DuD
Datenschutz und Datensicherheit

Datenschutzanforderungen an Dokumentenmanagement-Systeme (DMS)

Johann Bizer, Iris Hertel, Martin Rost

Dokument-Managementsysteme halten Einzug in die Verwaltungen. Besondere Aufmerksamkeit verlangt der Arbeitnehmerdatenschutz. Eine besondere Bedeutung kommt den Regelungen über den Umgang mit Meta-, Vorgangs- und Logdaten zu. Der folgende Beitrag fasst die zentralen Anforderungen an eine datenschutzkonforme Gestaltung zusammen.

Dr. Johann Bizer
Stellvertr. Landesbeauftragter für den Datenschutz. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

E-Mail: bizer @datenschutzzentrum.de

Iris Hertel

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD). Referat Öffentliche Verwaltung

E-Mail: hertel@datenschutzzentrum.de

Martin Rost

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD). Referat Systemdatenschutz

E-Mail: rost@datenschutzzentrum.de

1 Einleitung

Terry Winograd hatte 1972 eine komplexe Bauklötze-Welt in einem Computer formalisiert, in der Sprachverständnis und planvolle Tätigkeiten miteinander verbunden waren.[1] Winograd galt fortan als eines der vielversprechendsten Talente der „harten Künstlichen Intelligenz", die sich der Simulation menschlichen Denkens verschrieben hatte. In den 80er Jahren wandte sich Winograd dann jedoch der maschinellen Stützung der Kommunikation unter Menschen zu.[2] Die Kernidee bestand darin, Programme zu entwickeln, die die Kommunikation von Computernutzer beobachten, um diesen einen intelligenten Mehrwert anbieten zu können.

Seit dieser Entwicklung werden den Organisationsplanern zunehmend leistungsfähigere Programme zur technisch gestützten Entscheidungsfindung oder zur Gestaltung von Workflows bereitgestellt. Für Datenschützer bedeutet dies, dass sie sich dem schwierigen Thema ausgesetzt sehen, wie sich die Automatisierung der Beobachtung und Führung menschlicher Kommunikationen in und mit Organisationen datenschutzgerecht gestalten lässt.

2 Funktionale Entwicklung

Ende der 80er Jahre entwickelte sich unter dem Label CSCW („Computer Supportet Cooperative Working") ein Softwaregenre, zu dessen Pionieren das heute noch bekannte Lotus Notes zählt. Groupware, Workflow- und Dokumentmanagement-Systeme bezeichnen spezifische Schwerpunkte der elektronischen Unterstützung von Gruppenkommunikationen.

Unter Groupware versteht man eine Software, die die Zusammenarbeit (Kommunikation, Koordination, Kooperation) einer Gruppe bzw. Teilorganisationseinheit über räumliche und zeitliche Distanzen hinweg unterstützt. Gemeinsames Schreiben an einem Text mit Hilfe beispielsweise eines shared whiteboards oder mit Hilfe der Option „Änderungen verfolgen" oder die Nutzung einer gemeinsamen Ressourcenverwaltung bzw. eines Terminplaners wären hierfür Beispiele. Etwas anders gelagert ist der Schwerpunkt bei technisch gestützten Workflow-Managementsystemen, in denen vor allem Aspekte der Teil-Automatisierbarkeit von gut gegeneinander abgegrenzten bzw. aufeinander folgenden Arbeitsschritten im Vordergrund stehen. Hier ist technisch festgelegt und koordiniert, wer (oder was) welche Aufgabe zu einer bestimmten Zeit (oder in einem bestimmten Zeitraum) unter welchen Kontextbedingungen ausführt.

Seit wenigen Jahren konzentriert sich die Diskussion in den öffentlichen Verwaltungen Deutschlands auf Dokumentmanagement-Systeme (DMS). Diese Systeme wiesen inzwischen die wesentlichen Eigenschaften von Groupware- und Workflow-Systemen auf, nachdem man ursprünglich unter einem DMS eine Software vornehmlich zur Verwaltung von Aktenzeichen bzw. für den verbesserten Zugriff auf Akten verstand.

DMS werden nunmehr eingeführt, um absehbar die gesamte Aktenkommunikation vollständig elektronisch zu verwalten bzw. durchzuführen. Mit der Akte wird der operative Kernbereich der Verwaltungskommunikation durchtechnisiert.[3] Deshalb erwartet

[1] Vgl. „SHRDLU", http://hci.stanford.edu/~winograd/ shrdlu/index.html.

[2] Vgl. Winograd, Terry / Flores, Fernando, Erkenntnis Maschinen Verstehen. Zur Neugestaltung von Computersystemen, Berlin: Rotbuch Verlag.1989.

[3] Mit der vollzogenen Einführung der DMS wird sich der Druck auf andere eGovernment-Projekte noch einmal steigern, wenn man bspw. an die mehr als zögerliche Einführung digitaler Signaturen insbesondere im öffentlichen Bereich denkt. Nunmehr entsteht ein unabwendbarer

man gerade von DMS in Verwaltungen einen besonders ergiebigen Beitrag zur Einlösung des großen eGovernment-Versprechens, wonach die mit der anstehenden Technisierung einhergehende Verwaltungsreform den Wirkungsgrad der Verwaltungskommunikation nach Innen und Außen bei gleichzeitig drastischer Kostenreduktion verbessert.

Allerdings dürften die meisten Verwaltungen gegenwärtig papierene und elektronische Dokumente[4] nebeneinander verarbeiten, mit Folgen für den organisatorischen und regelungstechnischen Aufwand insbesondere bei rechtsverbindlichen Dokumenten. Häufig behilft man sich mit Regeln, dass das papierene Dokument bspw. das maßgebliche zu sein hat. Auf diese Weise werden jedoch in der Regel eher noch zusätzliche Kosten gegenüber der alten rein papierenen Lösung erzeugt.[5]

Das von Verwaltungen benötigte Leistungsspektrum eines rein elektronisch gestützten DMS wird beispielsweise im DOMEA-Konzept[6] formuliert, das zu berücksichtigen für Bundesverwaltungen verbindlich ist und inzwischen auch von vielen Landesverwaltungen als Maßgabe genutzt wird. Dem Datenschutz ist in diesem Katalog seit November 2005 in der Version DOMEA 2.1 nun endlich explizit ein Kapitel gewidmet. Einen Schwerpunkt dieses Kapitels bildet dabei der Umgang mit Protokolldateien. Es zeigt sich in wünschenswerter Klarheit, dass die datenschutzrechtlichen Anforderungen an ein System, in dem im Endausbau Dokumente rein elektronisch geführt werden, hoch sind.

3 Allgemeine Anforderungen

3.1 Verantwortliche Stelle

Die datenschutzrechtliche Verantwortlichkeit für die Einführung bzw. für den Betrieb eines DMS richtet sich danach, welche Stelle als Daten verarbeitende Stelle anzusehen ist. Daten verarbeitende Stelle ist jede öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt. Das bedeutet, dass das jeweilige Ressort, in dem ein DMS zur Anwendung kommt, Daten verarbeitende Stelle und damit auch datenschutzrechtlich für den Umgang mit den Daten verantwortlich ist.

3.2 System-Dokumente

Die verantwortliche Daten verarbeitende Stelle hat vor der Inbetriebnahme eine ganze Reihe an Dokumenten zu erstellen. Sie muss auf jeden Fall ein IT- bzw. Verfahrenskonzept sowie ein Sicherheitskonzept bzw. eine Risikoanalyse vorlegen.

In der in vielerlei Hinsicht vorbildlichen Schleswig-Holsteinischen Datenschutzverordnung (DSVO) regelt bspw. § 6, dass die Daten verarbeitende Stelle den Verfahrenszweck (§ 5 DSVO), eine Verfahrensbeschreibung (§ 4 DSVO), in der die Abgrenzung zu anderen Verfahren sowie die Programme und ihre Beziehungen zueinander zu dokumentieren sind, und ein Sicherheitskonzept (§ 6 DSVO) zu erstellen hat.

Das Sicherheitskonzept soll Angaben darüber enthalten, welche technischen und organisatorischen Maßnahmen unter Berücksichtigung der tatsächlichen örtlichen und personellen Gegebenheiten getroffen werden, um die Anforderungen an Datenvermeidung, Datensparsamkeit sowie Maßnahmen zur Datensicherheit beim Einsatz automatisierter Verfahren zu erfüllen. Es soll im Detail jeweils Maßnahmen in den Bereichen des allgemeinen Grundschutzes, der Arbeitsplatzebene, der Zentralrechnerebene, der Verfahren, der Administration, der Zugriffsrechte und Rollenkonzepte, der Revision/Kontrolle und der Notfallvorsorge bezeichnen.

Die verbleibenden Schwachstellen, die nicht oder nur zum Teil durch die getroffenen Maßnahmen ausgeschlossen werden können, können in Schleswig-Holstein dann in einer „Risikoanalyse" beschrieben werden, die als Verschlusssache zu behandeln ist. Eine Fortschreibung dieser Dokumente ist vorzusehen.

4 Spezifische Anforderungen

4.1 Feststellung des Schutzniveaus

Klärungsbedürftig ist zunächst, welche personenbezogenen Daten verarbeitet werden und ob es spezifische Verbote gibt, bestimmte personenbezogene Daten automatisiert zu speichern (z.B. bei Verschlusssachen). Bei bestimmten personenbezogenen Daten und vertraulichen Erklärungen können zudem Bedenken bestehen, diese wegen der besonderen Verfügbarkeit elektronischer Dokumente einzuscannen und auf diese Weise ihre elektronische Verbreitung zu erleichtern. Daten, die dem Sozialgeheimnis, dem Personalaktengeheimnis oder einem anderen Amts- oder Berufsgeheimnis unterliegen, sind nach spezialgesetzlichen Regelungen besonders geschützt.

Vor der Einführung eines DMS sollte daher jede verantwortliche Stelle eine Negativliste der Dokumente anlegen, die nicht eingescannt werden dürfen. Ferner ist darüber hinaus festzulegen, welche eingescannten Daten wegen ihrer Sensibilität besondere Sicherheitsmaßnahmen, wie beispielsweise eine Verschlüsselung, unmittel-

Anwendungsdruck innerhalb des Kernbereichs von Verwaltung.

[4] Ein Dokument bezeichnet die ganze Breite multimedialer Dateien. Es handelt sich dann um ein Dokument, solange es nicht im Sinne eines Programms ausführbar ist.

[5] Deswegen muss die Maßgabe gelten, die Migrationsphase von Papier auf EDV möglichst schnell zu durchlaufen. Es gibt vielfach generell Zweifel am ökonomischen Nutzen von DMSen: In den planenden, oberen Landesbehörden mit ihren vergleichsweise schwieriger standardisierbaren Workflows sieht man nach meiner Beobachtung eigentlich gar keinen Bedarf nach höherer Standardisierung. Und bei den ausführenden unteren Landesbehörden sind die meisten Verfahren faktisch bereits so weit durchstandardisiert, dass man dort wenn irgend möglich ohnehin auf dem gegenüber einem DMS höher auflösenden Strukturierungsniveau von Datenbanken arbeitet. Man kann sich fragen, ob sich eine derartige Geringschätzung der Standardisierungsleistung eines DMSs nicht dem Umstand verdankt, dass Führungspersonen sich nicht einer weitergehende Technisierung ihres Arbeitsplatzes, mit der latenten Gefahr der Leistungskontrolle auch ihres Tuns, zu unterwerfen bereit sind.

[6] "Wesentliches Ziel des DOMEA-Konzeptes ist die Einführung der elektronischen Akte. An die Stelle der Papierakten sollen künftig behördliche Geschäftsprozesse treten, die medienbruchfrei und vollständig elektronisch realisiert werden können. Die elektronische Akte wird in IT-gestützter Vorgangsbearbeitung erzeugt, erfasst und verwaltet. Dabei gelten die gleichen Anforderungen an das elektronische Schriftgut, die in Gesetzen, Geschäftsordnungen, sowie Richtlinien und Vorschriften für die Papierakten festgelegt sind. Behördliche Unterlagen müssen auch in elektronischer Form den Kriterien Vollständigkeit, Integrität und Authentizität, Zusammenfassung aufgabenbezogener und zusammengehöriger Schriftstücke, Nachvollziehbarkeit und Rechtmäßigkeit des Verwaltungshandelns genügen. So müssen auch elektronische Akten hinreichenden Inhalt und Struktur aufweisen und sich in einen Kontext einordnen lassen. Elektronische Akten sollen wie ihre Vorgänger im Papierformat über die unmittelbare Bearbeitung hinaus ihre Nachweisfunktion erfüllen." (vgl. http://www.kbst.bund.de/-,413/DOMEA-Konzept.htm).

bar nach dem Scannvorgang erfordern. Im Regelfall dürfte ein lückenloses, detailliertes *Zugriffskonzept* eine ausreichende Sicherheitsmaßnahme sein.

4.2 Umstellung von Papier- auf E-Akte

In einem *Migrationskonzept* ist festzulegen, auf welche Weise die Umstellung auf eine elektronische Aktenführung erfolgen soll und auf welche Weise der Medienbruch, der mit einer sukzessiven Umstellung von Papierakte auf elektronische Akte verbunden ist, bewältigt werden soll. Bestandteile sind bspw. die Anpassung der Organisationsstruktur und Arbeitsprozesse an das DMS, das Verhältnis zwischen dem alten und dem neuen Datenbestand sowie die Abbildung eines organisationsbedingten Aktenzeichenwechsels, eines Laufzeichenwechsels oder anderer organisatorischer Veränderungen, ohne dass die eindeutige Zuordnung von Rollen, Verfahren und Dokumenten oder auch nur die Verfügbarkeit der Daten gefährdet ist.

In diesem Zusammenhang ist auch zu klären, welche Typen an Verfahrenskommunikationen insgesamt vorliegen und wie diese in ihrer Differenziertheit elektronisch nachgebildet werden oder sich auch nach dem erfolgten Transfer verändern. So sind beispielsweise die zwar ungewöhnlichen aber nicht seltenen Fälle aufzugreifen, in denen aus einem Verwaltungsverfahren, beispielsweise durch eine Anfrage bei einer anderen Behörde, zwei Verfahren werden. Wie ist die Integrität des virtuellen Gesamtverfahrens gewährleistet?

4.3 Scann-Konzept

Der Umgang mit eingehenden Dokumenten ist abschließend festzulegen. So muss im *Sicherheitskonzept* festgelegt sein, welche Personen zum Scannen welcher Dokumente berechtigt und für diesen Vorgang verantwortlich sind.

Durch technische und organisatorische Maßnahmen ist vorzusehen, dass Fehler, wie bspw. ein unvollständiges Scannen, ein falsches Zusammenführen einzelner Dokumente oder eine falsche Zuordnungen zu Vorgängen, vermieden werden. Fehler müssen leicht zu korrigieren sein. Außerdem ist zu klären, wie mit dem Original, das eingescannt wurde, umzugehen ist. Insbesondere sind der Ort und die Dauer der Aufbewahrung des Originals festzulegen.

In jedem Falle ist sicherzustellen, dass eingescannte Dokumente die Beweiskraft haben, die der Absender mit seiner schriftlichen Einsendung intendiert hat. Ein sich aus dem Prozess des Einscannens ggf. ergebender Beweiswertverlust darf nicht zu Lasten des Einsenders gehen.

Festzulegen ist ferner, ob nach dem Scannen eine OCR-Erkennung eingesetzt werden darf. Soweit dies der Fall ist muss technisch sichergestellt werden, dass beim Übergang in die elektronische Form durch OCR-Erkennung Manipulationen ausgeschlossen und Fehler vermieden werden.

4.4 Zugriffsberechtigungen

Ein zentrales Element, um den Datenschutz durch geeignete technische und organisatorische Maßnahmen sicherzustellen, bildet die Festlegung der Zugriffsberechtigungen. Die Beschränkung der Zugriffsberechtigungen muss gewährleisten, dass personenbezogene Daten nur im Rahmen der Erforderlichkeit und nach dem Grundsatz der Zweckbindung verarbeitet werden.

Der Sachbearbeiter darf nur auf die Daten zurückgreifen können, die er im Rahmen seiner eigenen Aufgabenerfüllung benötigt. Dazu gehört auch eine Festlegung und Implementierung von Vertretungsregeln. Das *Rechte- bzw. Rollenkonzept* ist detailliert festzulegen, insbesondere im Hinblick auf die Unvereinbarkeit verschiedener Administrationsrollen. Wichtig ist ferner die Darlegung, auf welche Weise ressortübergreifende oder behördenübergreifende Arbeitsgruppen mit beschränkten Rechten ausgestattet werden können.

4.5 Datenintegrität

Es dürfen nur richtige (korrekte) Daten verarbeitet werden. Es ist die Integrität der Daten zu gewährleisten, d.h. die Daten müssen vor Manipulationen geschützt werden (können). Dies wird zum Beispiel über eine Protokollierung und Versionierungen bzw. Historisierung erreicht (siehe unten). Zugleich muss jedes Dokument und jede Änderung des Dokumentes einem eindeutigen Urheber zugeordnet werden können.

4.6 Sicherstellung der Bearbeitungswege

Der gesamte Umlauf von Dokumenten einschließlich der dazu gehörenden Verfügungen ist durch das DMS abzubilden. Es muss nachvollziehbar sein, wer welches personenbezogene Datum in welcher Aufeinanderfolge verändert hat.

Dem Empfänger eines Dokumentes muss bei Erhalt mitgeteilt werden, zu welchem Zweck er das Dokument erhält (zur Kenntnis, zur Bearbeitung, zum Mitzeichnen etc.). Bearbeitungsvermerke und Änderungen müssen dokumentiert werden und wiederum ihren Urheber und den Zeitpunkt der Bearbeitung zweifelsfrei erkennen lassen. Die Laufwege einer elektronischen Akte, insbesondere die behördeninternen Verfügungen, müssen abgebildet werden können.

4.7 Recherche

Die Zweckbindung der Datenverarbeitung erfordert neben der exklusiven Zuweisung von Zugriffsrechten auch eine Einschränkung der Suchfunktion. Die Gefahr bei elektronisch aufbereiteten Daten liegt unter anderem in der Möglichkeit der Verknüpfung von verschiedensten Daten mit automatisierten Such- und Auswertungsmöglichkeiten.

Erforderlich ist daher eine präzise Beschreibung der Suchfunktion (Volltextrecherche / Recherche über Metadaten) 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 beziehen, zu denen auch eine Zugriffsberechtigung besteht. Es kann deshalb erforderlich sein, nur eine begrenzte Zahl von Datenfeldern zur Einsicht zuzulassen. So sollte bspw. eine Registratur nur Registraturdaten, aber keine Inhaltsdaten zur Einsicht erhalten.

4.8 Vertraulichkeit

Vertraulichkeitsverluste sind zu vermeiden. Dies ist insbesondere über die oben genannten Zugriffsberechtigungen und ggf. durch eine Verschlüsselung eines Dokumentes zu gewährleisten. Zu klären ist, auf welche Weise die Zugriffe der Administratoren überwacht und kontrolliert werden.

4.9 Verfügbarkeit

Der Verlust der Verfügbarkeit der Daten ist zu verhindern. Die Dokumentenverwaltung

ist technisch so zu gestalten, dass alle Unterlagen während der Dauer der Aufbewahrungsfrist verfügbar sind. Diese müssen innerhalb einer angemessenen Zeit so lesbar gemacht werden können, dass sie dem Original entsprechen. Eine eindeutige Aktenzeichenvergabe ist zum Beispiel Grundvoraussetzung für die Verfügbarkeit der Daten. Auch eine regelmäßige Datensicherung gehört zu den zu treffenden Maßnahmen.

4.10 Metadaten

Es ist festzulegen, welche Metadaten (Dokumentenname, Verzeichnis, Autor, Datum, letzte Änderung) beim Anlegen eines Dokumentes automatisiert erstellt werden und welche manuell einzugeben sind. Dabei ist der datenschutzrechtliche Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten.

Bei der Ausgestaltung der konkreten Datenverarbeitungsprozesse ist darauf hinzuwirken, dass keine oder möglichst wenige personenbezogene Daten verarbeitet werden. Die Anzahl und der Inhalt der Metadaten sind auf das notwendige Maß zu beschränken. Freie Datenfelder, in denen beliebige Notizen eingetragen werden können, sind zu vermeiden, auch sofern diese bei einer Revision nicht einsehbar sind.

4.11 Protokollierung

Bei der Protokollierung der Tätigkeiten, die im Zusammenhang mit einem DMS stehen, wird der Bereich der System-Administration und der der Applikations-Nutzung im BDSG in der „Anlage zu § 9 Satz 5" unter dem Stichwort Eingabekontrolle nicht unterschieden. Der § 6 Abs. 2 LDSG Schleswig-Holstein, in Verbindung mit § 8 Abs. 5 DSVO, nimmt diesen Unterschied auf und regelt differenzierter, dass Zugriffe, mit denen strukturelle Änderungen an automatisierten Verfahren bewirkt werden, nur von ausdrücklich ermächtigten Administratoren vorgenommen werden.

4.11.1 Differenzierung nach Admin und Nutzer

Derartige Systemadministrations-Zugriffe sind zu protokollieren und zu kontrollieren; die Protokolle sind 5 Jahre aufzubewahren. Diese Protokolldaten müssen Aussagen enthalten über den Zeitpunkt des ändernden Zugriffs, die Gründe für den Zugriff, die veranlassenden und ausführenden Personen, die Art der Änderung, und den Zeitpunkt der Kontrolle und die kontrollierende Person.

Werden personenbezogene Daten ausschließlich automatisiert gespeichert und verarbeitet, ist nach § 6 Abs. 4 LDSG zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. Entsprechendes gilt für die Veränderung und Übermittlung der Daten. Diese Protokolldatenbestände sind ein Jahr zu speichern. Protokolldaten nach § 6 Abs. 4 LDSG müssen erkennen lassen wann, durch wen und in welcher Weise die personenbezogenen Daten gespeichert, verändert oder übermittelt wurden.

Es macht guten Sinn, die unterschiedlichen Typen von Protokolldaten auch unterschiedlich zu bezeichnen. Wir empfehlen, *Metadaten* als Bezeichnung für Protokolldaten mit Bezug zu Dokumenten, *Vorgangsdaten* als Bezeichnung für Protokolldaten bezüglich des Workflows und *Logdaten* als Bezeichnung für Protokolldaten in Bezug auf die strukturellen Tätigkeiten seitens der System- und Applikationsadministration zu benutzen.

4.11.2 Grundsätze der Protokollierung

Protokolldaten unterliegen einer strikten Zweckbindung. Sie dürfen gemäß § 13 Abs. 6 LDSG-SH ausschließlich datenschutzrechtlichen Kontrollen dienen (Zweckbindung).

Bei der Bestimmung des Umfanges der Protokollierung ist das Prinzip der Datensparsamkeit zu beachten. Dazu gehört zum Beispiel, dass der Umfang der Protokollierung aus bestimmten Anlässen erweitert werden kann. So ist zum Beispiel denkbar, dass – sofern keine besonderen Umstände vorliegen – die Protokollierung auf bestimmte, festzulegende Daten oder auf einen bestimmten Ausschnitt zu beschränken ist. Erst nach einem bestimmten Anlass, zum Beispiel nach Feststellung von unberechtigten Zugriffen von Außen, wird das Ausmaß der Protokollierung erhöht (Skalierung). Ist der Anlass behördenintern bedingt, so bestünde zugleich die Möglichkeit, vor einer solchen Ausweitung die Mitarbeiter zu informieren.

4.11.3 Auswertung der Protokolldaten

Festzulegen ist, auf welche Weise die Protokolldaten ausgewertet werden und wer diese Auswertung vornimmt. Dabei ist insbesondere zu klären, zu welchem Zweck eine Auswertung erfolgen darf, wie die Protokolldaten aufbereitet werden, wie eine Auswertung erfolgt und wer diese Aufbereitung und Auswertung vornimmt.

Die Auswertungen sollten technisch unterstützt und nach Möglichkeit auf der Grundlage pseudonymisierter Protokolldaten erfolgen. Außerdem ist zu klären, inwieweit regelmäßige Auswertungen vorgenommen werden. Grundsätzlich sollten regelmäßige Auswertungen auf ein Minimum reduziert werden und nach den oben genannten Grundsätzen anlassbezogene Auswertungen vorgezogen werden.

4.11.4 Revisionsfestigkeit der Protokolldaten

Der Umgang mit den Protokolldaten muss revisionsfest erfolgen. Dies betrifft die Manipulationsresistenz (z.B. durch Signatur oder Verschlüsselung), den Aufbewahrungsort (Protokolldaten nach § 6 Abs. 2 LDSG sollten auf einem gesonderten Protokollserver aufbewahrt werden und dort gesonderten Zugriffsberechtigungen unterliegen), die Aufbewahrungsdauer (s.o.: 1 bzw. 5 Jahre) und die Löschung.

4.11.5 Leistungs- und Verhaltenskontrolle

Mit der Protokollierung entstehen besondere Sammlungen personenbezogener Daten über die Nutzer der Anwendung, d.h. über die Mitarbeiter. Daraus lassen sich Nutzerprofile ableiten oder Listen über Auffälligkeiten erstellen. Das Datenschutzrecht lässt derartige Auswertungen ohne Einwilligung der Betroffenen grundsätzlich nicht zu. Nach § 23 Abs. 2 LDSG dürfen Daten von Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 5 und 6 LDSG gespeichert oder in einem automatisierten Verfahren gewonnen werden, nicht zu Zwecken der Verhaltens- oder Leistungskontrollen ausgewertet werden.

Protokolldaten dürfen nur zu Zwecken genutzt werden, die Anlass ihrer Speicherung waren, und dürfen auch nicht für

andere Zwecke verarbeitet werden (§ 13 Abs. 5 LDSG). Im Einzelfall kann eine Auswertung der Protokolldaten zur Aufdeckung von Missbräuchen aber zulässig sein.

Ein System, das grundsätzlich geeignet ist, Leistungs- und Verhaltenskontrollen durchzuführen, ist mitbestimmungspflichtig. Es empfiehlt sich, im Rahmen einer Dienstvereinbarung auf das gesetzliche Verbot von Verhaltens- und Leistungskontrollen ausdrücklich hinzuweisen. Zugleich ist festzulegen, zu welchen Zwecken und in welchen Verfahren personenbezogene Protokolldaten aus dem DMS verwendet werden dürfen.

Grundsätzlich sind die Mitarbeiter über die Prozesse aufzuklären, in denen ihre Daten personenbezogen verarbeitet werden. Aus dem datenschutzrechtlichen Gebot der Transparenz der Datenverarbeitung folgt, dass der Nutzer über die Möglichkeit einer Profilbildung informiert wird.

4.12 Aktenvernichtung

Es ist detailliert festzulegen, wie lange die einzelnen Dokumente aufzubewahren sind. Es müssen daher an der Erforderlichkeit ausgerichtete einheitliche Aufbewahrungsfristen festgelegt werden, die von dem System unterstützt werden. Zum Beispiel sollte eine automatisierte und fristgesteuerte Löschung möglich sein. Wichtig ist außerdem, dass Vorgänge bzw. Dokumente ohne Aufbewahrungsfristen aufgefunden werden können. Eine Löschung von gespeicherten, personenbezogenen Daten sollte frühest möglich stattfinden. Zu berücksichtigen ist, dass eine Löschung irreversibel sein muss, zugleich aber eine zufällige Löschung auszuschließen ist.

4.13 Archivierung

Es ist ein Archivierungskonzept zu erstellen, in dem die Übergabe der im DMS geführten Dokumente aus dem Verwendungszweck der Verwaltung in den Verwendungszweck der Archivierung festgelegt wird.

5 Ansprüche Dritter

Datenschutzrechtliche Rechte der Betroffenen wie die Auskunft über die zu seiner Person gespeicherten Daten, ihre Berichtigung, Sperrung oder Löschung müssen gewährleistet sein und technisch unterstützt werden. Zu klären ist, wie Informationszugangsrechte von privaten und juristischen Personen des Privatrechts technisch realisiert bzw. unterstützt werden können.

Nach § 4 Informationsfreiheitsgesetz Schleswig-Holstein hat jede natürliche und juristische Person Anspruch auf Zugang zu den bei einer Behörde vorhandenen Informationen. Das Recht auf Informationszugang besteht unabhängig von der Form, in der die Information vorliegt. Grenzen werden dem Anspruch durch den Schutz öffentlicher Belange, durch das Recht auf informationelle Selbstbestimmung Dritter und durch zu beachtende Geschäfts- und Betriebsgeheimnisse gesetzt. Es bietet sich daher an, das DMS dafür zu nutzen, die verlangten Informationen „komfortabel", aber auch unter Wahrung der gesetzlich geregelten Schutzrechte, zur Einsichtnahme bereit zu stellen.