

## **Datenschutzinfo 4-06**

### **DMS – Datenschutz-, und Datensicherheitsaspekte**

Autor: Georg Osner, Datenschutzberater und IT-Revisor

Nicht zu unterschätzen sind die rechtlichen wie auch die sicherheitstechnischen Aspekte bei der Einführung eines Dokumentenmanagementsystems.

Schwerpunkt aus rechtlicher Sicht bilden die allgemeinen Datenschutzgrundsätze für die Verarbeitung personenbezogener Daten mit inhaltlichen und insbesondere auch verfahrensbezogenen und abgeleiteten technischen Sicherheitsanforderungen, u.a.:

- Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit bei Speicherung, Verarbeitung und Nutzung
- Sicherstellung der Zweckbindung der Protokoll-, und Verfahrensdaten (Verhaltens-, und Leistungskontrolle)
- Sicherstellung der Rechte der Betroffenen auf Berichtigung, Sperrung und Auskunft
- Sicherstellung der Löschung unzulässig gespeicherter und nicht mehr benötigter Dokumente

Eine Arbeitsgruppe des Arbeitskreises eGovernment der Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedete im März 2006 die recht umfassende Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen“. Wichtige Themen hieraus, die auch für die Privatwirtschaft gelten, sind im folgenden Text zusammengefasst und auszugsweise wiedergegeben. Den vollständigen Text der Orientierungshilfe finden Sie unter der Homepage des Niedersächsischen Datenschutzbeauftragten : [http://cdl.niedersachsen.de/blob/images/C18440594\\_L20.pdf](http://cdl.niedersachsen.de/blob/images/C18440594_L20.pdf)

#### **Lösungsansätze: Das Datenschutz- und Datensicherheitskonzept**

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

- Art, Zweck, Umfang und Speicherdauer von Dokumenten sowie Verfahrens- und Protokolldaten
- das notwendige Niveau für das Authentisierungsverfahren
- Art und Umfang von Verschlüsselungs- und Signaturverfahren, orientiert an den Anforderungen aus Schutzbedarf, Beweiswert und Formerfordernis
- den Umgang mit Dokumenten, die eine bestimmte juristische Qualität erfüllen müssen, z. B. Sicherstellung der Nachsignierung vor Ablauf der Gültigkeit der kryptographischen Algorithmen
- den Einsatz von Verschlüsselungstechnik zur Transportsicherung und ggf. bei der Speicherung
- die Notwendigkeit einer Ende-zu-Ende-Verschlüsselung sowie die Erstellung von qualifizierten Signaturen

## **Datenschutzinfo 4-06**

### **DMS – Datenschutz-, und Datensicherheitsaspekte**

- die Sicherstellung der Rechte der Betroffenen auf Berichtigung, Sperrung, Auskunft und Löschung

Um Unberechtigten Zugang zu personenbezogenen Daten zu vermeiden, 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.

### **Sicherheitsziele und -maßnahmen bei der Behandlung von Dokumenten**

Die konkreten Sicherheitsmaßnahmen sind auf der Grundlage einer Bedrohungs- und Risikoanalyse individuell zu ermitteln. Dabei sind u.a. 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 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 (z.B. Datenbanksysteme, die eine Datenverschlüsselung ermöglichen) oder durch entsprechende Zusatzsoftware (z.B. Tools zur Verschlüsselung von Plattenbereichen).

Eine andere Möglichkeit zur Lösung dieses Problems besteht in der Verschlüsselung der Dokumente auf Anwendungsebene.

#### **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, wird damit nicht nur 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.

## Datenschutzinfo 4-06

### DMS – Datenschutz-, und Datensicherheitsaspekte

#### 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.

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

#### Sicherstellung der Zweckbindung der Protokoll-, und Verfahrensdaten

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.

Protokolldaten entsprechend Datenschutzgesetz dürfen 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.

Eine Auswertung der Verfahrens- und Protokolldaten ist immer dann zulässig, wenn das dem Zweck der Speicherung entspricht. So ist die Auswertung von Protokolldaten zur Aufdeckung von Missbräuchen erlaubt. Eine Auswertung von Verfahrensdaten ist zulässig, wenn sie zur Prüfung der Recht- und Zweckmäßigkeit der Erfüllung einer konkreten Aufgabe z.B. durch Vorgesetzte erforderlich ist. Eine darüber hinaus gehende Verhaltens- und Leistungskontrolle der Beschäftigten durch eine solche Auswertung ist jedoch unzulässig.

Die Zweckbindung muss daher technisch und organisatorisch (z. B. durch 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 Betriebsrates sind zu beachten. Darüber hinaus sind die Beschäftigten darüber zu informieren, in welchem Zusammenhang das DMS welche Verfahrens- und Protokolldaten über sie speichert.

## **Datenschutzinfo 4-06**

### **DMS – Datenschutz-, und Datensicherheitsaspekte**

#### **Sicherstellung der Rechte der Betroffenen auf Berichtigung, Sperrung und Auskunft**

Nach Datenschutzgesetz 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.

#### **Sicherstellung der Löschung unzulässig gespeicherter und nicht mehr benötigter Dokumente**

War die Speicherung personenbezogener Daten unzulässig, sind diese Daten nach den Datenschutzgesetzen zu löschen. 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. Des Weiteren sind personenbezogene Daten auch zu löschen, sobald deren Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist. Eine sichere Löschung setzt daher 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.