





# Revisionssichere Speicherung von Dokumenten in der öffentlichen Verwaltung

Ergebnisse und Handlungsempfehlungen zur Sicherstellung einer  
revisionssicheren elektronischen Aktenhaltung

## **Revisionssichere Speicherung von Dokumenten in der öffentlichen Verwaltung**

Ergebnisse und Handlungsempfehlungen zur Sicherstellung einer revisionssicheren elektronischen Aktenhaltung

Herausgegeben von PricewaterhouseCoopers und IMTB Consulting

Von Peter Detemple, Bastian Flemming, Irina Furbach, Wigand Grabner, Nadja Koerdt, Gerrit Kronenberg, Ralph Naumann, Dirk Nippert, Silvia Treschau

Alle Rechte vorbehalten. Vervielfältigungen, Mikroverfilmung, die Einspeicherung und Verarbeitung in elektronischen Medien sind ohne Zustimmung der Herausgeber nicht gestattet.

Die Ergebnisse der Studie sind zur Information unserer Mandanten bestimmt. Sie entsprechen dem Kenntnisstand der Autoren zum Zeitpunkt der Veröffentlichung. Für die Lösung einschlägiger Probleme greifen Sie bitte auf die in der Publikation angegebenen Quellen zurück oder wenden sich an die genannten Ansprechpartner. Alle Meinungsbeiträge geben die Auffassung der Autoren wieder.

Satz  
Nina Irmer, Digitale Gestaltung & Medienproduktion, Frankfurt am Main

Druck  
Kohlhammer und Wallishauser GmbH, Druckerei und Verlag, Hechingen

Printed in Germany

## Vorwort

Die öffentliche Verwaltung befindet sich in einem umfassenden Veränderungsprozess, bei dem sich das Arbeitsumfeld erheblich ändert. So gehört die elektronische Kommunikation auch in der Verwaltung seit Langem zum Standard. Viele Verwaltungsabläufe werden mittlerweile elektronisch unterstützt. Dieser Wandel macht auch vor der behördlichen Schriftgutverwaltung nicht halt. Als 1996 das Konzept „Papierarmes Büro“ veröffentlicht wurde, war nicht vorherzusehen, dass der damit angestoßene Veränderungsprozess fast 15 Jahre später noch nicht abgeschlossen sein würde. Die Einführung der elektronischen Akte ist jedoch in fast allen Verwaltungsbereichen das erklärte Ziel.

Ein Aspekt dieses Veränderungsprozesses ist, dass die technischen Möglichkeiten den organisatorischen und rechtlichen Entwicklungen meist weit voraus sind. So finden sich kaum noch reine Papierakten in den Behörden. Derzeit herrschen Hybridkonstrukte vor. Ihr Nachteil liegt darin, dass mit ihnen die Ordnungsmäßigkeit und Nachvollziehbarkeit des Verwaltungshandelns nicht sichergestellt werden können. Oft sind keine beweiswerterhaltenden, nachvollziehbaren und vollständigen Aktenbestände mehr vorhanden.

Vor diesem Hintergrund gewinnt die revisions sichere Speicherung von elektronischen Dokumenten auch in der öffentlichen Verwaltung immer mehr an Bedeutung. Es gibt zahlreiche Diskussionen über die Anforderungen und vielfältige Vorschläge dazu, welche konkreten Maßnahmen eine Behörde ergreifen muss, um elektronische Dokumente revisions sicher zu speichern. Dabei werden häufig neue Begriffe zur Beschreibung der Anforderungen an die Speicherung von elektronischen Dokumenten eingeführt.

Die vorliegende Studie von PricewaterhouseCoopers (PwC) und IMTB Consulting GmbH hat zum Ziel, den Stand der Einführung der revisions sicheren Speicherung von elektronischen Dokumenten in der öffentlichen Verwaltung darzustellen und strukturierte Vorschläge zur weiteren Umsetzung dieses wichtigen Vorhabens zu unterbreiten. Zunächst wurde daher in einer Umfrage ermittelt, wie die öffentliche Verwaltung Dokumentenmanagementsysteme (DMS) einsetzt, und ob in den Behörden ein Bewusstsein für die Bedeutung einer revisions sicheren Aktenführung herrscht. Die Ergebnisse sind in Kapitel B dargestellt.

Als ein Ergebnis der Umfrage konnte herausgearbeitet werden, dass sowohl die Nutzung von DMS als auch das Interesse daran in der öffentlichen Verwaltung stetig wachsen. Auf Länderebene sind DMS am weitesten eingeführt. Dagegen steht ihre Nutzung auf kommunaler Ebene noch am Anfang. Auf Bundesebene konnte ein Stillstand der Einführung festgestellt werden. Dies ist verwunderlich, da die Bundesverwaltung mit der Vorlage des Konzepts für Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang (DOMEA) einmal die treibende Kraft in der öffentlichen Verwaltung war.

Weiterhin konnte ermittelt werden, dass die revisions sichere Speicherung von elektronischen Dokumenten ein wichtiges Thema für die Verwaltung ist. Allerdings herrschen große Unsicherheit und Unwissenheit über die damit verbundenen Anforderungen.

Die Ursache dafür ist – wie die Analyse der rechtlichen Rahmenbedingungen in Kapitel C zeigt –, dass es derzeit keine eindeutige und trennscharfe Definition des Begriffs „Revisions sicherheit“ für den öffentlichen Sektor<sup>1</sup> gibt und der Katalog der Anforderungen an Revisions sicherheit daher aus dem privatwirtschaftlichen Umfeld „geborgt“ werden muss. Da derzeit keine verwaltungsspezifischen Best-Practice-Ansätze existieren, ist die Unsicherheit groß. Die einzelnen Behörden begegnen diesen Unsicherheiten mit individuellen Lösungsansätzen, was mit Blick auf die gesamte Verwaltung ein sehr heterogenes Bild ergibt und die Nachhaltigkeit des Verwaltungshandelns zum Teil stark gefährdet.

Vor diesem Hintergrund werden in Kapitel D Vorschläge zur Reduktion der Unsicherheit und zur Klärung des Umgangs mit elektronischen Akten unterbreitet und in drei Handlungsfeldern zusammengefasst:

#### 1. Anpassung rechtlicher Grundlagen

Empfohlen wird eine Konkretisierung der rechtlichen Vorgaben für die revisions sichere elektronische Aktenhaltung in der öffentlichen Verwaltung. Dabei kann auf den Erfahrungen aus der Privatwirtschaft oder der Sozialgesetzgebung aufgebaut werden, wobei aber die Bedingungen der öffentlichen Verwaltung beachtet werden müssen.

#### 2. Schaffung von Kriterien

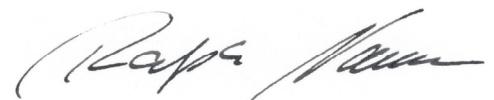
Vorgeschlagen wird die Aufstellung eines Katalogs spezifischer Anforderungen der öffentlichen Verwaltung an eine revisions sichere elektronische Aktenhaltung, der dazu beitragen kann, die vorhandenen Orientierungsschwierigkeiten zu beseitigen.

#### 3. Entwicklung eines Prüfverfahrens

Vorgeschlagen wird, ein Prüfverfahren ähnlich dem der Privatwirtschaft zu etablieren, das an die Bedürfnisse der öffentlichen Verwaltung angepasst ist und eine nachhaltige revisions sichere Speicherung elektronischer Akten sicherstellt.



WP Peter Detemple  
Partner  
PricewaterhouseCoopers AG  
Wirtschaftsprüfungsgesellschaft



Ralph Naumann  
Geschäftsführer  
IMTB Consulting GmbH



Wigand Grabner  
PricewaterhouseCoopers AG  
Wirtschaftsprüfungsgesellschaft

<sup>1</sup> Eine Ausnahme bilden die Regelungen des SGB IV für die Sozialversicherungsträger

## Inhaltsverzeichnis

Vorwort .....	3
Abbildungsverzeichnis.....	7
Abkürzungsverzeichnis .....	9
A Ausgangssituation .....	10
B Stand der elektronischen Aktenführung in der öffentlichen Verwaltung.....	12
1 Teilnahme an der Umfrage und Grunddaten .....	12
2 Analyse der Umfrageergebnisse.....	14
2.1 DMS-Einsatz.....	14
2.2 Einsatz DOMEA-zertifizierter Verfahren.....	16
2.3 Anpassung der Regelwerke im Zuge der DMS-Einführung.....	18
2.4 Elektronische Akten.....	20
2.5 Revisions sichere Speicherung.....	22
2.6 Wesentliche Ergebnisse und Fazit.....	27
C Bestehende Regelungen zur Revisions sicherheit in der Privatwirtschaft und in der öffentlichen Verwaltung.....	28
1 Regelungen für die Privatwirtschaft .....	28
1.1 Handelsgesetzbuch (HGB).....	28
1.2 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS).....	30
1.3 Bundesdatenschutzgesetz (BDSG) .....	31
2 Regelungen für die öffentliche Verwaltung .....	32
2.1 Grundgesetz (GG) .....	32
2.2 Verwaltungsverfahrensgesetz (VwVfG) .....	33
2.3 Sozialgesetzbuch (SGB) .....	33
2.4 Signaturgesetz (SigG) und Signaturverordnung (SigV).....	34
2.5 Bundesdatenschutzgesetz (BDSG) .....	34

2.6	Archivgesetze .....	34
2.7	DOMEA.....	34
3	Fazit.....	35
D	Handlungsempfehlungen .....	36
1	Handlungsfeld 1: Prüfung und Anpassung der rechtlichen Grundlagen.....	36
1.1	Verwaltungsverfahrensnormen .....	37
1.2	Normen des Datenschutzes .....	38
2	Handlungsfeld 2: Schaffung von Kriterien für die revisions sichere elektronische Aktenhaltung in der öffentlichen Verwaltung .....	38
2.1	Anforderungsdimension Technik.....	39
2.2	Anforderungsdimension Organisation.....	41
2.3	Anforderungsdimension Mensch.....	42
2.4	Anforderungsdimension Dokumentation.....	43
3	Handlungsfeld 3: Entwicklung eines Prüfverfahrens zur Sicherstellung der revisions sicheren Speicherung von elektronischen Akten .....	44
3.1	Rahmen für das Verfahren .....	44
3.2	Vorschlag für Prüfverfahren .....	46
3.2.1	Prüfung der Konzeption.....	46
3.2.2	Prüfung der Realisierung.....	47
3.2.3	Prüfung der Tests .....	48
3.2.4	Prüfung des Betriebs .....	48
4	Fazit.....	48
	Wir über uns .....	50
	Ansprechpartner.....	51

## Abbildungsverzeichnis

Abb. 1	Umfrageteilnehmer nach Verwaltungsebenen .....	12
Abb. 2	Teilnehmende Verwaltungen nach Verwaltungsebenen eingeteilt in Größenkategorien .....	13
Abb. 3	DMS-Einsatz .....	13
Abb. 4	DMS-Einsatz nach Verwaltungsebenen .....	14
Abb. 5	Gründe für einen DMS-Einsatz nur in einzelnen Bereichen .....	15
Abb. 6	Gründe dafür, dass bisher kein DMS eingesetzt wird .....	16
Abb. 7	Einsatz von DOMEA-zertifizierten und anderen DMS nach Verwaltungsebenen .....	17
Abb. 8	Begründungen für die Entscheidung gegen ein DOMEA-zertifiziertes Verfahren .....	17
Abb. 9	Im Rahmen der DMS-Einführung wurde die Schriftgutverwaltung durch Anpassung von Regelwerken auf den IT-Einsatz ausgerichtet .....	18
Abb. 10	Häufigkeit von Anpassungen der Regelwerke im Zuge der DMS-Einführung an den Beispielen Geschäftsordnung und Geschäftszeichen.....	19
Abb. 11	Durchführung einer Prozessanalyse und Ausrichtung der organisatorischen Abläufe auf den IT-Einsatz nach Verwaltungsebenen .....	20
Abb. 12	Die elektronischen Akten enthalten alle aktenrelevanten Schriftstücke (mit Ausnahme nicht scannbarer Dokumente).....	21
Abb. 13	Eingehende und gescannte Dokumente werden ausschließlich in der elektronischen Akte aufbewahrt.....	21
Abb. 14	Grundlagen, auf denen über Aufbewahrung oder Vernichtung von Papierschriftstücken nach dem Scanvorgang entschieden wurde.....	22
Abb. 15	Stellenwert der revisions sicheren Speicherung von elektronischem Schriftgut in den Behörden .....	23
Abb. 16	Stellenwert der revisions sicheren Speicherung nach Verwaltungsebenen .....	23
Abb. 17	Für das eingesetzte DMS in der von Ihnen vorgenommenen Anpassung existiert eine Dokumentation .....	24

Abb. 18	Für das eingesetzte DMS liegt eine Herstellererklärung bzw. ein Zertifikat vor, das die revisionssichere Speicherung von Dokumenten bestätigt.....	24
Abb. 19	Es existiert eine vollständige Dokumentation der organisatorischen Vorgaben für die Nutzung des Systems .....	25
Abb. 20	Es existiert eine zentrale Instanz, die die Einhaltung der organisatorischen Vorgaben zur Nutzung des eingesetzten Systems überprüft .....	25
Abb. 21	Die elektronische Aktenhaltung wurde von einem Dritten begutachtet bzw. zertifiziert .....	26
Abb. 22	Dimensionenmodell für die Entwicklung eines Anforderungskatalogs .....	39
Abb. 23	Dimensionen und revisionssichere Funktionen .....	39
Abb. 24	Qualitätsstufen der Revisionssicherheit der digitalen Aktenführung .....	45
Abb. 25	Prüfungsprozess .....	46

## Abkürzungsverzeichnis

AO	Abgabenordnung
BArchG	Bundesarchivgesetz (Gesetz über die Sicherung und Nutzung von Archivgut des Bundes)
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
DMS	Dokumenten-Management-System
DOMEA	Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang
E-GovG	E-Government-Gesetz (Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen)
GG	Grundgesetz
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
IKS	Internes Kontrollsystem
ITIL	IT Infrastructure Library
PK-DML	Prüfkriterien für Dokumenten Management Lösungen
PwC	PricewaterhouseCoopers
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SigV	Signaturverordnung
TR-VELS	Technische Richtlinie „Vertrauenswürdige Elektronische Langzeitspeicherung“
TR-ESOR	Technische Richtlinie „Beweiswerterhaltung kryptographisch signierter Dokumente“
VOI	Verband Organisations- und Informationssysteme e. V.
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz

## A Ausgangssituation

E-Government ist ein Eckpfeiler der Modernisierung der öffentlichen Verwaltung. Ein wichtiger Teil der E-Government-Vorhaben von Bund, Ländern und Kommunen ist die Einführung eines DMS als Grundstein für eine E-Government-Infrastruktur. Ein wesentliches Ziel ist dabei die Einführung der elektronischen Aktenführung, durch die eine vollständige und nachvollziehbare Dokumentation des Verwaltungshandelns in elektronischer Form sichergestellt werden soll. Dafür müssen nicht nur alle aktenrelevanten Dokumente in die (elektronische) Akte gegeben werden, sondern es ist auch sicherzustellen, dass die im elektronischen Aktensystem abgelegten Dokumente revisionsicher gespeichert werden.

Diese oft geäußerte Forderung zieht die Frage nach sich, was unter dem Begriff „Revisionsicherheit“ aus Sicht der öffentlichen Verwaltung zu verstehen ist und auf welcher Grundlage diese Forderung erhoben wird.

In der Privatwirtschaft hat der Gesetzgeber die Revisionsicherheit bei DMS schon lange rechtlich geregelt. Einer verbreiteten Definition zufolge bezieht sich der Begriff „Revisionsicherheit“ auf die ordnungsgemäß durchgeführte Langzeitspeicherung von aufbewahrungspflichtigen oder aufbewahrungswürdigen Informationen in elektronischen Archivsystemen. Dabei sind die gesetzlichen Anforderungen des Handelsgesetzbuchs (HGB), der Abgabenordnung (AO) und der daraus abgeleiteten Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) sowie andere steuerrechtliche und handelsrechtliche Vorgaben zu beachten.

Bei der Betrachtung der Rahmenbedingungen für die öffentliche Verwaltung ist zunächst das Prinzip der Aktenmäßigkeit als ein Grundprinzip des Verwaltungshandelns zu beachten. Daraus lässt sich ableiten, dass Verwaltungshandeln jederzeit nachvollziehbar sein muss und vollständig in Form von Akten zu dokumentieren ist.

Bei der Einführung der elektronischen Aktenführung gelten diese Prinzipien sicher weiter. Vor diesem Hintergrund wurde im Rahmen des Konzeptes zu Dokumentenmanagement und elektronischer Archivierung im IT-gestützten Geschäftsgang (DOMEA-Konzept) auch gefordert, dass elektronische Akten, Vorgänge und Dokumente nachvollziehbar und revisionsicher zu speichern sind. Diese Forderung bezieht sich auf den gesamten Lebenszyklus einer Akte.

Für eine Behörde bedeutet dies, dass sie von der Erzeugung über die Bearbeitungsphase und gesamte Aufbewahrungsfrist – unabhängig vom System in dem die Akten, Vorgänge und Dokumente verwaltet werden – eine „revisionsichere“ Speicherung ihrer elektronischen Akten sicherstellen muss. Erst nach Ablauf der Aufbewahrungspflicht und der damit verbundenen Abgabe der Akten an das zuständige Archiv bzw. der Vernichtung endet diese Pflicht für die Behörde.

Neben dieser Forderung findet sich im Glossar des DOMEA-Konzeptes auch eine allgemeine Erklärung was im Rahmen des Konzeptes unter dem Begriff Revisionsicherheit zu verstehen ist. Ein Hinweis auf eine konkrete Vorgabe oder Regelung findet sich nicht.

Für die elektronische Aktenführung und Langzeitspeicherung in Behörden wurde der Begriff „Revisionssicherheit“ weitgehend adaptiert, ohne eine konkrete Regelung für die speziellen Anforderungen der öffentlichen Verwaltung zu treffen. Dies bewirkt erhebliche Unklarheiten bezüglich des revisionssicheren Umgangs mit elektronischen Akten. Insbesondere aus verfassungsrechtlichen Gründen (Rechtsstaatsprinzip) ist dieser Zustand ungenügend. Zwar ist weitgehend anerkannt, dass bei elektronischer Aktenführung alle aktenrelevanten Dokumente in die (elektronische) Akte aufgenommen werden und wieder auffindbar (recherchierbar) und lesbar (benutzbar) sein müssen. Aus Art. 20. GG kann außerdem abgeleitet werden, dass die Authentizität, Integrität und Beweiskraft der im VBS abgelegten Dokumente gewahrt werden muss. Das DOMEA-Konzept, das mehr Sicherheit im Umgang mit der elektronischen Aktenhaltung schaffen will, empfiehlt hierfür die revisionssichere Datenspeicherung. Konkrete Rechtsnormen und Kriterien zur Prüfung der Revisionssicherheit fehlen jedoch.

Das kaufmännische Recht fordert bereits eine revisionssichere Datenspeicherung. Eine ständige Überwachung durch Verfahrensdokumentationen und Sicherheitszertifikate bietet im Wirtschaftsbereich – im Gegensatz zur öffentlichen Verwaltung – schon heute ein effektives Instrument für lückenlosen Rechtsschutz bei der elektronischen Datenverarbeitung.

Da in der öffentlichen Verwaltung entsprechende Normen fehlen, finden sich hier Unklarheiten und Sicherheitslücken. Eine direkte Adaption der Regelungen des kaufmännischen Rechts erscheint nicht sinnvoll, da die öffentliche Verwaltung einem größeren und differenzierteren Anforderungsspektrum gerecht werden muss. Beispielsweise braucht sie konkrete Regeln für den Beweiswerterhalt von Dokumenten. Auch Regelungen aus dem Privatrecht können nicht direkt übernommen werden, da es sich in erster Linie auf den Finanzbereich konzentriert und auf steuerrechtlichen Regelungen basiert.

## B Stand der elektronischen Aktenführung in der öffentlichen Verwaltung

### 1 Teilnahme an der Umfrage und Grunddaten

455 deutsche Verwaltungen wurden um ihre Teilnahme an der Befragung zum Thema „revisions sichere Speicherung“ gebeten. 190 Verwaltungen haben sich beteiligt. Die Rücklaufquote betrug 41,8 %. Aufgrund von unvollständigen Angaben oder Bearbeitungsfehlern konnten nur 169 der 190 abgegebenen Fragebögen ausgewertet werden. Der Umfragezeitraum endete am 31. Juli 2010.

Die 169 Teilnehmer mit auswertbaren Fragebögen repräsentieren alle Verwaltungsebenen.

- Von 90 angefragten Bundesbehörden nahmen 27 an der Umfrage teil. Die Rücklaufquote lag bei 30 %.
- Mit 68 Teilnehmern bei 155 Anfragen erreichten die Landesbehörden eine Rücklaufquote von 43,9 %. Hierbei ist zu berücksichtigen, dass sich mehrere Landesverwaltungen nicht an der Befragung beteiligt haben (u. a. aus Hamburg, dem Saarland und Schleswig-Holstein). Sie begründeten es damit, dass in ihren Ländern jeweils eine Landeseinrichtung zentral für die DMS-Einführung verantwortlich und demzufolge auch für die Beantwortung des Fragebogens zuständig ist. Somit kann davon ausgegangen, dass tatsächlich etwa 50 % der Landesverwaltungen in dieser Befragung repräsentiert sind, da Fragen zu ihrem Einführungsstand und zum Umgang mit dem Thema Revisions sicherheit zentral beantwortet wurden.
- Die Kommunalverwaltungen erreichten mit 67 Antworten bei 210 Anfragen eine Rücklaufquote von 31,9 %.

Landes- und Kommunalverwaltungen sind etwa gleich stark unter den Teilnehmern vertreten (40,3 % bzw. 43,7 %), Bundesbehörden mit 16 %.

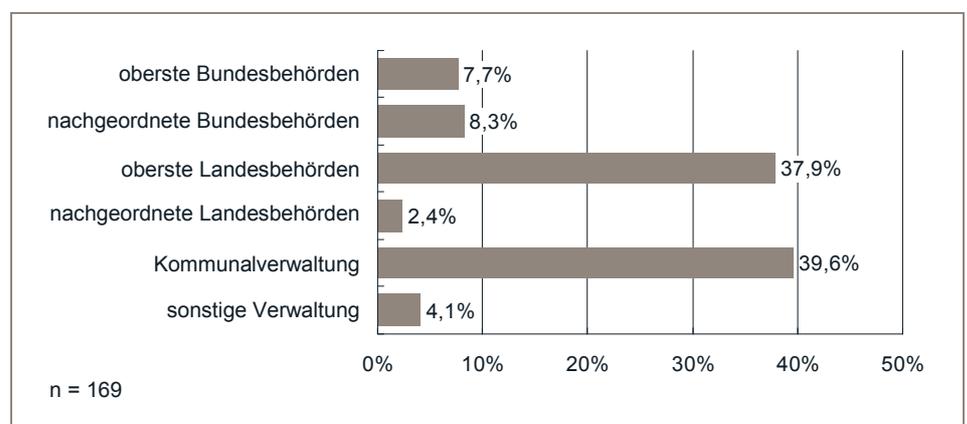


Abb. 1 Umfrageteilnehmer nach Verwaltungsebenen

37,3 % der befragten Behörden beschäftigen mehr als 1.000 Mitarbeiter. Aus dieser obersten Größenklasse stammen aber 72 % der befragten Kommunalverwaltungen, weil für diese Befragung ausschließlich Verwaltungen von Kommunen mit mehr als 100.000 Einwohnern kontaktiert

wurden. Weniger als 100 Mitarbeiter haben nur 7,2 % der befragten Kommunalverwaltungen.

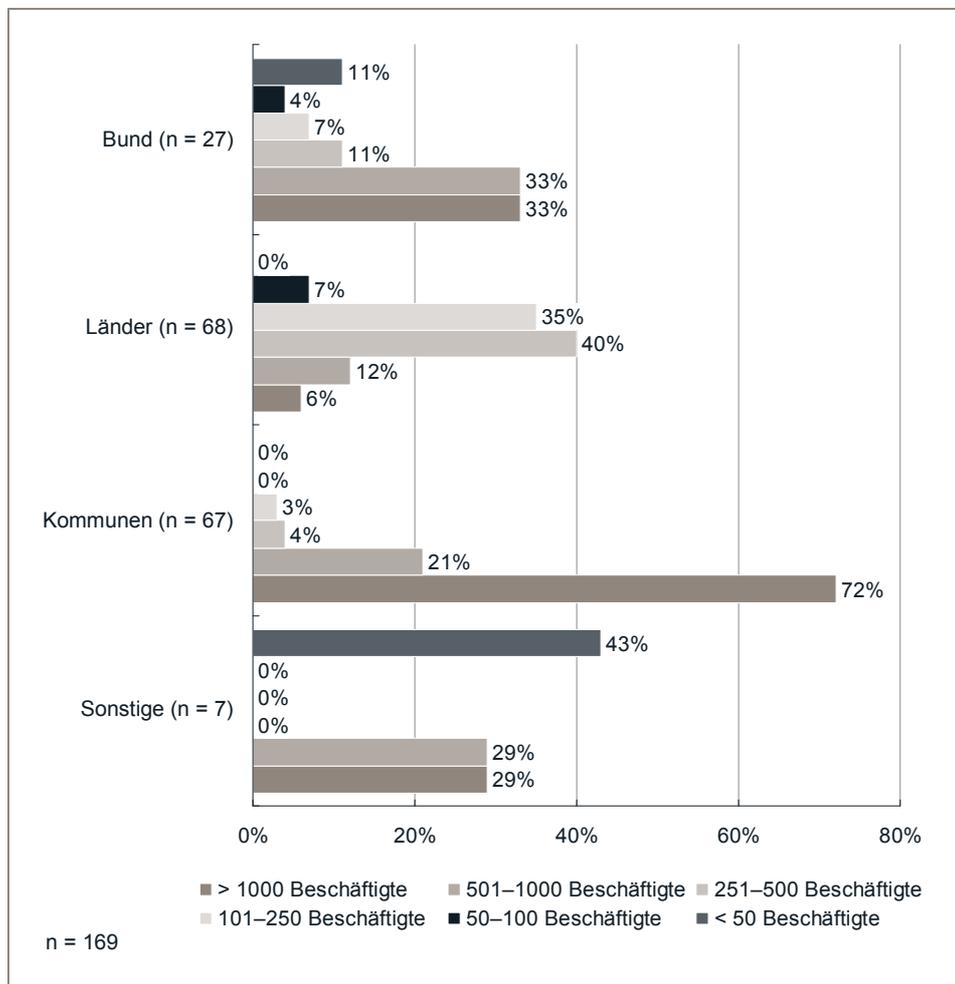


Abb. 2 Teilnehmende Verwaltungen nach Verwaltungsebenen eingeteilt in Größenkategorien

62,7 % der befragten Behörden setzen zumindest in ausgewählten Bereichen ein DMS ein. Etwas mehr als ein Drittel (37,3 %) hat bisher kein DMS.

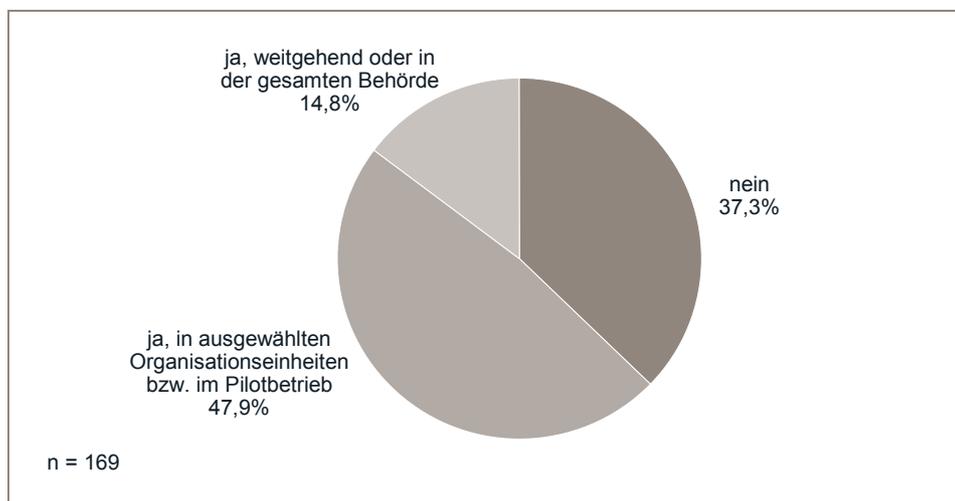


Abb. 3 DMS-Einsatz

**Wertung der Rücklaufquoten und Grunddaten**

Es lässt sich feststellen, dass das Thema „revisions sichere Speicherung“ von Dokumenten von hohem Interesse für die öffentliche Verwaltung ist. Dies zeigt sich an der relativ hohen Zahl von Rückläufen bei der Befragung sowie an den Bitten um Zusendung der fertiggestellten Studie.

Das Thema „Dokumentenmanagementsysteme in der öffentlichen Verwaltung“ griff die Bundesverwaltung 1996 mit dem Konzept „Papierarmes Büro“ auf und diskutierte es erstmals im größeren Rahmen auf dieser Ebene. Nun – 14 Jahre später – haben ca. zwei Drittel der befragten Verwaltungen ein DMS eingeführt bzw. mit der Einführung begonnen.

## 2 Analyse der Umfrageergebnisse

### 2.1 DMS-Einsatz

Ein Zusammenhang zwischen der Anzahl der Beschäftigten und dem DMS-Einsatz einer Verwaltung lässt sich nicht feststellen. Dagegen existiert ein Zusammenhang zwischen dem Umfang des DMS-Einsatzes (Anteil an Arbeitsplätzen mit DMS-Zugang) und der Verwaltungsebene.

62,2 % der Umfrageteilnehmer setzen bisher an weniger als einem Zehntel der Arbeitsplätze ein DMS ein. Mit 79 % sind die Kommunalverwaltungen in der Gruppe mit weniger als 10 % DMS-Einsatz überrepräsentiert. Sie stehen bei der Einführung des DMS noch am Anfang. Auch in der Bundesverwaltung ist der DMS-Einsatz noch wenig verbreitet. 63 % der befragten Bundesbehörden haben weniger als ein Zehntel der Arbeitsplätze mit einem DMS-Zugang ausgestattet.

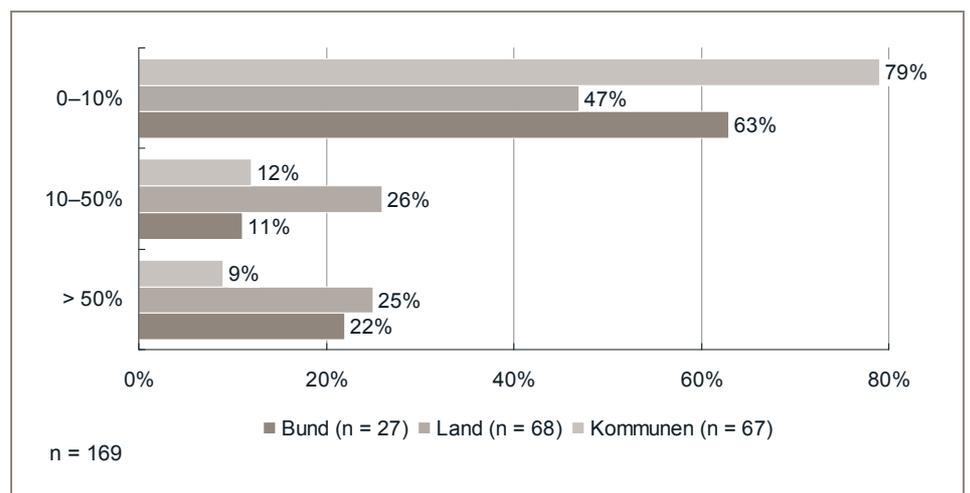


Abb. 4 DMS-Einsatz nach Verwaltungsebenen

Auffallend ist, dass nur wenige Behörden in der Bundesverwaltung eine mittlere DMS-Ausstattung von 10 bis 50 % aufweisen. Die teilnehmenden Bundesbehörden haben zum großen Teil entweder keine bzw. eine sehr geringe DMS-Ausstattung oder einen hohen Einführungsgrad mit DMS-Zugang an mehr als 50 % der Arbeitsplätze. Dies lässt den Schluss zu, dass die Projekte zur DMS-Einführung im Bundesbereich entweder abgeschlossen sind bzw. kurz vor der Vollendung stehen (hoher DMS-Ein-

führungsgrad) oder noch nicht bzw. nur als Pilotprojekte angelaufen sind (kein oder nur sehr geringer DMS-Einführungsgrad).

Die Verwaltungen, die bisher nur in einzelnen Bereichen ein DMS einsetzen, geben zu 65,4 % an, dass sie sich noch in der Laufzeit des Einführungsprojekts befinden bzw. dass ein DMS erst in Zukunft eingeführt werden soll. Nur etwa einem Fünftel (19,8 %) dieser Verwaltungen ist der Aufwand für eine weitere Einführung im Vergleich zum erwarteten Nutzen zu hoch.

Als andere Gründe dafür, dass der DMS-Einsatz nicht auf weitere Bereiche ausgedehnt wird, werden fehlender interner Druck (23,5 %), eine Blockadehaltung des Personalrats (6,2 %), die unklare Rechtslage (8,6 %) sowie die bewusste Beschränkung des Einsatzes auf ausgewählte Bereiche (11,3 %) genannt.

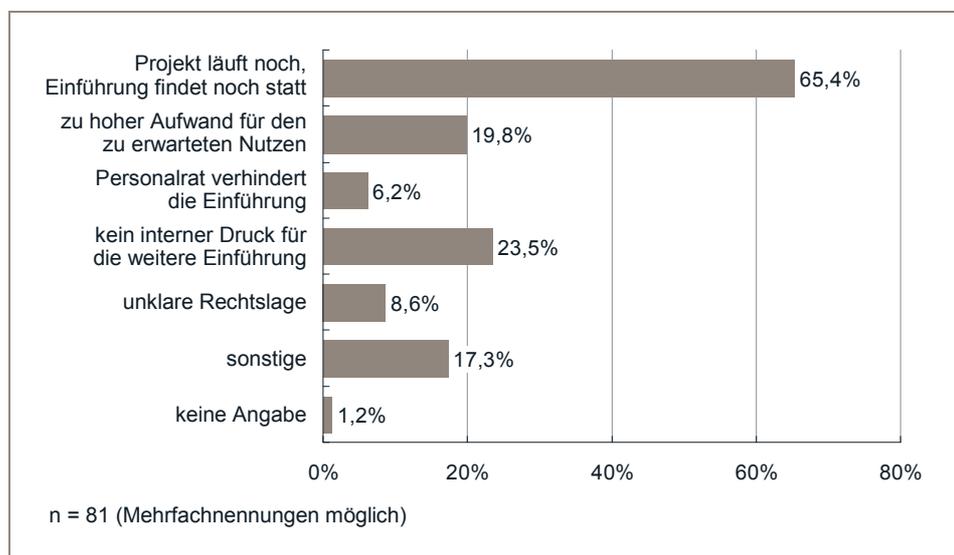


Abb. 5 Gründe für einen DMS-Einsatz nur in einzelnen Bereichen

Ein Großteil der Verwaltungen (65,1 %), die bisher kein DMS einsetzen, will künftig mit der Einführung beginnen. Auf Ebene der Landesverwaltung (15 von 21) und der Kommunalverwaltung (20 von 28) planen dies jeweils 71 %. Von den 14 befragten Bundesverwaltungen haben nur sechs (43 %) entsprechende Pläne. In den kommenden Jahren werden also verstärkt Landes- und Kommunalverwaltungen die DMS-Einführung vorantreiben. Trotz ihrer einstigen Vorreiterrolle dürfte die Bundesverwaltung zukünftig die Verwaltungsebene mit dem geringsten DMS-Einführungsgrad sein.

Verwaltungen, die sich gegen eine DMS-Einführung entschieden haben, begründen dies mit zu hohem personellem (31,7 %) oder monetärem Aufwand (28,6 %). Hier ist im Einzelfall zu hinterfragen, ob in diese Entscheidungen auch Annahmen über zukünftige Ressourceneinsparungen durch medienbruchfreie Prozessbearbeitung sowie über die mögliche Reduktion der Transport-, Liege- und Recherchezeiten von Akten und Vorgängen eingeflossen sind.

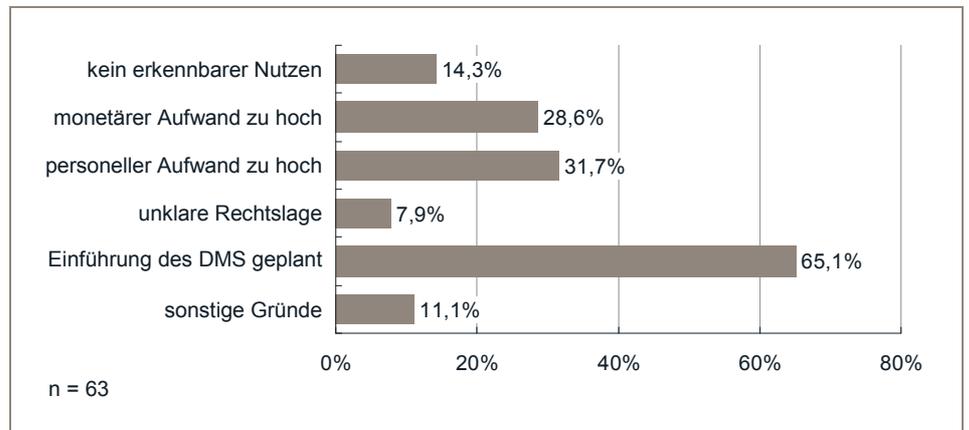


Abb. 6 Gründe dafür, dass bisher kein DMS eingesetzt wird

### Zusammenfassende Wertung der Angaben zum DMS-Einsatz

War einstmals die Bundesverwaltung Treiber der Einführung von DMS – nicht zuletzt durch die Anstrengungen im Rahmen der Initiative BundOnline2005 –, so ist mittlerweile der Einsatz von DMS in den Landesverwaltungen am weitesten verbreitet. In den Kommunen scheint das Thema an Bedeutung zu gewinnen, allerdings stehen die meisten Kommunen noch am Anfang ihrer Bemühungen. Die Kommunal- und Landesverwaltungen, die bisher kein DMS eingeführt haben, beabsichtigen mehrheitlich, dies zu tun.

In der Bundesverwaltung scheint das Interesse an diesem Thema aktuell geringer als in den Kommunal- und Landesverwaltungen zu sein. So plant nur ein kleiner Prozentsatz der Bundesbehörden ohne DMS dessen Einführung. Auch der Anteil der Bundesbehörden, die sich augenscheinlich aktuell in der hausweiten DMS-Einführung befinden (Behörden mit 10 bis 50 % DMS-Ausstattung), ist kleiner als der der Landes- und Kommunalbehörden.

## 2.2 Einsatz DOMEA-zertifizierter Verfahren

DOMEA-zertifizierte Produkte werden in 62,3 % der Verwaltungen eingesetzt. 35,8 % der Umfrageteilnehmer setzen andere Verfahren ein und 1,9 % machen diesbezüglich keine Angabe.

Obwohl DOMEA von der Bundesverwaltung konzipiert wurde und die Zertifizierung der Systemanbieter durch die Bundesverwaltung erfolgt, finden DOMEA-zertifizierte Produkte nur in 50 % der Bundesbehörden mit DMS-Einsatz Anwendung. Auch in der Kommunalverwaltung werden zu etwa gleichen Teilen DOMEA-zertifizierte und andere Verfahren eingesetzt. Die Ursache ist möglicherweise, dass das DOMEA-Konzept ursprünglich nicht auf die Kommunalverwaltung ausgerichtet war und sich für den kommunalen Markt spezifische DMS-Nischenanbieter etabliert haben. Dagegen setzen fast 80 % der Landesbehörden DOMEA-zertifizierte Produkte ein. Dies ist darauf zurückzuführen, dass in vielen Bundesländern landeseinheitliche Systeme eingeführt werden und im Beschaffungsprozess zumeist DOMEA-zertifizierte Verfahren ausgewählt wurden.

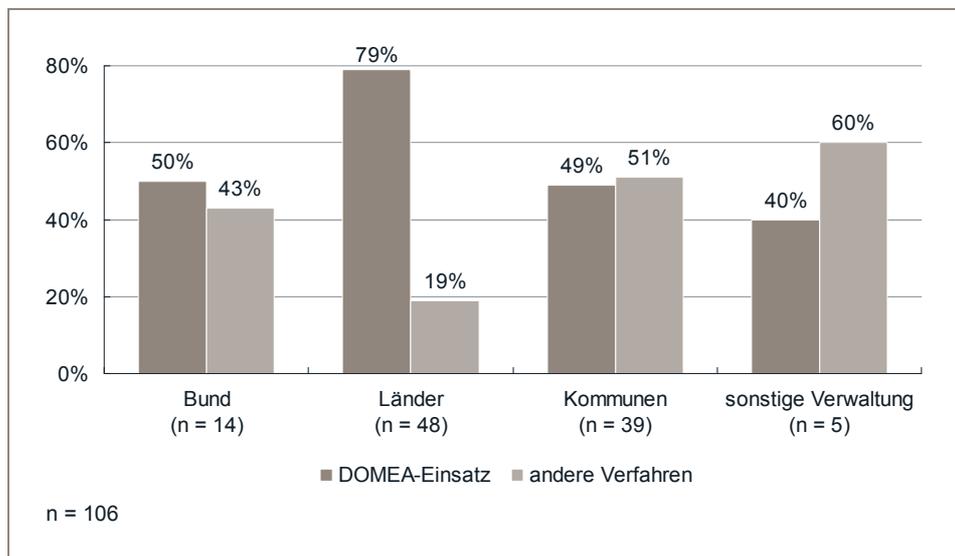


Abb. 7 Einsatz von DOMEA-zertifizierten und anderen DMS nach Verwaltungsebenen

Als Grund für den Einsatz eines nicht-DOMEA-zertifizierten DMS nennen die meisten befragten Kommunalverwaltungen (45 %) den geringen Bekanntheitsgrad der DOMEA-zertifizierten Produkte zum Einführungszeitpunkt.

Von den Bundesbehörden begründen 43 % den Verzicht auf DOMEA-zertifizierte Produkte damit, dass diese zu komplex seien. Ebenfalls 43 % geben an, dass diese Produkte nicht die benötigten Anforderungen erfüllen.

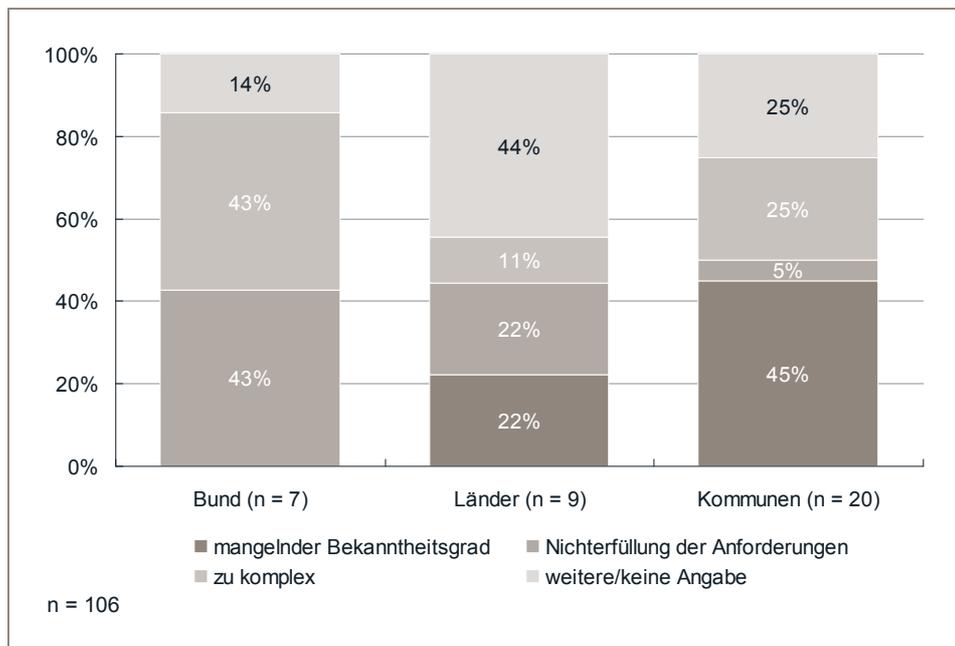


Abb. 8 Begründungen für die Entscheidung gegen ein DOMEA-zertifiziertes Verfahren

### Zusammenfassende Wertung der Angaben zum Einsatz DOMEA-zertifizierter Verfahren

Die Mehrheit der befragten Verwaltungen setzt DOMEA-zertifizierte Produkte ein. Auffallend ist, dass deren Einsatz in den Landesverwaltungen überwiegt, während er in der Bundes- und Kommunalverwaltung nur je 50 % erreicht. Dies überrascht zumindest insofern, als die Anforderungen an die Produkte im Rahmen der DOMEA-Zertifizierung vornehmlich aus Sicht der Bedürfnisse der Bundes- und Landesverwaltungen definiert wurden. Scheinbar erfüllt trotzdem ein Großteil der zertifizierten Produkte nicht die Bedürfnisse der Bundesverwaltung.

Interessant hierbei ist, dass sich Bundesverwaltungen zu gleichen Teilen wegen unzureichender Erfüllung der Anforderungen und wegen zu hoher Komplexität gegen DOMEA-zertifizierte Produkte entschieden haben. Im Zuge der aktuell stattfindenden Überarbeitung des DOMEA-Konzeptes wäre zu analysieren,

- welche Anforderungen der Verwaltungen bisher nicht durch DOMEA-zertifizierte Produkte erfüllt werden sowie
- welche bisher im DOMEA-Anforderungskatalog formulierten Anforderungen zu einer unnötigen Komplexität der Produkte führen.

## 2.3 Anpassung der Regelwerke im Zuge der DMS-Einführung

Bei der Einführung von DMS müssen die internen organisatorischen Regeln an den DMS-Einsatz angepasst werden. Erforderlich für die Standardisierung der Schriftgutverwaltung und einen einheitlichen Einsatz des DMS in einer Behörde sind die Definition und Umsetzung einheitlicher Aktenpläne, einer einheitlichen Geschäftszeichensyntax sowie klarer Aktenstrukturen. Somit stellen diese Maßnahmen auch die Grundlage für den Aufbau behördenweiter Informations- und Wissensstrukturen dar.

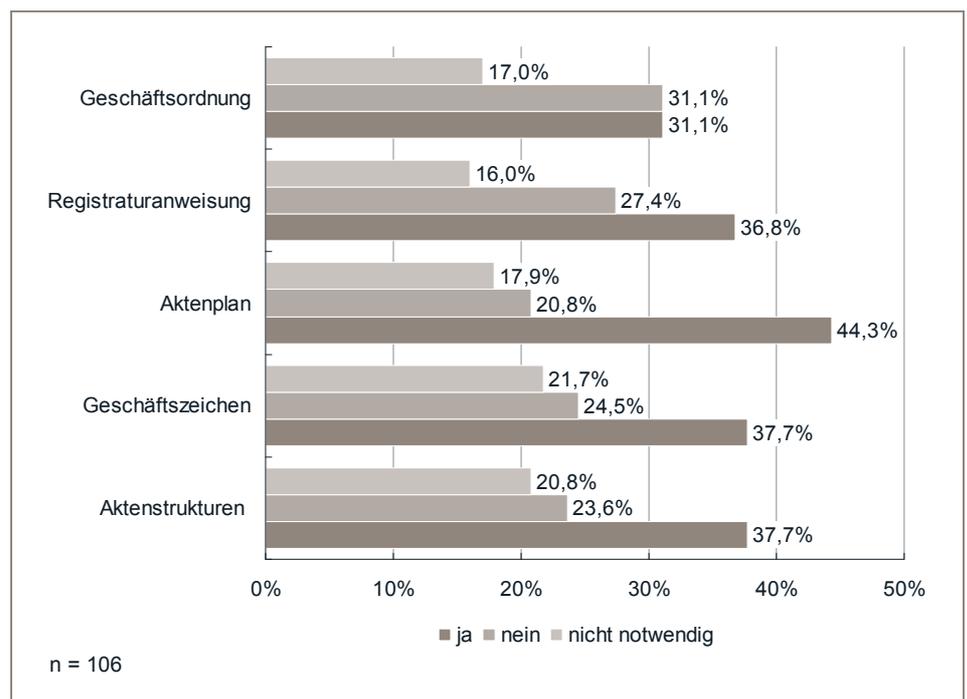


Abb. 9 Im Rahmen der DMS-Einführung wurde die Schriftgutverwaltung durch Anpassung von Regelwerken auf den IT-Einsatz ausgerichtet

Bei den Antworten auf die Frage, welche organisatorischen Regelwerke durch die einzelnen Verwaltungsebenen im Zuge der DMS-Einführung überarbeitet wurden, fällt auf, dass Landesverwaltungen die meisten Anpassungen vorgenommen und sich bewusst mit der Anpassung der Schriftgutverwaltung auseinandergesetzt haben. Bundes- und Kommunalverwaltungen haben der Anpassung der Regelwerke weniger Gewicht beigemessen.

Dieses unterschiedliche Vorgehen von Landesverwaltungen einerseits und Bundes- sowie Kommunalverwaltungen andererseits dürfte an den unterschiedlichen Einführungsansätzen in den Verwaltungsebenen liegen. Während Kommunen und Bundesverwaltungen sich meist isoliert – gegebenenfalls unterstützt durch einzelne Einrichtungen wie zum Beispiel der Bundesstelle für Informationstechnik – dem Thema DMS-Einführung widmen, haben viele Landesverwaltungen Kompetenzzentren oder federführende Ressorts bestimmt, die eine landesweite und einheitliche Einführung des DMS betreiben. Durch diesen zentralisierten Wissensaufbau und die darauffolgende Einführungsunterstützung können wesentliche konzeptionelle Grundlagen einer DMS-Einführung besser auf andere Behörden übertragen und Synergieeffekte genutzt werden.

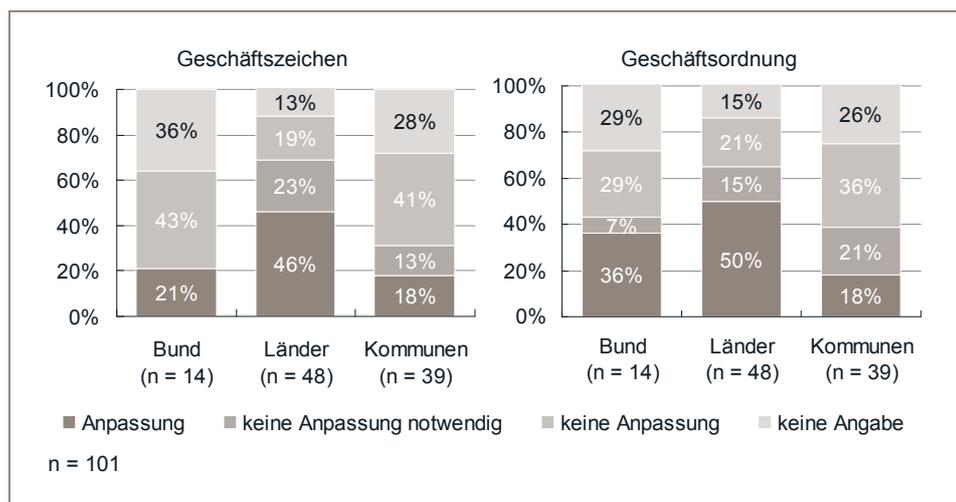


Abb. 10 Häufigkeit von Anpassungen der Regelwerke im Zuge der DMS-Einführung an den Beispielen Geschäftsordnung und Geschäftszeichen

Intensiver als mit den Regelwerken befassen sich die befragten Teilnehmer mit der notwendigen Ausrichtung der organisatorischen Abläufe auf die DMS-Einführung. Großen Wert im Vergleich zu den anderen Verwaltungsebenen legt die Bundesverwaltung auf vollständige Prozessanalysen und die Ausrichtung der organisatorischen Abläufe auf den IT-Einsatz.

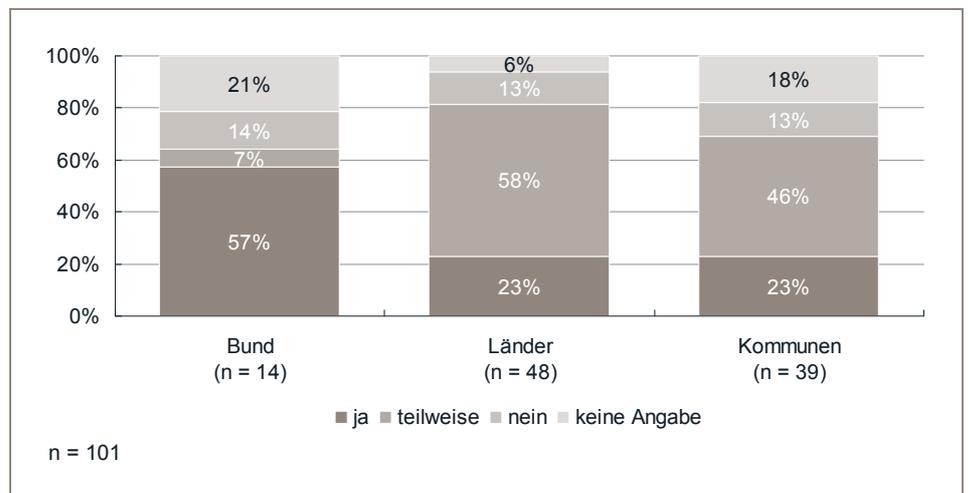


Abb. 11 Durchführung einer Prozessanalyse und Ausrichtung der organisatorischen Abläufe auf den IT-Einsatz nach Verwaltungsebenen

#### Zusammenfassende Wertung der Angaben zur Anpassung der Regelwerke im Zuge der DMS-Einführung

In vielen Verwaltungen, die noch konventionell papiergebunden arbeiten, zeigt die Schriftgutverwaltung ein heterogenes Bild: Aktenpläne sind veraltet oder werden nicht bzw. nur in einzelnen Bereichen genutzt. Das Schriftgut ist uneinheitlich strukturiert. Geschäftszeichen werden nicht oder uneinheitlich verwendet. Die Aufbewahrungsdauer von Schriftgut wird von den Kapazitäten der Lager- und Kellerräume bestimmt.

Eine Definition grundlegender Standards der Schriftgutverwaltung bildet jedoch den unverzichtbaren Rahmen einer über den Einsatz in einzelnen Bereichen hinausgehenden Verwendung von DMS.

Vor diesem Hintergrund geben erstaunlich wenige der befragten Verwaltungen an, dass sie ihre Regelwerke entsprechend anpassen. Dies deutet erstens darauf hin, dass DMS-Projekte in vielen Verwaltungen nach wie vor vornehmlich als IT-Projekte verstanden und häufig federführend von IT-Organisationseinheiten betrieben werden. Zweitens könnte es auf einen Mangel an standardisierten Vorgehensweisen und an Einführungsunterstützung hindeuten. Die Anpassung der organisatorischen Rahmenbedingungen an den DMS-Einsatz ist der zentrale Erfolgsfaktor von DMS-Projekten und erfordert die Einbindung der Organisationsreferate. Zudem gilt es, grundlegendes Wissen über die Schriftgutverwaltung, das in großen Teilen der Belegschaften nicht oder nicht mehr vorhanden ist, wieder in den Verwaltungen zu verankern.

## 2.4 Elektronische Akten

49,1 % der DMS-Nutzer geben an, dass die elektronische Akte in ihrem Haus auch die führende Akte ist. In 66 % der befragten Verwaltungen enthalten die elektronischen Akten alle aktenrelevanten Schriftstücke mit Ausnahme nicht scannbarer Dokumente. Das bedeutet, dass in zahlreichen Behörden trotz vollständiger elektronischer Akte die Papierakte noch das führende Medium ist.

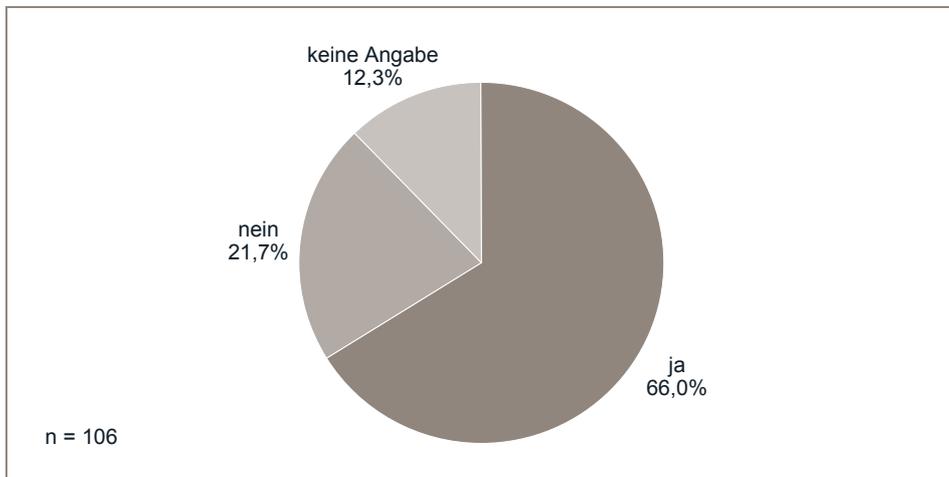


Abb. 12 Die elektronischen Akten enthalten alle aktenrelevanten Schriftstücke (mit Ausnahme nicht scannbarer Dokumente)

Folglich wird ein großer Teil der Dokumente in elektronischen Akten auch in Papierform (und somit redundant) aufbewahrt. Nur in 23 % der befragten Behörden werden eingehende und gescannte Dokumente ausschließlich in der elektronischen Akte aufbewahrt.

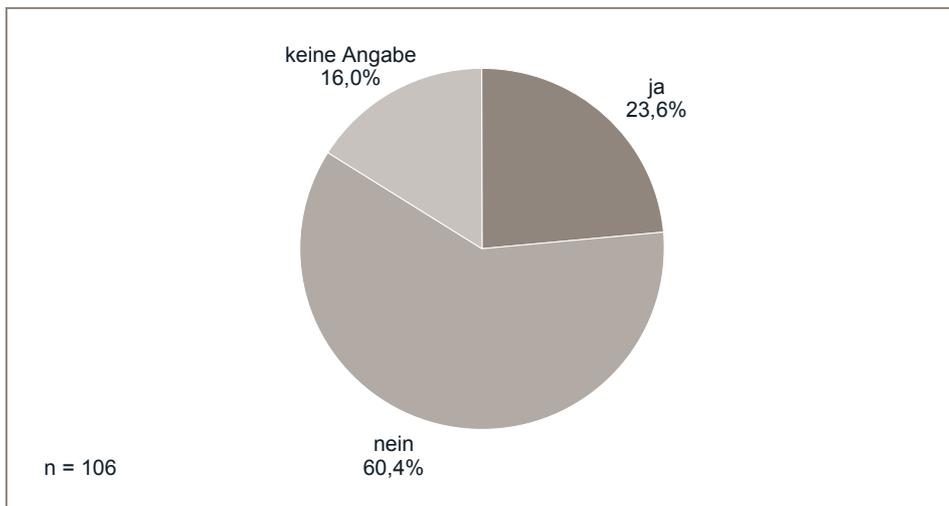


Abb. 13 Eingehende und gescannte Dokumente werden ausschließlich in der elektronischen Akte aufbewahrt

Auch in Verwaltungen, in denen die elektronische Akte die führende Akte ist, werden gescannte Dokumente parallel in Papierform abgelegt.

Der Grund für diese Mehrfachablage lässt sich aus den Antworten auf eine weitere Frage ableiten. Es wurde gefragt, an welchen Grundlagen sich die Teilnehmer orientierten, als sie den Umgang mit Papierschriftstücken nach dem Scanvorgang festlegten.

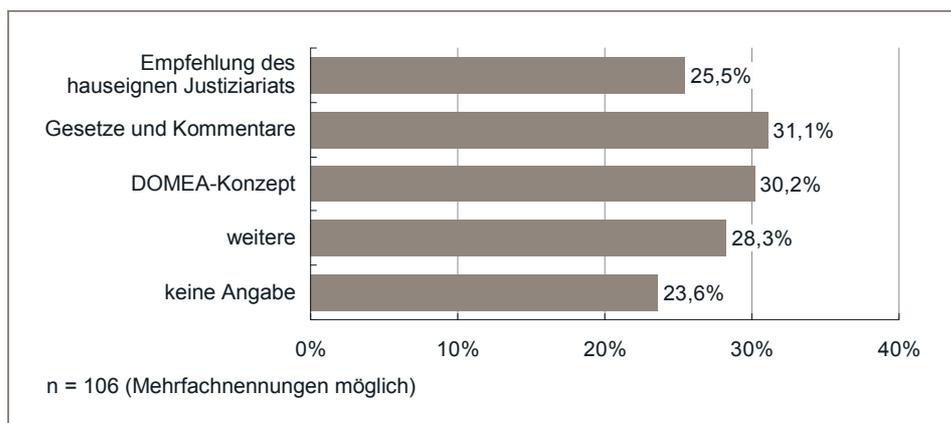


Abb. 14 Grundlagen, auf denen über Aufbewahrung oder Vernichtung von Papierschriftstücken nach dem Scanvorgang entschieden wurde

Aus der Vielfalt und Streuung der Antworten – im Feld zur freien Texteingabe unter „weitere“ wurden sieben abweichende Möglichkeiten angegeben – kann geschlossen werden, dass die Entscheidung zwischen Vernichtung und Aufbewahrung sehr individuell getroffen wird und dass in den Verwaltungen große Unsicherheit über den Umgang mit gescanntem Schriftgut herrscht.

Sechs befragte Verwaltungseinrichtungen geben beispielsweise an, dass sie sich bei der Festlegung des Umgangs mit Papierschriftstücken nach dem Scanvorgang an den Vorgaben der Hausleitung, des Projektleiters oder des zuständigen Fachdienstes orientieren. Drei weitere Verwaltungen haben aufgrund der Erfahrungen anderer Behörden entschieden. Andere orientieren sich am DOMEA-Konzept oder an den Empfehlungen der haus-eigenen Justiziarate. Ein einheitliches Vorgehen bei der Aufbewahrung des gescannten Schriftguts gibt es nicht. Insgesamt lässt sich auf Basis der Angaben feststellen, dass erhebliche Unsicherheit bezüglich der einschlägigen Rechtsgrundlagen und sonstigen Vorschriften herrscht.

#### Zusammenfassende Wertung der Angaben zu elektronischen Akten

Die Antworten zeigen das Dilemma vieler Verwaltungen. Einerseits kann bereits durchgehend auf elektronische Akten zugegriffen werden, andererseits herrscht Unsicherheit darüber, in welchem Umfang weiterhin Papierschriftstücke aufzubewahren sind. Dies zeigen insbesondere die Antworten auf die Frage, auf welcher Grundlage der Umgang mit Papierschriftstücken nach dem Scanvorgang festgelegt wird. Da es keine eindeutigen Regelungen gibt, ziehen die Behörden zur Lösungsfindung viele Quellen heran – von der Hausleitung über Lösungsansätze anderer Verwaltungen bis hin zu bestehenden Gesetzen und Kommentaren.

## 2.5 Revisionssichere Speicherung

Die revisionssichere Speicherung ist den befragten Verwaltungen sehr wichtig. Die genaue Bedeutung des Begriffs und die damit einhergehenden Anforderungen scheinen jedoch weitgehend unbekannt zu sein. Der Anteil der Befragten, der zur Frage nach dem Stellenwert keine Angaben machte, ist auffallend hoch.

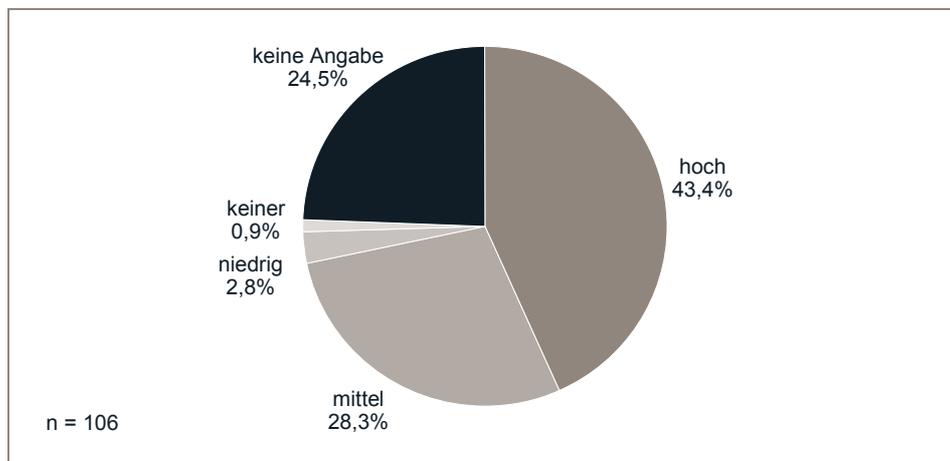


Abb. 15 Stellenwert der revisions sicheren Speicherung von elektronischem Schriftgut in den Behörden

Insbesondere Bundes- und Landesverwaltungen legen großen Wert auf revisions sichere Speicherung. Die Kommunalverwaltungen, die sich überwiegend noch im Prozess der Einführung eines DMS befinden, scheinen sich mit diesem Thema vergleichsweise wenig auseinandergesetzt zu haben.

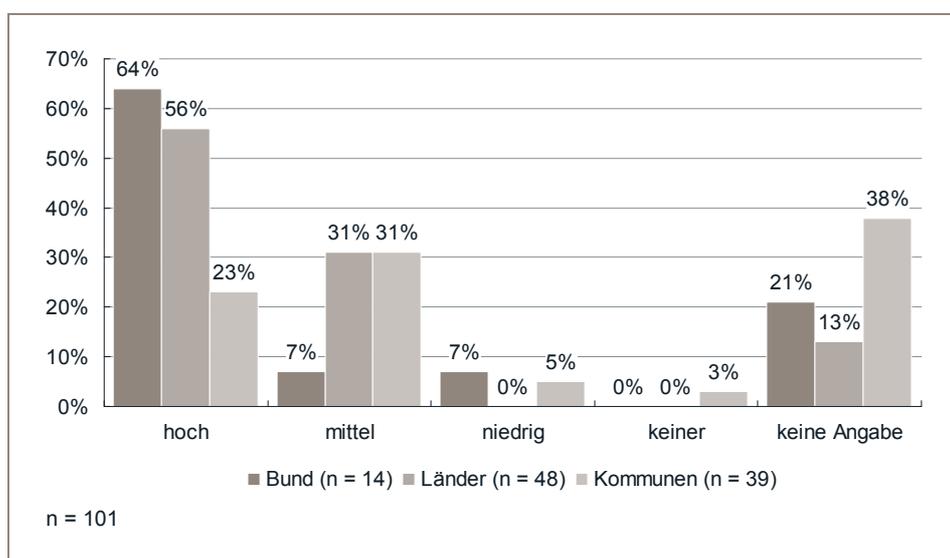


Abb. 16 Stellenwert der revisions sicheren Speicherung nach Verwaltungsebenen

Über 60 % der befragten DMS-Nutzer sind der Auffassung, dass es für das eingesetzte DMS in der jeweils vorgenommenen Anpassung eine Dokumentation gibt. Es ist jedoch zu vermuten, dass damit meist die allgemeine Dokumentation des jeweiligen DMS-Verfahrens gemeint ist (Benutzerhandbuch des Systemherstellers). Interessant wäre aber zu erfahren, inwieweit individualisierte, vollständige, an hausinterne Spezifika und Umsetzungen angepasste Dokumentationen vorliegen. Die Praxiserfahrungen von PwC und IMTB zeigen, dass keinesfalls 61 % der Behörden über derartige Dokumentation verfügen.

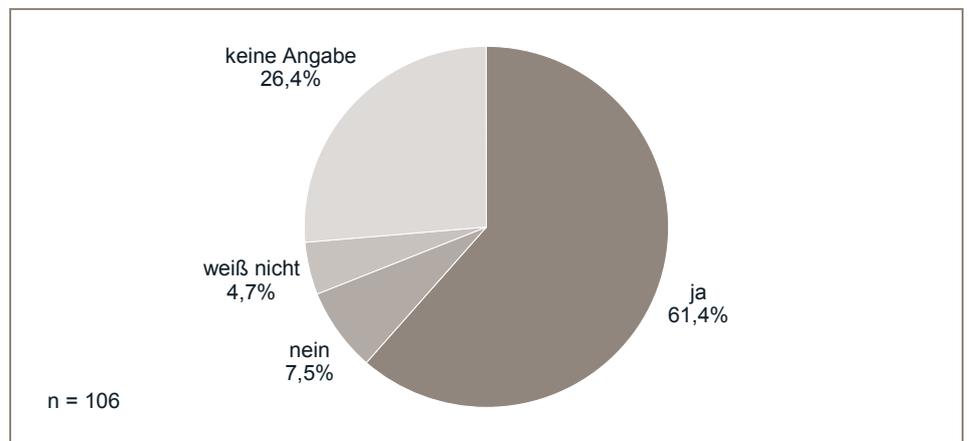


Abb. 17 Für das eingesetzte DMS in der von Ihnen vorgenommenen Anpassung existiert eine Dokumentation

41,5 % der Befragten sind auch der Ansicht, dass für das in ihrer Behörde eingesetzte DMS eine Herstellererklärung bzw. ein Zertifikat vorliegt, das die revisions sichere Speicherung von Dokumenten bestätigt.

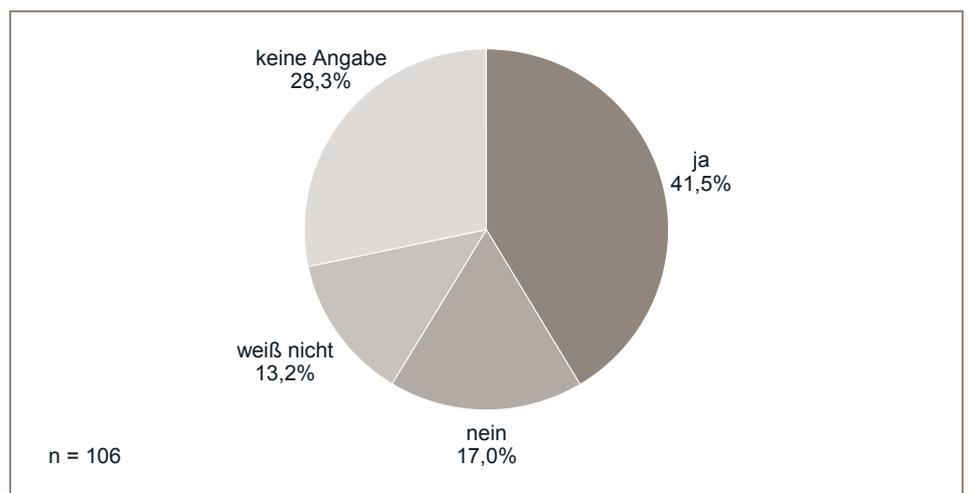


Abb. 18 Für das eingesetzte DMS liegt eine Herstellererklärung bzw. ein Zertifikat vor, das die revisions sichere Speicherung von Dokumenten bestätigt

Eine Herstellererklärung kann zwar ein Indikator für Revisions sicherheit sein, reicht aber keinesfalls aus, diese sicherzustellen, da in ihr die konkrete Ausgestaltung des Systems in der jeweiligen Verwaltung nicht betrachtet wird.

Zudem geben nur 28,3 % der Umfrageteilnehmer an, dass es in ihrer Behörde eine vollständige Dokumentation der organisatorischen Vorgaben für die Nutzung des DMS gibt. Eine solche Dokumentation ist jedoch Voraussetzung für die Etablierung revisions sicherer Prozesse und somit einer revisions sicheren Datenspeicherung.

Die irr t umlichen Annahmen über das Vorliegen und die Bedeutung von Dokumentationen und Hersteller erklä rungen sind ein weiteres Indiz für Unsicherheiten über die Begriffsdefinitionen und die bestehenden Normen.

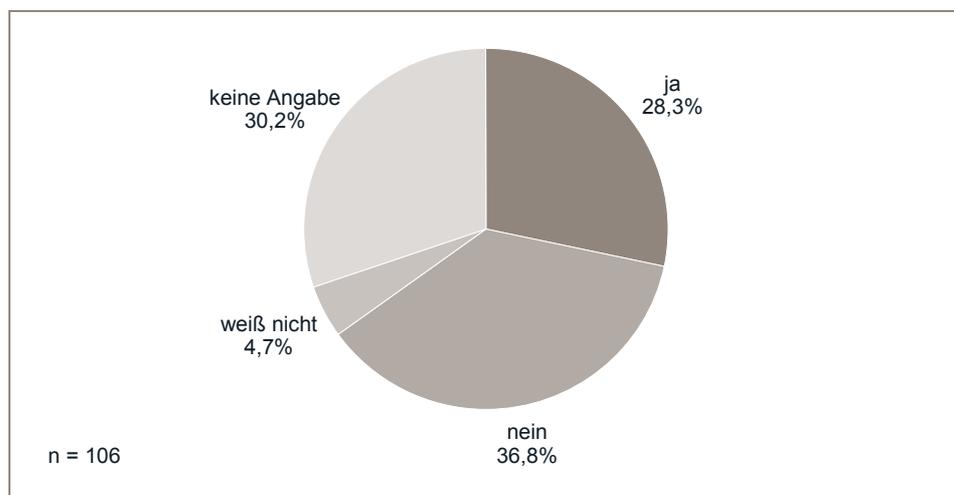


Abb. 19 Es existiert eine vollständige Dokumentation der organisatorischen Vorgaben für die Nutzung des Systems

Die Frage, ob eine zentrale Instanz in der Behörde die Einhaltung der definierten Regeln überprüft, beantworten 25,5 % der Teilnehmer mit nein. 31,1 % machen keine Angabe. Es liegt nahe, dass Unklarheiten über die Notwendigkeit und organisatorische Eingliederung einer zentralen Instanz bestehen.

Es gilt also, eine inhaltliche Debatte über die Anforderungen an eine solche zentrale Instanz zu führen und die Prüfinhalte einheitlich zu definieren. Diese Festlegungen sind unabdingbar für eine transparente und nachvollziehbare Aktenführung sowie deren Prüfung.

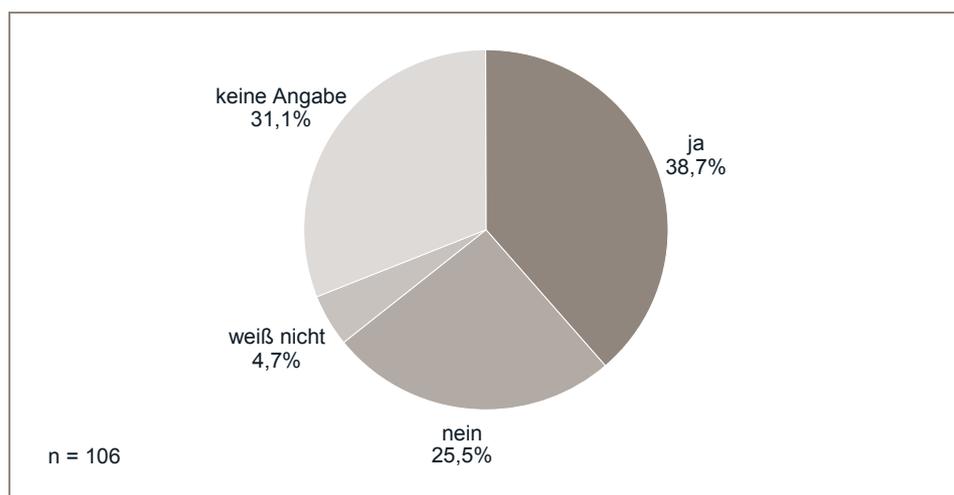


Abb. 20 Es existiert eine zentrale Instanz, die die Einhaltung der organisatorischen Vorgaben zur Nutzung des eingesetzten Systems überprüft

Nur 12,3 % der teilnehmenden Verwaltungen haben die elektronische Aktenhaltung durch einen Dritten begutachten bzw. zertifizieren lassen. Selbst die Teilnehmer, welche die eingehenden und gescannten Dokumente ausschließlich in einer elektronischen Akte aufbewahren, haben nur zur Hälfte eine Begutachtung oder Zertifizierung durch einen Dritten durchführen lassen.

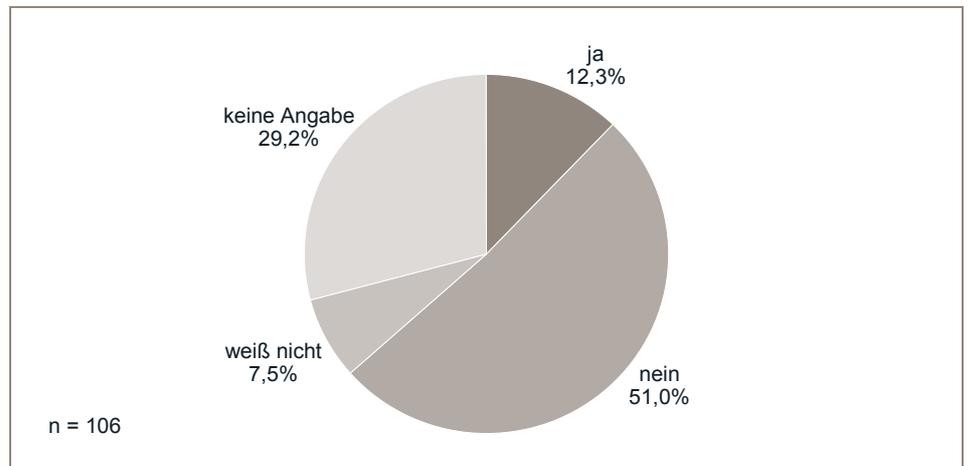


Abb. 21 Die elektronische Aktenhaltung wurde von einem Dritten begutachtet bzw. zertifiziert

### Zusammenfassende Wertung der Angaben zur revisions sicheren Speicherung

Für die befragten Verwaltungen ist die revisions sichere Speicherung ein wichtiges Thema. Allerdings scheint es wenig Klarheit über die damit einhergehenden Anforderungen zu geben.

Bei den Fragen zu Voraussetzungen für eine revisions sichere Speicherung von Dokumenten entspricht das Antwortverhalten nicht den Erwartungen. Angeblich erfüllen große Gruppen der Teilnehmer die Voraussetzungen:

- 61,3 % geben an, dass für das DMS eine angepasste Dokumentation existiert.
- 46,2 % geben an, dass diese Dokumentation kontinuierlich gepflegt wird.
- 41,5 % geben an, dass für das DMS eine Herstellererklärung bzw. ein Zertifikat vorliegt, das die revisions sichere Speicherung von Dokumenten bestätigt.
- 38,7 % geben an, dass eine zentrale Instanz in der jeweiligen Behörde die Einhaltung der definierten Regeln für den DMS-Einsatz überprüft.

Diese Antworten passen nicht zu den in den vergangenen Jahren gesammelten Erfahrungen. Augenscheinlich werden keine ausgeprägten Anstrengungen zur Dokumentation der im Einsatz befindlichen Systeme unternommen. Daher liegt der Schluss nahe, dass die Fragen teilweise missverstanden wurden. So sind mit den in der Studie abgefragten Dokumentationen und Herstellerklärungen nicht allgemeine Beschreibungen der Grundkonfiguration eines Systems gemeint, sondern Dokumentationen der konkreten Ausprägung des Systems in der jeweiligen Behörde.

Eine trennscharfe und eindeutige Definition des Begriffs Revisions sicherheit ist im öffentlichen Sektor bisher nicht verankert. Die festgestellten Unsicherheiten und Umsetzungslücken resultieren weitgehend aus Wissenslücken. Derzeit gibt es keine verwaltungsspezifischen Best-Practice-Ansätze. Die einerseits in diesem Abschnitt aufgeführten Widersprüche im Antwortverhalten und andererseits die heterogenen Antworten auf Fragen nach rechtlichen Grundlagen/ Regelungen (siehe Erläuterungen zu Abbildung 14) sind lediglich als logische Konsequenz dieses Umstands zu betrachten. Erfahrungswerte existieren aber in der Industrie. Es gilt folglich, aufbauend auf den Erfahrungen und definierten Regeln der Industrie, ein verlässliches Gesamtsystem (DMS, organisatorische Vorgaben, Prüfmechanismen etc. zu entwickeln. Erfolgsentscheidend ist, dass ein solches Gesamtsystem einheitlich bereitgestellt und implementiert wird. Die revisions sichere Speicherung ist die Voraussetzung für die Einführung eines DMS: Nur mit verbindlichen Regelwerken, Hilfestellungen und qualifizierten Prüfinstanzen ist eine ordnungsgemäße Schriftgutverwaltung möglich.

Ein zentraler Erfolgsfaktor für den Einsatz von DMS in der öffentlichen Verwaltung ist die Schaffung rechtlicher Klarheit über den Umgang mit elektronischen Akten und die revisions sichere Speicherung sowie ein Konsens über die damit einhergehenden Anforderungen. Im Kapitel D werden entsprechende Handlungsempfehlungen gegeben.

## 2.6 Wesentliche Ergebnisse und Fazit

Auf Grundlage der Umfrageergebnisse lässt sich als erstes positives Fazit festhalten, dass die Einführung der elektronischen Aktenführung für den Großteil der Kommunalverwaltung ein Thema ist oder ein Thema sein wird. Darüber hinaus konnten wir folgende wesentliche Erkenntnisse zusammentragen:

1. Die starke Beteiligung an der Studie lässt auf ein ausgeprägtes Interesse am Thema „revisionssichere Speicherung“ schließen und belegt dessen Aktualität und Relevanz.
2. DMS-Verfahren werden bisher zumeist in wenigen Einzelbereichen der Verwaltungen eingesetzt. Insbesondere Kommunalverwaltungen stehen weitgehend noch am Anfang der DMS-Einführung.
3. Kommunalverwaltungen werden in den kommenden Jahren verstärkt DMS einführen. Landesbehörden werden den DMS-Ausbau weiterhin vorantreiben. Auf Ebene der Bundesverwaltung scheint das Thema eher zu ruhen.
4. DOMEA-zertifizierte Produkte werden in Kommunalverwaltungen aufgrund ihres geringen Bekanntheitsgrades weniger als in Landesbehörden eingesetzt.
5. Bundesbehörden, die keine DOMEA-zertifizierten Produkte einsetzen, sind fast durchgängig der Ansicht, dass diese ihre Anforderungen nicht erfüllen oder zu komplex sind.
6. Aufgrund des in der Vergangenheit zentralisiert organisierten Wissenstransfers auf Landesebene haben sich Landesbehörden bewusst mit der Anpassung der Schriftgutverwaltung auseinandergesetzt.
7. Infolge erheblicher Unsicherheiten bezüglich der einschlägigen Rechtsgrundlagen und sonstigen Vorschriften wird ein großer Teil der Dokumente sowohl in Papierform als auch elektronisch (und somit redundant) aufbewahrt.
8. Es gibt offenkundig Verständnisprobleme hinsichtlich der Bedeutung des Begriffs „Revisionssicherheit“ bzw. der entsprechenden Anforderungen und Normen.
9. Allgemeingültige Definitionen und Normen des öffentlichen Rechts für die revisionssichere Speicherung von elektronischen Dokumenten fehlen bisher. Zur Behebung der oben genannten Verständnisprobleme müssen die rechtlichen Regelungen zeitnah konkretisiert werden.
10. Es gilt, eine inhaltliche Debatte über die Anforderungen an eine zentrale Prüfinstanz zu führen und Prüfinhalte einheitlich zu definieren.

## C Bestehende Regelungen zur Revisionssicherheit in der Privatwirtschaft und in der öffentlichen Verwaltung

Die Umfrage zeigt, dass es in der öffentlichen Verwaltung Unklarheiten über die Definition der revisionssicheren elektronischen Aktenspeicherung sowie rechtliche Ungewissheiten über die elektronische Aktenführung gibt. Wegen unzureichenden Vorgaben haben verschiedene Verwaltungen individuelle Lösungen für das elektronische Verwaltungshandeln entwickelt und damit heterogene Vorgehensweisen in den Behörden etabliert. Dies wiederum führt zu Problemen bei der revisionssicheren Aktenführung, woraus sich diverse Hindernisse vor allem rechtlicher Art ergeben, die das elektronische Verwaltungshandeln erschweren.

Im Anschluss soll – vorbereitend für die Handlungsempfehlungen in Kapitel D – zunächst die rechtliche Problematik dargestellt werden. Dabei werden die Rahmenbedingungen für die Revisionssicherheit der Aktenspeicherung im Privatrecht und im öffentlichen Recht einander gegenübergestellt. Insbesondere im öffentlichen Recht soll dabei auch auf Regelungslücken aufmerksam gemacht werden, die zu Unklarheiten im Umgang mit der revisionssicheren elektronischen Akte führen.

### 1 Regelungen für die Privatwirtschaft

Die Dichte der Regelungen zur revisionssicheren Speicherung von Daten im privatwirtschaftlichen Bereich ist national wie international hoch. Für den Betrieb eines revisionssicheren DMS gelten in Deutschland vor allem Regeln des kaufmännischen Rechts, das dem Privatrecht zuzuordnen ist. Insbesondere sind dies die Rechtsnormen des HGB, der AO und der daraus abgeleiteten GoBS.

Bei den genannten Rechtsnormen handelt es sich zwar um Regeln für den kaufmännischen, steuerrechtlichen Bereich sowie für das Rechnungswesen, jedoch besagt der erste Absatz der GoBS, dass diese Regeln unmittelbar auch für DMS gelten. Hier sind also die Voraussetzungen für einen revisionssicheren Betrieb von Dokumentenmanagementlösungen sowie für die Datenspeicherung beschrieben.

#### 1.1 Handelsgesetzbuch (HGB)

Das HGB schafft mit den Paragraphen 239<sup>2</sup> und 257<sup>3</sup> den grundsätzlichen Rahmen für eine revisionssichere Datenspeicherung und ist damit maßgeblich für den Einsatz von DMS.

§ 257 HGB regelt die Aufbewahrung der Geschäftsunterlagen. § 239 HGB definiert Kriterien für die Revisionssicherheit, woraus sich alle Anforderungen an ein elektronisches Datenverarbeitungssystem ableiten lassen. Demnach müssen sich die Unternehmen an folgenden Kriterien orientieren:

---

<sup>2</sup> § 239 Führung der Handelsbücher.

<sup>3</sup> § 257 Aufbewahrung von Unterlagen. Aufbewahrungsfristen.

### Ordnungsmäßigkeit

Jedes Dokument muss gemäß den rechtlichen und organisatorischen Anforderungen behandelt und aufbewahrt werden.

### Vollständigkeit

Geschäftsvorgänge müssen frühzeitig, vollständig und richtig erfasst werden (Vorgänge und zugehörige Dokumente).

### Sicherheit des Gesamtverfahrens

Die Sicherheit muss durch regelmäßige Prüfung der Einhaltung und Umsetzung der technischen und organisatorischen Anforderungen gewährleistet werden (Verfahrenskontrollen zur Vollständigkeit und Richtigkeit). Dazu gehört auch die stetige Pflege und Anpassung der Prozessdokumentationen.

### Schutz vor Veränderung und Verfälschung

Zur Verhinderung von Manipulationen an einem Dokument müssen dessen Identität und Authentizität durch automatische Erzeugung von Protokoll- und Bearbeitungsinformationen (geordnete Darstellung der Entstehung und Abwicklung der Vorgangsbearbeitung = Protokollierung) in Verbindung mit Rollen und Zugriffsrechten gewahrt werden.

### Sicherung vor Verlust

Kein Dokument darf durch Nutzung oder Übergabe in das Archiv verloren gehen.

### Zugriffsschutz (siehe auch BDGS)

Die Verwendung der Daten darf ausschließlich berechtigten Personen möglich sein.

### Einhaltung der Aufbewahrungsfristen

Jedes Dokument darf erst nach Ablauf seiner spezifischen Aufbewahrungspflicht vernichtet oder dem Archiv übermittelt werden.

### Dokumentation des Verfahrens

Die vorgeschriebene Verfahrensdokumentation stellt einen Vorgangszusammenhang her und registriert die wesentlichen Metadaten für jedes verwaltete Objekt (z. B. Absender, Eingangsdatum, Betreff etc.).

### Nachvollziehbarkeit

Für jedes Dokument muss jede Veränderung eines Objekts bzw. der Bearbeitungsprozess eines Vorgangs vollständig nachvollziehbar sein.

### Prüfbarkeit

Die verwalteten aktenrelevanten Informationen müssen für einen sachverständigen Dritten in angemessener Zeit nachvollziehbar sein.

Diese Kriterien sind wesentlich für den Beweiswerterhalt von Dokumenten in DMS und Datenspeicherungssystemen. Folgerichtig beinhalten neben dem HGB auch die GoBS diese Prüfsteine.

## 1.2 Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)

Die rechtliche Grundlage für die Revisionssicherheit ergibt sich aus dem HGB, in dem Grundzüge wie Ordnungsmäßigkeit, Nachvollziehbarkeit, Unverfälschbarkeit und andere Vorgaben definiert sind.

Die GoBS sind das eigentliche rechtliche Konstrukt, das die Anforderungen für revisionssichere Datenverarbeitungssysteme definiert. Sie erläutern die im HGB und der AO geforderten Prüfsteine. Wie erwähnt, gelten die GoBS konkret für die Verwendung von DMS. Neben den bekannten Vektoren wie Ordnungsmäßigkeit, Nachvollziehbarkeit, Integrität und Vollständigkeit regeln die GoBS auch die Verfahrensdokumentation.

Ein wichtiger Bereich, der in den GoBS geregelt ist, ist der Umgang mit gescannten und originär elektronischen Daten. Diese Regelung beinhaltet zunächst die Pflicht, Instrumente bereitzustellen, welche die Daten auf dem Datenträger originalgetreu wiedergeben können.

Bei der Speicherung und Archivierung von originär digitalen Dokumenten muss sichergestellt werden, dass während der Speicherung keine Bearbeitung möglich ist. Bei diesen Dokumenten handelt es sich um solche, die in einem System selbst durch entsprechende Verarbeitungsschritte entstanden sind. Nach dem Digitalisierungsprozess müssen alle Dokumente unveränderbar indexiert werden. Das gespeicherte digitale Dokument kann danach ausschließlich unter dem zugeteilten Index bearbeitet und verwaltet werden. Um alle Bearbeitungsvorgänge nachvollziehen zu können, müssen sie protokolliert und mit dem Dokument abgespeichert werden. Für die Überprüfung dieser Prozesse muss das Unternehmen ein internes Kontrollsystem (IKS) installieren.

Das IKS stellt die Ordnungsmäßigkeit der Datenverarbeitungssysteme sicher. Die Konformität zu den Vorgaben (Gesetze, Verträge, unternehmensinterne Normen) soll das IKS gewährleisten und regelmäßig kontrollieren. Das Unternehmen muss die Kontrollmaßnahmen abstimmen und dokumentieren und eine klare Verantwortungsstruktur für das IKS sowie die exakte Reihenfolge der Arbeitsabläufe festlegen. Die GoBS definieren Anforderungen an das IKS und fordern Richtlinien für folgende Punkte:

- Programmierung
- Programmtests
- Programmfreigaben
- Programmänderungen
- Änderungen von Stamm- und Tabellendaten
- Zugriffs- und Zugangsverfahren
- Einsatz von Datenbanken, Betriebssystemen und Netzwerken

Die GoBS definieren auch Anforderungen an die Sicherung und Bereitstellung von elektronisch gespeicherten Daten und ergänzen die Regelungen des Bundesdatenschutzgesetzes (BDSG). Sie fordern ein Daten- und IT-Sicherheitskonzept, um die Informationen gegen Verlust zu

sichern und vor unberechtigten Veränderungen zu schützen. Letzteres erfordert Zugangskontrollen und Zugriffskontrollen. Zugangskontrollen beschränken den Zugang zu den Räumen, in denen die Datenträger gelagert werden. Zugriffskontrollen beschränken den Zugriff auf die Daten. Für die Daten muss in einem Verzeichnis festgehalten werden, wo sich der Datenträger befindet, welchen Inhalt er hat, wann sie gespeichert wurden und wann sie gelöscht werden können. Diese Kontrollen müssen regelmäßig auf Ihre Wirksamkeit überprüft werden. Für Unternehmen mit elektronischen Datenverarbeitungssystemen bedeutet das, dass sie ein dynamisches Konzept für ihre Sicherheits- und Kontrollmechanismen benötigen, da diese ständig neuen Anforderungen angepasst werden müssen.

Nachvollziehbarkeit erfordert eine Verfahrensdokumentation. Sie sollte so beschaffen sein, dass ein sachverständiger Dritter die Verfahrensbestandteile des Unternehmens bzw. des Bereichs exakt nachvollziehen kann. Nach Punkt sechs der GoBS bedeutet dies im Detail, dass Inhalt, Aufbau und Ablauf der Geschäftsverfahren abgebildet werden müssen. Insbesondere muss die Verfahrensdokumentation belegen, dass die Anforderungen für eine revisions sichere Speicherung umgesetzt wurden.

Die Stellungnahme des Instituts der Wirtschaftsprüfer (IDW) zur Rechnungslegung Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3) definiert Anforderungen für den Betrieb und Kriterien für die Prüfung eines Archivierungssystems. Es richtet sich insbesondere an Wirtschaftsprüfer, die die Ordnungsmäßigkeit eines Archivsystems entsprechend den Vorgaben aus HGB und AO prüfen.

IDW RS FAIT 3 definiert Kriterien zur Prüfung verschiedener Bereiche des Archivsystems. Die zu prüfenden Bereiche sind:

- die zur Archivierung eingesetzte IT-Infrastruktur
- die zur Archivierung eingesetzten IT-Anwendungen
- die IT-gestützten Archivierungsprozesse

Dem Wirtschaftsprüfer obliegt zu prüfen, ob der Buchführungspflichtige die Kriterien erfüllt. Er kann somit eine Entscheidung über die Ordnungsmäßigkeit (nach HGB und AO) fällen.

### 1.3 Bundesdatenschutzgesetz (BDSG)

Neben den oben aufgeführten Normen ist auch im privatwirtschaftlichen Bereich das BDSG zu beachten. Es regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Hinblick auf Datenschutz, Datensicherheit und Auswertbarkeit. Das erfordert unter anderem Sicherheitssysteme zur Benutzerverwaltung, Zugangskontrollen und -protokollierung sowie die Löschung von Dokumenten und Protokollierung der Löschung. Der Datenschutzbeauftragte sollte eingebunden werden, wenn nicht gesetzlich anders gefordert.

## 2 Regelungen für die öffentliche Verwaltung

In der öffentlichen Verwaltung gibt es deutlich weniger spezifische Regelungen für die revisionssichere Speicherung von Daten als in der Privatwirtschaft. Man muss auf die allgemeinen Vorgaben zur Schriftgutverwaltung zurückgreifen, die sich ohne spezielle Regelung im Wesentlichen aus dem Grundgesetz (Rechtsstaatsprinzip) und den Verwaltungsverfahrensgesetzen ableiten lassen. Darüber hinaus gibt es eine Reihe von Fachnormen, die die Aufbewahrung von fachspezifischem Schriftgut regeln (z. B. Sozialgesetzbuch). Diese Normen beinhalten bereits eine Reihe von Regeln zum elektronischen Verwaltungshandeln. Allerdings findet man so gut wie keine Aussagen zur revisionssicheren elektronischen Aufbewahrung von Schriftgut. Die vorhandenen Normen werden im Folgenden näher vorgestellt.

### 2.1 Grundgesetz (GG)

Für die elektronische Verwaltung sowie die elektronische Aktenführung gelten die gleichen verfassungsrechtlichen Regelungen wie für die Verwaltung allgemein. Das GG setzt mit den Artikeln 1, 19, 20 und 28 das Rechtsstaatsprinzip fest und fordert ein rechtmäßiges Handeln der öffentlichen Verwaltung. Das Rechtsstaatsprinzip begrenzt qua Recht und Gesetz die Machtausübung der Staatsgewalt und hat das Ziel, Freiheit und Gerechtigkeit zu wahren. Damit trägt die öffentliche Verwaltung eine besondere Verantwortung gegenüber dem Bürger. Das Rechtsstaatsprinzip ist durch sechs Merkmale definiert:

- Grundsatz der Gewaltenteilung
- Grundsatz der Gesetzmäßigkeit
- Gewährleistung eines effektiven Rechtsschutzes gegenüber staatlichen Hoheitsakten und im Verhältnis der Bürger untereinander
- Gebot der Rechtssicherheit und des Vertrauensschutzes
- Bestehen von Grundrechten
- Grundsatz der Verhältnismäßigkeit

Aufgrund der Forderungen nach effektivem Vertrauensschutz und Rechtssicherheit (Art. 19 Abs. 4 GG) müssen öffentliche Träger im Umgang mit Dokumenten und Daten der Bürger besondere Maßnahmen ergreifen. Dies trifft insbesondere auf die elektronische Datenverarbeitung und -speicherung zu, da Daten und Dokumente in der elektronischen Welt stärker gefährdet und manipulierbarer sind.

Aus dem Rechtsstaatsprinzip nach Art. 1 Abs. 1 und Art. 20 Abs. 3 GG kann abgeleitet werden, dass die elektronische Aktenverwaltung transparent, nachvollziehbar und kontrollierbar sein muss, um Aktenmäßigkeit und eine legale Verwaltungstätigkeit zu garantieren. Weiterhin müssen Daten und Dokumente in einem DMS der öffentlichen Verwaltung beweiswerterhaltend aufbewahrt werden. Das heißt, dass das DMS allen Anforderungen zum Schutz vor Manipulation, Missbrauch und rechtswidrigem Verhalten gerecht werden muss. Wie man im kaufmännischen Recht sieht, kann dies durch

eine Prüfung durch unabhängige Dritte sowie durch komplette und ständige Dokumentationen gewährleistet werden.

Für den öffentlichen Bereich existieren allerdings zu wenig unmittelbare Regelungen, die die geforderten Maßnahmen konkretisieren. Bei der Nutzung elektronischer Datenverarbeitung können Rechtssicherheit und Rechtsschutz nicht allein durch die Vorgaben des GG garantiert werden.

## 2.2 Verwaltungsverfahrensgesetz (VwVfG)

§ 3 a VwVfG erklärt den Umgang mit elektronischen Dokumenten für zulässig. Insbesondere werden die Verwendung des elektronischen Verwaltungsaktes (§ 37 Abs. 2 VwVfG) sowie seine Begründung und die elektronische Bekanntgabe (§ 41 Abs. 2 und 3 VwVfG) genannt. Für das elektronische Verwaltungshandeln schreibt das VwVfG bei Schriftform-erfordernis die Anwendung der elektronischen Signatur vor. Das elektro-nische Bearbeiten von Verwaltungsakten nennt das VwVfG zwar als Möglichkeit, regelt es allerdings nicht weiter. Daher erscheint es sinnvoll, das VwVfG um eine Regelung für revisions sichere Datenspeicherung in der öffentlichen Verwaltung zu ergänzen. Die Verwaltungsverfahrensgesetze der Länder orientieren sich meist an dem des Bundes.

## 2.3 Sozialgesetzbuch (SGB)

Da in Deutschland die Verwaltung im Sozialbereich einen großen Teil des Verwaltungsspektrums darstellt, wird hier kurz die Regelungstiefe des SGB betrachtet. Die Sozialversicherungsträger müssen sich bei der elektro-nischen Kommunikation und Datenverarbeitung an die Bücher des SGB halten.

Im siebten Buch des SGB IV wird für die Sozialversicherungsträger gefordert, dass alle für die öffentlich-rechtliche Verwaltungstätigkeit nötigen Unterlagen nach den dort definierten Grundsätzen ordnungsmäßiger Auf-bewahrung aufbewahrt werden. Diese Grundsätze beziehen auch viele Aspekte der Revisions sicherheit ein. Weiterhin orientiert sich das SGB in seinen Regelungen zur elektronischen Kommunikation an denen des VwVfG. In einer Klausel weicht das SGB jedoch vom VwVfG ab. Die Sozial-versicherungsträger sowie ihre Verbände werden durch § 36 a Abs. 4 SGB I verpflichtet, „unter Beachtung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit im jeweiligen Sozialleistungsbereich Zertifizierungsdienste nach dem Signaturgesetz, die eine gemeinsame und bundeseinheitliche Kommunikation und Übermittlung der Daten und die Überprüfbarkeit der qualifizierten elektronischen Signatur auf Dauer sicherstellen“, zu nutzen. Weiter heißt es: „Diese Träger sollen über ihren jeweiligen Bereich hinaus Zertifizierungsdienste im Sinne des Satzes 1 verwenden.“

Damit wurde für den Bereich der Sozialgesetzgebung eine Regelung zur Aufbewahrung von Dokumenten geschaffen, welche jedoch keine Gültigkeit für die übrige Verwaltungslandschaft in Deutschland besitzt.

## 2.4 Signaturgesetz (SigG) und Signaturverordnung (SigV)

Das SigG regelt den Begriff sowie die Voraussetzung der elektronischen Signatur und ihrer Infrastruktur. Es unterscheidet zwischen einfachen, fortgeschrittenen und qualifizierten Signaturen. Qualifizierte Signaturen müssen nach § 17 SigV erneuert werden, wenn sie als nicht mehr sicher gelten. Dies dient dem Beleg der Beweishaltigkeit eines Dokuments. Die elektronische Signatur wahrt die Integrität und Authentizität signierter Dokumente und wird nach BGB, VwVfG, Verwaltungsgerichtsordnung (VwGO) und SGB gefordert, wenn die Schriftform zu ersetzen ist. Für die Nutzung von Signaturen im Bereich der Sozialverwaltung müssen die Behörden gemäß SGB Dienstanweisungen erstellen.

## 2.5 Bundesdatenschutzgesetz (BDSG)

Auch für die öffentliche Verwaltung gilt das BDSG wie in Kapitel C 1.3 beschrieben.

## 2.6 Archivgesetze

Die Archivgesetze des Bundes (BArchG) und der Länder regeln die Aufgaben der Archive bei der Ermittlung, Übernahme, Verwahrung, Erhaltung, Instandsetzung, Erschließung und Nutzbarmachung des Archivguts. Archive sind auch für die Archivierung von elektronischen Daten und Datenträgern verantwortlich. Jedes Bundesland hat ein eigenes Archivgesetz, das sich weitgehend an die Bundesnorm anlehnt. Die Verwendung von Datenverarbeitungssystemen wie DMS und die revisionssichere Aufbewahrung von Dokumenten sind darin meist nicht geregelt. Hier gelten vorerst noch die übergeordneten Gesetze wie zum Beispiel das GG.

## 2.7 DOMEA

Das DOMEA-Konzept enthält Richtlinien für die rechtskonforme Einführung der elektronischen Akte in einer Behörde sowie folgende Forderung: „IT-gestützte Vorgangsbearbeitungssysteme müssen [...] u. a. in der Lage sein, mindestens das gleiche Maß an Integrität, Authentizität, Vertraulichkeit und Nachweisbarkeit der elektronischen Bearbeitungs- und Kommunikationsprozesse zu gewährleisten wie die papiergebundene [Aktenführung].“

Das DOMEA-Konzept ist somit die Quelle, in der für die öffentliche Verwaltung die revisionssichere Datenspeicherung konkret gefordert und durch einen Anforderungskatalog untermauert wird.

Allerdings ist das DOMEA-Konzept keine Rechtsnorm, sodass aus ihm keine konkreten Pflichten zur revisionssicheren Datenspeicherung in Behörden abgeleitet werden können. Außerdem ist durch das DOMEA-Zertifizierungsverfahren der Eindruck entstanden, dass ein DOMEA-zertifiziertes DMS von vornherein revisionssicher ist. Die für die revisionssichere Speicherung von

Dokumenten wichtigen Aspekte der Dokumentation und des Betriebs von DMS spielen im DOMEA-Konzept aber nur eine geringe Rolle.

### 3 Fazit

Wie man bei der Gegenüberstellung erkennen kann, gibt es im öffentlichen Recht ein breites Spektrum an Rechtsnormen, die das Thema der Revisionssicherheit berühren, denen es aber an Regelungstiefe fehlt. Eine Ausnahme bildet dabei der Bereich der Sozialverwaltung für die solche Regelungen existieren. Jedoch sind diese wiederum nicht auf andere Verwaltungsträger außerhalb des Sozialbereichs anwendbar. Im Privatrecht gibt es weniger Normen, die jedoch tief in die Materie gehen. Um die Unklarheiten der Regelungen im öffentlichen Sektor zu beseitigen, müssen die rechtlichen Regelwerke konkretisiert werden. Die Lösungen im SGB und im Privatrecht können dabei Orientierung geben.

Als Grundlage für den Umgang mit elektronischen Akten ist es zunächst erforderlich, eine Definition der revisionssicheren Aktenspeicherung, die den Anforderungen des öffentlichen Sektors gerecht wird, gesetzlich zu verankern. Das Ziel ist, die Unklarheiten in der öffentlichen Verwaltung zu minimieren und ein effektives und rechtlich einwandfreies elektronisches Verwaltungshandeln zu ermöglichen. Aufbauend auf den Erkenntnissen dieses Kapitels, werden in Kapitel D Handlungsempfehlungen für die Implementierung der Revisionssicherheit in Behörden gegeben.

## D Handlungsempfehlungen

Die Studienergebnisse zeigen, dass ca. 60 % der befragten Behörden sich mit der Einführung elektronischer Akten beschäftigen. Ferner ist herauszulesen, dass die Aufmerksamkeit für das Thema Revisions sicherheit auf allen Verwaltungsebenen groß ist. Bei der Umsetzung sind jedoch schon bei grundsätzlichen Anforderungen, wie zum Beispiel den Dokumentationspflichten, erhebliche Defizite festzustellen. Die Ursachen dafür ist eine Kombination aus der unzureichenden Definition von Revisions sicherheit einerseits und fehlenden konkreten rechtlichen Anforderungen für den öffentlichen Rechtsraum andererseits. Die Studie konnte zeigen, dass erheblicher Handlungsbedarf zur Lösung dieser Probleme besteht.

Vor diesem Hintergrund wurden drei Handlungsfelder identifiziert, auf denen Maßnahmen zur Reduktion der Unsicherheit und zur Klärung des Umgangs mit elektronischen Akten vorgeschlagen werden:

### Anpassung der rechtlichen Grundlagen

Für Handlungsfeld eins (siehe Abschnitt D 1) wird eine Konkretisierung der rechtlichen Vorgaben für die revisions sichere elektronische Aktenhaltung in der öffentlichen Verwaltung empfohlen. Dabei kann auf den Erfahrungen aus der Privatwirtschaft aufgebaut werden. Diese müssen jedoch an die Bedingungen der öffentlichen Verwaltung angepasst werden.

### Schaffung von Kriterien

Für Handlungsfeld zwei (siehe Abschnitt D 2) wird vorgeschlagen, einen Katalog der speziellen Anforderungen der öffentlichen Verwaltung an eine revisions sichere elektronische Aktenhaltung anzulegen, der dazu beitragen kann, die Orientierungsprobleme in der öffentlichen Verwaltung zu beseitigen.

### Entwicklung eines Prüfverfahrens

Für Handlungsfeld drei (siehe Abschnitt D 3) wird vorgeschlagen, für die öffentliche Verwaltung ein Prüfverfahren ähnlich dem der Privatwirtschaft zu etablieren, um die nachhaltige revisions sichere Speicherung elektronischer Akten sicherzustellen.

## 1 Handlungsfeld 1: Prüfung und Anpassung der rechtlichen Grundlagen

Wie bereits mehrfach festgestellt, fehlen für große Teile der öffentlichen Verwaltung klare Normen für die revisions sichere Aktenhaltung. Deshalb werden uneinheitliche Verfahren eingesetzt und keine optimalen Ergebnisse erzielt, wie zum Beispiel Hybridakten oder eine unvollständige Dokumentation. Zum einen lassen sich die im Handelsrecht verankerten Regelungen bzw. abgeleitete Regelungen wie die GoBS aufgrund der weiterreichenden Notwendigkeiten der öffentlichen Verwaltung (Aktenführungspflicht zur Dokumentation des Verwaltungshandelns, Anforderungen der Archive für dauerhafte Aufbewahrung öffentlichen Schriftguts) bzw. die Regelungen des SGB IV nicht einfach übertragen. Zum anderen erscheint eine reine Ableitung aus dem verfassungsrechtlichen Rahmen aufgrund der sehr allgemeinen und interpretationswürdigen Formulierungen des Grundgesetzes auf Dauer problematisch. Als Grund-

lage des elektronischen Verwaltungshandelns muss daher eine Verankerung der Anforderungen an die Revisions sicherheit im öffentlichen Recht Einzug halten. Eine Ableitung von Normen allein aus dem Verfassungsrecht wegen der sehr allgemeinen und interpretationsbedürftigen Formulierungen des GG problematisch. Als Grundlage des elektronischen Verwaltungshandelns müssen angepasste Anforderungen an die Revisions sicherheit in das öffentliche Recht aufgenommen werden.

Im Folgenden wird ausgeführt, in welchen Bereichen die aktuelle Rechtslage angepasst werden müsste, um eine revisions sicheren Aktenhaltung zu ermöglichen.

## 1.1 Verwaltungsverfahrensnormen

Grundsätzlich besteht wohl kein Zweifel daran, dass die Revisions sicherheit des elektronischen Verwaltungshandelns ein Aspekt des Rechtsstaatsprinzips ist. In dieser Studie hat sich herausgestellt, dass aus diesem Prinzip keine Normen zur Revisions sicherheit für die elektronisch handelnde öffentliche Verwaltung definiert wurden. Da der Zweck des VwVfG (bzw. der VwGO) die Beschreibung und Festsetzung der Prozesse des (elektronischen) öffentlichen Verwaltungshandelns ist, wäre eine Anpassung der Normen eine konsequente Weiterführung des elektronischen Verwaltungshandelns und sollte Unklarheiten beseitigen.

Im Zuge der Digitalisierung wurde zwar das elektronische Verwaltungshandeln in das VwVfG (bzw. die VwGO) des Bundes aufgenommen, jedoch fehlt jedwede weitere Konkretisierung der Handhabung elektronischer Akten. Da sich die Verwaltungsverfahrensgesetze der Länder, die auch für die Kommunen gelten, überwiegend an das des Bundes anlehnen, besteht diese Regelungslücke auch in der Landesgesetzgebung.

Angesichts des Regelungsbedarfs erscheint eine Ergänzung des VwVfG oder eine entsprechende Berücksichtigung in den E-Government-Gesetzen (E-GovG) sinnvoll. Hier sollte ein Anforderungskatalog für die revisions sichere Speicherung von Dokumenten eingebunden werden. Alternativ wäre auch ein Verweis auf die Regelung des Handelsrechtes oder der Sozialgesetzgebung denkbar. Generell sollten für die Beweiswerterhaltung und Revisions sicherheit von elektronisch signierten Dokumenten die schon angesprochene Technische Richtlinie 03125 (TR-VELS)<sup>4</sup> des BSI berücksichtigt werden, die sich mit der Wahrung der Authentizität und Integrität elektronisch signierter Dokumente befasst und Vorgaben zur sicheren Aufbewahrung von elektronischen Dokumenten enthält.

---

<sup>4</sup> Die Technische Richtlinie 03125 (TR-VELS) wird nach Information des BSI in Zusammenarbeit mit dem VOI überarbeitet und soll künftig „Beweiswerterhaltung kryptographisch signierter Dokumente“ lauten, kurz TR-ESOR heißen.

## 1.2 Normen des Datenschutzes

Datenschutz und Datensicherheit sind ebenfalls wichtige Voraussetzungen für die Revisionssicherheit der elektronischen Aktenhaltung. Das elektronische Verwaltungshandeln muss gewährleisten, dass personenbezogene und sensible Daten vor Manipulation, Missbrauch und unberechtigter Nutzung geschützt sind. Die Normen zum Datenschutz sind nicht in einem Regelungsbereich gebündelt, sodass der Überblick über die Rechtslage erschwert ist. Die Auswertung der Studienergebnisse zeigt, dass auch die Regelungen zum Datenschutz angepasst werden müssen.

Die Verarbeitung personenbezogener Daten regelt das BDSG bzw. die Datenschutzgesetze der Länder. Für die (revisionssichere) Datenverarbeitung gibt es in den relevanten Gesetzen keine spezifischen Regeln. Dadurch besteht eine gewisse Intransparenz und Unklarheit im Umgang mit personenbezogenen Daten. Einen Lösungsansatz kann hier der IT-Grundschutz des BSI bieten.

Im Kontext der Revisionssicherheit ist insbesondere auch der Schutz der Vertraulichkeit der externen Kommunikation ein kritischer Punkt. Auch in diesem Bereich gibt es Regelungsdefizite. Es existieren zum Beispiel keine Bestimmungen für Authentifizierungs- und Integritätsverfahren wie etwa den Einsatz von Signaturen.

## 2 Handlungsfeld 2: Schaffung von Kriterien für die revisionssichere elektronische Aktenhaltung in der öffentlichen Verwaltung

Wie bereits festgestellt wurde, sind die Normen zur revisionssicheren Aktenhaltung in der Privatwirtschaft tief strukturiert, während im öffentlichen Rechtsraum noch viel Interpretationsspielraum vorhanden ist. Auf der Grundlage des gegebenen Rechtsrahmens für die Privatwirtschaft hat der „Verband Organisations- und Informationssysteme e.V.“ (VOI) einen Katalog entwickelt (Prüfkriterien für Dokumenten Management Lösungen [PK-DML]), in dem die rechtlichen Vorgaben in Form von Prüfkriterien für eine effektive revisionssichere Aktenbehandlung konkretisiert werden.

Vor dem Hintergrund der zum Teil anders gelagerten Anforderungen der öffentlichen Verwaltung (zum Beispiel im Bereich der Abgabe von Akten und Vorgängen an ein Archiv) wird vorgeschlagen, einen auf den Bedarf der öffentlichen Verwaltung angepassten Katalog zu erstellen, der als Leitfaden oder Empfehlung für die Prüfung der revisionssicheren Aktenführung dienen soll.

In Anlehnung an die Erkenntnisse aus der Privatwirtschaft werden an dieser Stelle vier thematische Dimensionen benannt, die einen Rahmen für einen solchen Anforderungskatalog in der öffentlichen Verwaltung bieten sollen.



Abb. 22 Dimensionenmodell für die Entwicklung eines Anforderungskatalogs

Die vier Dimensionen zeigen alle Aspekte, die für eine revisions sichere elektronische Aktenhaltung wichtig sind. Insbesondere umfassen sie die technische Infrastruktur und die Funktionen der Revisionssicherheit. Diese sind Erfassung/Erzeugung, Speicherung, Verarbeitung/Bearbeitung, Veränderung, Zugriff auf und Reproduktion von Daten. Die Dimensionen erfassen auch den Dokumentenlebenszyklus (siehe Abbildung 23).

Für die öffentlichen Träger liegt die Aufgabe darin, mithilfe der vier Dimensionen einen Anforderungskatalog zu erstellen, mit dessen Hilfe die elektronische Aktenhaltung der öffentlichen Verwaltung angepasst und somit überprüfbar gemacht werden kann.

Nachfolgend soll anhand der Dimensionen eine mögliche Anpassung der Anpassungskriterien für die öffentliche Verwaltung vorgestellt und mit Beispielen unterlegt werden.



Abb. 23 Dimensionen und revisions sichere Funktionen

## 2.1 Anforderungsdimension Technik

Die Dimension Technik ist die Grundlage des elektronischen Verwaltungshandelns und umfasst die gesamte IT-Infrastruktur (Software- sowie Hardwarebasis). Revisionssicherheit bedeutet hier, unter Wahrung rechtsstaatlicher Strukturen den Schutz der Komponenten und der Daten zu garantieren. Deshalb ist es bei der elektronischen Aktenhaltung notwendig, konkrete Vorgaben zur IT-Sicherheit (z. B. in einem IT-Sicherheitskonzept) sowie zur Betriebsführung zu machen und umzusetzen. Ziel ist es, den

ordnungsgemäßen Betrieb überprüfbar zu machen und ihn dadurch kontinuierlich sicherzustellen.

#### IT-System (Hard- und Softwarekomponenten)

Das IT-System hat eine Hardware- und eine Softwarekomponente. Beide Bereiche müssen im Zusammenspiel den ordnungsgemäßen Umgang mit der elektronischen Akte garantieren. Zunächst sollte demnach das DMS organisationsinternen und rechtlichen Forderungen angepasst und dann revisions sicher ausgestaltet werden. Leider zeigen die Studienergebnisse, dass viele Behörden diese Verpflichtung nicht wahrnehmen und das System nicht an die elektronische Aktenhaltung anpassen, was die Revisions sicherheit gefährdet.

Ein sicherer Betrieb der IT-Infrastruktur soll garantieren, dass die Daten nicht verloren gehen. In der Privatwirtschaft bedeutet dies, beim Betrieb des Systems die vom HGB geforderte Sicherung vor Verlust zu gewährleisten. Dazu muss zum Beispiel das DMS im Rahmen eines Maßnahmenplans für Störungsbehebung so strukturiert werden, dass Störungen oder Fehler verhindert werden oder schnellstmöglich behoben werden können. Die IT Infrastructure Library (ITIL) könnte Orientierung bei der Einrichtung eines Service-Managements geben. Für die Beweiswerterhaltung digitaler Signaturen gibt die Technische Richtlinie 03125 „Vertrauenswürdige Elektronische Langzeitspeicherung“ (TR-VELS), die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt wurde, eine Orientierungshilfe. Sie gibt Standards im Umgang mit elektronischen signierten Dokumenten vor, die insbesondere die Authentizität und Integrität absichern sollen.

Zusätzlich muss das eingesetzte IT-System jederzeit die originalgetreue Reproduktion der Dokumente ermöglichen. Davon kann der Beweiswert erhalt eines Dokuments abhängen. Ist ein Dokument im IT-System nicht verfügbar ist es nicht existent. Mögliche Rechtsansprüche können somit nichtig werden. Vor dem Hintergrund des Rechtsstaatsprinzips ist das nicht vereinbar. Darum müssen das IT-System und seine Komponenten ständig aktualisiert werden. Das IT-System ist der Grundstein für die Nachvollziehbarkeit des elektronischen Verwaltungshandelns.

#### IT-Sicherheit

Ein revisions sicheres DMS zur elektronischen Aktenhaltung muss stets die Vollständigkeit der elektronischen Akte garantieren. Es muss Kontrollmechanismen haben, die eine lückenlose Erfassung von Dokumenten, die Datenverarbeitung, die originalgetreue Reproduktion sowie die Archivierung bzw. Vernichtung gewährleisten.

Damit die Revisions sicherheit eines DMS zur elektronischen Aktenhaltung garantiert werden kann, wird unbedingt ein IT-Sicherheitskonzept gebraucht, das Datenschutz und Datensicherheit regelt. Aus einer Risikoanalyse und der Ermittlung des Schutzbedarfs der Systemkomponenten und insbesondere der im System vorgehaltenen Daten werden Schutzmaßnahmen abgeleitet und im IT-Sicherheitskonzept erfasst. Zum Sicherheitskonzept gehört zum Beispiel ein Berechtigungskonzept mit Zugangs-, Zutritts- und Zugriffsrechten, das Veränderungen der Daten kontrollierbar und die Bearbeitungsschritte nachvollziehbar macht. Schriftgut sollte stets nur von Berechtigten bearbeitet oder eingesehen werden dürfen. Ebenfalls zum Sicherheitskonzept gehört eine Backuplösung zur Daten-

sicherung, durch die das System verlorene Dokumente wiederherstellen kann.

Ein IT-Sicherheitskonzept ist einer der wichtigsten Bestandteile der Revisions sicherheit. Das BSI hat eigens für die Sicherheitsprüfung von IT-Systemen Kriterien und ein Verfahren für ein Audit entwickelt. Beim Audit des IT-Grundschutzes gemäß ISO 27001 wird die Referenzdokumentationen<sup>5</sup> auf Konformität mit der IT-Sicherheit geprüft und mit der Umsetzung der Sicherheitsmaßnahmen im eingesetzten DMS abgeglichen. Erfüllen die sicherheitsrelevanten Dokumentationen und die im System umgesetzten Sicherheitsmaßnahmen die Anforderungen, wird die geprüfte Organisation zertifiziert. Behörden, die ihr Sicherheitskonzept durch das BSI zertifizieren lassen, nähern sich der revisions sicheren Aktenhaltung. Jedoch reicht IT-Sicherheit allein für eine revisions sichere Aktenhaltung nicht aus. Dafür sind weitere Dimensionen zu beachten, die nachfolgend erläutert werden.

## 2.2 Anforderungsdimension Organisation

Technik und Organisation können nicht unabhängig voneinander agieren und müssen immer im Zusammenhang betrachtet werden. Die Dimension Organisation umfasst die Struktur und die Prozesse der einzelnen Organisationen. Das IT-System unterstützt bzw. optimiert die Organisation und steigert die Effizienz und Effektivität des Verwaltungshandelns.

### Organisationsaufbau

Für die revisions sichere Aufbewahrung von Akten in der öffentlichen Verwaltung und insbesondere zur Herstellung der Nachvollziehbarkeit und der Integrität der Daten muss die Organisationsstruktur einer Behörde betrachtet werden. An ihr orientiert sich das für die Revisions sicherheit erforderliche Zugriffs- und Rollenkonzept (vgl. Kapitel C 1. 2). Durch das Zusammenspiel einer (automatischen) Protokollierung der Daten mit der Verfahrensdokumentation (siehe Kapitel C 1. 1) kann der Schutz vor Verfälschung oder Löschung von Daten erhöht werden. Die Orientierung des Zugriffs- und Rechtekonzepts an der Organisationsstruktur ist jedoch nur dann sinnvoll, wenn in das Konzept auch die Prozessbetrachtung einfließt. Eine reine Abbildung der Organisationsstruktur hat wenig Sinn.

Die Studie zeigt, dass die Größe einer Behörde die Entscheidung für den Einsatz eines DMS nicht zwingend beeinflusst und dass viele Institutionen DMS zunächst als Pilotprojekte in einzelnen Organisationseinheiten einführen, bevor es in der gesamten Behörde eingesetzt wird. Die Einführung des DMS orientiert sich also oft am Aufbau der Behörde.

### Prozesse

Die Prozesse der Erfassung, Indexierung und Bearbeitung von Dokumenten müssen im DMS lückenlos dokumentiert werden und nachvollziehbar sein, um Rechtssicherheit zu gewährleisten. Die elektronische Aktenführung soll vollständig erfolgen, das heißt, die elektronische Akte soll die führende sein. Die Studie zeigt, dass trotz DMS-Nutzung in weiten Teilen der öffentlichen Verwaltung noch immer hybride Aktenstrukturen existieren. Aktenrelevante

<sup>5</sup> Diese besteht im Wesentlichen aus IT-Strukturanalyse, Schutzbedarfsfeststellung, Modellierung des IT-Verbunds, Basissicherheitschecks, ergänzender Sicherheitsanalyse und Risikoanalyse.

Inhalte liegen zum Teil in elektronischer Form und zum Teil in Papierform vor. Zwar sind die Akten oft vollständig, jedoch schränken die Medienbrüche die Nachvollziehbarkeit der Aktenführung erheblich ein.

Für eine revisionssichere elektronische Aktenhaltung müssen aktenrelevante Inhalte zum frühestmöglichen Zeitpunkt in das DMS überführt werden. So sollen hybride Strukturen vermieden und die Vollständigkeit, Integrität und Authentizität der Daten effektiver gesichert werden. Dazu sind auch ein Scankonzept und eine interne Richtlinie zum Umgang mit E-Mails und zu ihrer Speicherung erforderlich.

Für elektronisch erzeugte Dokumente mit besonderem rechtlichem Wert (z. B. Verträge) kann es erforderlich sein, die Rechtsstellung besonders abzusichern. Dies kann durch den Einsatz elektronischer Signaturen erfolgen. Die Rechtsgültigkeit der eingesetzten Signaturen muss für die gesamte Aufbewahrungszeit gewährleistet werden. Einen Ansatzpunkt dafür bietet die Technische Richtlinie 03125 (TR-VELS) des BSI. Sie gibt Standards zum revisionssicheren Umgang mit elektronisch signierten Dokumenten vor.

Nach Ablauf der Aufbewahrungsfrist wird das Dokument am Ende seines Lebenszyklus dem zuständigen Archiv angeboten und gegebenenfalls dorthin überführt oder vernichtet. Für ein revisionssicheres Vorgehen sollte auch das Verfahren nach Ablauf der Aufbewahrungsfristen beschrieben werden. So sind für die Übergabe von Schriftgut an das Archiv revisionssichere Schnittstellen zu beschreiben.

Im Rahmen revisionssicherer Prozesse ist es wichtig Konzepte zu entwickeln, in denen beschrieben wird, wie ein IT-System revisionssicher und wirtschaftlich betrieben werden kann. Wird zum Beispiel dem Eigenbetrieb des Systems oder einem externen Betreiber der Vorzug gegeben? Im Falle einer Auslagerung des Betriebs (Outsourcing) an ein Shared-Service-Center (z. B. ein öffentlich-rechtliches Rechenzentrum) sollte allerdings klar sein, dass der revisionssichere Betrieb durch den externen Betreiber vertraglich abgesichert werden muss.

Oft wird auch in Einführungsprojekten ein zu hoher personeller Aufwand im Verhältnis zum Nutzen ermittelt. Der spätere Nutzen eines produktiven DMS ist jedoch erheblich höher, als in einem Einführungsprojekt festgestellt werden kann.

## 2.3 Anforderungsdimension Mensch

Technik und Organisation können nicht ohne die Mitarbeiter und Mitarbeiterinnen einer Behörde funktionieren. Der Mensch ist ein kritischer Erfolgsfaktor für die Revisionssicherheit.

### Qualifikation

Der Mensch ist ein kritischer Faktor für den Erfolg von DMS-Projekten. Wichtig ist die Erkenntnis, dass zur korrekten Anwendung von DMS oder auch anderen IT-Systemen die Qualifikation der Mitarbeiter und Mitarbeiterinnen gehört. Die Mitarbeiter müssen aber nicht nur für die Anwendung eines IT-Systems geschult werden. Vielmehr müssen sie auch für

die Einhaltung interner Richtlinien und die Erfüllung von Dokumentationspflichten – also den revisionsicheren Umgang mit dem System und der elektronischen Akte – sensibilisiert und qualifiziert werden.

#### Akzeptanz

Die Studie zeigt, dass die Einführung eines revisionsicheren DMS oder der elektronischen Akte an fehlender Akzeptanz der Nutzer scheitern kann. Ihre Einführung verändert grundlegend die Arbeitsweise der öffentlichen Verwaltung, was auch eine Verschiebung kultureller Werte bedeutet. Mitarbeiter müssen ihre gewohnte Umgebung verlassen und sich auf neue Strukturen umstellen. Revisionsicherheit bedeutet auch, informelle Regeln und Arbeitsweisen aufzugeben und die offiziellen Regeln streng zu befolgen. Die Zeit, die für die eigentlichen Aufgaben des Mitarbeiters zur Verfügung steht, wird dadurch zusätzlich beschnitten. Die Veränderung fest etablierter, kultureller Werte in der öffentlichen Verwaltung löst natürlich Widerstand und Konflikte aus. Abhilfe können ein frühzeitiges, bewusstes Veränderungsmanagement und Instrumente bringen, die Akzeptanz schaffen und dem Widerstand entgegenwirken.

Veränderungen können nur im Zusammenspiel von Strategie, Kultur und Struktur etabliert werden. Aufgabe des Veränderungsmanagements ist es, engen Kontakt zu den Mitarbeitern zu halten und frühzeitig die Ziele und Strategien einer revisionsicheren Ausgestaltung der digitalen Systeme zu vermitteln. Revisionsicherheit ist an sich ein klassischer Wert der öffentlichen Verwaltung und somit kulturell fest verankert. Trotzdem wird die Einführung damit einhergehender organisatorischer Veränderungen besser akzeptiert, wenn die Mitarbeiterinnen und Mitarbeiter frühzeitig eingebunden werden und die Projektergebnisse stetig kommuniziert werden. Veränderungsmanagement lebt von einer stetigen Kommunikation und, damit verbunden, einer ganzheitlichen Betreuung der Anspruchsgruppen. Deshalb sollte das Veränderungsmanagement frühzeitig auch die strategische Ebene eines Projektes einbinden, da so die Erfolgsaussichten erheblich gesteigert werden. Die Unterstützung der Behördenleitung kann dem Prozess zusätzlichen Schwung verleihen und ist insbesondere in akzeptanzkritischen Phasen wesentlicher Faktor für eine erfolgreiche Projektdurchführung.

## 2.4 Anforderungsdimension Dokumentation

Die Dimension Dokumentation berührt alle Strukturen und Prozesse technischer und nichttechnischer Art. Eine ständig gepflegte und angepasste Dokumentation ist die Basis für ein revisionsicheres DMS. Sie gewährleistet die Nachvollziehbarkeit und Ordnungsmäßigkeit der Prozesse und Strukturen des Datenmanagements. Alle Veränderungen an Strukturen und Prozessen technischer oder nichttechnischer Art müssen sich in der Verfahrensdokumentation wiederfinden. Gleichzeitig muss die Dokumentation immer auch den rechtlichen Anforderungen sowie den internen organisatorischen Richtlinien entsprechen. Ein Beispiel ist die Ausrichtung des IT-Systems sowie der Datenmanagementprozesse auf gesetzlich vorgeschriebene Aufbewahrungsfristen.

Wie schon bei der Betrachtung der Dimensionen Technik, Organisation und Mensch erläutert, sollen z. B. Bearbeitungsprozesse und Sicherheits-

maßnahmen dokumentiert werden. Die Dokumentationen können von Mitarbeiterinnen und Mitarbeitern oder automatisch erstellt werden. Alle Dokumentationen und die ihnen zugrunde liegenden Richtlinien sollen sich schließlich in einer umfassenden Verfahrensdokumentation wiederfinden. Die Verfahrensdokumentation wird in einer externen Prüfung unterzogen. Bei erfolgreichem Abschluss erfolgt eine Testierung.

### 3 Handlungsfeld 3: Entwicklung eines Prüfverfahrens zur Sicherstellung der revisionssicheren Speicherung von elektronischen Akten

Um die Revisionsicherheit der elektronischen Aktenführung in den Behörden nachhaltig sicherzustellen, schlagen wir in Anlehnung an Prüfverfahren aus der Privatwirtschaft ein gesondertes Prüfverfahren zur Sicherstellung der revisionssicheren Speicherung vor. Dies soll dazu dienen, dass die Umsetzung der entsprechenden Vorgaben in die Verwaltungsrealität Einzug hält.

Die reine Orientierung von IT-Lösungen an bestimmten Konzepten (siehe DOMEA-Zertifizierungen), Herstellererklärungen oder das Vorhandensein einer internen Revision im Betrieb reichen nicht aus, um in konkreten Einzelfällen eine revisionssichere Aktenführung sicherzustellen. Das Prüfverfahren sollte sich deshalb an einem Anforderungskatalog für die revisionssichere Aktenspeicherung in der öffentlichen Verwaltung orientieren. Dadurch würden die Besonderheiten im öffentlichen Sektor berücksichtigt und die Prüfung wäre effektiver. Die Kriterien für Revisionsicherheit aus der Privatwirtschaft können in vielen, wenn auch nicht allen Fällen übernommen werden. Förderlich und notwendig ist allerdings eine Anpassung dieser Kriterien zur Revisionsicherheit des elektronischen Verwaltungshandelns im öffentlichen Recht.

Eine solche Prüfung sollte durch eine unabhängige Prüfinstanz erfolgen (z. B. externe Wirtschaftsprüfer oder Rechnungshöfe), da externe Prüfer unabhängig von der geprüften Behörde und an keinerlei Weisungen gebunden sind. In Anlehnung an die Zertifizierungsvorgaben in der Wirtschaft soll im Folgenden ein Prüfverfahren für die revisionssichere Aktenführung beispielhaft skizziert werden. Aus Gründen der Transparenz wird in dieser Studie ausschließlich Bezug auf die wesentlichen, aus der Privatwirtschaft entlehnten Grundlagen genommen. Aufbauend auf diesem System sollte künftig eine detaillierte Betrachtung der Besonderheiten in der öffentlichen Verwaltung sowie eine diesbezügliche Konkretisierung erfolgen.

#### 3.1 Rahmen für das Verfahren

Die Zertifizierung eines revisionssicheren Datenverarbeitungssystems bestätigt die Beweisqualität digitaler Dokumente in der öffentlichen Verwaltung. Vor dem Hintergrund der immer tiefer greifenden Nutzung von Informationstechnik und den damit verbundenen Manipulationspotenzialen ist es zur Wahrung des an rechtsstaatliche Prinzipien gebundenen

Verwaltungshandelns von großer Bedeutung, digitale Dokumente revisions sicher zu schützen.

Der falsche Umgang mit digitalen Dokumenten muss gar nicht immer beabsichtigt sein. Dokumente werden in der öffentlichen Verwaltung nach bestem Wissen und Gewissen gesichert und archiviert. Jedoch fehlen oftmals der Überblick und das Fachwissen für die korrekte Handhabung der Schriftgutverwaltung. So besteht die Gefahr, dass für viele Vorgänge keine Nachvollziehbarkeit gegeben ist. Um diesen Zustand zu ändern, ist es notwendig, die Handhabung, die Prozesse und die Dokumentationen in der Behörde zu überprüfen und gegebenenfalls anzupassen. Das Hauptziel der Einführung der elektronischen Aktenführung sollte es deswegen immer sein, die vollständige, integere und nachvollziehbare Dokumentation des Verwaltungshandelns sicherzustellen.

Die Revisions sicherheit der digitalen Aktenführung kann auf mehreren Qualitätsebenen überprüft werden. Wie Abbildung 24 zeigt, steigt die Rechtssicherheit des Systems, je strenger und unabhängiger die Prüfungen sind. Beispielsweise ist die Zertifizierung des IT-Grundschutzes ein Schritt hin zur Revisions sicherheit in der Behörde und kann im Zertifizierungs verfahren berücksichtigt werden. Mit zunehmender Revisions sicherheit wird es erforderlich, das System und die Dokumentationen regelmäßig zu kontrollieren und gegebenenfalls zu modifizieren. Wegen der Neutralität von Prüfern ohne Bindung an die zu prüfende Behörde bietet ein externes Prüf verfahren die größte Sicherheit und schafft ein Höchstmaß an Vertrauen in einen rechtstaatlichen Umgang mit elektronischen Dokumenten.

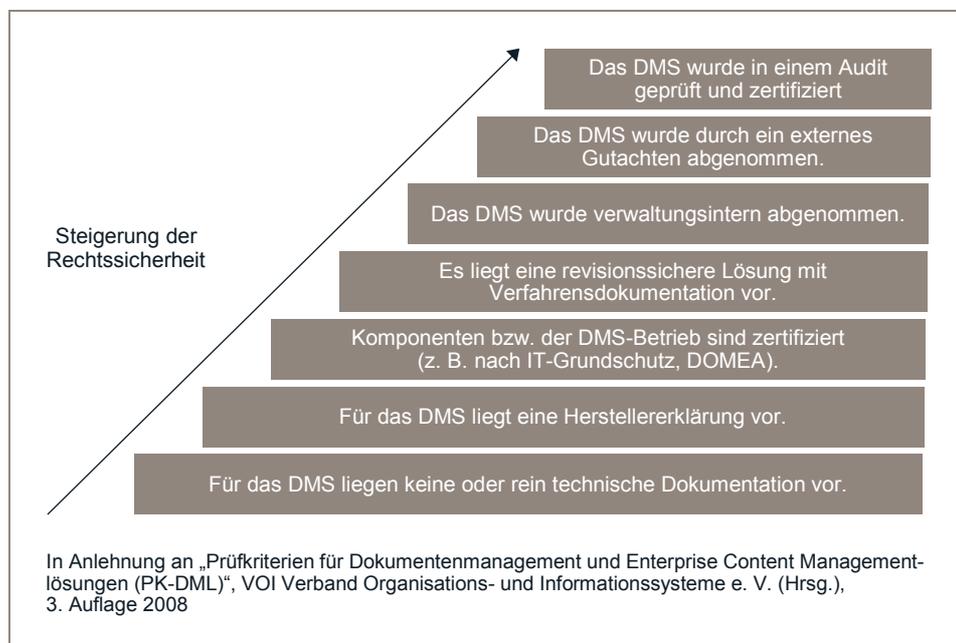


Abb. 24 Qualitätsstufen der Revisions sicherheit der digitalen Aktenführung

Die Studie zeigt allerdings, dass vielen Behörden auf allen Verwaltungsebenen nicht bewusst ist, wie wichtig für die Revisions sicherheit ein Höchstmaß an Nachvollziehbarkeit, Integrität und Authentizität ist. Nur 12 % der befragten Behörden lassen sich von spezialisierten Wirtschaftsprüfern oder einem Rechnungshof auf revisions sichere elektronische Aktenhaltung

prüfen. Die überwiegende Mehrheit der Behörden kann also ein DMS nicht revisions sicher betreiben.

## 3.2 Vorschlag für Prüfverfahren

Die Prüfung eines DMS richtet sich nach den Vorgaben des IDW und besteht aus vier Phasen:

- Prüfung der Konzeption
- Prüfung der Realisierung
- Prüfung der Tests
- Prüfung des Betriebs

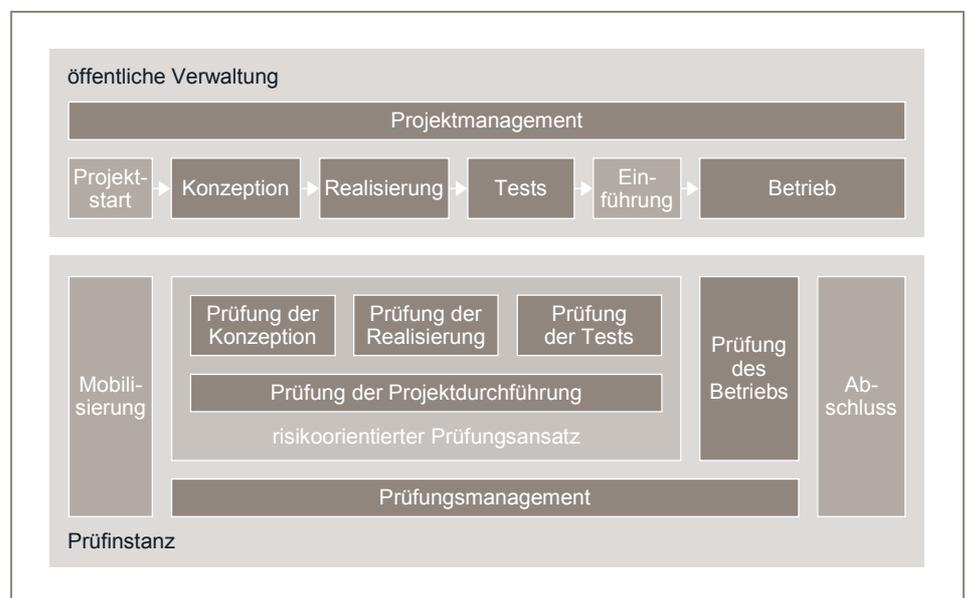


Abb. 25 Prüfungsprozess

### 3.2.1 Prüfung der Konzeption

Die Ausgangspunkte für das Prüfverfahren bilden einerseits die technisch umgesetzte und verwendete Dokumentenmanagementlösung der Verwaltung und andererseits eine Verfahrensdokumentation, die die Anforderungen zur Revisions sicherheit des Systems darlegt, wie zum Beispiel Originaltreue, Verfügbarkeit und Zugriffssicherheit des DMS. Die Verfahrensdokumentation erläutert den Umgang mit den Dokumenten im verwendeten DMS. Sie basiert auf externen und internen Normen und soll gleichzeitig deren Einhaltung sicherstellen.

Neben dem technischen System werden in der Verfahrensdokumentation die Organisationsstruktur der Behörde und die Prozesse im Umgang mit den Dokumenten beschrieben. Die Grundlagen dafür sind Dienst anweisungen und Richtlinien der Verwaltung. Zusätzlich müssen ein IT-Sicherheitskonzept (z. B. auf Basis des IT-Grundschutzes des BSI) sowie die internen Maßnahmen zur Kontrolle des revisions sicheren Umgangs mit den Daten und dem System beschrieben werden. Die Verfahrens-

dokumentation zeigt dem Träger durch ihre Genauigkeit eventuelle Regelungslücken und ist damit bereits ein erster Schritt zur Revisionsicherheit. Eine spätere Zertifizierung setzt an diesem Punkt an, deshalb sollte die Dokumentation ernsthaft und sorgfältig erstellt werden.

Bei der Verfahrensdokumentation sollten folgende Inhalte berücksichtigt werden:

- allgemeine Beschreibung des öffentlichen Trägers und von dessen Arbeitsfeld
- Größe und Organisation der Dokumentenbestände
- rechtliche Anforderungen
- Beschreibung des technischen Systems
- Beschreibung von Datenmigration und Schnittstellen
- Beschreibung des technischen Betriebs
- IT-Sicherheit
- (Fach-)Prozesse im Umgang mit Dokumenten
- Mitarbeiterqualifikation
- Tests
- Wartung
- Beschreibung des IKS

Die Verfahrensdokumentation ist der Dreh- und Angelpunkt für die Revisionsicherheit der Datenspeicherung in einer öffentlichen Verwaltung. Eine Veränderung von Prozessen in den genannten Bereichen würde eine Anpassung der Verfahrensdokumentation nach sich ziehen. Ein Prüfverfahren nimmt die Dokumentation als Grundlage für die Überprüfung und Bewertung der Verfahren. Dementsprechend hat die Verfahrensdokumentation einen strategischen Wert, der nicht unterschätzt werden sollte. Mit ihrer Hilfe können zudem Optimierungspotenziale der Institution ermittelt werden.

Einige der befragten Behörden sind sich der Bedeutung der Dokumentationspflicht bereits bewusst. Es muss jedoch noch deutlicher werden, dass die Verfahrensdokumentation ein eigenes strategisches und sicherheitssteigerndes Projekt ist, das ein gutes Projektmanagement und die Unterstützung der Leitungsebene erfordert.

### 3.2.2 Prüfung der Realisierung

Die Prüfung der Realisierung soll für ausgewählte Prozesse und Systeme sicherstellen, dass die in der Konzeptionsphase definierten Vorgaben eingehalten werden. Dabei werden insbesondere die Ordnungsmäßigkeit und Sicherheit wesentlicher Systemeinstellungen und die Wirksamkeit von automatischen Kontrollen im DMS betrachtet. Zudem werden die Einhaltung organisationsspezifischer Vorgaben und die Systemdokumentation geprüft.

Weitere Prüfkriterien sind die Sicherstellung der Projektintegrität bei der Bearbeitung von Change Requests und die Bereitstellung einer ordnungsgemäßen Entwicklungsumgebung.

### 3.2.3 Prüfung der Tests

Die anschließende Prüfung der im Rahmen der Einführung durchgeführten Systemtests soll vor allem die entsprechend den GoBS definierte Programmidentität sicherstellen. Programmidentität im weiteren Sinne bedeutet, dass die konzipierten und realisierten Prozesse und Systeme den Anforderungen entsprechend arbeiten. Insbesondere werden bei der Prüfung der Tests folgende Aspekte untersucht:

- angemessener Testumfang
- ordnungsgemäße Anwendung und Sicherheit der davon betroffenen Geschäftsprozesse
- Wirksamkeit der (programminternen) Kontrollen
- ordnungsgemäße Durchführung der Tests und der Fehlerverfolgung
- technische Funktionsfähigkeit im Gesamtablauf
- nachvollziehbare Testdokumentation
- Abnahme- und Freigabeverfahren
- ordnungsgemäßer Rollout

### 3.2.4 Prüfung des Betriebs

Nach der Einführung des DMS steht der ordnungsgemäße Betrieb im Vordergrund. Eine Prüfung der Betriebsphase untersucht im Besonderen folgende Aspekte:

- Inbetriebnahme des Systems und Monitoring von Problemen nach Roll-out
- Ordnungsmäßigkeit von eventuellen Datenübernahmen
- Wirkung der Customizing-Einstellungen sowie Ordnungsmäßigkeit der Ergebnisse im produktiven Umfeld
- Einhaltung und Wirkung der organisatorischen Kontrollen
- Ordnungsmäßigkeit und Sicherheit des Programmbetriebs
- Systemsicherheit im Hinblick auf einen restriktiven Zugriff

## 4 Fazit

In der Studie wurde gezeigt, dass die revisions sichere Speicherung von Dokumenten für die öffentliche Verwaltung weiter an Bedeutung gewinnt. Allerdings fehlen bislang hierfür klare rechtliche Vorgaben.

Bei der konventionellen, papiergebundenen Aktenführung war die Erfüllung der Anforderungen an die Revisions sicherheit ein wesentlicher Teil der

Verwaltungskultur. Allerdings konnten diese traditionellen Regelungen nicht auf die Veränderungen, die durch die Etablierung elektronischer Kommunikationswege und der Erzeugung elektronischer Dokumente eingehen, übertragen werden. Eine Ausnahme bildet hierbei der Sozialbereich, der bereits eigene Regelungen definiert hat, wobei auch hier eine Konkretisierung in Form genauerer Kriterien erfolgen sollte.

Vor diesem Hintergrund wurden drei Handlungsfelder identifiziert, in denen Maßnahmen zur Reduktion der Unsicherheit und zur Klärung des Umgangs mit elektronischen Akten vorgeschlagen werden. Diese betreffen

- die Anpassung der rechtlichen Grundlagen,
- die Definition eines Kriterienkatalogs mit den speziellen Anforderungen der öffentlichen Verwaltung an eine revisions sichere elektronische Aktenhaltung sowie
- die Entwicklung eines Prüfverfahrens, um die nachhaltige revisions sichere Speicherung elektronischer Akten sicherzustellen.

## Wir über uns

### PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft

Die PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft ist in Deutschland mit 8.700 Mitarbeitern und einer Gesamtleistung von rund 1,33 Milliarden Euro eine der führenden Wirtschaftsprüfungs- und Beratungsgesellschaften. An 29 Standorten arbeiten Experten für nationale und internationale Mandanten jeder Größe. PwC bietet Dienstleistungen an in den Bereichen Wirtschaftsprüfung und prüfungsnahe Dienstleistungen (Assurance), Steuerberatung (Tax) sowie Beratung in den Bereichen Deals und Consulting (Advisory).

### IMTB Consulting GmbH

Die IMTB ist ein innovatives und unabhängiges Beratungshaus mit Standorten in Berlin und Köln. Unsere Kunden sind vornehmlich Verwaltungsorganisationen aus dem öffentlichen Sektor. Die Beschäftigten der IMTB verfügen über ausgewiesene und umfangreiche Kenntnisse und Erfahrungen im Bereich der öffentlichen Verwaltung. Die IMTB ist eines der führenden Beratungshäuser im Aufgabenbereich der Dokumenten- und Vorgangsbearbeitungssysteme, Geschäftsprozessmanagement, Archivmanagement, Wissensmanagement, Veränderungsmanagement und Vergabemanagement für die öffentliche Verwaltung.

Unser Ziel ist es, gemeinsam mit unseren Kunden erfolgreiche Projekte durchzuführen – dabei sehen wir unsere Kunden auch als Partner. Um diesem Ziel gerecht zu werden, beraten wir in Bezug auf Informationen, Menschen und Technik.

## Ansprechpartner

### PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft

#### **Peter Detemple**

Partner  
PricewaterhouseCoopers AG  
Wirtschaftsprüfungsgesellschaft  
Am Halberg 4  
66121 Saarbrücken  
Tel.: +49 681 9814-152  
peter.detemple@de.pwc.com

#### **Wigand Grabner**

PricewaterhouseCoopers AG  
Wirtschaftsprüfungsgesellschaft  
Potsdamer-Platz 11  
10785 Berlin  
Tel.: +49 30 2636-1492  
wigand.grabner@de.pwc.com

#### **Irina Furbach**

PricewaterhouseCoopers AG  
Wirtschaftsprüfungsgesellschaft  
Elsenheimerstraße 33  
80687 München  
Tel.: +49 30 2636-144  
irina.furbach@de.pwc.com

#### **Dirk Nippert**

PricewaterhouseCoopers AG  
Wirtschaftsprüfungsgesellschaft  
Olof-Palme-Straße 35  
60439 Frankfurt am Main  
Tel.: +49 69 9585-1739  
dirk.nippert@de.pwc.com

### IMTB Consulting GmbH

#### **Bastian Flemming**

IMTB Consulting GmbH  
Schumannstraße 14b,  
10117 Berlin  
Tel.: +49 30 440483-24  
Mobil: +49 178 4682011  
bastian.flemming@imtb.de

#### **Ralph Naumann**

Geschäftsführer  
IMTB Consulting GmbH  
Schumannstr. 14b  
10117 Berlin  
Telefon: +49 30 440483-24  
Mobil: +49 178 4682081  
ralph.naumann@imtb.de

#### **Nadja Koerdt**

IMTB Consulting GmbH  
Schumannstraße 14b  
10117 Berlin  
Tel.: +49 30 440483-24  
Mobil: +49 178 4682011  
nadja.koerdt@imtb.de

#### **Silvia Treschau**

IMTB Consulting GmbH  
Schumannstraße 14b  
10117 Berlin  
Tel.: +49 30 440483-24  
Mobil: +49 178 4682096  
silvia.treschau@imtb.de





[www.pwc.de](http://www.pwc.de)  
[www.imtb.de](http://www.imtb.de)