicher Zugriff auf alle Bestandteile der Akte von unterschiedlichen Standorten
- Minimierung der Transportzeiten von Schriftgut
- Verbesserung des kooperativen Arbeitens
- Bearbeiterin und Bearbeiter erwerben Unabhängigkeit von der Registratur
- Unmittelbare Bearbeitung der Dokumente mit elektronischen Bürokommunikationswerkzeugen
- Einbindung sämtlicher digitalisierter Informationen

Da Papierdokumente auch mit der Einführung eines DMS nicht wegzudenken sind, wird die Hybridakte bis zum völligen Wegfall der Papierdokumente den Regelfall darstellen. Dies auch schon deshalb, weil bestimmte Dokumente z. B. aus rechtlichen Gründen nicht digitalisiert werden dürfen oder im Original aufbewahrt werden müssen (siehe unten Ziff. 5.3.1). Da Papierdokumente weiterhin unumgänglich sind, wird in heutigen DMS verstärkt eine Mischform verwendet, bei der in einer Akte sowohl Papier- als auch elektronische Dokumente enthalten sind. Die elektronischen Bestandteile einer solchen Hybridakte können angezeigt werden, ohne dass sie dupliziert werden müssen. Bei Hybridakten sind für Dokumente, die im Papieroriginal aufgehoben werden müssen, in digitalisierter Form Verweise auf diesen Papieraktenteil aufzunehmen. Dies verbessert die Übersicht und erleichtert die Verfolgung des Bearbeitungsstatus. Es ist aber auch denkbar, dass die Papierakte die „verbindliche“ Akte darstellt, in die dann Verweise auf elektronische Dokumente aufzunehmen sind.

2.5 Zweckbindung der Protokolldaten und der Verfahrensdaten im DMS

In einem Dokumentenmanagementsystem sind Protokolldaten, die zu Zwecken der Datensicherheit anfallen und Verfahrensdaten, die im Zusammenhang mit dem Verfahrensablauf bzw. mit der Bearbeitung von Inhaltsdaten anfallen, zu unterscheiden. Sie unterliegen hinsichtlich des Zugangs und der Auswertbarkeit unterschiedlichen Regeln.

Die Protokolldaten, die aufgrund der Datenschutzgesetze (vgl. Anlage zu § 9 Ziffer 5 BDSG, § 10 Abs. 2 HDSG und entsprechende andere Landesdatenschutzgesetze) aus Datensicherheitsgründen gespeichert werden, unterliegen einer strikten Zweckbindung und dürfen nicht für andere Zwecke verwendet werden. Sie dürfen insbesondere nicht zur Verhaltens- und Leistungskontrolle der Beschäftigten, die mit einem Dokumentenmanagementsystem arbeiten, ausgewertet werden. Von diesen Daten sind Verfahrensdaten zu unterscheiden, die im Bearbeitungsablauf in einem Dokumentenmanagementsystem entstehen, wie etwa die Dokumentation der Mitzeichnung im Verwaltungsverfahrensablauf. Die Auswertung dieser Daten ist im DMS nicht anders zu beurteilen als bei einer herkömmlichen Aktenbearbeitung.

Die unten beschriebenen Protokolldaten und Verfahrensdaten müssen nicht bei jedem DMS und in jeder der angegebenen Komponenten anfallen. Abhängig von der Architektur kommen manche Komponenten nicht vor oder bauen auf eine andere Komponente auf. So könnten Datenbankprotokolle, d.h. Protokolle die das Datenbankmanagementsystem schreibt, für die Protokollierung auf Anwendungsebene genutzt werden.

Das jeweilige Sicherheitskonzept gibt vor, in welchen Fällen welche Protokolldaten bzw. Verfahrensdaten gespeichert werden und wie sie auszuwerten sind. Dabei gibt es Daten die optional sind, während andere in jedem Fall erzeugt werden. So werden in der Regel lesende Zugriffe durch das Betriebssystem oder in Anwendungen nicht protokolliert, während entsprechende Einträge in der Log-Datei einer Datenbank vorhanden sind.

Je nach Systemansatz können die Daten, wer wann welches Dokument wie bearbeitet hat, an mehreren Stellen aufgezeichnet werden. Die rechtlich zulässige Auswertung von Vorgesetzten, welche Dokumente eine Beschäftigte oder ein Beschäftigter bearbeitet hat, müssen aber aus

dem dafür vorgesehenen Datenbestand extrahiert werden. Hierbei wird es sich in der Regel um eine Protokolldatei der Anwendung handeln.

Die folgende Tabelle gibt einen groben Überblick, wo Protokoll- und Verfahrensdaten anfallen bzw. anfallen können. Es kann nötig werden, auch Betrachtungen zur Protokollierung auf Ebene des Kommunikationsnetzes zu machen. Die dort anfallenden Daten dürfen jedoch nur für Zwecke der Datensicherung ausgewertet werden.

Protokoll- und Verfahrensdaten können je nach Anwendung in einer Datei oder in einer Datenbank(-tabelle) gespeichert werden. Für die Zweckbindung spielt der Speicherort keine Rolle. Die Frage, ob eine (strenge) Zweckbindung ausschließlich zu Zwecken der Datenschutzkontrolle gegeben ist, oder auch eine Auswertung zur Leistungskontrolle zulässig sein kann, richtet sich nach dem Zweck der Aufzeichnung.

- Protokolldaten sind Daten, die den Zweck haben, im Rahmen eines Datensicherheitskonzepts unzulässige Zugriffe nachzuweisen oder Zugriffe befugter Personen zu dokumentieren, die auf eine nach dem Sicherheitskonzept unzulässige Art und Weise erfolgen. Sie unterliegen der Zweckbindung. Sie sind nach den Regeln des Sicherheitskonzepts auszuwerten. Diese Daten fallen vorrangig auf Netz-, Betriebssystem- und Datenbankebene an.
- Verfahrensdaten sind Daten, die den Zweck haben, die Entstehung und Bearbeitung der Akten oder Dokumente nachvollziehbar zu machen. Sie können von Vorgesetzten auch unter dem Gesichtspunkt einer Leistungskontrolle ausgewertet werden. Die nötigen rechtlichen Voraussetzungen müssen natürlich eingehalten werden (s. Ziff. 5.5.2 Verfahrens- und Protokolldaten). Diese Daten sind entweder in der Anwendung oder bei der Akte oder dem Dokument gespeichert.

Komponente	Funktion, zu der Daten gespeichert werden	Gespeicherte bzw. protokollierte Daten (Auszug, i. d. R. weitere)	Auswertung für Zwecke der Datensicherheit zulässig	Auswertung zur Leistungs- und Verhaltenskontrolle zulässig
Betriebssystem				
	Anmeldung <i>(mit Benutzerkennung, Passwort o.ä.)</i>	Datum, Uhrzeit, Benutzerkennung, Fehlversuche	ja	nein
	Zugriffe auf Dateien	Zugriff (Lesend, schreibend)	ja	nein *)
	Verstöße gegen Zugriffsrechte		ja	nein
Datenbank				
	Anmeldung	Datum, Uhrzeit, Benutzerkennung, Fehlversuche <i>Beschäftigte der Administration mit eigener Kennung, andere Nutzende oft mit einer gemeinsamen Kennung für die Anwendung</i>	ja	nein
	Zugriff auf Datenbankelement <i>(zum Beispiel Akte, Dokument,)</i>	Benutzerkennung (DB), Datum, Uhrzeit, Zugriff (Lesen, Schreiben, Löschen, ...)	ja	nein *)
	Inhaltliche Änderung Datenbankelement <i>(Dokument)</i>	Änderungsdaten <i>(des Dokuments)</i>	nein <i>(außer im begründeten Einzelfall)</i>	nein *)

*) Etwas anderes gilt - soweit rechtlich zulässig, siehe auch Ziffern 2.2, 2.5, 4.8, 4.8.1, 5.5.2 - ausnahmsweise, wenn die Anwendung unmittelbar auf die Protokolldaten derart zugreift, dass der Protokolleintrag gleichzeitig auch ein Verfahrensdatum darstellt.

Komponente	Funktion, zu der Daten gespeichert werden	Gespeicherte bzw. protokollierte Daten (Auszug, i. d. R. weitere)	Auswertung für Zwecke der Datensicherheit zulässig	Auswertung zur Leistungs- und Verhaltenskontrolle zulässig
Anwendung				
	Anmeldung <i>(etlv. vom Betriebssystem übernommen)</i>	Datum, Uhrzeit, Benutzerkennung, Fehlversuche	ja	nein
	Zugriff auf Akte / Vorgang Dokument	Datum, Uhrzeit, Benutzerkennung Zugriff (Lesen, Schreiben, ...) Bearbeitungsvermerk	ja	ja *)
	Verstöße gegen Zugriffsrechte		ja	nein
Akte / Vorgang				
	Zugriff auf / Historie von Dokumenten (Verfahrensdaten)	Datum, Uhrzeit, Benutzerkennung Zugriff (Anlegen, Lesen, Schreiben, Löschen, ...)	ja	ja *)
Dokument				
	Zugriff auf / Historie von (Verfahrensdaten)	Datum, Uhrzeit, Benutzerkennung Zugriff (Lesen, Schreiben, ...) Bearbeitungsvermerk	ja	ja *)
	Änderung im Dokument	Änderungsdaten	nein <i>(außer im begründeten Einzelfall)</i>	ja *)

*) soweit rechtlich zulässig, siehe auch Ziffern 2.2, 2.5, 4.8, 4.8.1, 5.5.2

2.6 Ausblick

Auch wenn das eindeutige Schwergewicht beim Dokumentenmanagement derzeit auf den klassischen Funktionen der Aktenverwaltung und des Workflow liegt, kann ein DMS in Zukunft auch die Grundlage für weitergehende Nutzungen, insbesondere für Auswertungen über den Inhalt der Dokumente in Form eines **Wissensmanagements** bilden. Derartige Auswertungen, für die Instrumente des Data mining zur Verfügung stehen und technisch auch in der Verwaltung eingesetzt werden könnten, werden dann datenschutzrechtlich relevant, wenn sie über den konkreten Vorgang oder das jeweilige abgegrenzte Aufgabenfeld hinaus oder ggf. sogar behörden- oder verwaltungsübergreifend vorgenommen werden und dabei Informationen unmittelbar personenbezogen zugeordnet oder zumindest personenbeziehbar bleiben. So sehr die Aktivierung des in dem jeweiligen Aufgabenfeld oder in der jeweiligen Behörde vorhandenen, in den Akten und Vorgängen niedergelegten Wissens zur Vervollständigung der Entscheidungsgrundlagen und damit auch zur Verbesserung der Entscheidungsqualität von Nutzen sein kann, aus Datenschutzsicht stellt sich hier sehr deutlich insbesondere das Problem, inwieweit der Grundsatz der Zweckbindung eine derartige, von dem jeweiligen Einzelvorgang abgelöste Nutzung personenbezogener oder zumindest personenbeziehbarer Informationen zulässt. Denn der Zweck der Auswertung in Form des Wissensmanagements ist nicht deckungsgleich mit dem Zweck, zu dem die Informationen Eingang in die ursprüngliche Vorgangsbearbeitung und in die Akten gefunden haben. Insbesondere besteht die Gefahr, dass durch die Verknüpfung der Informationen Persönlichkeitsprofile generiert oder automatisierte Vorhersagen von Verhaltens- und Handlungsweisen ermöglicht werden und dass die Informationen länger als für die Erledigung des ursprünglichen Zweckes geboten verfügbar gehalten werden.

Erfordert allerdings die ordnungsgemäße Bearbeitung eines Vorgangs zwingend auch die Kenntnis anderer Vorgänge, so muss der Zugang zu diesen Vorgängen eröffnet werden und es muss auch die Recherche über die Existenz solcher Vorgänge möglich sein. Hierzu sollten aber besondere Mechanismen eingerichtet werden, z.B. zentrale Recherchestellen und die Entscheidung über die Zugriffseröffnung durch einen übergeordneten Funktionsträger. Soweit ein Wissensmanagement nur auf die Kenntnis der abstrakten Sachverhalte bzw. Entscheidungen der Behörde ausgerichtet ist und der Personenbezug dabei keine Rolle spielt, bietet es sich an, hier die Zugriffsrechte auf die Teile der Vorgänge zu beschränken, die diese abstrakten Informationen enthalten, bzw. nach Abschluss der Vorgangsbearbeitung solche abstrakten Informationen für das Wissensmanagement durch dauerhafte und verlässliche Eliminierung des Personenbezuges zu erzeugen.

Eine weitere zukünftige Nutzungsmöglichkeit auf der Grundlage eines Dokumentenmanagements besteht darin, mit seiner Hilfe Verwaltungsleistungen zusammenzufassen und bestehende Zuständigkeiten zu überspringen bzw. zusammen zu führen. Erste Ansätze dazu gibt es bereits bei den so genannten „Bürgerbüros“ oder bei Pilotprojekten zum sogenannten „mobile government“, bei dem die Verwaltung den Bürgerinnen und Bürgern aufgabenübergreifend Verwaltungsleistungen außerhalb der Dienstgebäude (und ggf. auch der üblichen Sprechzeiten) unmittelbar vor Ort anbietet und die dazu notwendige Informationsverarbeitung über Laptop und elektronischen Zugriff auf die Behördendokumente realisiert. Auch hier bildet der Grundsatz der Zweckbindung, der sich in einem Dokumentenmanagementsystem in einem ausdifferenzierten Rollen- und Berechtigungskonzept niederschlagen muss und der multifunktionalen Berechtigungen und Nutzungen enge Grenzen setzt, den entscheidenden Prüfstein für die Frage der rechtlichen Zulässigkeit.

Diese weitergehenden, als Zukunftsoption anzusehenden Nutzungsmöglichkeiten sollen und können im Rahmen dieser Handreichung aber nicht näher betrachtet werden; die Fragen ihrer grundsätzlichen datenschutzrechtliche Zulässigkeit und der Anforderungen an eine datenschutzgerechte Ausgestaltung im Einzelnen bleibt einer gesonderten Bewertung vorbehalten, wenn auch die Konturen dieser zukünftigen Nutzungsmöglichkeiten genauer erkennbar geworden sind.

3 Datenhaltungsmodelle

DMS können auf unterschiedlichen Datenhaltungsmodellen aufgesetzt werden. Jedes DMS lässt sich einer der unten beschriebenen Kategorien zuordnen oder bildet eine Kombination der Kategorien ab. Damit wird es möglich, DMS einzuordnen und die zu den einzelnen Szenarien getroffenen Aussagen entsprechend auf das jeweils zu betrachtende System zu übertragen.

3.1 Dezentrale Modelle

Bei der dezentralen Datenhaltung werden die Daten in einem DMS dort gespeichert, wo sie auch erzeugt wurden bzw. die Dokumente als „Post“ eingehen. Somit hat jede Daten verarbeitende Stelle ihre eigene Datenhaltung. DMS verschiedener Daten verarbeitender Stellen können zwar über ein Netz miteinander kommunizieren, sind aber ansonsten als vollständig autonom anzusehen. Systemübergreifende einheitliche Dienste gibt es nicht. Bei einer dezentralen Architektur muss für jeden Kommunikationsvorgang explizit eine Kommunikationsverbindung zwischen dem sendenden und dem empfangenden System aufgebaut werden.

3.2 Zentrale Modelle

Bei der zentralen Datenhaltung werden Daten, deren Verarbeitung in der Verantwortung verschiedener Daten verarbeitender Stellen liegen, technisch zentral in einem DMS zusammengeführt und in einem zentralen System gespeichert. Dies bedeutet, dass bei den verschiedenen beteiligten Einrichtungen selbst keine Daten gespeichert werden. Dabei können logisch die Datenbestände in einzelne jeweils einer bestimmten Daten verarbeitenden Stelle zugewiesene Datenbestände unterteilt werden, so dass die logische Struktur einer dezentralen Datenhaltung entspricht.

3.3 Verteilte Datenhaltung

Bei der verteilten Datenhaltung werden, wie im Falle der dezentralen Datenhaltung, die Daten auf den Systemen der Daten verarbeitenden Stellen gespeichert, die sie auch erzeugt haben, bzw. die sie als Posteingang erhalten haben. Darüber hinaus gibt es aber systemübergreifende Dienste, die dafür sorgen, dass die einzelnen dezentralen Systeme zu einem Kommunikationsverbund (z.B. alle öffentlichen Stellen der Region Hannover) zusammengeschlossen werden. Damit sind die dezentralen Systeme Subsysteme des durch den Verbund entstandenen Gesamtsystems. Den Anwendern eines verteilten Systems bleibt die physikalische Verteilung der Daten auf eine Vielzahl von Subsystemen verborgen, und ihnen wird der Eindruck vermittelt, als arbeiteten sie mit einem Zentralsystem. Ein verteiltes System benötigt übergeordnete Metainformationen über die bei den einzelnen Subsystemen gespeicherten Dokumente.

3.4 Dezentrale Datenhaltung mit zentraler Komponente

Bei dieser Datenhaltungsform findet eine dezentrale Datenhaltung bei den einzelnen Daten verarbeitenden Stellen statt. Außerdem können Dokumente der verschiedenen Einrichtungen an einer zentralen Stelle temporär (technisch) zusammengeführt werden. Bei diesem Modell bildet die zentrale Speicherkomponente einen Puffer, der allen angeschlossenen Einrichtungen zum Up- und Download zur Verfügung steht. Dokumente werden vom Sender auf diesen zentralen Speicher übertragen (Upload) und können dann vom Empfänger von dort abgeholt werden (Download).

4 Organisatorische Rahmenbedingungen

Die Nutzung eines DMS verändert die Arbeit in jeder Behörde erheblich. Dies nicht nur, weil es sich um ein zentrales Arbeitsmittel handelt, sondern auch, weil es die Abläufe innerhalb der Behörde und an den Schnittstellen nach außen erheblich verändert. Erster Schritt vor der Einführung eines DMS muss deshalb eine gründliche organisatorische Vorbereitung sein.

Im Rahmen einer gesamtheitlichen Betrachtungsweise sind neben technischen, personellen, finanziellen und rechtlichen Konsequenzen der Einführung eines DMS in der jeweiligen Behörde insbesondere auch die **organisatorischen** Rahmenbedingungen im Vorfeld zu analysieren und zu bewerten. Die Entwicklung bzw. Einführung von Informationssystemen ist immer Anstoß für die Verwaltung, die bestehende Organisation einer kritischen Betrachtung zu unterziehen und im Ergebnis der Untersuchung entsprechende Konsequenzen zu ziehen. Dieses Kapitel skizziert die notwendigen Aktivitäten bei der Einführung eines DMS in Anlehnung an die Phasenpläne des eGovernment-Handbuches des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie am Handbuch für Organisationsuntersuchungen in der Bundesverwaltung. Auf die hierbei typischen Projektplanungsstufen – Zielformulierung, Analyse der Ist-Situation, Entwicklung von Lösungskonzepten, Entscheidung zum weiteren Vorgehen – kann an dieser Stelle nur punktuell eingegangen werden. Insofern sind die nachstehenden Hinweise als ergänzende Informationen zu betrachten, so wie sie aus Sicht des Datenschutzes im Hinblick auf die Einführung eines DMS erforderlich sind.

4.1 Vorabkontrolle

Öffentliche Stellen des Bundes und der Länder bzw. behördlich bestellte Datenschutzbeauftragte haben (je nach Regelung im jeweiligen Datenschutzgesetz) grundsätzlich vor Einführung automatisierter Verarbeitungen zu prüfen, ob die mit der automatisierten Verarbeitung verbundenen besonderen Risiken für die Rechte und Freiheiten der Betroffenen wirksam beherrscht werden können. Diese Risikoabschätzung ist im Rahmen einer Vorabkontrolle (z.B. nach § 4 d Abs. 5 und 6 BDSG) durchzuführen (s.u. Ziff. 5.5.1).

4.2 Projektinitialisierung

Der Einsatz eines DMS wirkt sich innerhalb der Behörde auf verschiedene Verantwortungsbereiche und Organisationseinheiten aus, so dass es geboten ist, die Einführung eines DMS von Beginn an durch ein Projektteam vorbereiten und durchführen zu lassen. Hierbei hat sich die schon frühe Beteiligung folgender Funktionsträgerinnen und Funktionsträger als empfehlenswert herausgestellt:

IT-Sicherheitsbeauftragte, behördliche Datenschutzbeauftragte, Personalvertretung, Verantwortliche von betroffenen Fachverfahren, Revision, Poststelle, Registratur, IT-Bereich (ggf. auch externe Dienstleister) und auch weitere Beschäftigte aus den jeweils betroffenen Behördenbereichen.

4.3 Ist-Analyse, Aufbau- und Ablauforganisation

Im Zuge der Ist-Analyse wird hinsichtlich der Organisationsstrukturen die Gewichtung auf der Ablauf- und weniger auf der Aufbauorganisation im Fokus der Betrachtungen liegen; dies ist in der eher prozessorientierten Sicht bei der Implementierung eines DMS-Systems begründet.

Dabei sind die bei allen Systemeinführungen obligatorischen Analysen zur Festlegung organisatorischer und technischer (Sicherheits-) Maßnahmen wie z.B.:

- Ist-Aufnahme der Organisation (Rollen, Aufgaben, Befugnisse, Qualifikationen, etc.) zur Entscheidung der Ergänzung oder Modifizierung der Organisationsstruktur,

- Ist-Aufnahme der bestehenden und künftigen IT-Infrastruktur (Server-Systeme, Netze, verwendete Officeprogramme, E-Mail- und Web-Server, Anbindung an externe Netze, bestehende und mögliche künftige IT-Verfahren sowie von weiteren Funktionalitäten etc.) durchzuführen.

4.4 Analyse des Schutzbedarfs der Dokumente

Hauptaugenmerk aller Untersuchungen sind jedoch die zu speichernden Dokumente. Der umfassenden Analyse des tatsächlichen Schutzbedarfs der zu verarbeitenden Dokumente kommt eine Schlüsselrolle zu.

Das Bundesdatenschutzgesetz und die entsprechenden landesgesetzlichen Regelungen unterscheiden nur zwischen "besonderen Arten personenbezogener Daten", für die besondere Schutzvorschriften gelten, und den übrigen Daten, bei denen ganz bewusst keine weitere Gewichtung vorgenommen wird. Dementsprechend muss für alle personenbezogenen Daten – unabhängig von ihrer Sensitivität oder einer besonderen Schutzwürdigkeit – in jedem Fall zunächst ein Grundschutz gewährleistet sein. Besondere Arten personenbezogener Daten sind gem. der Definition in § 3 Abs. 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Daten, die dem Sozialgeheimnis, dem Personalaktengeheimnis oder einem anderen besonderen Amts- oder Berufsgeheimnis unterliegen, sind nach spezialgesetzlichen Regelungen besonders geschützt, was sich in einem erhöhten Schutzbedarf niederschlägt. Die Verarbeitung oder Nutzung von Personalakten in einem DMS ist nur zulässig, wenn die maßgeblichen Regelungen zur Personalaktenführung in den Beamtengesetzen des Bundes und der Länder dem nicht entgegenstehen.

Zur Feststellung des Schutzbedarfs der Dokumente wird die analoge Anwendung der Hinweise zur Schutzbedarfsfeststellung im entsprechenden Kapitel des IT-Grundschutzhandbuchs (www.bsi.de/gshb/) bzw. in den BSI-Standards 100-2 und 100-3 als Hilfsmittel zur Orientierung empfohlen. Diese sehen drei Schutzbedarfskategorien vor. Wenn Daten unterschiedlicher Schutzbedarfskategorien verarbeitet werden sollen, sind die technischen und organisatorischen Sicherheitsmaßnahmen an der jeweils höchsten Kategorie auszurichten (Maximum-Prinzip). Werden Daten mehrerer IT-Anwendungen auf einem System verarbeitet, so kann durch Kumulation mehrerer kleinerer Schäden ein größerer Gesamtschaden entstehen (Kumulationseffekt). Ein solches System muss dann gegebenenfalls einer höheren Schutzbedarfskategorie zugeordnet werden.

Die Schutzbedarfsfeststellung kann zu dem Ergebnis führen, dass die vom Grundschutzhandbuch empfohlenen Maßnahmen allein nicht ausreichend sind, um ein Schutzniveau zu erreichen, das der Sensibilität der Daten genügt. In diesem Fall müssen weitere Maßnahmen realisiert werden (Stichwort: „Grundschutz + x“, siehe 17. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, Kapitel 8.3).

Gesondert betrachtet werden muss in diesem Zusammenhang die Frage, ob aus rechtlichen Gründen (Schriftformerfordernis) die Anbringung einer qualifizierten Signatur erforderlich ist. Bei der Frage der Auswahl und des Einsatzes bestimmter Zertifikate muss das gewünschte Einsatzfeld betrachtet werden. Aus Sicht des DMS-Einsatzes können Zertifikate im Innen- und im Außenverhältnis der Behörde (z. B.: zur internen Ver- bzw. Umschlüsselung, Authentisierung von Behördenbeschäftigten, Vorgangsbearbeitung, Authentisierung der Behörde oder Organisationseinheit, Authentisierung von Servern und Clients) erforderlich sein. Die Verwendung von Signaturen ist in Ziff. 7 in diesem Dokument näher dargelegt.

Die im Ergebnis notwendigen organisatorischen und technischen Maßnahmen zur Gewährleistung des informationellen Selbstbestimmungsrechts des Einzelnen sind konsequent umzuset-

zen; ist dies nicht oder nur teilweise möglich, muss unter Umständen auf die weitere Realisierung des Vorhabens ganz oder teilweise verzichtet werden.

4.5 Organisationskonzept

Die aus den Ergebnissen der Ist-Analyse gewonnenen Erkenntnisse sind schließlich in ein Organisationskonzept zu überführen, das neben Festlegungen zur Aufbau- und Ablauforganisation auch dedizierte Aussagen zum **Funktionsumfang** des künftigen DMS enthalten muss (s. Ziff. 2.3). Hier sind die unerlässlichen Funktionen bzw. Fähigkeiten des künftigen Systems ebenso zu fixieren wie die notwendigen Beschränkungen (z. B. Einschränkung der Auswerte- und Recherchemöglichkeiten). Neben den erforderlichen Regelungen zum Umgang mit den unvermeidlichen Medienbrüchen sowie zu den weiterhin bestehenden Rest-Papierakten sind auch Festlegungen zu den künftig zu speichernden Dateiformaten in jedem Falle erforderlich (siehe hierzu die ausführlichen Hinweise des BSI zur Auswahl geeigneter Dokumentformate für eine Langzeitspeicherung im IT-Grundschutzhandbuch unter der Ziffer M 4.170; <http://www.bsi.bund.de/gshb/deutsch/m/m04170.html>).

4.6 DOMEA 2.1

Wertvolle Hinweise zur Erstellung von Organisationskonzepten liefern das KBSt-DOMEA-Organisationskonzept Version 2.1 von November 2005 sowie die dazu komplementär nutzbaren Erweiterungsmodul wie Virtuelle Poststelle, Scanprozesse, Verfahrensintegration, innerbehördliche Kommunikation, Aussonderung und Archivierung, Formularmanagement, Contentmanagement, Zahlungsverkehrsplattform, Projektleitfaden zur Einführung von VBS/DMS sowie seit kurzem auch zum Datenschutz.

Die Kriterien im DOMEA-Ergänzungsmodul für Datenschutz werden hauptsächlich anhand des BDSG für Bundesbehörden abgebildet; auf landesrechtliche Besonderheiten wird nicht weiter eingegangen. Dies muss bei einer Verwendung bei Landes- oder Kommunalbehörden entsprechend berücksichtigt werden. So findet sich im Ergänzungsmodul bspw. keine Aussage über die Protokollierung und Dauer der Aufbewahrung der Protokolldaten der Zugriffe durch die Administration (vgl. z.B. § 6 Abs 2 LDSG S-H, § 8 Abs. 4, 5 DSVO S-H).

Das Zertifizierungsverfahren nach dem DOMEA-Anforderungskatalog 2.0 bezieht sich lediglich auf die Grundfunktionalitäten eines DMS. Die oben näher bezeichneten Erweiterungsmodul – so auch das Erweiterungsmodul Datenschutz – sind nicht Prüfungsgegenstand und somit auch nicht Bestandteil des Zertifizierungsverfahrens. Hier ist in jedem Falle zu prüfen, ob die zur Auswahl stehenden DMS-Produkte die spezifischen Datenschutzerfordernisse der Behörde erfüllen.

Eine Zusammenstellung aller Dokumente ist über den nachstehenden Link zu finden; sie stehen dort zum Download bereit:

(<http://www.kbst.bund.de/DOMEA-Konzept/-,414/Organisationskonzept.htm>)

4.7 Datenschutz- und Datensicherheitskonzept, Rollen- und Rechtekonzept

Der datenschutzgerechte Einsatz eines DMS erfordert klare Festlegungen, wer für welche Aufgaben verantwortlich ist und wer die Verantwortung für die Vollständigkeit und Korrektheit von Daten und Verfahren trägt. Hierfür ist ein **verfahrensbezogenes Datenschutz- und Datensicherheitskonzept** zu schaffen (s. u. Ziff. 6). Alle hierin festgelegten verfahrensmäßigen und technisch-organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit müssen konsequent umgesetzt und in ihren Wirkungen im Rahmen eines begleitenden Controllings intensiv beobachtet werden. Nur so ist sichergestellt, dass die Effektivität der Maßnahmen gewährleistet bleibt, Fehlentwicklungen oder Vollzugsdefizite frühzeitig entdeckt und notwendige Weiterentwicklungen zeitgerecht eingeleitet werden können. Dies ist primär Aufgabe der jeweiligen Daten verarbeitenden Stelle im Sinne der Datenschutzgesetze, d.h. der Behörde. Die be-

hördlichen Datenschutzbeauftragten sind hierbei rechtzeitig zu beteiligen. In Fragen des Datenschutzes und der Datensicherheit kann die Beratung der Datenschutzbeauftragten des Bundes und der Länder in Anspruch genommen werden.

Das Datenschutz- und Datensicherheitskonzept basiert auf der Analyse des Schutzbedarfs der Dokumente (Ziff. 4.4). Auf der Grundlage der hierbei gewonnenen Erkenntnisse sind insbesondere Entscheidungen zu treffen über:

- Art, Zweck, Umfang und Speicherdauer von Dokumenten sowie Verfahrens- und Protokoll-daten
- das notwendige Niveau für das Authentisierungsverfahren und - orientiert an den Anforderungen aus Schutzbedarf, Beweiswert und Formerfordernis - ggf. auch für das Verschlüsselungs- und Signaturverfahren;
- die Einrichtung von behörden- bzw. organisations- oder funktionsbezogenen elektronischen Postfächern; dieses schließt auch Überlegungen hinsichtlich der Implementierung einer virtuellen Poststelle mit ein,
- den Umgang mit Dokumenten, die eine bestimmte juristische Qualität erfüllen müssen (z. B.: Sicherstellung der Nachsignierung vor Ablauf der Gültigkeit der kryptographischen Algorithmen, s. u. Ziff. 5.2),
- den Einsatz von Verschlüsselungstechnik zur Transportsicherung und ggf. bei der Speicherung,
- die Notwendigkeit einer Ende-zu-Ende-Verschlüsselung sowie die Erstellung von qualifizierten Signaturen;
- die zentrale oder dezentrale kryptografische Behandlung der ausgehenden Post.

Eine mangelhafte Benutzer- und Rechteverwaltung kann dazu führen, dass Unberechtigten Zugang zu personenbezogenen Daten gewährt wird. Derartige Gefährdungen entstehen, wenn beispielsweise eine gemeinsame Benutzerkennung von mehreren Beschäftigten genutzt wird, Anwendungen durch Beschäftigte ausgeführt werden, die die betreffenden Daten für ihre Aufgabenstellung nicht benötigen, oder Personen innerhalb eines spezifischen Verfahrens über Rechte verfügen, die sie für die Aufgabenerledigung nicht benötigen. Um diesen Gefahren entgegenzutreten, ist ein detailliertes **Rollen- und Rechtekonzept** zu erarbeiten und im DMS manipulationssicher zu implementieren.

Fehler beim Einrichten der Protokollierungsfunktionen und beim Umgang mit Protokolldaten führen leicht zur Verletzungen des Datenschutzes bei Beschäftigten und anderen Betroffenen. Deshalb ist auch ein **Protokollierungskonzept** zu verfassen und umzusetzen.

In DMS-Projekten sind daher frühzeitig Verantwortungsbereiche und Befugnisse für alle Beteiligten schriftlich festzulegen. Es ist ein Rollen- und Zugriffsrechtekonzept zu erstellen, das regelt, welche Personen im Rahmen ihrer jeweiligen Funktion (Anwendungsentwicklung, Systemadministration, Anwenderbetreuung, Sachbearbeitung, Revision, behördliche Datenschutzbeauftragte) welche Funktionen und welche Daten nutzen dürfen. Dabei dürfen immer nur so viele Zugriffsrechte vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist. Die Festlegung und Veränderung von Zugriffsrechten ist von den jeweils Verantwortlichen zu veranlassen und zu dokumentieren. Alle am DMS-Projekt beteiligten Personen sind vor der Aufnahme des Wirkbetriebes intensiv zu schulen. Die erforderlichen Maßnahmen sind in einem Schulungskonzept zusammenzufassen. In größeren Behörden bzw. Unternehmen kann es sinnvoll sein, eine zentrale Stelle (User-Help-Desk) mit der Betreuung der IT-Benutzerinnen und -Benutzer zu beauftragen und diese den Betroffenen bekannt zu geben.

4.8 Organisatorische Regelungen

Durch die Möglichkeiten der Inhaltskontrolle und Protokollierung in DMS-Projekten können die einbezogenen Beschäftigten einer Verwaltung prinzipiell überwacht und ihre Leistung und ihr Verhalten kontrolliert werden. Deshalb ist die frühzeitige Beteiligung der Personalvertretung und der behördlichen Datenschutzbeauftragten vor der Einführung eines solchen Systems unerlässlich. Siehe hierzu auch die Ausführungen zu Protokoll- und Verfahrensdaten unter Ziff. 2.5 und 5.5.2.

4.8.1 Dienstvereinbarung

Es empfiehlt sich, eine Dienstvereinbarung mit der gewählten Personalvertretung abzuschließen. Inhalte einer Dienstvereinbarung können Eckpunkte über die Verarbeitung und Nutzung der personenbezogenen Daten der Beschäftigten, Daten- und Persönlichkeitsschutz, Rechte des Personalrats, Arbeitsplatzgestaltung und Arbeitsschutz, Benutzerbetreuung, Weiterbildungsangebote usf. sein. Hierbei ist insbesondere zu regeln, was protokolliert wird bzw. welche Verfahrensdaten gespeichert werden, zu welchem Zweck diese Daten verwendet werden, wer sie auswerten darf und wie lange sie aufbewahrt werden. Soweit die Protokollierungen der Aufrechterhaltung der Datensicherheit dient, ist festzuhalten, dass diese in allen Fällen den besonderen Zweckbindungsvorschriften des § 14 Abs. 4 BDSG bzw. der entsprechenden Vorschriften der Landesdatenschutzgesetze unterliegen.

4.8.2 Dienstanweisung

Im Rahmen der Dienstanweisung zur Nutzung des DMS sollten u. a. folgende Regelungen Berücksichtigung finden:

- Bestimmungen zur Aufbau- und Ablauforganisation,
- Festlegung der Zuständigkeiten (behörden-, organisations-, funktionsbezogen; zentral oder dezentral in Abhängigkeit von den Ergebnissen der Organisationsanalyse- insbesondere dort wo es zu fach- oder amtsübergreifender Verantwortlichkeit kommt),
- Festlegung von Verfahrens- und Bearbeitungsregelungen (Festlegung der Zeichnungsbefugnisse, Bestimmungen zur Vertretungsregelung und zur Verwaltung von internen Vertretungs- und Berechtigungsregelungen, Festlegung eines Rollen- und Zugriffsrechtekonzeptes - z. B.: Administration, Revision, Sachbearbeitung -, Sicherstellung der regelmäßigen Abfrage der Arbeitskörbe, Bearbeitungsregelungen für Dokumente mit höherem Vertraulichkeitsbedarf, Behandlung und Weiterleitung von verschlüsselten E-Mails),
- Verfahrensregelungen zur Behandlung nicht geeigneter Eingänge (z. B. Speicherung von Dokumenten mit unvollständiger oder fehlerhafter Signatur oder von Dokumenten, die nicht entschlüsselt werden konnten, Behandlung von Dokumenten in einem nicht akzeptablen Datenformat),
- Regelung zum Einsatz der verschiedenen Signaturen,
- Sicherstellung einer Information an den Absender und ggf. den Empfänger bei Nachrichten, die fehlerhaft sind oder einen schädlichen Inhalt haben,
- Verpflichtung zur Datensicherung und Datenarchivierung (Übernahme in ein elektronisches Archiv) und Festlegung von Formaten mit Eignung für eine Langzeitspeicherung.

5 Rechtsrahmen und datenschutzrechtliche Einordnung

5.1 Aufgabenstellung und Rechtsrahmen beim Einsatz von DMS

Für die nachfolgende datenschutzrechtliche Betrachtung ist von Bedeutung, welche Aufgabe einem DMS zukommt, und welche rechtlichen Rahmenvorschriften zu beachten sind, da dieser Rechtsrahmen die Rechtsgrundlage für die Datenverarbeitung ist.

DMS dienen beim Einsatz in der öffentlichen Verwaltung der Aufgabe, die **konventionelle Aktenführung und Aufgabenerledigung elektronisch abzubilden** bzw. sie durch eine elektronische zu ersetzen. Deshalb müssen sie eingehende Informationen, Schriftverkehr, Anträge, Eingaben, alle Bearbeitungsschritte und ausgehenden Schriftverkehr ebenso dokumentieren wie alle in der Verwaltung erzeugten Vorgänge (z.B. Entstehungsgang von Rechtsvorschriften, Planungsverfahren, Verträge, Beschaffungen, Haushaltsvorgänge). Die Dokumentation muss bei Verwaltungsverfahren und zivilrechtlichen Rechtsgeschäften aber auch unter dem Gesichtspunkt von Haftungstatbeständen ebenso revisionssicher und „gerichtsfest“ wie die herkömmliche Akte sein. Die Funktion eines DMS im Bearbeitungsgang endet nach Ablauf von Aufbewahrungsfristen mit dem Anbieten der Dokumente für das nach den Archivgesetzen zuständige öffentliche Archiv, schlussendlich also mit dem Übergang archivwürdiger Dokumente in ein Archivierungssystem und der Löschung im DMS.

Im Hinblick auf bereits derzeit im Bund und einigen Bundesländern bestehende (und für die anderen Länder zu erwartende) Notwendigkeiten der Eröffnung eines allgemeinen Informationszugangs zu Handlungen und Entscheidungen der Verwaltung sollten Überlegungen zum Aufbau eines DMS auch die Zusammenführung solcher Potenziale mit einbeziehen. Auf eine Einzelbetrachtung der möglichen Szenarien wurde hier verzichtet; sie würde den Rahmen dieser Orientierungshilfe sprengen.

Bereits heute wird ein erheblicher Teil der Korrespondenz, sei es verwaltungsintern zwischen einzelnen Daten verarbeitenden Stellen oder mit Bürgerinnen und Bürgern, elektronisch abgewickelt. Bei allen Vorgängen, die nicht an eine bestimmte Form gebunden sind, ist das völlig unproblematisch. Es erfordert bei Führung einer Papierakte nur die Dokumentation durch Ausdrucken und Ablegen in der Akte. Zu betrachten sind aber Dokumente, für die eine bestimmte Form vorgeschrieben ist oder die ggf. als Beweis in Gerichtsverfahren dienen müssen. Der Gesetzgeber hat in vielen Bereichen die Gleichstellung von Schriftform und elektronischer Form zugelassen und z.B. im BGB und in den Verwaltungsverfahrensgesetzen entsprechende Vorschriften eingefügt. Eine Vielzahl von fachspezifischen Einzelvorschriften sind bisher daraufhin überprüft worden, ob und welche Art der elektronischen Form welche Arten der Schriftform ersetzen kann.

Gleichwohl gibt es noch explizite Ausnahmen, für die die Ersetzung der Papierform durch die elektronische Form ausgeschlossen ist. Dazu zählen z.B. die Ernennungsurkunde im Beamtenverhältnis (z.B. § 6 Abs. 2 Satz 4 BBG, § 9 Abs. 2 Satz 3 HBG), der Vollstreckungstitel (§ 167 VwGO, § 724 ZPO), die Ausstellung von Urkunden in Staatsangehörigkeitssachen (§ 38a Staatsangehörigkeitgesetz) und die Regelung in den Beamtengesetzen, die die Verarbeitung medizinischer und psychologische Befunde von Beamten in automatisierter Form in Personalakten ausschließt (z.B. § 90g Abs. 3 BBG, § 101h Abs. 1 NBG, § 107g Abs. 3 HBG).

5.2 Anforderungen an elektronische Dokumente

Schriftstücke in der Verwaltung werden bereits heute elektronisch hergestellt. Ihre Einspeisung in das DMS ist unproblematisch. Anders verhält es sich bei elektronischen Dokumenten, die von außen als Posteingang kommen. Die Daten verarbeitende Stelle wird nicht alle, sondern nur gängige Dateiformate und Anwendungen unterstützen. Wenn sie den elektronischen Geschäftsverkehr eröffnet, muss sie die technischen Randbedingungen in geeigneter Form öffentlich ma-

chen. Dabei sind die Vorschriften der Verwaltungsverfahrensgesetze zu beachten (z.B. § 3a VwVfG).

Im Verwaltungsverfahren kann nach § 3a VwVfG und den entsprechenden Landesregelungen die Schriftform durch die elektronische Form ersetzt werden, sofern nicht besondere Rechtsvorschriften dies ausschließen (vergleichbare Regelungen enthalten z.B. auch §§ 87a AO, 36a SGB I und 126a BGB). Dazu ist es erforderlich, das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen.

Um seine Unterstützungsfunktion erfüllen zu können, muss ein DMS mit elektronischer Signatur versehene Dokumente verarbeiten können. Im organisatorischen Arbeitsgang für den Umgang mit eingehenden signierten Dokumenten muss die Prüfung der Signatur und ggf. die längerfristige Verfügbarkeit der dabei entstehenden Verifikationsdaten vorgesehen werden. Bei der längerfristigen Aufbewahrung sind signierte Dokumente regelmäßig nach § 17 SigV neu zu signieren (s. o. 4.7).

5.3 Bewältigung der Medienbrüche

Beim Übergang auf die elektronische Akte im DMS muss damit umgegangen werden, dass derzeit und auch noch künftig ein Teil der Kommunikation in Papierform abgewickelt wird und weiterhin werden muss. Nachfolgend werden Medienbrüche behandelt, die entstehen, wenn die Papierform in die elektronische Form umzuwandeln ist oder umgekehrt.

5.3.1 Rechtliche Probleme beim vollständigen Übergang auf elektronische Dokumente

Ein vollständiger Übergang auf elektronische Dokumente setzt voraus, dass alle Papierdokumente in elektronische Dokumente umgewandelt werden können, ohne dass sie dabei den Beweiswert im Rechtsverkehr verlieren. Folgt man der Vorstellung, ausschließlich elektronisch Akten zu führen, das eingehende Papier also zu vernichten, setzt das zusätzlich voraus, dass Einsenderinnen und Einsender von Dokumenten kein Rückgaberecht für ihre Originale zusteht. Das ist im Einzelfall zu prüfen. Datenschutzfragen sind berührt, wenn es um unzulässige Verfälschung (z.B. dadurch, dass die Beweisfunktion verloren geht oder die Inhalte geändert werden) oder Löschung (durch Vernichtung des Dokumentes) geht.

Bei der Mehrzahl der Posteingänge wird die Arbeit nur mit dem elektronischen Dokument ohne Papieroriginal unproblematisch sein. Das gilt weitgehend für verwaltungsinterne Schreiben und für Schreiben von Dritten außerhalb der Verwaltung, denen kein Beweiswert zukommt und die nicht Eingang in ein Verwaltungsverfahren finden.

Bei Papierdokumenten, denen **Beweiswert** zukommt, (die also zu irgendeinem späteren Zeitpunkt in einem gerichtlichen Verfahren relevant sein können) stellt sich allerdings die Frage, ob das Papierdokument und seine Überführung in elektronische Form gleiche Beweiswirkungen auslösen. Auf das Papieroriginal finden die Vorschriften des Urkundsbeweises Anwendung (§ 420 ZPO). Das bedeutet, dass die Unrichtigkeit (Unwahrheit) dieser Urkunde nur durch einen expliziten Gegenbeweis erschüttert werden kann. Das durch Einscannen gewonnene elektronische Dokument ist kein Original, ihm fehlt deshalb diese Beweiswirkung. Auch eine Beglaubigung oder/und elektronische Signatur bei der Überführung in die elektronische Form nach § 33 Abs. 4 Nr. 4a, Abs. 5 Nr. 2 VwVfG (bzw. den entsprechenden Landesbestimmungen) kann dies nicht leisten. Die Beglaubigungserklärung eines in elektronische Form umgesetzten Papierdokuments verbunden mit der Signatur der beglaubigenden Behörde bestätigt nur die inhaltliche Übereinstimmung mit dem Original. Beim Beweistritt steht zwar das beglaubigte Dokument, wenn es sich um eine öffentliche Urkunde handelt, dem Original gleich (§ 435 ZPO), und im verwaltungsgerichtlichen Verfahren ist nach § 86 Abs. 5 VwGO auch die Einreichung von Abschriften durch die Behörde zugelassen. Gleichwohl kann im Zweifelsfall die Vorlage des Originals verlangt werden. Privaturkunden sind zum Beweistritt im Prozess immer im Original vorzulegen. Für die durch Überführung in die elektronische Form gewonnenen Dokumente gelten die Regeln des Augenscheinsbeweises; dem Richter steht die freie Beweiswürdigung zu und dieje-

nige Prozesspartei, die das Dokument zur Stützung der verfolgten Ansprüche einbringt, muss den Nachweis der „Echtheit“ erbringen.

Deshalb müssen Papierdokumente, wie z. B. ein Vertragsangebot, das bereits von der anderen Vertragspartei unterzeichnet ist, oder ein von beiden Parteien unterzeichneter Vertrag, ein Antrag, eine Eingabe oder eine rechtsverbindliche Erklärung im Verwaltungsverfahren, weiterhin in Papierform aufbewahrt werden. Möglich ist zwar, sie für die Bearbeitung in elektronischer Form zur Verfügung zu stellen, aber immer dann, wenn es auf den Inhalt solcher Dokumente ankommt, muss auf das Original zurückgegriffen werden können.

5.3.2 Übertragung von elektronischen Dokumenten mit Beweisfunktion in Papierform

Der umgekehrte Fall, dass aus einem elektronischen Dokument mit Beweisfunktion ein gleichwertiges Papierdokument entstehen soll, ist für den Fall relevant, dass die langfristige Aufbewahrung oder Archivierung in herkömmlicher Form (Papier) erfolgen soll. Sie ist auch von Bedeutung, solange die Aktenführung in Papier als führendes System gewählt wird.

Die Vorschriften in der ZPO und der Verwaltungsverfahrensgesetze (VwVfG) regeln diesen Fall nicht. Immer dort, wo an die elektronische Form eine Beweisfunktion geknüpft ist - wie z.B. bei einem mit qualifizierter elektronischer Signatur versehenen Dokument - ersetzt dieses die Schriftform (vgl. § 3a VwVfG und § 126a BGB). Der Beweiswert solcher elektronischer Dokumente geht beim Übergang in ein anderes Medium verloren. Das bedeutet, dass auch die vollständige Überführung in Papier durch schlichtes Ausdrucken bei qualifiziert signierten elektronischen Dokumenten keine Lösung ist, da damit elektronische Originale nicht ersetzt werden können.

5.4 Kein vollständiger Übergang auf elektronische Aktenführung

Fazit aus den in Ziff. 5.3.1 und 5.3.2 getroffenen Feststellungen ist, dass eine rein elektronische Aktenführung derzeit noch nicht möglich ist. Dazu wäre es erforderlich, dass der Rechtsverkehr ausschließlich elektronisch abgewickelt wird. Das ist nicht der Fall. Zum einen gibt es Dokumente, für die nur die papiergebundene Form zulässig ist. Zum anderen ist die für manche Vorgänge erforderliche qualifizierte elektronische Signatur derzeit in der Verwaltung noch nicht im Einsatz. Es ist nicht zu erwarten, dass sie in den nächsten Jahren bei allen Bürgerinnen und Bürgern vorhanden ist, ebenso wie nicht alle Bürgerinnen und Bürger über die Ausstattung verfügen, die ihnen eine elektronische Kommunikation ermöglicht. Die Verwaltung kann von ihnen auch nicht fordern, die Kommunikation mit ihr elektronisch abzuwickeln. Deshalb werden auf nicht absehbare Zeit Papierdokumente eingehen, und es ist deren besondere Behandlung und Aufbewahrung im Original im Einzelfall sicherzustellen.

Solange die Sach- und Rechtslage so bleibt, ist ein vollständiger Übergang auf elektronische Aktenführung genau sowenig möglich wie eine vollständig papiergebundene Akte. Bei Einführung eines DMS ist deshalb in allen Phasen zu berücksichtigen, dass nicht ausschließlich elektronische Dokumente eine Akte bilden und die Hybridakte entsprechende Verweise enthält.

5.5 Datenschutzrechtliche Anforderungen an ein DMS

Für die Verwendung eines Dokumentenmanagementsystems sind die allgemeinen datenschutzrechtlichen Grundsätze zu beachten: Personenbezogene Daten dürfen nur erhoben, verarbeitet oder sonst genutzt werden, wenn und soweit das zur rechtmäßigen Erfüllung der Aufgaben der Daten verarbeitenden Stelle für den gesetzlich zugelassenen oder durch Einwilligung eröffneten Zweck erforderlich ist. Die Daten verarbeitende oder die in deren Auftrag arbeitende Stelle hat diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten. Zentrale Datenschutzfrage beim Einsatz eines DMS ist, wie wirksam verhindert wird, dass

- Dokumente unzulässig im DMS gespeichert werden oder bleiben,
- auf im DMS gespeicherte Dokumente unzulässig zugegriffen werden kann,
- Dokumente manipuliert werden und
- auf Protokolldaten der Beschäftigten zur Leistungs- und Verhaltenskontrolle unzulässig zugegriffen wird.

5.5.1 Vorabkontrolle

Öffentliche Stellen des Bundes und der Länder haben grundsätzlich vor Einführung eines IT-Verfahrens zu prüfen, ob die mit der automatisierten Verarbeitung verbundenen Risiken für die Rechte der Betroffenen wirksam beherrscht werden können. Die Risikoabschätzung dient dazu, die Abläufe der automatisierten Datenverarbeitung transparent zu machen, Gefahren für die Rechte der betroffenen Bürgerinnen und Bürger aufzuzeigen, Sicherungsmaßnahmen zu entwickeln und Restrisiken abzuschätzen, um im Ergebnis einen datenschutzgerechten Technikeinsatz zu erreichen. Soweit das entsprechende Datenschutzgesetz eine Vorabkontrolle nicht generell vorschreibt (wie z.B. § 7 Abs. 6 HDSG, § 10 Abs. 3 DSG NRW), ist sie insbesondere dann durchzuführen, wenn sensitive personenbezogene Daten (§ 3 Abs. 9 BDSG) verarbeitet werden oder die Verarbeitung dazu bestimmt ist, die Persönlichkeit Betroffener zu bewerten einschließlich ihrer Fähigkeiten, ihrer Leistungen oder ihres Verhaltens. Andere Landesdatenschutzgesetze (§ 19 Abs. 2 DSG M-V, § 10 Abs. 5 SächsDSG, § 14 Abs. 2 DSG SA) schreiben eine Vorabkontrolle dann vor, wenn das DMS als automatisiertes Abrufverfahren konzipiert ist. Das ist dann der Fall, wenn das DMS für mehrere Daten verarbeitende Stellen eingesetzt wird und damit einer Stelle der Zugriff auf den Datenbestand einer anderen Stelle eröffnet wird.

Die Vorabkontrolle setzt voraus, dass der Einsatz des Verfahrens, der rechtliche Rahmen und die technischen und organisatorischen Einsatzbedingungen so beschrieben und festgelegt sind, dass auf dieser Grundlage eine Bewertung erfolgen kann, ob beim Einsatz Risiken für das informationelle Selbstbestimmungsrecht vermieden werden. Dazu sind Festlegungen zu treffen, und abhängig von diesen Festlegungen ist eine Vielzahl von Maßnahmen organisatorischer und technischer Art erforderlich. Die Festlegungen, Maßnahmen und das Sicherheitskonzept (s. u. Ziff. 6) sind Bestandteile der Vorabkontrolle. Auch wenn eine Vorabkontrolle nicht zu erfolgen hat, setzt die erforderliche Festlegung der technisch-organisatorischen Maßnahmen eine Risikoanalyse voraus.

5.5.2 Notwendige Festlegungen zur datenschutzgerechten Gestaltung

In der der Einführung des DMS vorausgehenden Konzeptionsphase sind die nachfolgend aufgeführten Festlegungen zu treffen:

- **Es ist die verantwortliche Stelle für den Einsatz des DMS festzulegen.**

Die verantwortliche Stelle hat die nachfolgend genannten Festlegungen zu treffen und die Vorabkontrolle sowie das Sicherheitskonzept (s. u. Ziff. 6) zu erstellen. Wird ein DMS nur in einer Daten verarbeitenden Stelle und nur für deren Dokumente eingesetzt, ist die Bestimmung der verantwortlichen Stelle einfach. Wenn aber ein übergreifender Einsatz und Zugriff auf Dokumente geplant ist, sind die Verantwortlichkeiten vorher festzulegen. Es sind die einschlägigen Vorschriften der Datenschutzgesetze für **automatisierte Abrufverfahren** (z.B. § 10 BDSG, § 12 NDSG, § 7 DSG SA) oder - soweit nach dem jeweiligen Landesrecht vorgesehen - für **gemeinsame Verfahren** (§ 8 DSG SH, § 15 HDSG, § 11a HmbgDSG) einzuhalten.

- **Bei Auftragsdatenverarbeitung ist der Auftrag schriftlich zu fixieren.**

Wird das DMS ganz oder teilweise nicht von der Daten verarbeitenden Stelle, sondern durch eine andere Stelle im Wege der Auftragsdatenverarbeitung betrieben, so sind die Vorschriften für die Datenverarbeitung im Auftrag zu beachten (z. B. § 11 BDSG). Die Verantwortlich-

keit für die Datenverarbeitung verbleibt beim Auftraggeber. Er hat den Auftrag genau schriftlich festzulegen und sich insbesondere von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

- **Es muss der Kreis der Dokumente festgelegt werden, die in das DMS einbezogen werden, und der Schutzbedarf dieser Dokumente ermittelt werden.**

Entsprechend dem Grundsatz der Erforderlichkeit und der Datensparsamkeit ist festzulegen, was dokumentationswürdig ist. Wie bei der herkömmlichen Aktenbehandlung gibt es Dokumente, die von vornherein keinen Eingang in Akten finden (z.B. Werbung, Einladungen zu Veranstaltungen, persönliche Post, Verschlussachen). Hierfür muss es konkrete Festlegungen geben, sofern in der jeweiligen GGO und den Registraturrichtlinien nicht konkrete Festlegungen getroffen sind. Es ist sicherzustellen, dass nur die Dokumente in das DMS eingespeist werden, die für die Aufgabenerfüllung erforderlich sind, und dass sie nur im Rahmen der Zweckbindung verwendet werden. Außerdem ist eine Analyse der in das Dokumentenverwaltungssystem einzuspeisenden Dokumente hinsichtlich ihres **Schutzbedarfes** vorzunehmen, um die erforderlichen technisch-organisatorischen Maßnahmen festzulegen (s. o. 4.3). Je größer der Kreis der potenziellen Nutzerinnen und Nutzer ist, umso komplexer sind die Maßnahmen zur Abschottung der Bereiche, auf die jeweils zugegriffen werden darf. Das Restrisiko steigt ebenso mit der Sensitivität der Daten wie mit der Größe des Nutzerkreises. Die Abwägung kann im Hinblick auf das Sicherheitsrisiko dazu führen, dass bestimmte Dokumente besonders gegen unberechtigten Zugriff geschützt werden müssen (z. B. durch Verschlüsselung), überhaupt nicht eingestellt werden dürfen (z. B. Verschlussachen in Geheimhaltungsstufen, für die das DMS nicht zugelassen ist) oder bei grundsätzlich zentralen Lösungen bestimmte Bereiche auszunehmen sind (z. B. Dokumente von Sicherheitsbehörden), also nicht in das zentral geführte DMS integriert werden dürfen, sondern dezentral zu betreiben sind.

- **Es ist eine Analyse der den Beteiligten übertragenen Aufgaben und der Arbeitsabläufe zu erstellen.**

Aus der Analyse muss ableitbar sein, wer aus welchem Grund oder in welcher Situation auf welche Dokumente wie zugreifen darf. Die Analyse der Arbeitsabläufe ist an den datenschutzrechtlichen Grundsätzen der Erforderlichkeit und Zweckbindung zu messen, und ggf. sind die vorhandenen Abläufe in einem Sollkonzept zu korrigieren (s. o. 4.2 und 4.6). Neue durch die Einführung eines DMS verursachte Abläufe sind festzulegen (z.B. für das Scannen der Dokumente, für Signieren und Signaturprüfung, für die regelmäßige Signaturerhaltung). Die Aufgaben und Abläufe sind Basis für das Rollen- und Berechtigungskonzept (s. u. 8.2).

Die Rolle legt dabei ein bestimmtes Benutzerprofil fest; ihr werden bestimmte Eigenschaften zugeordnet, die den Grund für den berechtigten Zugriff auf einen nach formalen Kriterien eingrenzenden Kreis von Dokumenten bilden.

Die Berechtigung wird der jeweiligen Rolle zugeordnet und stellt technisch sicher, dass der Person, die die Rolle konkret inne hat, nur die für diese Rolle erlaubten Zugriffe möglich sind, und legt den Umfang möglicher Datenverarbeitung (z.B. nur lesen oder lesen und verändern der Dokumente) fest.

- **Der Umgang mit Medienbrüchen und die Verbindung zur Rest-Papierakte sind zu regeln.**

Wie unter 5.3 erläutert gibt es derzeit noch Dokumente, die weiter in Papierform geführt werden müssen. Auch werden in absehbarer Zeit nicht alle Dokumente in elektronischer Form eingehen und nicht alle in elektronischer Form abgesandt werden können. Für die Übergabe der nicht elektronisch eingehenden Dokumente in das Dokumentenverwaltungssystem müssen Vorgehensweisen gewählt werden, die Verlust und Verfälschung verhindern.

Außerdem müssen Vorgehensweisen zur Verbindung der aus rechtlichen Gründen nicht in die elektronische Form überführbaren oder nicht authentisch elektronisch vorliegenden Dokumente mit den elektronischen Dokumenten im DMS festgelegt werden.

- **Das Datenhaltungskonzept und diesem entsprechende Sicherheitsmaßnahmen sind festzulegen.**

Vom Datenhaltungskonzept (s. Ziff. 3) hängt zum einen ab, wer die für die Datenverarbeitung verantwortliche Stelle ist, und welche Gefährdungslagen bestehen. Es ist eine der Grundlagen für die Umsetzung der Zugriffsrechte, und je nach Art der Datenhaltung sind unterschiedliche Sicherheitsmaßnahmen erforderlich.

Bei einem **dezentralen Modell** (s. Ziff. 3.1) ist jede Einrichtung Daten verarbeitende Stelle i.S. der Datenschutzgesetze für ihre eigenen Daten. Datenübermittlungen sind nur aufgrund einer rechtlichen Legitimation zulässig. Diese Lösung birgt datenschutzrechtlich die wenigsten Probleme, weil durch die Art der Datenhaltung keine besonderen Möglichkeiten unberechtigter Zugriffe durch Beschäftigte anderer Daten verarbeitender Stellen geschaffen werden.

Bei dem **zentralen Modell** (s. Ziff. 3.2) werden die Daten mehrerer Daten verarbeitender Stellen in einer zentralen Stelle vorgehalten. Die Datenhaltung wird regelmäßig über die Vergabe einer Datenverarbeitung im Auftrag an einen externen Dritten (z.B. eine Datenzentrale) realisiert. Die Verantwortung verbleibt jeweils bei den Daten verarbeitenden Stellen i.S. der Datenschutzgesetze für ihre eigenen Datenbestände. Die rechtlichen Voraussetzungen für eine Datenverarbeitung im Auftrag müssen erfüllt sein (s. o.). In jedem Fall müssen die Möglichkeit der Kenntnisnahme personenbezogener Daten durch den Auftragnehmer, soweit wie erforderlich, ausgeschlossen und die Datenwege von und nach der zentralen Stelle abgesichert werden. Die Sicherstellung der Eröffnung der Zugriffe nur für Personen, die berechtigt sind, stellt höhere Anforderungen als bei dezentraler Datenhaltung, weil der Kreis der potenziellen Nutzenden deutlich größer ist. Nur, wenn auch eine Datenübermittlung datenschutzrechtlich zulässig wäre, dürfen Dokumente einer Daten verarbeitenden Stelle einer anderen Stelle zur Verfügung gestellt werden. Dies ist technisch sicherzustellen. Die logische und physische Trennung der Datenbestände ist dabei die vorzuziehende Lösung. Datenübermittlungen zwischen den beteiligten Stellen können dann - analog der herkömmlichen Akte - mit Weiterreichung einer „Kopie“ gelöst werden.

Soll jedoch ein einziger gemeinsamer zentraler Datenbestand bestehen, auf den alle beteiligten Daten verarbeitenden Stellen zugreifen können, sind besonders hohe Anforderungen an das Berechtigungskonzept zu stellen, da nicht nur intern, sondern auch über die einzelne Stelle hinausgehende Kommunikationsbeziehungen zu untersuchen und die Zugriffsberechtigungen dafür zu hinterlegen sind. Darüber hinaus wirft die Darstellung in nur einer „Akte“ für alle Beteiligten Probleme bei der Einhaltung von unterschiedlichen Aufbewahrungsfristen und bei der Löschung auf (s.u.). Außerdem ist eine solche Konzeption nach einigen Datenschutzgesetzen an besondere gesetzliche Anforderungen geknüpft (z.B. als „gemeinsames Verfahren“ nach den Datenschutzgesetzen in Hessen und Schleswig-Holstein; als „Abrufverfahren“ nach § 10 BDSG oder § 9 DSG NRW). Die zentrale Datenhaltung birgt spezielle Missbrauchsmöglichkeiten hinsichtlich der Zusammenführung und Auswertung von Daten und erfordert deshalb besondere Schutzmaßnahmen, um diese zu verhindern.

Bei der **verteilten Datenhaltung** (s. Ziff. 3.3) bleiben die einzelnen Daten verarbeitenden Stellen i.S. der Datenschutzgesetze für ihre eigenen Datenbestände verantwortlich. Einige Dokumente befinden sich jedoch auf Subsystemen, deren Standort bei anderen Stellen ist. Ein verteiltes System benötigt übergeordnete Metainformationen über die bei den einzelnen Subsystemen gespeicherten Dokumente sowie einen systemweiten Zugriffskontrollmechanismus. Die Komplexität übertrifft die einer zentralen Datenhaltung. Datenübermittlungen zwischen den verschiedenen Einrichtungen, d.h. zwischen dezentralen Subsystemen, erfor-

dern wie bei der zentralen Datenhaltung eine rechtliche Legitimation und entsprechende Vergabe der Zugriffsrechte. Bei der verteilten Datenhaltung wird die Gefahr einer unzulässigen Auswertung von Daten im Vergleich zur zentralen Datenhaltung gemildert, da selbst im „worst case“ nur die Daten zusammengeführt werden können, die für externe Zugriffe freigegeben wurden.

Auch bei der **dezentralen Datenhaltung mit zentraler Komponente** (s. Ziff. 3.4) bleiben die verschiedenen Daten verarbeitenden Stellen i.S. der Datenschutzgesetze für ihre eigenen Daten verantwortlich. Dies gilt insbesondere für die zentrale Speicherung eines Teildatenbestandes. Rechtlich handelt es sich beim Up- und dem zugehörigen Download um eine Datenübermittlung, die einer rechtlichen Legitimation bedarf. Zusätzlich muss in jedem Einzelfall die rechtliche Legitimation für einen Abruf der Daten vorliegen. Die Möglichkeiten einer Kenntnisnahme personenbezogener Daten durch den externen Dritten müssen in jedem Fall soweit wie möglich ausgeschlossen werden. Bei der dezentralen Datenhaltung mit zentraler Komponente entsteht eine der zentralen Datenhaltung vergleichbare Gefährdungslage, denn es entsteht eine neue zentrale (Teil-)Datensammlung. Den Gefährdungspotentialen ist auch hier mit entsprechenden Schutzmaßnahmen zu begegnen.

- **Es sind die Aufbewahrungsfristen festzulegen.**

Maßgeblich für die Frage der Aufbewahrungsdauer bzw. der Löschung personenbezogener Daten in DMS sind entweder Spezialvorschriften (z.B. die Personalaktenvorschriften der Beamten-gesetze, die Verwaltungsvorschriften zu den Haushaltsordnungen) oder die einschlägigen Bestimmungen der Datenschutzgesetze. Nach den Datenschutzgesetzen dürfen personenbezogene Daten nur solange aufbewahrt werden, wie ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist (z.B. § 20 Abs. 2 Nr. 2 BDSG und entsprechende Vorschriften der Landes-DSG). Aus Spezialvorschriften können sich längere Zeiträume für die Aufbewahrung von Dokumenten ergeben, z.B. von 10 Jahren (Haushalts- und Rechnungslegungsunterlagen) bis hin zur dauernden Aufbewahrung (z.B. für Unterlagen im Bauleitplanverfahren und für Einbürgerungsvorgänge). Die jeweiligen Aufbewahrungsfristen sollten entweder generell auf Aktenzeichenebene oder für Dokumentenarten mindestens aber auf Dokumentenebene bei der Erstellung der Dokumente in das DMS festgelegt werden.

Sofern ein DMS genutzt wird, um Daten aus Fachverfahren zu verwalten, sind Archivierungs- und Löschzeitpunkte aus dem Fachverfahren in das DMS zu übernehmen. Falls durch die Fachverfahren keine solchen Zeiträume übergeben werden können, ist auf eine Ergänzung dieser Zeiträume im DMS hinzuwirken. Außerdem sind mit den zuständigen staatlichen Archiven bereits bei Einführung eines DMS die Anforderungen an die Übergabe elektronischer Akten für den Zweck der dort erfolgenden Langzeitarchivierung zu vereinbaren.

Das DMS muss Unterstützungsfunktionen für die Kontrolle der Aufbewahrungsfristen und für die daran anschließende Übergabe an Archivsysteme und die Löschung der Dokumente im DMS anbieten. Zur Unterstützung der Kontrolle der Aufbewahrungsfristen kann z.B. eine entsprechende Nachricht des DMS dienen.

Bei abgeschlossenen Vorgängen ist jeweils zu prüfen, ob die Daten nach speziellen Vorschriften einem unmittelbaren Zugriff zu entziehen sind und dann z.B. nur noch eine Recherche auf die Metadaten zulässig ist oder eine sonstige Änderung/Beschränkung der Zugriffsberechtigungen erforderlich wird (vgl. z.B. diesbezügliche Regelung in § 36 Abs. 7 Landeskrankenhausgesetz Rheinland-Pfalz).

Soweit elektronisch verarbeitete Daten zu löschen sind, muss - neben den eingesetzten Fachverfahren - auch ein allgemeines DMS die Datenlöschung technisch unterstützen. Hierbei ist auch sicherzustellen, dass eingesetzte Sicherungsmedien diese mit umsetzen.

Hierbei sind Archivierungs- oder Löschezitpunkte durch das System abzufragen. Entsprechende Vorgänge sind zu protokollieren.

Insbesondere bei langfristigen Aufbewahrungszeiten ist sicherzustellen, dass wechselnde Zuständigkeiten bei der Sachbearbeitung der Vorgänge durch das DMS entsprechend abgebildet werden können. Hierbei ist auch auf Vertretungsregelungen und Zugriffsbefugnisse einzugehen.

Wird ein einheitlicher Datenbestand vorgehalten, auf den mehrere Daten verarbeitende Stellen zugreifen können, erfordert das Problem unterschiedlicher zeitlicher Aufbewahrungsnotwendigkeiten (Beispiel: eine Abgabe an eine andere Stelle wegen Unzuständigkeit wird bei der abgebenden Stelle regelmäßig einer kurzen Aufbewahrungsfrist unterliegen, während sie bei der bearbeitenden Stelle schon deshalb länger aufzuheben sein wird, weil die Frist erst ab Schluss der Bearbeitung beginnt) differenzierte technische Lösungen. Rechtliche Anforderung ist, dass die Aufbewahrungsfristen des Vorgangs oder sogar einzelner Dokumente für jede Daten verarbeitende Stelle gesondert festgelegt werden müssen. Zum Zeitpunkt des Ablaufs der kürzesten Aufbewahrungsfrist müssen die Zugriffsrechte der betreffenden Stelle geändert werden (Sperrung), andererseits darf das Dokument (der Vorgang) wegen der Einhaltung der weiteren Aufbewahrungsfristen nicht gelöscht werden; es verbleibt im Datenbestand, bis die längste Aufbewahrungsfrist abgelaufen und die Prüfung der Archivwürdigkeit abgeschlossen ist.

- **Es sind Maßnahmen festzulegen, die die Verfügbarkeit, Vollständigkeit, Integrität, Vertraulichkeit, Unverfälschbarkeit und Verkehrsfähigkeit elektronischer Dokumente über lange Aufbewahrungszeiträume sicherstellen.**

Der Einsatz eines DMS - schon wenn er zunächst nur zur Arbeitsunterstützung erfolgt, erst recht aber bei vollständigem Einsatz - verändert das Arbeitsverhalten der Beschäftigten. Ihre Arbeitsgrundlage ist die elektronische Akte - auch wenn die Papierform in der Übergangszeit noch als verbindliche Akte geführt wird. An die Verfügbarkeit, Vollständigkeit, Integrität, Vertraulichkeit und Unverfälschbarkeit der elektronischen Dokumente müssen deshalb hohe Anforderungen gestellt werden (s. Ziff. 6). Besonders hoch sind die Anforderungen allerdings dann, wenn im DMS zur Ersetzung der Schriftform elektronisch signierte Dokumente enthalten sind.

Während der kompletten Zeit des Verbleibs im DMS sind diese Anforderungen zu erfüllen. Bei Vorgängen, für die längere Aufbewahrungsfristen bestehen, sind Maßnahmen zu ergreifen, die die Beweiskraft elektronisch signierter Dokumente (regelmäßige Signaturneuerung nach § 17 SigV) und die Verkehrsfähigkeit (Sicherstellung langfristig kompatibler Dateiformate s. u. Ziff. 6 zur Rechtssicherheit) erhalten.

Im Anschluss an die Aufbewahrung im Rahmen der Erforderlichkeit und der Aufbewahrungsvorschriften verpflichten die Archivgesetze des Bundes und der Länder die Behörden und sonstigen öffentlichen Stellen dazu, grundsätzlich alle Unterlagen, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen, dem für sie zuständigen Archiv zur Übernahme anzubieten. Die Maßnahmen, die sicherstellen, dass Dokumente über längere Zeiträume sicher, unverfälscht und lesbar bleiben sowie nach Ablauf der Frist für die Aufbewahrung bei der Daten verarbeitenden Stelle technisch in ein Archivsystem überführt werden können, sind im Sicherheitskonzept (s. u. Ziff. 6) zu beschreiben.

- **Es sind Maßnahmen festzulegen, die die Löschung unzulässig gespeicherter sowie nicht mehr benötigter und nicht archivwürdiger Dokumente sicherstellen.**

War die Speicherung personenbezogener Daten unzulässig, sind diese Daten nach den Datenschutzgesetzen zu löschen. Es muss deshalb die Löschung einzelner Dokumente si-

chergestellt sein, und das Verfahren muss gleichzeitig so gestaltet sein, dass unzulässige Löschungen ausgeschlossen werden.

Nach den Löschungsvorschriften der Datenschutzgesetze sind personenbezogene Daten auch zu löschen, sobald deren Kenntnis für die Daten verarbeitende Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Eine sichere Löschung setzt die Festlegung von Aufbewahrungsfristen voraus. Bei Einsatz eines DMS ist außerdem wegen der Fülle der Dokumente zumindest eine automationsgestützte Lösung für Aussonderung und Löschung notwendig. Auch archivwürdige Dokumente sind im DMS der Daten verarbeitenden Stelle zu löschen. Dies darf allerdings erst erfolgen, wenn der Übergang in das Archiv gesichert ist. Eine Löschung der elektronischen Dokumente ist immer vorzunehmen, unabhängig davon, ob das DMS das einzige, das führende oder das untergeordnete System ist. Es genügt - auch solange die Papierakte noch führendes System ist - nicht, nur die Papierdokumente auszusondern, sondern es ist jede Speicherung unabhängig von dem Speichermedium zu löschen. Das Sicherheitskonzept muss auch dazu Maßnahmen enthalten. Bei einer logisch zentralen Datenhaltung (gleichgültig ob sie physisch zentral oder verteilt ist) muss das Problem gelöst werden, dass aus Rechtsgründen für ein Dokument unterschiedliche Aufbewahrungsfristen bestehen können. Die Lösung führt zu komplexen Abläufen, die eine der Rechtslage entsprechende Veränderung der Zugriffsberechtigungen der beteiligten Stellen auslösen müssen. Bei dezentraler Datenhaltung entsteht das Problem nicht, weil Kommunikationswege beschränkt werden und jede Stelle nur ihre „Akte“ führt. Bei logisch dezentraler Datenhaltung sollte das Problem dadurch gelöst werden, dass in jedem (weiteren) Datenbestand eine Kopie nur für die Dauer der dortigen Erforderlichkeit vorgehalten wird. Ferner ist festzulegen, ob und in welchem Umfang die Löschung von Dokumenten protokolliert wird. Eine Protokollierung der Löschung unzulässig gespeicherter Dokumente darf nicht erfolgen, weil sie das Ziel der Löschung konterkarieren würde und damit die Datenschutzrechte Betroffener verletzt. In den anderen Fällen ist dagegen ein Nachweis der Löschung durch die Protokollierung erforderlich.

- **Es sind Verfahrensweisen festzulegen, die die Rechte der Betroffenen auf Berichtigung, Sperrung und Auskunft sicherstellen.**

Nach §§ 19 und 20 BDSG bzw. den entsprechenden Vorschriften der Länderdatenschutzgesetze haben Betroffene ein Recht auf Berichtigung unrichtiger Daten, auf Sperrung von Daten, bei denen aus bestimmten Gründen eine Löschung nicht erfolgen darf, und auf Auskunft zu den über sie gespeicherten Daten. Das DMS sollte alle diese Funktionen unterstützen. Die Berichtigung könnte z. B. mit einer (protokollierten) Löschung und Neueinstellung des berichtigten Dokuments gewährleistet werden. Die Sperrung kann durch Beschränkung der Zugriffe umgesetzt werden, und das Auskunftsrecht kann durch spezielle Recherchen unterstützt werden. Die Verfahrensweisen sind darzulegen und in der Vorabkontrolle zu bewerten.

- **Es sind Maßnahmen zu treffen, die verhindern, dass auf Verfahrens- und Protokolldaten von Beschäftigten unzulässig zugegriffen wird.**

Die Arbeit mit dem DMS erfordert aus verschiedensten Gründen, dass festgehalten wird, wer bestimmte Aktionen wann vorgenommen hat. So ist es z.B. erforderlich, im Rahmen des Workflow den Bearbeitungsgang für ein Dokument oder einen Vorgang mit den Schritten und Bearbeitungsdaten nachvollziehbar und jeweiligen Beschäftigten zugeordnet zu dokumentieren oder Eingriffe durch die Administration wie z.B. die Vergabe von Rollen und Berechtigungen, Fehlerbehebungen etc. entsprechend zu protokollieren (zu den Verfahrens- und Protokolldaten siehe auch Ziff. 2.5).

Bei diesen beim Einsatz des DMS gespeicherten beschäftigtenbezogenen Daten handelt es sich nicht um typische Beschäftigendaten, wie sie die in einigen Datenschutzgesetzen vorhandenen Regelungen zur Verarbeitung von Personaldaten erfassen (z.B. § 34 HDSG, § 28 HmbDSG), sondern um Daten, die anlässlich der Durchführung der übertragenen Arbeit an-

fallen; die sich also nicht auf die Person, sondern auf die Ausübung der übertragenen Funktion beziehen. Potenziell eröffnet die Speicherung dieser Daten aber die Möglichkeit einer Leistungs- und Verhaltenskontrolle, z.B. durch Auswertung der Daten nach Bearbeitungsmenge oder -dauer.

Soweit nicht explizit ein Verbot der Verwendung von Daten, die für technische und organisatorische Datenschutzmaßnahmen gespeichert wurden, zu anderen Zwecken in den Datenschutzgesetzen geregelt ist (z.B. § 14 Abs. 4 BDSG, § 34 Abs. 6 HDSG), lässt sich aus dem allgemeinen datenschutzrechtlichen Grundsatz der Zweckbindung die gleiche Rechtsfolge ableiten. Danach dürfen Daten von Beschäftigten der Anwendung und Administration des DMS, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs gespeichert werden, grundsätzlich nicht für andere Zwecke, insbesondere nicht für eine Verhaltens- und Leistungskontrolle verarbeitet werden. Die Zweckbindung muss daher technisch und organisatorisch (z. B. durch Dienst-anweisung) sichergestellt werden. Für Art, Umfang und Aufbewahrung der Protokoll- und Verfahrensdaten gilt der Grundsatz der Erforderlichkeit. Soweit technisch möglich und ausreichend sollte auf personenbezogene Daten verzichtet werden. Die Beteiligungsrechte des Personalrates sind zu beachten (§ 75 Abs. 1 Nr. 17 Bundespersonalvertretungsgesetz und entsprechenden Ländervorschriften). Darüber hinaus sind die Beschäftigten darüber aufzuklären, in welchem Zusammenhang das DMS welche Verfahrens- und Protokoll Daten über sie speichert. Das folgt aus dem datenschutzrechtlichen Transparenzgebot (§ 19a BDSG und entsprechende Ländervorschriften).

Eine Auswertung der Verfahrens- und Protokoll Daten ist immer dann zulässig, wenn das dem Zweck der Speicherung entspricht.

So ist die Auswertung von Protokoll Daten zur Aufdeckung von Missbräuchen erlaubt. Eine Auswertung von Verfahrensdaten ist zulässig, wenn sie zur Prüfung der Recht- und Zweckmäßigkeit der Erfüllung einer konkreten Aufgabe durch Vorgesetzte oder Aufsichtsbehörden bzw. Kontrollstellen erforderlich ist. Dann ist sie nämlich Teil von deren Aufgabenerfüllung. So wie sich Vorgesetzte bei der herkömmlichen Aktenbearbeitung von ihren Bediensteten zur Erfüllung ihrer Aufsichtsfunktion im Einzelfall die Bearbeitung eines Vorgangs vorlegen lassen dürfen oder auch bei entsprechendem Anlass die Bearbeitung aller Vorgänge, z.B. in einem bestimmten Zeitraum, so dürfen sie dies für diese Aufgabe unter den genannten Voraussetzungen auch, wenn die Bearbeitung im DMS erfolgt. Die Verwendung der Daten hierfür stellt keine Zweckänderung dar, weil sie Teil der Aufgabenerfüllung ist. Eine darüber hinaus gehende Verhaltens- und Leistungskontrolle der Beschäftigten durch eine solche Auswertung ist jedoch unzulässig.

In Abhängigkeit von allen aufgeführten Festlegungen ist das **Sicherheitskonzept** (s. u. Ziff. 6) zu entwickeln.

5.6 Akteneinsicht und Informationszugang bei Verwendung von DMS

Neben dem datenschutzrechtlichen Auskunftsrecht sind auch Akteneinsichtsrechte sicherzustellen. Solche Rechte bestehen aufgrund von § 29 VwVfG sowie § 100 VwGO oder auch von spezialgesetzlichen Regelungen wie z.B. § 90c BBG und der entsprechenden Landesregelungen. Spezielle Regelungen für die Akteneinsicht in eine elektronisch geführte Akte gibt es partiell schon (z.B. Akteneinsicht im Zivilprozess § 299 Abs. 3 ZPO, im Verwaltungsgerichtverfahren § 100 Abs. 2 VwGO, von Beamtinnen und Beamten in ihre Personalakte § 90c Abs. 3 BBG) aber noch nicht in allen Rechtsmaterien. Die praktische Umsetzung solcher Einsichtsrechte bei elektronischer Aktenführung muss sichergestellt werden. Es ist das Verfahren festzulegen. Steht es nach den einschlägigen Rechtsvorschriften im Ermessen der Daten verarbeitenden Stelle, wie sie den Anspruch erfüllt, so kann er ggf. auch mit einem Papierausdruck erfüllt werden; anderenfalls müssen die technischen Randbedingungen geschaffen werden, um den Beteiligten, die Anspruch auf Akteneinsicht haben, auch die elektronische Akte zugänglich zu machen.

Im Bund und in einigen Bundesländern (derzeit in Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein) gibt es außerdem Informationsfreiheitsgesetze, die einen Anspruch für jedermann auf Informationen der Verwaltung begründen, sofern nicht gesetzlich normierte Versagungsgründe entgegenstehen. Für den Bereich der Umweltinformationen gibt es Ansprüche nach dem Bundesumweltinformationsgesetz bzw. den entsprechenden Ländergesetzen.

Die Unterstützung der Ansprüche aus den Informationsfreiheitsgesetzen könnte z.B. dadurch erfolgen, dass bereits beim Einstellen von Dokumenten in das DMS die Frage geklärt wird, ob Dokumente nach den Informationsfreiheitsgesetzen freizugebende Informationen enthalten oder nicht, bzw. auf welche Weise diese freien Informationen aus dem DMS zur Verfügung gestellt werden.

Bereits in der Konzeptionsphase sollten Vorkehrungen für die Erfüllung der Ansprüche aus den Vorschriften für Akteneinsicht und Informationszugang beim Einsatz von DMS getroffen werden.

6 Sicherheitsziele und -maßnahmen bei der Behandlung von Dokumenten

Die Umsetzung der organisatorischen und rechtlichen Rahmenbedingungen muss ergänzt werden durch technische Maßnahmen, damit das Recht auf informationelle Selbstbestimmung der Betroffenen beim Einsatz eines DMS sichergestellt werden kann. Es ist ein **Sicherheitskonzept** zu erstellen, in dem Maßnahmen zur Erreichung der grundlegenden Sicherheitsziele darzulegen sind.

Grundlegende **Sicherheitsziele** sind die Gewährleistung beziehungsweise Sicherstellung der Vertraulichkeit, Authentizität, Integrität, Verfügbarkeit und Revisionsfähigkeit der erhobenen, gespeicherten, übermittelten oder sonst verarbeiteten Daten sowie der Rechtssicherheit im Hinblick auf die beweisbare Überprüfbarkeit von Verarbeitungsvorgängen und die Nicht-Abstreitbarkeit von Datenübermittlungen.

Die konkreten Sicherheitsmaßnahmen sind auf der Grundlage einer Bedrohungs- und Risikoanalyse individuell zu ermitteln. Dabei sind die folgenden Sicherheitsziele zu betrachten:

- **Sicherstellung der Vertraulichkeit**

Es ist in jeder Phase der Datenverarbeitung sicher zu stellen, dass nur befugte Personen die Daten zur Kenntnis nehmen können. Sind an die Dokumente hohe Vertraulichkeitsanforderungen zu stellen, ist eine Verschlüsselung mit starken kryptografischen Verfahren vorzusehen. Zum einen ist eine Verschlüsselung aller Daten zu fordern, die über ein Kommunikationsnetz übertragen werden und zwar unabhängig davon, ob es sich um ein lokales oder um ein öffentliches Netz handelt. Daneben sind alle bei den datenhaltenden Systemen gespeicherten Daten zu verschlüsseln. Nur so kann verhindert werden, dass Systemadministration, Wartungspersonal oder sonstige Dritte (etwa durch Diebstahl) Kenntnis von Daten erhalten.

Die Verschlüsselung zu übertragender Daten kann auf der Transportebene erfolgen, wenn alle Nutzerinnen und Nutzer dem Zugangs- und Zugriffskontrollmechanismus des Systems unterliegen. Ansonsten ist sie auf der Anwendungsebene vorzunehmen.

Die verschlüsselte Speicherung der Daten bei den datenhaltenden Systemen kann realisiert werden durch den Einsatz entsprechender Systemsoftware (beispielsweise Datenbanksysteme, die eine Datenverschlüsselung ermöglichen) oder durch entsprechende Zusatzsoftware (beispielsweise Tools zur Verschlüsselung von Plattenbereichen). Eine andere Möglichkeit zur Lösung dieses Problems besteht in der Verschlüsselung der Dokumente auf Anwendungsebene. Das Verschlüsselungskonzept muss ein Verfahren vorsehen, das in konkret zu definierenden Ausnahmefällen gewährleistet, dass die Daten verfügbar sind.

- **Sicherstellung der Integrität**

Mit dem elektronischen Signieren eines Dokumentes zur Sicherstellung der Authentizität wird gleichzeitig die Echtheit, Korrektheit und Vollständigkeit des Dokumenteninhalts bescheinigt. Wird ein Dokument elektronisch signiert, also elektronisch unterschrieben, wird damit nicht nur die Urheberin oder der Urheber bestätigt, sondern auch, dass das Dokument echt sowie inhaltlich korrekt und vollständig ist. Darüber hinaus sichert das der elektronischen Signatur zugrunde liegende Verfahren die Erkennbarkeit einer nachträglichen Veränderung eines Dokuments. Die erfolgreiche Verifikation der Signatur eines Dokuments stellt damit gleichzeitig die Unversehrtheit des Dokumenteninhalts sicher.

Weitere Mittel zur Sicherstellung der Integrität sind beispielsweise die Versionsverwaltung von Dokumenten und die Protokollierung von Änderungen.

- **Sicherstellung der Verfügbarkeit**

Bei der Sicherstellung der Verfügbarkeit sind die verschiedenen Systemarchitekturansätze zu betrachten. Sowohl im Falle der zentralen Datenhaltung als auch im Falle der dezentralen Datenhaltung ist eine hohe Verfügbarkeit für das gesamte System realisierbar.

Bei der dezentralen und verteilten Datenhaltung hängt die Verfügbarkeit des Gesamtsystems von der Verfügbarkeit aller beteiligten (Sub-)Systeme ab. Bei der verteilten Datenhaltung müssen Kommunikationsprozesse - im Gegensatz zum dezentralen Fall - nicht explizit von den Nutzenden eines Subsystems initiiert werden, sondern können durch systemweit verfügbare Kommunikationsmechanismen angestoßen werden. Allerdings kann es zu technisch bedingten Ausfällen von Subsystemen kommen, die ohne Eingriffe vor Ort nicht beherrschbar sind. Solchen Schwierigkeiten kann technisch dadurch begegnet werden, dass Datenreplikate an verschiedenen Speicherorten vorgehalten werden. Bei Nichtverfügbarkeit eines bestimmten Subsystems wird dann auf das entsprechende Replikat zurückgegriffen. Diese Vorgehensweise ist allerdings datenschutzrechtlich als sehr problematisch einzustufen, wenn die Replikate sich nicht im selben Herrschaftsbereich befinden wie ihre Originale. Außerdem ergeben sich durch Replikate nicht zu unterschätzende Konsistenzprobleme.

Sollen Dokumente langfristig verfügbar bleiben, so sind sie in einem geeigneten Format zu speichern wie ASCII (7 bit), TIFF, PDF/A und XML.

- **Gewährleistung der Authentizität**

Dokumente, deren Authentizität sicher zu stellen ist, sind von ihrer Urheberin oder ihrem Urheber beziehungsweise von den Verantwortlichen elektronisch zu signieren und mit einem Zeitstempel zu versehen. Durch die Nutzung einer elektronischen Signatur kann gewährleistet werden, dass die Authentizität von Dokumenten geprüft werden kann. Weitere Mittel zur Sicherstellung der Authentizität sind beispielsweise die Versionsverwaltung von Dokumenten und die Protokollierung der Urheberschaft sowie des Zeitpunktes von Änderungen.

- **Gewährleistung der Revisionsfähigkeit**

Eine Möglichkeit für die Gewährleistung der Revisionsfähigkeit ist das elektronische Signieren von Dokumenten, weil hiermit die Verantwortlichkeit beziehungsweise Urheberschaft anerkannt wird. Da der Inhalt eines signierten Dokuments nachträglich nicht mehr verändert werden kann, ohne dass die Signatur noch zum Dokument passt, können inhaltliche Änderungen nur in Form von Ergänzungen einem Dokument angefügt werden. Wird das Ursprungsdokument plus Ergänzungen wiederum digital signiert, kann die Historie eines Dokuments manipulationssicher festgehalten werden.

Eine elektronische Signatur gilt derzeit nicht länger als fünf Jahre. Muss die Revisionsfähigkeit länger gesichert werden, so ist die Signatur rechtzeitig zu prüfen und das Dokument gemeinsam mit dem Prüfergebnis erneut zu signieren. Die Langzeitarchivierung ist jedoch nicht Gegenstand dieser Orientierungshilfe (siehe Ziff. 2.1).

Die von der Dokumentensignatur nicht erfassbaren Verarbeitungsschritte des Übermittels eines Dokuments und des Lesens eines Dokuments sind mittels einer manipulationssicheren Protokollierung einer Revision zugänglich zu machen. Das vollständige Löschen eines Dokuments muss aus Gründen der Dokumentationspflicht vom Zugriffskontrollmechanismus unterbunden werden, es sei denn, die Löschung ist aus Rechtsgründen erforderlich wie z.B. nach Ablauf der Aufbewahrungsfrist für nicht archivwürdige Unterlagen oder wenn ein Anspruch auf Löschung nach den Datenschutzgesetzen besteht.

Eine Protokollierung ist recht einfach und umfassend zu realisieren, wenn die Datenverarbeitung von nur einem System vorgenommen wird, welches damit auch die Kontrolle über alle Verarbeitungsphasen eines Dokuments hat und außerdem die einzelnen Verarbeitungsschritte den Personen zuordnen kann, die sie verursacht haben. Durchläuft ein Dokument im Zuge seiner Verarbeitung mehrere lokale Systeme, erfolgt auch die Protokollierung auf mehreren Systemen. Für die Revision der Gesamtheit aller Verarbeitungsschritte eines Dokuments ist das Zusammenführen der relevanten Protokolldaten aller Systeme erforderlich, die das Dokument durchlaufen hat.

- **Gewährleistung der Rechtssicherheit**

Die Voraussetzung für die Rechtssicherheit ist das qualifizierte elektronische Signieren eines Dokuments. Die qualifizierte Signatur gewährleistet eine rechtswirksame Überprüfbarkeit der Zuordnung einer Signatur zu der Person, die diese Signatur erzeugt hat. Die Rechtssicherheit erfordert aber auch, dass die Dokumente verkehrsfähig bleiben, also in Dateiformaten gespeichert werden, die die langfristige Lesbarkeit auch außerhalb der speichernden Stelle gewährleisten. In Fachkreisen gelten derzeit als solche Dateiformate ASCII (7bit), TIFF, PDF/A und XML.

- **Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen**

Die Nichtabstreitbarkeit des Sendens und Empfangs spielt primär eine Rolle in Architekturen mit dezentraler Ausrichtung, da aufgrund der Autonomie der lokalen Systeme eine Datenübermittlung explizit von einem Systemnutzer oder einer Systemnutzerin angestoßen werden muss und es keine systemübergreifenden Kontrollmechanismen gibt, die einen Übermittlungsvorgang technisch überwachen und im Fehlerfall entsprechende Maßnahmen einleiten. Nicht-Abstreitbarkeit ist nur über ein Quittungsverfahren unter Verwendung elektronischer Signaturen zu realisieren.

Die Signatur von Dokumenten zur Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen darf nicht verwechselt werden mit der Signatur von Dokumenten zur Gewährleistung der Authentizität. Im ersten Fall dient die Signatur der Zuordnung eines Dokuments zur sendenden Person, im zweiten Fall der Zuordnung eines Dokuments zu seiner Urheberin oder seinem Urheber. Da die sendende Person eines Dokuments aber nicht notwendigerweise auch die Urheberin oder der Urheber ist, muss jedes Dokument bei einer Übermittlung von der sendenden Person elektronisch signiert werden.

- **Zugriffskontrolle**

Bei dezentralen Systemen (s. Ziff. 3.1) sind Nutzungsrechte mittels des Zugriffskontrollmechanismus jeweils für die lokalen Systeme definierbar. Wird ein Dokument von einem lokalen System an ein anderes übermittelt, müssen die unter Umständen bestehenden Nutzungsrechte beziehungsweise Nutzungsausschlüsse mit dem Dokument übermittelt werden.

Die empfangende Person oder das empfangende System müssen dann für deren Einhaltung sorgen.

Bei zentralen Modellen (s. Ziff. 3.2) wirkt der Zugriffskontrollmechanismus systemweit. Bei der Erstellung des Berechtigungskonzepts und bei der Vergabe von Berechtigungen sind daher alle im System verfügbaren Funktionen und alle Nutzenden zu berücksichtigen.

7 Anforderungen an das Signieren in einem Dokumentenmanagementsystem

Eine zentrale Bedeutung beim Einsatz eines DMS kommt dem Signieren von Dokumenten zu, das für verschiedene Zwecke eingesetzt werden kann, nämlich als Maßnahme zur Sicherstellung der Authentizität, der Integrität, der Revisionsfähigkeit und Rechtssicherheit. Deshalb werden nachfolgend die verschiedenen Anforderungen an das Signieren erläutert. Das Umfeld der Public-Key-Infrastruktur, die sich in der öffentlichen Verwaltung im Aufbau befindet, ist zu berücksichtigen.

7.1 Public-Key-Infrastructure (PKI)

Bei elektronischen Dokumenten gibt es einige allgemeine Aspekte des sicheren und datenschutzgerechten Umgangs mit Signier- und Verschlüsselungsschlüsseln zu berücksichtigen. Diese Aspekte müssen von Organisationen im Rahmen einer ohnehin bestehenden PKI (Public-Key-Infrastructure) thematisiert und abgearbeitet werden. Ein wichtiger Aspekt ist die Aufklärung der Anwenderinnen und Anwender. Die Anwendenden eines Signaturschlüssels müssen verstehen, wie die Verfahren zur Erzeugung und Verteilung von Schlüsseln gestaltet sind, damit sie berechtigt in das Verfahren vertrauen können. Hierbei ist der heikelste Punkt anzusprechen, wie nämlich die *Certification Authority* (CA) bzw. das Trustcenter mit dem privaten Schlüssel (*private key*) der Anwenderinnen und Anwender, der zum Signieren geeignet ist und von dessen Verlässlichkeit die gesamte Rechtskonstruktion abhängt, umgeht. Erzeugen Nutzende ihr Schlüsselpaar nicht selbst, so müssen sie ferner eine Chance haben, sich von der technischen Infrastruktur (Gebäudesicherheit, Trägerschaft des Trustcenters, dem Personal, der Hardware, der Software, dem Netz), in der ihr privater Schlüssel erzeugt wird, ein Bild zu machen. Nicht zuletzt muss der private Schlüssel nach der Herstellung von Schlüsselpaaren für die Nutzenden vertrauenswürdig nachvollziehbar gelöscht werden. All diese Fragen müssen innerhalb eines PKI-Konzepts und einer organisationsinternen Signier- und Verschlüsselungs-Richtlinie (*Policy*) grundsätzlich gelöst werden und werden deshalb hier nicht tiefer gehend bearbeitet. Es wird demnach vorausgesetzt, dass nachfolgend Authentisierungs-, Signier- und Verschlüsselungsschlüssel und die zugehörigen Zertifikate vorhanden sind. Aus der Policy und der Risikoanalyse werden sich auch Anforderungen an die – in der Regel unterschiedlichen – PINs ergeben, mit denen die privaten Schlüssel freigeschaltet werden.

7.2 Spezifische Problemfelder des Dokumentmanagementsystems

In Bezug auf ein Dokument-Managementssystem sind zumindest vier spezifische Problemfelder anzusprechen, deren Probleme es zu lösen gilt:

- Dem Autor bzw. der Autorin muss Transparenz darüber verschafft werden, welcher Inhalt einer Datei bzw. eines Dokuments tatsächlich signiert wird (Prinzip: „What You See Is What You Sign“).
- Die Verwaltung getrennter Schlüssel, für die Authentisierung, für die Verschlüsselung sowie für das Signieren unter verschiedenen Kommunikationskontexten, muss gewährleistet sein.

- Die differenzierten „händischen“ Verwaltungs-Zeichnungen, die Art der Bewertung eines Dokuments betreffen, müssen in die Praxis elektronischen Authentisierens und Signierens übernommen werden, weil sie für die sie nutzenden Personen mit differenzierten rechtlichen Folgen verbunden sein können.
- Eine besondere Bedeutung kommt dem Signieren der Metadaten sowie den Protokolleinträgen zu.

Für diese vier, spezifisch elektronische Dokumente bzw. elektronische Akten betreffende Problemfelder sollen nachfolgend alltagstaugliche Lösungen vorgestellt werden.

Problemfeld 1: What You See Is What You Sign

Ein Dokument, das beispielsweise als Worddatei vorliegt, enthält unter Umständen sehr viel mehr Informationen, als auf dem Bildschirm angezeigt werden. Denn eine Datei entspricht nicht einem Blatt Papier, sondern enthält, sozusagen in die Tiefe des Papiers hinein, eine dritte, technisch operativ zugängliche Dimension. Es gilt somit sicherzustellen, dass das, was auf dem Bildschirm angezeigt wird – und was man als Bearbeiterin oder Bearbeiter zu signieren bereit ist – und das, was als Datei tatsächlich signiert wird, übereinstimmen.

Eine relativ wirksame Maßnahme zur Sicherstellung, dass Dateiinhalt und Bildschirmdarstellung übereinstimmen, besteht darin, beim Abspeichern das Dokumentformat zu wechseln und dabei sicherzustellen, dass möglichst nur die auf dem Bildschirm angezeigten „Rohdaten“ gespeichert werden. Optimal wäre in diesem Sinne als das zeichensparsamste Format „.txt“, das naturgemäß keine Struktur- oder Layoutangaben enthalten kann. Soll das Layout erhalten bleiben, und nur diese Variante ist praxisgerecht, böten sich das RTF- oder PDF-Format als Dateiformat an, bevor diese Datei dann signiert wird. Natürlich enthalten auch diese Formate unter Umständen mehr Informationen, als die Nutzenden tatsächlich kontrollieren können. Aber es ist immerhin sichergestellt, dass keine als gelöscht markierten Textreste, die ein modernes Textverarbeitungsprogramm verwaltet, enthalten sind.

Problemfeld 2: Differenzierung von Schlüsseln zum Verschlüsseln, zum Authentisieren und zum Signieren

Wichtige Einsatzmöglichkeiten für das Verschlüsseln, das Signieren und das Authentisieren sind folgende:

- Vertraulichkeit im Sinne des Schutzes der Daten vor unberechtigtem Zugriff wird technisch sichergestellt durch **Verschlüsseln**.
- Die Authentizität bzw. das Sichern der Autorenschaft im Sinne einer sicheren Identifikation der beteiligten Computer bzw. Personen wird sichergestellt durch **Authentisieren**.
- Die Nichtabstreitbarkeit bzw. die Verbindlichkeit, dass die Datei geöffnet wurde, wird je nach Inhalt der damit beabsichtigten Erklärung sichergestellt durch **Signieren bzw. Authentisieren**.
- Dass eine bestimmte Aktion stattgefunden hat, wird durch Protokollieren sichergestellt, wobei die Integrität des Protokolls wiederum sichergestellt wird durch **Signieren**.
- Auch die Wertung der Abgabe einer Willenserklärung im Sinne eines aktiv-selbstbestimmten Tuns geschieht durch **Signieren**.

Eine **Verschlüsselung** dient der Sicherstellung von Vertraulichkeit zwischen Sender und Empfänger. Sie muss deshalb, wenn irgend möglich, im Modus einer Ende-Zu-Ende-Verschlüsselung geschehen, weil jede Informationen verarbeitende Instanz dazwischen Zweifel an der Vertraulichkeit der Nachricht aufkommen lassen könnte. Hierbei stellt sich in Bezug auf Organisationen die Frage: Was bedeutet „Ende-zu-Ende-Verschlüsselung“, wenn Organisationen zugleich Vertretungs-, Kontroll- und Revisionsanforderungen zu erfüllen haben? Ende-zu-Ende-Verschlüsselung kann dann nicht bedeuten „Person-zu-Person“, sondern nur, dass die Organisation – oder zumindest die Unterorganisationen (Abteilungen) der Organisation - einen organisationsbezogenen privaten Schlüssel für Verschlüsselung nutzen darf, jedoch nicht die einzelnen Beschäftigten. Zwar kann man als Kompromissformel, die sowohl persönliche als auch organisatorische Verschlüsselung ermöglicht, auf so genannte Key-Recovery-Lösungen verfallen, die im Ergebnis jedoch nichts am Sachverhalt ändern, dass Vertraulichkeit technisch nur bis zur Organisationsgrenze gilt: Das Ende ist die Organisation.

Das **Signieren** von Dokumenten muss jedoch tatsächlich durch die einzelnen Beschäftigten zugeordnete personenbezogene Signatur geschehen (gem. § 2 Nr. 3 Signaturgesetz). Das Ende ist eine Person.

Aus diesen beiden unterschiedlichen Anforderungen beim Verschlüsseln und Signieren folgt, dass grundsätzlich verschiedene Schlüssel für das Verschlüsseln und das Signieren existieren müssen.

Aber es ist noch ein weiterer Aspekt einzuflechten: Ein Schlüssel, über den sich die Nutzenden authentisieren, ist zu unterscheiden von einem Schlüssel, mit dem signiert wird, um z.B. die Integrität oder die Autorschaft eines Textes zu bestätigen. Es bedarf deshalb verschiedener Schlüssel für verschiedene Situationen der Authentisierung und die mit Rechtsfolgen verbundene Signatur.

Fazit: Alle Nutzenden müssen über verschiedene Schlüssel verfügen, also mindestens

- einen organisationsbezogenen zum Ent- sowie
- natürlich zahlreiche Schlüssel zum Verschlüsseln und zur Signaturprüfung, sowie
- (mindestens) einen personenbezogenen privaten Schlüssel zum Signieren
- einen personenbezogenen Schlüssel zur Authentisierung

In der Alltagspraxis ist festzulegen, wie die Nutzenden diese verschiedenen Schlüssel praktisch sicher und ergonomisch verwalten sollen. Das muss im Rahmen des PKI-Konzepts bzw. einer Dienstanweisung der Organisation zum Authentisieren, Verschlüsseln und Signieren geschehen. Typischerweise wird dafür eine Chipkarte (oder ein USB-Stick mit Chip) benutzt. Der Chip enthält ein Zertifikat (unter anderem mit dem öffentlichen Schlüssel) und den jeweils zugehörigen privaten Schlüssel für die entsprechende Funktion, wobei mehrere Signatur- (z.B. qualifiziert und nicht qualifiziert) und Verschlüsselungszertifikate (z.B. persönliche und gruppenbezogene) möglich sind.

Problemfeld 3: Übertragung des differenzierten händischen Zeichnens der Verwaltung in die Signierpraxis

Eine händisch erfolgende Unterschrift erfüllt eine ganze Reihe an Funktionen. So erfüllt sie die Anforderung

- der Dauerhaftigkeit („dokumentenechte Farbe“),
- des Abschlusses („Unter-Schrift“ (Integrität)),
- der Identifikation / Authentifizierung der Autorinnen und Autoren (Nicht-Abstreitbarkeit),
- der Dokumentation der Echtheit („Original“),
- zu signalisieren, dass es sich um eine Willenserklärung handelt.

In der Verwaltung gibt es darüber hinaus gehende Formen des Anzeigens, dass eine Mitarbeiterin oder ein Mitarbeiter sich auf eine bestimmte Weise an der Kommunikation beteiligt hat:

- Paraphe (bedeutet: „ging über meinen Schreibtisch“)
- Z.K. („Zur Kenntnis genommen“ bedeutet: keine inhaltliche Bewertung)
- Mitzeichnen (bedeutet: „dem Inhalt der Aussage wird zugestimmt.“)

Hier zeigt sich das Problem, dass ein und dieselbe Signatur für ganz unterschiedliche Zwecke der Kommunikation mit unterschiedlichen Rechtsfolgen eingesetzt werden kann. Es ist zu fragen, ob zukünftig möglicherweise undifferenziert mit möglicherweise nur einer einzigen Signatur signiert wird ohne festzulegen, welche der oben aufgezählten Funktionen die Signatur eigentlich erfüllen soll. Damit können für die Nutzenden Rechtsfolgen entstehen, die als solche nicht absehbar sind und die mit der Einführung der Signatur auch gar nicht beabsichtigt waren. Dies ist dann misslich, wenn vielfach nicht einmal ein Schriftformerfordernis vorliegt. Es ist deshalb grundsätzlich zu klären, welche rechtlichen Konsequenzen eine möglicherweise zwangsläufig undifferenziert gegebene Signatur für die Ausstellenden haben kann. Als Lösung bietet sich an, explizit auszuweisen, wie die Signatur innerhalb der Organisationskommunikation interpretiert werden soll. Auf diese Weise lässt sich verhindern, dass bspw. eine Signatur, die faktisch nur die Integrität einer Grafik nach einem Scann-Vorgang bestätigen soll, als darüber hinausgehende inhaltliche Kenntnisnahme oder gar Zustimmung gewertet wird.

Signaturen sind funktional, rechtlich abgesichert und generell sparsam einzusetzen. Eine Signatur muss immer dann gesetzt werden, sobald ein Statuswechsel des Dokuments vollzogen wurde. Ein Statuswechsel kann bedeuten, dass das Dokument bspw. eine Abteilung verlässt, oder dass ein gewisser Zwischenschritt oder ein Abschluss der Entscheidungsfindung, etwa im Sinne der „Reinschrift“, stattgefunden hat. Hier muss die Organisation Regeln vorgeben, in welchem Stadium der Entscheidungsfindung und auf welche Weise beim Weiterreichen von Dokumenten welche Form der Signatur zu leisten ist.

Als unmittelbar pragmatisch umsetzbarer erster Schritt zur Einführung der Signatur ließe sich diese zunächst allein im Sinne einer Methode der Sicherung von Integrität und Authentizität einsetzen, wobei die Art der Kennzeichnung der Beteiligung an der Kommunikation, ob zur Kenntnis nehmend oder mitzeichnend, dem Text herausgehoben anzufügen ist.

Problemfeld 4: Signieren von Metadaten, Verfahrensdaten oder Protokolldateneinträgen

Eine Forderung (aus Datenschutzgründen, zur Dokumentation der Abläufe und zur Revisionsfähigkeit) ist, dass nachvollziehbar sein muss, welche Nutzenden wann welche Aktionen an dem Dokument oder Workflow oder im technischen System (Software, Hardware, Netzeinstellungen) ausgelöst haben. Auch hierfür kommt der Einsatz von Signaturen in Betracht.

In einem DMS fallen an:

- **Metadaten**, die formale und inhaltliche Eigenschaften des Dokuments bezeichnen,
- **Verfahrensdaten**, die Eigenschaften der Organisation bzw. des Workflows, in denen das Dokument und Personen eingebunden sind, bezeichnen sowie
- **Protokolldaten**, die systemtechnische Aktivitäten und Konfigurationsdaten enthalten.

Protokolldaten müssen unabhängig davon aufgezeichnet werden, ob der Auslöser sie ausdrücklich bestätigt. Ihre Protokollierung muss verlässlich sein, das heißt tatsächlich revisionsicher erfolgen. Hierfür bietet sich ein Signieren nicht an, sondern eine systemseitige revisionsfeste Protokollierungslösung.

Für die anderen Daten kommt eine Signatur als Bestätigung und Nachweis dafür in Betracht, dass diese Einträge korrekt sind und vom Autor, Projektleiter oder Systemadministrator selbst oder dessen Vorgesetzten erzeugt oder ausgelöst wurden. Wird dafür eine praxisgerechte Lö-

sung mit Bestätigung durch eine Signatur nicht eingesetzt, ist eine generelle revisionsfeste Protokollierungslösung umzusetzen, die eine zweckgebundene Kontrollmöglichkeit der Einträge einschließt.

8 Technische Maßnahmen gegen unbefugte Kenntnisnahme

8.1 Dokumentenkategorien nach Schutzbedarf

Bei dem Umgang mit elektronischen Dokumenten ist die Definition des notwendigen Schutzbedarfs der Informationen von grundlegender Bedeutung. Je höher der Schutzbedarf, umso größer wird der erforderliche Aufwand.

Bei der Umsetzung von Geschäftsprozessen auf der Basis einer elektronischen Akte im DMS liegen die Anforderung auf den Schwerpunkten der Zugriffsberechtigung in Verbindung mit den Sicherheitszielen Integrität, Authentizität, Revisionsfähigkeit.

Die Berechtigung und die Verfügbarkeit beim Zugriff auf Informationen werden vorab geprüft.

8.2 Rollenkonzept / Berechtigungskonzept / Zugriffe

Für die Steuerung und Einstufung der Programme und der Nutzenden ist ein nach Schutzzielen und Zuständigkeiten strukturiertes Rollenkonzept mit Berechtigungs- und Zugriffsregeln notwendig. Jede Anwenderin und jeder Anwender dürfen nur die Rechte erhalten, die sie für die Erfüllung ihrer dienstlichen Aufgaben benötigen. Insbesondere sind die Zugriffe von übergeordneten Dienststellen auf Dokumente einer Behörde auf das Nötigste zu beschränken.

Diese Zuweisung von Rechten und Sicherheitsprofilen ist bereits bei der Anmeldung erforderlich. Über diese Identifikation wird die Berechtigung und Zuweisung von Anwendungen, Speicherbereichen und Kommunikationsverbindungen vorbestimmt.

Eine weitere Profilverordnung erfolgt in der Ausführung der Anwendungen eines DMS. Je nach der Art der Profilverordnung (nochmalige Anmeldung und Berechtigungsabfrage, Single-Sign-On, Gruppenberechtigung) wird geregelt, welche Bearbeitungsfunktionen erlaubt sind.

Als nächste Stufe der Zugriffssicherung sind die Berechtigungen einzelner Datenbanken, Datensätze und Datenfelder zu bestimmen. Nach der Bewertung der Schutzbedürftigkeit eines Datensatzes richten sich die Maßnahmen, die für die Sicherheit erforderlich sind. Es ist festzulegen, welche Zugriffsart für welche Nutzende auf welche Datenfelder zulässig ist. Hierunter fallen beispielsweise Leseschutz, Schreibschutz oder die Beschränkung der Zugriffe nur auf die Metadaten verbunden mit einer strikten Beschränkung der Inhalte dieser Daten.

8.3 Verschlüsselung in DMS

Bei der Festlegung der Schutzbedürftigkeit von Daten und Betrachtung der Möglichkeiten, diese Anforderungen technisch zu erfüllen, sind die Maßnahmen der Verschlüsselung auf den unterschiedlichen Ebenen von grundlegender Bedeutung. Durch die Unkenntlichmachung von Daten kann der Missbrauch durch unberechtigte Dritte eingeschränkt werden.

Hierbei ist zu betrachten, in welchem Umfang, in welcher Funktion und mit welchem Ziel die Ver- und Entschlüsselung von Daten erfolgt.

Wir können im Zusammenhang mit dem DMS verschiedenen Bereiche zuordnen:

- Verschlüsselte Speicherung auf einem Datenträger oder einer Datenbank
- Verschlüsselte Datenfelder in einer Datenbank
- Verschlüsselte Übertragung der Daten auf dem Transportweg
- Eine Ende zu Ende Verschlüsselung zwischen Client-Anwendung und Speicherort
- Eine Ende zu Ende Verschlüsselung zwischen Anwender und Speicherort

Auf Basis solcher definierten Schutzmaßnahmen kann die Sicherheit der Daten und Dokumente gewährleistet werden. Doch damit entstehen aber auch wieder neue Probleme wie die Mehrfachbearbeitung, Weitergabe, Recherchemöglichkeit, Archivierung.

Es ist zu definieren, welche Daten schützenswert sind. Wie bei einer E-Mail kann hier zwischen den Inhaltsdaten und den Adressdaten oder Header-Informationen unterschieden werden.

9 Übernahme eingehender Post in das Dokumentenmanagementsystem

Dieser Abschnitt behandelt die datenschutzrechtlichen Themen, die mit der Übernahme eingehender Post in das DMS zusammenhängen. Um die datenschutzrechtlichen Abwägungen deutlich zu machen, sind hier exemplarisch die Abläufe, mögliche Schwachstellen und Maßnahmen dargestellt.

Dabei werden sowohl der Übergang elektronischer Dokumente – wie z.B. E-Mail, Fax oder auf Datenträger gespeicherte Dokumente – als auch die Überführung von Papierdokumenten in das DMS betrachtet. Die nachfolgende Tabelle gibt Auskunft, welche der unten beschriebenen Schritte bei welchen Dokumenten durchlaufen werden müssen.

Dokumenteneingang bzw. –zuführung

Schritte	Papierdokumente	Urkunden / Pläne	CI-Dokumente	NCI-Dokumente
Vorbereitung	X	X		
Imaging und Validierung	X			
OCR-Erkennung und Validierung	(X)			(X)
Metadateneingabe	X	X	X	X
Ausdruck für Papierakte			X	X
Verweis auf die Papierakte in elektronischer Akte	X	X		

Der Schritt Umwandlung der gescannten Dokumente in Textdokumente (OCR-Erkennung) ist nur erforderlich, wenn eine spätere Bearbeitung der Dokumente mit Textverarbeitungsprogrammen oder eine Volltextrecherche auf die Inhalte der Dokumente gewünscht wird. Ist das nicht der Fall, ist zur Vermeidung der damit verbundenen Datenschutzrisiken auf diesen Schritt zu verzichten.

9.1 Vorbereitung der in Papierform eingehenden Post

Die eingehende Papierpost wird geöffnet, sofern sie nicht erkennbar Privatpost oder VS-Sachen betrifft, und nach organisatorischen Vorgaben sortiert. Diese Vorgaben müssen Angaben ent-

halten, welche Post nicht „aktenwürdig“ ist, und ggf. für welche Posteingänge welche besonderen Vorgaben gelten. Z.B:

- Post, die nicht in das DMS übernommen wird
- Post, für deren Behandlung besondere Schutzmechanismen vorgesehen sind
- aus Rechtsgründen in Papierform aufzubewahrende Schriftstücke wie z.B. Verträge und Vertragsangebote. Hier muss die elektronische Akte Hinweise auf die Aufbewahrung des Papiers enthalten.

Dokumente oder deren Anlagen sind auszusondern, bei denen das Scannen aus technischen Gründen nicht möglich ist (z.B. weil sie zu großes Format haben, nicht in Einzelblätter trennbar sind wie Notarurkunden oder Bücher oder andere gegenständliche Beilagen der Post). Wenn Dokumente nicht gescannt werden können, sind in der elektronischen Akte Hinweise auf die Art und die Aufbewahrung erforderlich. Bei der scannbaren Post werden einzelne Dokumente getrennt (z.B. durch Trennblätter oder Barcode auf der ersten Seite des Schriftstücks). Schriftstücke und Anlagen werden zusammengefügt.

Datenschutzrechtliche **Schwachstellen** sind

1. Unvollständigkeit der Akte und datenschutzrechtliche Unrichtigkeit dadurch, dass
 - aktenwürdige Dokumente nicht in die Akte gelangen
 - Anlagen nicht dem betreffenden Dokument zugeordnet werden
 - Hinweise fehlen, dass aus rechtlichen Gründen Dokumente in der Papierakte vorzuhalten sind oder dass Anlagen aus technischen Gründen nicht gescannt werden können
2. Unberechtigte Kenntnisnahme:
 - Nicht oder außerhalb der zugänglichen Akten aufbewahrte Dokumente (VS-Sachen, private Post oder andere Dokumentenarten wie Personalsachen) gelangen in das DMS.
 - Dokumente für Empfänger in organisatorischen Bereichen, die aufgrund einer Organisationsanweisung außerhalb des DMS geführt werden, werden in das DMS übernommen.
 - durch Zusammenfassung sachlich nicht zusammengehörender Dokumente zu einem Dokument

Mögliche **Maßnahmen** sind:

Zu 1.:

- Überarbeitung der Anweisungen an die Poststellen
- besondere Verfahren für die Verbindung von Dokumenten mit Anlagen
- besondere Regelungen für die Hinweise auf Dokumente in der Papierakte
- Vorsortierung der Post im Hinblick auf nicht scannbare Teile
- Vorsortierung der Poststücke mit Anlagen
- besondere Stapel für Poststücke mit Anlagen
- besondere Behandlung der Anlagen bei Trennblättern oder Barcode
- Auswahl qualifizierten Personals für die Aufgabe und regelmäßige Schulung
- Nachkontrolle der nicht dem DMS zugeführten Dokumente (Sind Dokumente enthalten, die fälschlich nicht in das DMS eingebracht wurden?)
- Nachkontrolle der dem DMS zugeführten Dokumente (Zuordnung von Anlagen zu Dokumenten und Verweise auf Papierakte)

Zu 2.:

- Überarbeitung der Anweisungen an die Poststellen
- Auswahl qualifizierten Personal für die Aufgabe und regelmäßige Schulung
- Trennung der Dokumente (Trennblätter, Barcode etc. vor der Stapelbildung)
- Nachkontrolle der dem DMS zugeführten Dokumente

9.2 Scannen

Mit dem Scannen wird aus dem Papierdokument eine Grafikdatei erzeugt. Mögliche datenschutzrechtliche **Schwachstellen** sind:

1. Unberechtigte Kenntnisnahme durch Unbefugte beim Einscannen
2. Fehler beim Einscannen eines Dokuments, die die Vollständigkeit oder Lesbarkeit beeinträchtigen
3. Unbefugte Zugriffe auf den Speicherort der gescannten Dokumente
4. Unbefugte Veränderungen der Dokumente
5. Ausfall eines Scanners

Mögliche **Maßnahmen** sind:

Zu 1.:

- Räumliche Sicherungsmaßnahmen wie z.B. Aufstellung des Scanners in einem gegen Zutritt Unbefugter gesicherten Raum

Zu 2.:

- Visuelle Nachkontrolle der Images und ggf. Wiederholung des Scannvorgangs für unvollständige oder unleserliche Dokumente

Zu 3.:

- sichere Benutzerauthentisierung, ggf. kombiniert mit Single-Sign-On-Verfahren
- detailliertes Rollen- und Berechtigungskonzept
- Verschlüsselung der temporären Dateien auf dem Scan-Pc
- Verhinderung eines Zugriffs über Netzwerke. Single-Sign-On-Verfahren haben aber den Nachteil, dass die Nutzenden ständig auf alle Daten Zugriff haben, auch auf solche, deren Zugriff sie momentan nicht benötigen. Dies nutzen vermehrt „Trojaner“ aus.

Zu 4.:

- Unterbindung der Bearbeitungsmöglichkeiten von Tiff-Dateien am Scann-PC und an den Servern

Zu 5.:

- Redundante Auslegung der Scann-PCs

9.3 Behandlung der in elektronischer Form eingehenden Post

Elektronische Post kann entweder in der zentralen Poststelle eingehen oder – falls diese Möglichkeit eröffnet ist – in Postfächern der Beschäftigten. Sie kann Anlagen enthalten. Sie kann mit einer elektronischen Signatur versehen und/oder verschlüsselt sein. Sie kann selbst oder als Anhang Dokumente enthalten, die keine Textdateien sind (Fax, Image, Video). Die Übergabe der elektronischen Dokumente in das DMS erfordert weitere organisatorische Vorgaben. Dabei hat die Daten verarbeitende Stelle zu entscheiden, ob alle Dokumente ausschließlich von einer zentralen Stelle in das DMS eingespeist werden oder ob sie auch den Weg eröffnet, dass direkt bei den Mitarbeiterinnen und Mitarbeitern eingegangene elektronische Dokumente von diesen unmittelbar in das DMS überführt werden. Die Einheitlichkeit der Behandlung eingehender Post kann besser bei einer zentralen Stelle gewahrt werden; auch bei der Qualitätssicherung bringt eine solche Lösung Vorteile. Die Eröffnung des direkten Wegs zu den Bearbeitenden ist allerdings die schnellere Variante.

Für die Überleitung elektronischen Dokumente in die elektronische Aktenführung sind folgende **Schwachstellen** zu betrachten:

1. Unvollständigkeit der Akte und datenschutzrechtliche Unrichtigkeit, dadurch dass aktenwürdige Dokumente nicht in die Akte gelangen (wie bei 7.1)
2. Verschlüsselt eingehende Emails können nicht entschlüsselt werden
3. Besondere Probleme der signierten Dokumente wie: Signaturen nicht prüfbar, erfüllen nicht die Formvorschriften, Dokument verändert.
4. Irrtümliche Dokumentenänderung durch Befugte
5. Manipulative Dokumentenänderung

Mögliche **Maßnahmen** sind:

Zu 1.:

- Überarbeitung der Anweisungen an die Poststellen und ggf. der Dienstanweisung für Beschäftigte, die eigene elektronische Postfächer haben
- Schulung der Beschäftigten

Zu 2.:

- Konzept zum Umgang mit verschlüsselten Emails

Zu 3.:

- Anweisung für die Prüfung von Signaturen
- Regelung der Folgeschritte, die abhängig vom Ergebnis zu erfolgen haben

Zu 4.:

Wie zu 1.

Zu 5.:

Wie zu 1.

9.4 Umwandlung der Grafikdateien in Textdateien (OCR Erkennung)

Ist die Verarbeitung der gescannten Dokumente und sonstiger elektronischer Grafikdokumente in Textdokumente vorgesehen, so schließt sich an dieser Stelle die OCR-Erkennung an. Das nach der OCR-Erkennung entstandene Dokument wird mit Fehlererkennungsprogrammen nachbearbeitet. Die Qualität der Texterkennung hängt von der Vorlagenqualität (Original), der Qualität des Scanners, der Qualität der Wörterbücher und Musterdatenbank bei der OCR-Erkennung und der Qualität der Algorithmen zur Fehlererkennung ab. Datenschutzrechtlich ist wichtig, dass die Dokumenteninhalte bei der Umsetzung nicht verändert werden.

Datenschutzrechtliche **Schwachstellen** sind:

1. Die Verfälschung der Dokumente durch fehlerhafte Funktion der eingesetzten Programme
2. Die Unvollständigkeit der Dokumente, wenn Teile nicht übertragen werden
3. Unbefugte Zugriffe auf den Speicherort der gescannten Dokumente
4. Unbefugte Veränderungen der Dokumente durch das Personal
5. Unbefugte Veränderungen durch Externe

Mögliche **Maßnahmen** sind:

Zu 1.:

- Auswahl eines qualitativ sehr guten OCR-Erkennungsprogramms
- Einsatz verschiedener Erkennungsprogramme
- Qualitätssicherung beim Scannen, damit die Vorlagen optimale Qualität haben
- Qualitätsüberprüfung durch visuelle Nachkontrolle

Zu 2.:

wie bei 1

Zu 3.:

- sichere Benutzerauthentisierung, ggf. kombiniert mit Single-Sign-On-Verfahren
- detailliertes Rollen- und Berechtigungskonzept

Zu 4.:

- Authentizität der Informationen durch eine Benutzeranmeldung
- Funktionalitäten der Versionierung und
- das Speichern von lauffähigen Informationen aller akten- und vorgangsrelevanter Änderung

Zu 5.:

- Verhinderung des Zugriffs über Netze
- Trennung administrativer Zugang zur Datenbank von der Möglichkeit zur Bearbeitung von Daten, das heißt, auf Computern, die der Administration des Servers dienen, sollten keine Bearbeitungsprogramme verfügbar sein.

9.5 Metadateneingabe

Um elektronische Dokumente im DMS auffindbar zu machen, werden sie mit Metadaten versehen. Die Daten verarbeitende Stelle hat unter Beachtung der datenschutzrechtlichen Grundsätze der Erforderlichkeit und Datensparsamkeit die Inhalte der Metadaten, die regelmäßig in DMS als Freifelder vorgesehen sind, festzulegen.

DMS sehen als Pflichtfeld bei den Metadaten das Aktenzeichen vor. Alle weiteren Einträge müssen festgelegt werden. Regelmäßig werden der Absender und der Betreff, das Datum des Schreibens und ein Aktenzeichen des Absenders notiert. Notwendig ist auch die Festlegung einer Aufbewahrungsfrist, sofern sie nicht auf höherer Ebene (z.B. Aktenzeichen) vorgegeben ist oder wenn sie von dieser Vorgabe im Einzelfall abweichen muss. Die Aufbewahrungsfrist kann bei der erstmaligen Eingabe oder später durch die Bearbeitenden vergeben werden.

Die datenschutzrechtlich zulässigen Inhalte der Metadaten hängen sowohl mit dem Inhalt der Dokumente zusammen als auch mit der Ausprägung der Rechercherechte. Sind z.B. Beschäftigten über die ihrem Zuständigkeitsbereich originär zugeordneten Dokumente Möglichkeiten eröffnet, zur Aufgabenerfüllung Recherchen über Metadaten eines größeren Kreises von Dokumenten durchzuführen, so müssen die Inhalte der Metadaten besonders kritisch eingeschränkt werden. Die in den Metadaten enthaltenen Hinweise auf die Inhalte der Dokumente – insbesondere im Betreff – dürfen keine sensitiven personenbezogenen Daten (§ 3 Abs. 9 BDSG) beinhalten.

Schwachstellen entstehen

1. durch fehlende oder fehlerhafte Organisationsanweisungen für die Metadaten: Kenntnisnahme Unbefugter von Dokumenten- und Metadateninhalten
2. durch fehlerhafte Metadateneingaben:
Ein falsches Aktenzeichen eröffnet unberechtigten Zugriff auf nicht dem Zuständigkeitsbereich zugewiesene Dokumente.
Die Eingabe von sensitiven Daten im Betreff oder anderen Metadaten eröffnet eine unzulässige Kenntnisnahme dieser Daten, wenn Metadatenrecherchen über den engen Zuständigkeitskreis hinaus eröffnet sind.
3. unbefugte Zugriffe bei der Übertragung
4. ggf. falsche Eingabe der Aufbewahrungsfristen

Maßnahmen sind

Zu 1.:

- Klare und datenschutzrechtlich abgesicherte Organisationsanweisungen für alle mit der Eingabe von Metadaten befasste Beschäftigte
- ggf. Konzentration der Überführung in das DMS in einer zentralen Stelle

Zu 2.:

- Sorgfältige Auswahl des zentral mit der Metadateneingabe betrauten Personals und Schulung bei Einspeisung von Dokumenten auch durch Bearbeitende und Metadateneingabe durch diese Schulung der Bearbeitenden
- Überprüfung der zentralen Metadateneingabe (4-Augen-Prinzip)
- Anweisungen für die Behandlung von falsch zugeordneten Dokumenten

Zu 3.:

- Verschlüsselte Übertragung

Zu 4.:

- Vorgabe eines kurzen Standardwertes
- Vergabe der Aufbewahrungsfrist auf Aktenzeichenebene

10 Workflow-Management

Einen wesentlichen Nutzen des Einsatzes von DMS erwartet man von der Funktion des so genannten Workflow, der elektronischen Weiterbearbeitung bis zum Abschluss der Vorgänge in der Verwaltung.

Workflow ist ein Prozess bzw. ein Vorgang, der sich aus einzelnen Aktivitäten zusammensetzt. Dabei hat jeder Workflow einen definierten Anfang, einen organisierten Ablauf und ein vorbestimmtes Ende. Ein Workflow-Management ist die technische Umsetzung dieser Arbeitsabläufe bzw. der Vorgangsbearbeitung. Verbunden mit einem DMS ermöglicht das Workflow-Management die vollständige Bearbeitung eines Vorgangs in einem elektronischen Medium vom Anfang bis zum Ende, d.h. bis zur Aussonderung zur Archivierung. Die gesamte Vorgangsbearbeitung wird so elektronisch gesteuert.

Bei Einsatz eines solchen Workflow-Management-Systems gibt es einige spezielle Aspekte, die die Daten verarbeitende Stelle besonderes berücksichtigen muss. Hierzu gehört insbesondere die Abbildung und Sicherstellung des Bearbeitungsweges sowie die Behandlung der Leistungs- und Verhaltenskontrolle. Durch die systemgesteuerte Vorgangsbearbeitung werden die Laufwege dokumentiert, und es entstehen Protokolldaten, die eine Auswertung des Nutzerverhaltens ermöglichen.

10.1 Festlegung der Arbeitsabläufe

Mit der Einführung eines Workflow-Managements werden Prozessabläufe (Arbeitsabläufe) innerhalb einer Organisation - ggf. auch organisationsübergreifend - standardisiert. Dies setzt voraus, dass die Arbeitsabläufe im Vorfeld der Einführung des Systems analysiert und festgelegt werden. Erforderlich ist daher eine Ist-Aufnahme der Workflows zur Festlegung der u. U. für die durchgängig elektronische Bearbeitung modifizierten Arbeitsabläufe. Erst durch diese Festlegung kann auch die datenschutzrechtlich erforderliche Sicherstellung des Bearbeitungsweges gewährleistet werden. Wird die gesamte Bearbeitung elektronisch mittels eines Workflow-Managements gesteuert, sind vor Implementierung eines solchen Systems die Arbeitsabläufe abzubilden (siehe auch unter 4.2 und 8.2).

10.2 Sicherstellung des Bearbeitungsweges

Die zuvor behördlich festgelegten Bearbeitungsverläufe sind im Dokumentenmanagementsystem abzubilden und nachvollziehbar festzuhalten. Es muss nachvollziehbar sein, wer welche personenbezogenen Daten verändert hat. Die Tatsache, dass jemand grundsätzlich befugt ist, auf bestimmte Datenbestände zuzugreifen, Daten hinzuzufügen, sie zu ändern, zu löschen oder sie zu übermitteln, bedeutet nicht, dass derartige Aktivitäten im Einzelfall auch tatsächlich erforderlich und damit zulässig sind. Es muss daher zweifelsfrei festgestellt werden können, wer für die einzelne Datenverarbeitung verantwortlich ist (vgl. u.a. Nr. 5 der Anlage zu § 9 Satz 1 BDSG, § 5 Abs. 1 Nr. 3 LDSG SH). Bei jedem einzelnen Bearbeitungsschritt bzw. bei Änderungen von personenbezogenen Daten ist die Urheberschaft zweifelsfrei auszuweisen. Hier müssen die gleichen Anforderungen an die Nachvollziehbarkeit der Datenverarbeitung gestellt werden, die bei Bearbeitung einer papierernen Akte zu beachten sind.

Zu diesem Zweck sind die Datenverarbeitungen zu protokollieren. Eine zweifelsfreie Zuordnung zu einer Urheberin oder einem Urheber ist auch durch Versionierung möglich. Es ist sicherzustellen, dass während der gesamten Speicherdauer der Daten Verfahren bzw. Geräte zur Verfügung stehen, die diese abgelegten Informationen lesbar machen.

Den Personen, die ein Dokument erhalten, muss dabei mitgeteilt werden, zu welchem Zweck dies geschieht (zur Bearbeitung, zur Kenntnis etc.). Dies bedeutet, dass die vollständige Abbildung der in der jeweiligen Behörde verwandten Verfügungen erforderlich ist. Diese müssen als Annex jedem Dokument zugeordnet werden können. Eine nachträgliche Änderung muss dabei ausgeschlossen werden.

Weiter ist sicherzustellen, dass erkennbar ist, wann ein Dokument das Stadium des Vorentwurfs verlässt und damit nach den Grundsätzen des Verwaltungsrechts zur Akte zu nehmen ist. Dies hat auch Bedeutung für Ansprüche nach den Informationsfreiheitsgesetzen, denn ein Antrag auf Informationszugang kann abgelehnt werden für Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen und alsbald vernichtet werden (vgl. § 10 Abs. 3 IFG-SH, § 7 Abs. 2c) IFG NRW).

10.3 Verhaltens- und Leistungskontrolle

Die Dokumentation der Laufwege der behördlichen Vorgänge bzw. die Protokollierung der Datenverarbeitungsvorgänge führen zu einer Ansammlung von auswertbaren Daten über die Personen, die die Anwendung nutzen. Aus diesen Daten lassen sich Nutzerprofile ableiten oder Listen über Auffälligkeiten erstellen. Das Datenschutzrecht lässt derartige Auswertungen nur unter bestimmten Bedingungen zu (s. auch Ziff. 2.5 und 5.5.2 Verfahrens- und Protokolldaten). Die Betroffenen sind vor unzulässigen Überwachungsmaßnahmen (Verhaltens-/Leistungskontrollen) zu schützen.

10.4 Weitere spezifische Problemfelder

Wird ein Workflow-Management verbunden mit einem DMS eingerichtet, ist das gleiche Maß an Integrität, Authentizität, Vertraulichkeit, Verfügbarkeit und Revisionssicherheit zu erreichen, das in den vorherigen Kapiteln dargestellt wurde. Werden in einem DMS nicht nur Dokumente vorgehalten, sondern wird es zur Vorgangsteuerung genutzt, so ist dies im Rahmen der zu erstellenden Risikoanalyse zu beachten und bei den Sicherheitszielen und den erforderlichen Sicherheitsmaßnahmen zu berücksichtigen. So ist zum Beispiel in jeder Phase des Workflows sicherzustellen, dass nur befugte Personen Kenntnis von den Daten nehmen können. Eine nachträgliche Änderung der Dokumentation der Lauf- / Verfügungswege muss ausgeschlossen werden.

Bei der Einrichtung eines Workflow-Managements ist die Notwendigkeit der Erstellung von Signaturen zu berücksichtigen. Es muss sichergestellt werden, dass das Weiterreichen von Dokumenten im Workflow revisionssicher nachvollziehbar ist (vgl. Ziff. 6 Gewährleistung der Authen-

tizität und Revisionsfähigkeit). Wird ein über die Daten verarbeitende Stelle hinausgreifender Workflow eingerichtet, ist ein besonderes Augenmerk auf die Schnittstellen zu legen. Die Transfersicherheit bei der Kommunikation nach außen muss durch geeignete Verschlüsselung gewährleistet werden. Es muss geprüft und festgelegt werden, welche Metadaten der Person, die das Dokument empfängt, zur Verfügung gestellt werden. Es dürfen nur die Metadaten weitergegeben werden, die sie zur Erfüllung ihrer Aufgaben benötigt.

11 Recherche

Bei der Akten- und Vorgangsbearbeitung mit einem DMS wird es – wie auch bei der klassischen Aktenbearbeitung – zur Aufgabenerfüllung oft erforderlich sein, nach Dokumenten und Vorgängen zu suchen. Ein DMS bietet gegenüber der Papierakte den Vorteil, dass verschiedene Möglichkeiten der Suche in einem System vereint sind und nicht nur nach Aktenzeichen oder einem Eintrag in einem Briefftagebuch und den dort notierten Kennzeichen des Dokuments, sondern zielgenau und effektiv gesucht werden kann.

Bei der Recherche in Dokumentenmanagementsystemen unterscheidet man generell drei Recherchearten:

- **Recherche in Metadaten**

Diese Rechercheart ermöglicht eine Suche in den einzelnen Feldern der Metadaten. Dieses könnte z.B. eine Suche nach Dokumenten in einem bestimmten Erstellungszeitraum sein (1.8.2005 bis 31.8.2005). Eine Kombination der Suche in verschiedenen Feldern ist möglich.

- **Volltextrecherche in Metadaten**

Diese Rechercheart ermöglicht eine Volltextsuche nach beliebigen Wörtern in den Feldern der Metadaten. Dieses könnte z.B. eine Suche nach Vorgängen sein, die in einem beliebigen Feld der Metadaten das Wort Videoüberwachung beinhalten. Eine Kombination der Suche nach mehreren Wörtern ist möglich.

- **Volltextrecherche in Dokumenten**

Diese Rechercheart ermöglicht eine Volltextsuche nach beliebigen Wörtern in den Dokumentinhalten. Dieses könnte z.B. eine Suche nach Dokumenten sein, in denen das Wort Straßenbenutzungsgebühren vorkommt. Eine Kombination der Suche nach mehreren Wörtern ist möglich.

Bei den modernen Dokumentenmanagementsystemen lassen sich die aufgeführten Recherchearten auch untereinander beliebig kombinieren, wobei auch verschiedene Verknüpfungsarten wie z.B. UND, ODER, NICHT, verwendet werden können.

11.1 Datenschutzrisiken

Der wesentliche datenschutzrechtliche Aspekt der Recherche betrifft die vollständige Beachtung der vorhandenen Zugriffsrechte. Die Zweckbindung der Datenverarbeitung erfordert neben der exklusiven Zuweisung von Zugriffsrechten z.B. auch eine Einschränkung der Suchfunktion. Die Gefahr liegt unter anderem in der Möglichkeit der Verknüpfung der oben dargestellten Such- und Auswertungsmöglichkeiten, wobei dieses auch automatisiert erfolgen kann. Ein Zugriff auf Meta- oder Inhaltsdaten, für die keine Zugriffsberechtigung existiert, ist deshalb technisch auszuschließen.

11.2 Problemlösung

Erforderlich ist eine präzise Beschreibung der Suchfunktion und der Maßnahmen, die sicherstellen, dass über die Suchfunktion nicht die datenschutzrechtlichen Grundsätze der Zweckbindung und der Erforderlichkeit sowie der gebotene Vertraulichkeitsschutz umgangen werden können. Das Suchergebnis darf sich nur auf diejenigen Dokumente und Metadaten beziehen, zu denen auch eine Zugriffsberechtigung besteht. Ein Suchergebnis darf nicht als Treffer angezeigt werden, wenn keine Zugriffsberechtigung besteht. Eine leere Trefferliste muss demnach nicht bedeuten, dass es keine Ergebnis zur Suchanfrage gab, sondern eben vielmehr, dass es keinen Treffer in der Zugriffsberechtigung der abfragenden Person gibt. Es kann auch erforderlich sein, den Zugriff nur auf die Metadaten zu erlauben, auf die dazugehörigen Dokumenteninhalte jedoch nicht. Es kann ggf. auch erforderlich sein, den Zugriff nur auf eine begrenzte Zahl von Feldern der Metadaten zuzulassen.

11.3 Fazit

Die Ergebnisse von Recherchen in Dokumentenmanagementsystemen müssen die Zugriffsrechte abbilden. Entscheidend ist die Definition und Vergabe von Zugriffsberechtigungen (s. Kapitel 8.2). Es muss festgelegt werden welche Nutzenden, Benutzergruppen und Rollen welche Zugriffsberechtigungen (z.B. Lesen von Metadaten, Schreiben von Dokumentinhalten) auf welche Objekte besitzen.

Glossar

Akte	geordnete Zusammenstellung von Dokumenten mit eigenem Aktenzeichen und eigener Inhaltsbezeichnung
Aktenzeichen	Ordnungskennzeichen der Akte (numerisch oder alphanumerisch)
Archivierung	langfristige, revisionssichere Aufbewahrung von Dokumenten und Akten
Authentizität	Unter dem Begriff Authentizität versteht man die Eigenschaft, die gewährleistet, dass der Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein bzw. dass die vorliegenden Informationen von der angegebenen Quelle erstellt wurden.
Benutzergruppe	Mehrzahl von Nutzenden, denen im Gruppenkontext gleiche Zugriffsrechte auf Dateien, Dokumente und Ressourcen zugeordnet sind. Üblicherweise ist die Benutzergruppe verbunden mit der Zuordnung einer bestimmten Rolle.
Benutzerprofil	Die zu einer Benutzerkennung gehörenden Einstellungen und Einträge in einem IT-System. Dazu gehören beispielsweise zugeordnete Laufwerke, E-Mail-Ordner oder persönliche Verzeichnisse.
Benutzerrolle	siehe Rolle
CI	(Coded Information) kodierte und damit in der Regel maschinell einfach weiterzuverarbeitende Information
Data Mining	Unter Data Mining versteht man das systematische (in der Regel automatisierte oder halbautomatisierte) Entdecken und Extrahieren unbekannter Informationen aus großen Mengen von Daten.
Dokument	ein Informationsobjekt beliebiger Erstellungsform oder Dateiformats. Es kann sich sowohl um elektronische, papiergebundene oder Informationsobjekte auf anderen Trägern handeln. Unter den Begriff fallen Schriftstücke herkömmlicher Art, Grafiken und Zeichnungen (z.B. Baupläne, Konstruktionspläne), aber auch elektronische Informationsobjekte wie E-Mails, Telefax, Multimedia-Objekte (z.B. Power-Point Präsentationen, Videoclips) und verschiedenste Arten von Dateien (z.B. Word und Excel, Bilddateien).
Dokumenten-Management-System	(DMS), Oberbegriff für informationstechnische Systeme zur Verwaltung von Dokumenten von der Erfassung bis zur Archivierung
Elektronische Akte	Zukünftige rechtsverbindliche Akte, die vollständig elektronisch geführt wird
Hybride Aktenführung	Sowohl ein papierbasiertes wie ein elektronisches Vorgangsbearbeitungssystem wird genutzt; keine der beiden Ablageformen erfasst aber sämtliche Dokumente.
Image	hier: Bezeichnung für ein aus einzelnen Bildpunkten zusammengesetztes elektronisches Abbild eines Papierdokuments. Der Begriff wird landläufig für gescannte Dokumente benutzt.

Integrität	Unversehrtheit von Informationen und Daten. Bei der elektronischen Kommunikation heißt dies, dass die Daten bei der Übertragung nicht verändert worden sind.
Link	elektronischer Verweis auf eine bestimmte Internetseite oder ein Dokument innerhalb des Dokumentenverwaltungssystems.
Medienbruch	eine Stelle in einem (Geschäfts-)Prozess, an der Daten von einem Speichermedium auf ein anderes übertragen werden, also z.B. von Papier in digitale Form oder umgekehrt
Metadaten	Informationen, die andere Informationen (z.B. ein Dokument) beschreiben. Es kann sich z.B. handeln um Eingangsdatum, Einsender, Ersteller, Aktenzeichen, Betreff, Ausgangsdatum, Dokumenttyp. Welche Informationen als Metadaten ein Dokument beschreiben sollen, muss für ein Dokumentenmanagementsystem festgelegt werden.
Mobile Government	Die Mitarbeiterinnen und Mitarbeiter der Verwaltung arbeiten direkt bei den Bürgerinnen und Bürgern und nutzen dort vor Ort Daten der Verwaltung.
NCI	(Non Coded Information) Nicht kodierte Informationen sind Bilder, Sprache, Ton, Video etc. Sie sind vom Rechner nicht unmittelbar und eindeutig interpretierbar.
OCR	Optical character recognition: Erkennung von Zeichen und Texten aus digitalen Abbildungen analoger Vorlagen, um diese in elektronische Textdokumente umzuwandeln. Vorlagen sind meist Papierdokumente, die eingescannt wurden.
PKI	public key Infrastructure: Sicherheitsstruktur, die es ermöglicht, in nicht gesicherten Netzen (z.B. Internet) auf der Basis eines von einer vertrauenswürdigen Stelle ausgegebenen Schlüsselpaares (asymmetrische Verschlüsselung) verschlüsselt Daten auszutauschen bzw. Signaturen zu erzeugen oder zu prüfen.
Rolle	Zusammenfassende Bezeichnung für Funktionen, die für eine bestimmte Aufgabe ausgeführt werden müssen. Mit einer Rolle sind Zugriffsrechte verbunden. Benutzerrollen werden verwendet, um die Rechte nicht für jeden Nutzenden einzeln festlegen zu müssen, was die Rechteverwaltung erleichtert, weil bei Änderungen nur die Rechte der Rolle, nicht aber die Rechtezuweisung für einzelne Nutzende geändert werden müssen. Eine Person kann mehrere Rollen haben.
Scannen	digitale Erfassung von Papierdokumenten, die so zu elektronischen Images werden
Schutzbedarf	Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.
Signatur, elektronische	nach § 2 Signaturgesetz „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. Die fortgeschrittene elektronische Signatur ermöglicht nach § 2 Ziff. 2 Signaturgesetz eine verlässliche Identifizierung.

fizierung des Unterzeichners und soll die Integrität der signierten Daten wirksam schützen. Die qualifizierte Signatur ist eine fortgeschrittene elektronische Signatur, die auf einem von einem angezeigten oder akkreditierten Zertifizierungsdiensteanbieter erstellten qualifizierten Zertifikat beruht und mit besonders sicheren Produkten (Signaturerstellungseinheiten) erzeugt wird. Qualifizierte Signaturen ersetzen die gesetzliche Schriftform im Privatrecht und weitgehend auch im öffentlichen Recht; sie sind ein Äquivalent zur eigenhändigen Unterschrift.

Virtuelle Poststelle	Als virtuelle Poststelle wird das Abbild einer Poststelle in einem Unternehmen oder Behörde bezeichnet. Die Poststelle nimmt elektronische Dokumente entgegen, prüft und protokolliert die Integrität und Authentizität der elektronisch empfangenen Dokumente und leitet sie an die zuständige Stelle weiter. Gegebenenfalls werden verschlüsselt eingehende Dokumente entschlüsselt.
Volltextrecherche	Elektronischer Suchvorgang über Textdokumente, bei dem der Suchvorgang über den gesamten Text des Dokumentes läuft, d.h. der Suchbegriff eine im Text vorkommende beliebige Zeichenfolge sein kann
Vorgang	Zusammenfassung aller inhaltlich zusammengehörigen Dokumente zu einem bestimmten Geschäftsvorfall innerhalb einer Akte
Wissensdatenbank	Eine Wissensdatenbank ist eine spezielle Datenbank für das Wissensmanagement. Sie stellt die Grundlage für die Sammlung von Informationen dar. Für gewöhnlich besteht eine Wissensdatenbank aus expliziten Informationen einer Organisation, die Problemlösungen, Artikel, White Papers und Benutzerhandbücher enthält.
Wissensmanagement	bezeichnet eine Richtung der Managementlehre, die darauf abzielt, in Organisationen das Wissen einzusetzen und zu entwickeln, um die Unternehmensziele bestmöglich zu erreichen.
Workflow	(engl.: ursprünglich Arbeitsfluss) auf dem Computer ausführbare Beschreibung eines Geschäftsprozesses, oft auch als Vorgangsbearbeitung bezeichnet
Workflow-Management-System	Computergestützte Automatisierung von Geschäftsprozessen oder Vorgängen, die zur Definition, Verwaltung und Ausführung von (Standard-)Arbeitsabläufen, sog. Geschäftsprozessen, dient.
Zertifikat	Elektronische Bescheinigung, mit der öffentliche Schlüssel einer Person zugeordnet werden

Checkliste Dokumentenmanagement-System

Diese Checkliste berücksichtigt die wesentlichen Schritte, die vor Einführung eines DMS erfolgen müssen. Dabei sind Vorarbeiten zu leisten, Festlegungen zu treffen und das Organisations- und das Sicherheitskonzept zu erstellen. Funktionsträgerinnen und Funktionsträger sind im erforderlichen Umfang zu beteiligen. Sofern eine Risikoabschätzung im Rahmen einer **Vorabkontrolle** nach dem jeweiligen Datenschutzgesetz vorgeschrieben ist, sind die Festlegungen und Prüfungen Basis für die Einschätzung, ob die mit der automatisierten Verarbeitung verbundenen besonderen Risiken für die Rechte und Freiheiten der Betroffenen wirksam beherrscht werden können (z.B. nach § 4d Abs. 5 und 6 BDSG).

Zur Durchführung der Selbstkontrolle Ihres DMS sollten Sie zunächst folgende Informationen und Unterlagen zusammentragen und auswerten:

Informationen und Unterlagen	Bemerkungen
Bestandsaufnahme aller Systeme PC/Client/Notebook, Server, Scanner, Drucker, Anwender-Software	
Netztopologie Verbindungen der Rechner untereinander, Zugangspunkte zu fremden Netzen und Systemen	
Dokumentation über die DMS-Software Funktionseinstellungen, Rechte je Nutzerin und Nutzer, Authentisierung, Referenzen	
Dokumentation über die Administrierung Gliederung, Funktionskennzeichnung, Schutz vor Fehlbedienung, Art und Umfang der Inanspruchnahme	
Dokumentation der Verantwortlichkeiten Systemverwaltung, Netzadministration, Anwendung	
Art und Umfang der Wartungsverträge (ggf. beifügen)	

Zur Beantwortung der Checklisten-Fragen wird es in der Regel ausreichen, bei Varianten das Zutreffende anzukreuzen und ggf. durch Bemerkungen zu ergänzen. Auf diese Weise können Sie selbst kontrollieren, ob Sie alle zu treffenden Maßnahmen durchgeführt haben. Die in der Checkliste genannten Ziffern beziehen sich auf die Ziffern der Orientierungshilfe, die jeweils nähere Erläuterungen enthalten.

Bei den mit * gekennzeichneten Feldern sind besondere Aktionen erforderlich; hier reicht es nicht, die Felder auszufüllen, sondern es sind ggf. sogar über die in der Orientierungshilfe gegebenen Hinweise hinausgehende Überlegungen anzustellen und besondere Maßnahmen erforderlich.

1	Allgemeine Vorarbeiten und Festlegungen (im Klammerzusatz finden Sie einen Verweis auf das jeweilige Kapitel der Orientierungshilfe)			
Aktenverwaltung und Dokumentation	<input type="checkbox"/>			
Workflow	<input type="checkbox"/>			
Mailing	<input type="checkbox"/>			
Wissensmanagement *	<input type="checkbox"/>			
Informationszugang *	<input type="checkbox"/>			
Sonstiges (bitte benennen) *	<input type="checkbox"/>			
	Erfüllt			
	Nicht erfüllt			
	Trifft nicht zu			
	Bemerkungstext			
Ist-Analyse der Aufbau- und Ablauforganisation erstellen (4.2, 5.5.2 Analyse der Aufgaben und Arbeitsabläufe).				
Das Projektteam und die beteiligten Stellen festlegen (4.1).				
Die Beteiligung der Personalvertretung sicherstellen (4.1, 4.7).				
Die Beteiligung der oder des behördlichen Datenschutzbeauftragten sicherstellen (4.1, 4.7)				
Die Beteiligung der oder des IT-Sicherheitsbeauftragten sicherstellen (4.1)				

2	Analyse der Dokumente (2.3, 2.6, 4.5, 5.1)	Zutreffendes ankreuzen	
Schutzbedarfsfestellung	<ul style="list-style-type: none"> • Niedrig bis mittel • Hoch * • Sehr hoch * 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Bildung von Dokumentenkategorien für die Übernahme in das DMS nach	<ul style="list-style-type: none"> • Bewiswert und Formerfordernis • Erforderlichkeit • Eignung für die Übernahme in DMS (4.3, 5.2, 5.3, 5.5.2 Kreis der Dokumente, Schutzbedarf)	Zutreffendes ankreuzen <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Aktionen Bes. Vorkehrungen treffen Nicht in DMS Nicht in DMS, aber Verknüpfung herstellen

3	Organisationskonzept (4.5) (Sollkonzept der Auf- und Ablauforganisation einschl. des erforderlichen Regelwerkes)	Erfüllt		
			Nicht erfüllt	
				Trifft nicht zu
				Bemerkungstext
Entscheidung zu Art, Umfang und Implementierung einer virtuellen Poststelle (4.3)				
Art, Umfang und Einsatz eines sicheren Authentifizierungsverfahrens festlegen (8.2, 9.2, 9.4)				
Entscheidung, ob nur zentrale oder auch dezentrale Postfächer genutzt werden (4.3, 9.3)				
Entscheidung, ob nur zentrale oder auch dezentrale Eingabe in das DMS erfolgt (4.3, 9.3)				
Entscheidung, ob nur zentrale oder auch dezentrale kryptografische Behandlung der ausgehenden Post erfolgt (4.3, 9.3)				
bestehende Zuständigkeiten und Abläufe auf Zweckmäßigkeit überprüfen und ggf. anpassen (4.2)				
neue, durch die Nutzung des DMS verursachte Abläufe, z.B. Scannen, Eingabe der Metadaten, festlegen (5.5.2 Analyse der Aufgaben und Arbeitsabläufe)				
Arbeitsabläufe für Workflowmanagement standardisieren und festlegen (10.1)				
Verantwortungsbereiche und Befugnisse der Anwender festlegen (4.7, 5.5.2 Analyse der Aufgaben und Arbeitsabläufe)				
Organisatorische Regelungen für die Einspeisung von Dokumenten in das DMS erstellen (5.5.2 Kreis und Schutzbedarf der einbezogenen Dokumente, Medienbrüche, 9.1, 9.3, 9.5)				
Inhalte der Metadaten festlegen und ggf. einschränken (9.5)				
Regeln erstellen für die Hybridakte (2.4) zur Verbindung von zu Beweis Zwecken aufzubewahrenden oder aus anderen Gründen nicht in die elektronische Form zu überführenden Papierdokumenten mit der elektronischen Akte (5.3, 5.4, 5.5.2 Medienbrüche, Verbindung zur Rest-Papierakte)				
die Aufnahme von Aufbewahrungsfristen und die Aussonderung nach deren Ablauf regeln (5.5.2 Aufbewahrungsfristen)				

3	Organisationskonzept (4.5) (Sollkonzept der Auf- und Ablauforganisation einschl. des erforderlichen Regelwerkes)	Erfüllt		
		Nicht erfüllt		
		Trifft nicht zu		Bemerkungstext
die Übergabe archivwürdiger Dokumente an öffentliche Archive nach dem Archivgesetz regeln (5.5.2 Aufbewahrungsfristen)				
den Umgang mit signierten elektronischen Dokumenten, denen Beweisfunktion zukommt (rechtzeitige Nachsignierung, Notwendigkeit und Ansiedlung einer Signaturprüfungsstelle), regeln (4.3 und 5.2)				
an Schutzbedarf, Beweiswert und Formerfordernis der Dokumente orientierte Entscheidung über den Einsatz von Authentisierungs-, Signatur- und Verschlüsselungsverfahren treffen und organisatorische Regelungen dazu erlassen (4.3, 5.5.2, 7.2, 8.3, 9.3)				
Schulungskonzept erstellen (4.7, 9)				
insbesondere beim Workflow entscheiden, wo Protokollierung oder Versionierung eingesetzt wird				
klären, welche Bearbeitungs- und Protokolldaten der Beschäftigten vom System geführt werden, und Form der Unterrichtung der Beschäftigten bestimmen				
Schnittstellen zu Fachverfahren, für die Aussonderung (5.5.2 Aufbewahrungsfristen) und beim Workflow einrichten und beschreiben (11.4)				
Dienstanweisung/-vereinbarung zur Verarbeitung, Auswertung und Aufbewahrung von Protokolldaten von Beschäftigten ausarbeiten und in Kraft setzen (4.8, 5.5.2 Zugriff auf Verfahrens- und Protokolldaten von Beschäftigten, 10.3)				
bei Auftragsdatenverarbeitung schriftlichen Vertrag unter Beachtung der Rechtsvorschriften der Datenschutzgesetze schließen (5.5.2 Auftragsdatenverarbeitung)				

4	Sicherheitskonzept erstellen	Erfüllt		
		Nicht erfüllt		
		Trifft nicht zu		
				Bemerkungstext
Datenhaltungskonzept festlegen 3, 5.5.2 Datenhaltungskonzept, 6 Sicherstellung der Verfügbarkeit)				
Verantwortliche Stelle für den Einsatz des DMS festlegen (5.5.2 Verantwortliche Stelle)				
Rollen- und Berechtigungskonzept ausprägen (4.6, 5.5.2 Analyse der Aufgaben und Arbeitsabläufe, 8.2)				
Dateiformate für die Speicherung von Dokumenten im DMS bestimmen (6 Gewährleistung der Rechtssicherheit)				
Maßnahmen bestimmen, die zur Löschung unzulässig gespeicherter, nicht mehr benötigter und nicht archivwürdiger Dokumente vorgesehen sind (5.5.2 Löschung unzulässig gespeicherter sowie nicht mehr benötigter und nicht archivwürdiger Dokumente)				
Maßnahmen beschreiben, die zur Sicherstellung der Verfügbarkeit, Vollständigkeit, Integrität, Vertraulichkeit, Unverfälschbarkeit, Revisionsfähigkeit und Verkehrsfähigkeit der Dokumente auch für lange Zeiträume vorgesehen sind (5.5.2 Sicherstellung von Verfügbarkeit, Vollständigkeit, Integrität, Vertraulichkeit, Unverfälschbarkeit, Revisionsfähigkeit und Verkehrsfähigkeit der Dokumente, 6 Sicherstellung der Vertraulichkeit, Sicherstellung der Integrität, Sicherstellung der Verfügbarkeit, Gewährleistung der Authentizität, Gewährleistung der Revisionsfähigkeit, Gewährleistung der Rechtssicherheit)				
Maßnahmen beschreiben, die zur Sicherung der Rechte der Betroffenen (Löschung, Sperrung, Berichtigung, Auskunft) vorgesehen sind (5.5.2 Löschung, Sperrung, Berichtigung, Auskunft)				
Maßnahmen zur Sicherung der Nicht-Abstreitbarkeit von Datenübermittlungen beschreiben (6 Sicherstellung der Nicht-Abstreitbarkeit von Datenübermittlungen)				
Technische Mechanismen für die verschiedenen Zeichnungsformen festlegen (7.3 Problemfeld 3 und 10.2)				
Räumliche Sicherung der Scan-Stelle festlegen (9.2)				
Ausprägung der Rechercherechte festlegen (11)				
Technische Maßnahmen zur Sicherstellung von Rechten Betroffener auf Akteneinsicht und nach den Informationsfreiheitsgesetzen festlegen (5.6)				

Wichtige Linkadressen

In der Handreichung sind zu den wesentlichen Aussagen und Empfehlungen Internet-Adressen zur weiteren Recherche aufgenommen worden. An dieser Stelle finden Sie noch einmal die wichtigsten übergreifenden Internet-Adressen zum Thema „DMS“.

Linkadressen	Stelle - Inhalt
www.datenschutz.de	Virtuelles Datenschutzbüro
www.bsi.de	Bundesamt für Sicherheit der Informationstechnik
www.koopa.de/	Im Kooperationsausschuss ADV (KoopA ADV), dem der Bund, die Länder und die kommunalen Spitzenverbände angehören, werden die gemeinsamen Grundsätze des Einsatzes der Informations- und Kommunikationstechniken (IT) und wichtige IT-Vorhaben in der öffentlichen Verwaltung besprochen.
www.kbst.bund.de/	Domea-Konzept