

ArchiSafe

Verwaltungsrechtliche Rahmenbedingungen

Dokumententitel: ArchiSafe Verwaltungsrechtliche Rahmenbedingungen
Dateiname: 2005-09-04_Verwaltungsrechtliche_Rahmenbedingungen_V10.doc
Version: 1.0
Anzahl Seiten: 47
Status: Abgestimmte Version zur Vorlage für Nutzerbeirat

erstellt am: 04.09.2005 von: Jobst Biester
geprüft am: von:
geändert am: von:
Freigegeben am: von:

Standort: PTB
Verteiler:

Inhalt

0	Versionshistorie	4
0.1	Dokumentverantwortlicher	4
0.2	Verteilerliste.....	4
1	Zielsetzung des Dokumentes	5
2	Rechtsvorgaben	6
3	Erfordernisse langfristiger Aufbewahrung	7
3.1	Aufbewahrungsinteresse	7
3.1.1	<i>Verfügbarkeit</i>	7
3.1.2	<i>Nachweis eines Rechtszustandes</i>	8
3.1.3	<i>Revisionssicherheit</i>	8
3.1.4	<i>Dauerhafte Aufbewahrung</i>	9
3.2	Aktenmäßigkeit des Verwaltungshandelns	9
3.2.1	<i>Gemeinsame Geschäftsordnung der Bundesministerien (GGO)</i>	10
3.2.2	<i>Registerrichtlinie (RegR)</i>	11
3.2.3	<i>Verwaltungsverfahrensgesetz (VwVfG)</i>	11
3.2.4	<i>DOMEA-Konzept</i>	12
3.3	Archivanforderungen	13
4	Sicherung der Integrität und Authentizität durch qualifizierte elektronische Signaturen	15
4.1	Schriftformerfordernis	15
4.2	Erfordernis hoher Beweissicherheit	17
4.3	Dauerhafte Überprüfbarkeit	18
5	Die Signaturerneuerung nach § 17 SigV	20
5.1	Obliegenheiten und Rechtspflichten	20
5.2	Sicherung der Integrität	21
5.3	Anforderungen an die erneute Signatur gemäß § 17 SigV	23
5.4	Sicherung der Authentizität	27
6	Beweiskraft elektronischer Dokumente	32

6.1	Allgemeine Beweisregeln	32
6.2	Besonderheiten im Verwaltungsprozess und bei der Beweisführung mit „öffentlichen“ Urkunden	32
6.3	Besondere Beweiskraft elektronischer Dokumenten mit qualifizierter Signatur	33
6.4	Beweiserleichterung des § 371a ZPO	36
6.4.1	<i>Voraussetzungen der Beweiserleichterung</i>	38
6.4.2	<i>Rechtsfolgen der Beweiserleichterung</i>	41
6.5	Verlust des Anscheinsbeweises mit Ablauf der Dokumentationsfrist	42
6.6	Erhaltung der Beweiskraft durch Signaturerneuerung	42
7	Aufbewahrungsfristen	45
7.1	Mindestaufbewahrungsfristen	45
7.2	Höchstaufbewahrungsfristen	45
7.2.1	<i>Datenschutzrecht</i>	45
7.2.2	<i>Bundesarchivgesetz</i>	46
7.2.3	<i>RegR</i>	46
8	Aufbewahrungsmodalitäten zur Sicherung des Daten- und Geheimnisschutzes	47
8.1	Sicherung der datenschutzrechtlichen Ansprüche des Betroffenen	47
8.2	Geheimschutz	47

0 Versionshistorie

Version	Editor	Datum	Kommentar
0.1	Jobst Biester	21.02.2005	Gliederungsentwurf
0.2	Jobst Biester	03.05.2005	Erster inhaltlich vollständiger Entwurf
0.3	Jobst Biester	26.05.2005	Überarbeitung anhand von Kommentaren
1.0	Jobst Biester	04.09.2005	Abgestimmte Version für Nutzerbeirat

0.1 Dokumentverantwortlicher

Rolle	Name / OE	Bemerkung
Dokumentverantwortlicher	Jobst Biester / CC DS	

0.2 Verteilerliste

Erläuterung: In dem Abschnitt „Verteilerliste“ wird die jeweilige Rolle mit der Person benannt, die das vorliegende Dokument benötigt.

Rolle	Name / OE	Bemerkung
Projektleiter PTB	Tobias Schäfer	
CC VBPO	Dr. Ulrike Rausch	
CAT	Uwe Hanewald Dr. Wolf Zimmer	
CC DS	Jobst Biester	

1 Zielsetzung des Dokumentes

Aufgabenstellung

Das vorliegende Dokument beschreibt die rechtlichen Rahmenbedingungen für die Verwaltung, die bei der Langzeitarchivierung elektronisch signierter Dokumente zu beachten sind. Es werden die Rechtsvorschriften zur Archivierung dargestellt, die für die gesamte Bundesverwaltung gelten. Dabei wird insbesondere auch auf die Beweiskraft elektronischer Dokumente eingegangen, deren Gewährleistung ein wesentliches Ziel des Projektes ArchiSafe ist.

Zielsetzung

Im Rahmen des Projektes ArchiSafe sollen die Grundlagen für eine skalierbare elektronische Archivlösung geschaffen werden, die in der gesamten Bundesverwaltung eingesetzt werden kann, um elektronisch signierte Dokumente für eine Zeitraum von 30 oder mehr Jahren sicher und beweiskräftig aufbewahren. Die rechtlichen Anforderungen an die zu entwickelnde Archivlösung sind dabei von besonderer Bedeutung.

Adressat

Das vorliegende Dokument ist an alle Bundesbehörden gerichtet, die elektronische Dokumente aufbewahren müssen.

Gültigkeit

Dieses Dokument wird durch die jeweilige Betriebsführung geprüft und freigegeben. Fragen Sie den Dokumentverantwortlichen welches die letzte Version des Dokumentes ist.

Historie

Im Abschnitt 0 des vorliegenden Dokumentes erfolgt der Nachweis aller Änderungen.

2 Rechtsvorgaben

Auflistung der für die Aufbewahrung elektronischer Daten zu betrachtenden Rechtsvorgaben:

BArchG	Das Gesetz über die Sicherung und Nutzung von Archivgut des Bundes hat den Zweck, Dokumente auf Dauer zu sichern, nutzbar zu machen und wissenschaftlich zu verwerten.
DOMEA-Konzept	Das DOMEA-Konzept enthält eine Empfehlung für das Dokumenten-Management und die elektronische Archivierung in der öffentlichen Verwaltung.
GGO	Die Gemeinsame Geschäftsordnung der Bundesregierung beschreibt wesentliche Prinzipien behördlicher Aufbau- und Ablauforganisation und ist die zentrale Norm für die Bearbeitung von Geschäftsvorfällen in der Bundesverwaltung. Länder- und Kommunalverwaltungen verwenden eine eigene GO.
RegR	Die Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien (kurz: Registrierungsrichtlinie) hat das Ziel, auf der Grundlage der herkömmlichen papierbezogenen Bearbeitung, Registrierung und Aktenführung Regelungen zu treffen, die - angepasst an den derzeitigen Entwicklungsstand - den Umgang mit elektronischen Dokumenten berücksichtigen, und gleichzeitig den weiteren Entwicklungsprozess in der IT-gestützten Vorgangsbearbeitung offen halten.
SigG	Das Gesetz über Rahmenbedingungen für elektronische Signaturen (kurz: Signaturgesetz).
SigV	Die Verordnung zur elektronischen Signatur enthält Ausführungsbestimmungen zum SigG.
VwVfG	Das Verwaltungsverfahrensgesetz des Bundes regelt die öffentlich-rechtliche Verwaltungstätigkeit der Behörden.

3 Erfordernisse langfristiger Aufbewahrung

Bei der Bestimmung der Erfordernisse der langfristigen Aufbewahrung elektronischer Daten sind verschiedene Zwecke und eine Vielzahl von Vorschriften zu berücksichtigen. Aufbewahrungsvorgaben können sich sowohl aus Gesetzen und Verordnungen als auch internen Verwaltungsvorschriften ergeben. Im Folgenden werden die Aufbewahrungsvorgaben dargestellt, die für die gesamte Bundesverwaltung von Bedeutung sind.

3.1 Aufbewahrungsinteresse

Für die Aufbewahrung elektronischer Daten gibt es verschiedene rechtliche Vorgaben, die zu ermitteln und zu beachten sind. Diese Vorgaben beziehen sich auf unterschiedliche Zwecke, die mit der langfristigen Aufbewahrung elektronischer Daten verfolgt werden. Mit der langfristigen Aufbewahrung können auch mehrere Zwecke verbunden sein, wobei die Interessen auch gegenläufig sein können.¹

3.1.1 Verfügbarkeit

Elektronische Daten müssen aufbewahrt werden, um sie bei Bedarf verfügbar zu haben. Dieser Aufbewahrungszweck dient der internen Verwaltungsdokumentation und ermöglicht insbesondere ein arbeitsteiliges Verwaltungshandeln. Er dient aber auch dem Zweck, dem Bürger Einblick in den Stand des Verfahrens geben zu können. Die Verwaltungsdokumentation dient möglicherweise auch einem Gericht als Quelle der Rechtsfindung.

¹ Weitergehende Informationen zum Aufbewahrungsinteresse: ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.1 (Die Ergebnisse des Projektes ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente – werden im Sommer 2005 in Buchform veröffentlicht. Allgemeine Informationen zum Projekt ArchiSig sind unter www.archisig.de abrufbar.)

3.1.2 Nachweis eines Rechtszustandes

Elektronisch Daten sind grundsätzlich geeignet, im Rechtsverkehr Beweis zu erbringen. Hierzu müssen die elektronischen Daten in einer verkehrsfähigen Form² aufbewahrt werden, um sie ggf. einem Gericht bei Beweisantritt vorlegen zu können. Die Beweiskraft der Daten hängt dabei entscheidend davon ab, ob z.B. ein Gericht die Daten für echt hält, d.h. davon ausgeht, dass sie seit ihrer Erzeugung nicht verändert worden sind und in der Form, wie sie vorliegen, von dem bezeichneten Aussteller herrühren (Integrität und Authentizität).

Ein besonderer Schutz der Integrität und Authentizität und damit des Vertrauen des Rechtsverkehrs oder z.B. eines Gerichts in die Echtheit der zu Beweis Zwecken vorgelegten Daten wird in der elektronischen Kommunikation durch qualifizierte elektronische Signaturen bewirkt (siehe hierzu Abschnitt 4). Ohne diesen Schutz kann die Integrität und Authentizität eines elektronischen Dokuments leicht(er) abgestritten werden.

3.1.3 Revisionssicherheit

Als revisionssicher wird eine Aufbewahrung elektronischer Daten gemäß dem Konzept papierarmes Büro der KBSt (DOMEA-Konzept) bezeichnet, wenn diese entsprechend den Vorgaben aus §§ 239, 257 HGB, §§ 146, 147 AO und GoBS³ sicher, unverändert, vollständig, ordnungsgemäß, verlustfrei reproduzierbar und datenbankgestützt recherchierbar sind.

Revisionssicherheit bedeutet danach, dass Veränderungen an den Daten jederzeit nachvollzogen werden können. Der Zustand der Daten muss zu jedem Zeitpunkt rekonstruierbar sein. Es kann jederzeit nachgewiesen werden, wer welche Datensätze geändert hat. Jede Änderung an ihren Daten, also jede Eingabe, wird gespeichert und historisiert. Der alte und der neue Zustand nach der Änderung wird mit einer Angabe des

² Elektronisch signierte Daten müssen so ausgetauscht werden können, dass ihr Beweiswert erhalten bleibt.

³ Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme

Zeitpunktes der Änderung und der Person, die die Änderung vorgenommen hat, gespeichert. Die Daten können zu jedem Zeitpunkt wiederhergestellt werden.⁴

3.1.4 Dauerhafte Aufbewahrung

Gemäß § 1 BArchG ist das Archivgut des Bundes durch das Bundesarchiv auf Dauer zu sichern, nutzbar zu machen und wissenschaftlich zu verwerten. Gleiches gilt mit ähnlichen Formulierungen für die Landesarchive.

Dauerhaft aufbewahrt werden diejenigen Unterlagen, denen bleibender Wert für die Erforschung oder das Verständnis der deutschen Geschichte, die Sicherung berechtigter Belange der Bürger oder die Bereitstellung von Informationen für Gesetzgebung, Verwaltung oder Rechtsprechung zukommt.

3.2 Aktenmäßigkeit des Verwaltungshandelns

Das Gebot der Aktenmäßigkeit des Verwaltungshandelns ist indirekt aus dem allgemeinen Rechtsstaatsgebot abgeleitet. Das Grundgesetz für die Bundesrepublik Deutschland führt in Art. 20 Grundsätze der Verfassung auf.⁵ Einer dieser Grundsätze ist das Rechtsstaatsgebot, das in Art. 20 Abs. 3 GG verankert ist und auch als „Vorbehalt des Gesetzes“ bezeichnet wird.⁶

Da sich aus allgemeinen Grundsätzen wie dem Rechtsstaatsprinzip direkt jedoch allenfalls Tendenzen, aber keine festen rechtlichen Vorgaben ableiten lassen, ist das Gebot der Aktenmäßigkeit in weiteren Vorschriften konkretisiert. Die für die gesamte Bundesverwaltung geltenden Vorschriften werden im Folgenden dargestellt.

⁴ KBSt, DOMEA-Konzept, Organisationskonzept, Version 2.0, Dokumentenmanagement und Archivierung im IT-gestützten Geschäftsgang, Oktober 2004

⁵ Diese sind so bedeutsam, dass Artikel 79 Abs. 3 GG deren Änderung untersagt

⁶ „Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden.“

In welcher Weise diesen Vorschriften Rechnung getragen wird, bleibt in der Regel letztlich der Verwaltung selbst überlassen. Regelmäßig sind hier technisch-organisatorische Vorkehrungen erforderlich, wie etwa ein Zugriffsmanagement, die Protokollierung von Änderungen, etc., um insbesondere die Gebote der Aktenwahrheit und Aktenvollständigkeit abzusichern.⁷

3.2.1 Gemeinsame Geschäftsordnung der Bundesministerien (GGO)

In der GGO werden die Grundsätze der Vorgangsbearbeitung mittels Akten für die Bundesministerien und die nachgeordneten Stellen des Bundes geregelt. Da die Erfordernisse einer langfristigen Aufbewahrung elektronischer Daten bereits während der Vorgangsbearbeitung zu berücksichtigen sind, sind diese Grundsätze hier von Bedeutung.

Der für die langfristige Aufbewahrung elektronischer Daten relevante allgemeine Grundsatz der Vorgangsbearbeitung mittels Akten lautet:

Der Stand einer Sache muss jederzeit aus den Akten vollständig ersichtlich sein.

Dieser allgemeine Grundsatz der Vorgangsbearbeitung hat in § 12 Abs.2 GGO seinen Niederschlag gefunden:

„Stand und Entwicklung der Vorgangsbearbeitung müssen jederzeit (im Rahmen der Aufbewahrungsfristen) aus den elektronisch oder in Papierform geführten Akten nachvollziehbar sein. Einzelheiten der Dokumenten- und Aktenverwaltung regelt die Registraturrichtlinie (RegR).“

Aus diesem allgemeinen Grundsatz lassen sich direkt keine festen Vorgaben für die langfristige Aufbewahrung elektronischer Daten ableiten. Dazu bedarf es weiterer ergänzender Regelungen.

⁷ Vor allem für den Bereich der Sozialversicherung gibt es hier allerdings mit den §§ 110a ff. SGB IV detaillierte gesetzliche Vorgaben.

3.2.2 Registraturrechtlinie (RegR)

Die Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien (kurz: Registraturrechtlinie, RegR) ergänzt die GGO und regelt das Bearbeiten von Geschäftsvorfällen und das Verwalten von Schriftgut in den Bundesministerien. Sie ist Rahmenrichtlinie für alle Bundesministerien und eine Leitlinie für die nachgeordneten Stellen des Bundes.

Ein allgemeiner Grundsatz für die Aktenführung lautet:

Die Aktenführung sichert ein nachvollziehbares transparentes Verwaltungshandeln und ist Voraussetzung für eine sachgerechte Archivierung.

Dieser Grundsatz hat in § 18 Abs. 1 RegR seinen Niederschlag gefunden:

Abschließend bearbeitetes Schriftgut ist bis zur Aussonderung (§§ 20 bis 22 RegR) vollständig im Aktenbestand aufzubewahren, vor einem unbefugten Zugriff zu sichern und vor Beschädigung und Verfall zu schützen. Bei elektronisch gespeichertem Schriftgut sind die Vollständigkeit, Integrität, Authentizität und Lesbarkeit durch geeignete Maßnahmen zu gewährleisten.

Auch aus der RegR lassen sich keine festen Vorgaben für die langfristige Aufbewahrung elektronischer Daten ableiten. Die RegR gibt vielmehr Aufbewahrungsziele vor, die dann durch geeignete Maßnahmen zu gewährleisten sind. Die Aufbewahrungsziele wären sicherlich durch das Signieren der Daten mit einer qualifizierten oder akkreditierten elektronischen Signatur sowie deren Pflege durch erneute Signaturen zu erreichen. Die RegR lässt jedoch offen, ob die Aufbewahrungsziele nicht auch durch andere Maßnahmen erreicht werden können.

3.2.3 Verwaltungsverfahrensgesetz (VwVfG)

Aus § 29 VwVfG, der die Akteneinsicht durch Beteiligte regelt, ergibt sich mittelbar die Verpflichtung zum Führen von Akten. Dass dies auch für elektronische Akten gilt ergibt sich aus dem umfassenden Aktenbegriff des VwVfG, welcher auch Datenträger sowie Dateien einschließlich der zu ihrer Auswertung erforderlichen Programme erfasst (materieller

Aktenbegriff). Ein behördliches Bedürfnis an einer sicheren Aktenführung bzw. Archivierung ergibt sich darüber hinaus auch aus Gründen der Beweissicherung.

Das Gebot der Aktenmäßigkeit beinhaltet ein Gebot der Vollständigkeit einschließlich des Gebots der Führung wahrheitsgetreuer Akten. Deshalb muss grundsätzlich auch die das Verwaltungsverfahren betreffende E-Mail-Kommunikation aus Verfahrensakten ersichtlich werden. Ob dies z. B. auch jede E-Mail betrifft, die innerhalb eines Verwaltungsverfahrens ausgetauscht wird, ist im Einzelfall zu prüfen.⁸

Auch aus dem VwVfG lassen sich keine festen Vorgaben für die langfristige Aufbewahrung elektronischer Daten ableiten. Konkrete Vorgaben können in den jeweiligen Aktenordnungen enthalten sein.

3.2.4 DOMEA-Konzept

Das DOMEA-Konzept – 1996 ins Leben gerufen – ist ein Konzept für das Dokumenten-Management und die elektronische Archivierung in der öffentlichen Verwaltung. Wesentliches Ziel des DOMEA-Konzepts ist die Einführung der elektronischen Akte. Die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) hat das Konzept ursprünglich erstellt und es entsprechend den neuen Herausforderungen der Informations- und Kommunikationstechnologien weiterentwickelt. Die KBSt hat die notwendigen Funktionalitäten in einem Anforderungskatalog zusammengefasst. Dieser Katalog hat sich inzwischen als Standard-Katalog für die elektronische Vorgangsbearbeitung in der öffentlichen Verwaltung etabliert und dient vielen behörden-spezifischen Anforderungskatalogen als Grundlage.

Gemäß dem DOMEA-Konzept wird die elektronische Akte in IT-gestützter Vorgangsbearbeitung erzeugt, erfasst und verwaltet. Dabei gelten die gleichen Anforderungen an das elektronische Schriftgut, die in Gesetzen, Geschäftsordnungen, sowie Richtlinien und Vorschriften für Papierakten festgelegt sind. Behördliche Unterlagen müssen auch in elektronischer Form den Kriterien Vollständigkeit, Integrität und Authentizität, Zusammen-

⁸ Je nach Bedeutung der E-Mail könnte sie dem Bereich des informellen Verwaltungshandelns zuzuordnen sein, der in Akten nicht dokumentiert sein muss.

fassung aufgabenbezogener und zusammengehöriger Schriftstücke, Nachvollziehbarkeit und Rechtmäßigkeit des Verwaltungshandelns genügen. So müssen auch elektronische Akten hinreichenden Inhalt und Struktur aufweisen und sich in einen Kontext einordnen lassen. Elektronische Akten sollen wie ihre Vorgänger im Papierformat über die unmittelbare Bearbeitung hinaus ihre Nachweisfunktion erfüllen.

Das DOMEA-Konzept gliedert sich in ein Grundmodul⁹ und mehrere Erweiterungsmodule. Für die langfristige Aufbewahrung elektronischer Daten ist insbesondere das Erweiterungsmodul zum DOMEA-Konzept relevant, dass die Aussonderung und Archivierung elektronischer Akten zum Gegenstand hat.¹⁰ Abschnitt 4.3.2 dieses Erweiterungsmoduls befasst sich mit der Erneuerung elektronischer Signaturen während der Aufbewahrungsfrist. Dort wird ein Verfahren vorgeschlagen, dass sich am ArchiSig-Projekt orientiert. Die Erneuerung elektronischer Signaturen wird im DOMEA-Konzept bisher jedoch nur cursorisch als Randthema behandelt. Aus diesem Grunde wurde auch bereit die Notwendigkeit erkannt, ein weiteres Erweiterungsmodul zum DOMEA-Konzept zu erstellen, das speziell dieses Thema behandelt.

Das DOMEA-Konzept hat für die Verwaltung lediglich empfehlenden Charakter, so dass sich auch aus diesem Konzept keine festen Vorgaben für die langfristige Aufbewahrung elektronischer Daten ableiten lassen.

3.3 Archivanforderungen

Die Archivanforderungen ergeben sich aus den jeweiligen Archivgesetzen (ArchivG) der Länder und des Bundes. Das Bundesarchivgesetz erfasst zwar auch alle elektronischen Unterlagen (§ 2 Abs. 8), trifft aber keine näheren Regelungen über deren langfristige Aufbewahrung.

§ 2 Abs. 5 BArchG schreibt den Stellen des Bundes allerdings vor, bei maschinell lesbaren

⁹ KBSt, DOMEA-Konzept, Organisationskonzept, Version 2.0, Dokumentenmanagement und Archivierung im IT-gestützten Geschäftsgang, Oktober 2004

¹⁰ KBSt, DOMEA-Konzept, Organisationskonzept 2.0, Erweiterungsmodul zum Organisationskonzept 2.0, Aussonderung und Archivierung elektronischer Akten, Oktober 2004



ArchiSafe



Datenträgern die Form der Übermittlung der Daten mit dem Bundesarchiv zu vereinbaren und dabei die allgemein anerkannten Regeln der Technik einzuhalten. Dementsprechend regelt § 21 RegR, dass zur Sicherstellung einer ordnungsgemäßen Aussonderung in Abstimmung mit dem Bundesarchiv eine Schnittstelle vorzusehen ist.

4 Sicherung der Integrität und Authentizität durch qualifizierte elektronische Signaturen

„Die Gewährleistung der Authentizität und Integrität von Daten und die zuverlässige Identifizierung dessen Urheber bilden das grundlegende Fundament des elektronischen Rechts- und Geschäftsverkehrs“.¹¹ Elektronische Signaturen sind das nach dem Stand der Wissenschaft am besten geeignete Sicherungsmittel, um die Integrität und Authentizität von Daten zu gewährleisten.

Das Signaturgesetz (SigG) und die Signaturverordnung (SigV) regeln die technischen Rahmenbedingungen für elektronische Signaturen. Das Signaturgesetz definiert vier Signaturstufen zur Unterscheidung von elektronischen Signaturen unterschiedlicher Qualität. Zu unterscheiden sind:

- Einfache elektronische Signaturen
- Fortgeschrittene elektronische Signaturen
- Qualifizierte elektronische Signaturen
- Qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung (kurz „akkreditierte Signaturen“)¹²

4.1 Schriftformerfordernis

Gemäß § 10 VwVfG ist das Verwaltungsverfahren im Grundsatz formfrei. Dabei handelt es sich um einen allgemeinen Rechtsgrundsatz, der auch über das VwVfG hinaus Anwendung findet (Vermutung der Formfreiheit). Der Grundsatz der Formfreiheit gilt sowohl im Bereich des Verwaltungshandelns (einschließlich des Erlasses von Verwaltungsakten¹³) als auch für Handlungen und Erklärungen eines Bürgers / Unternehmens gegenüber der Behörde.

¹¹ ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.5

¹² Weitergehende Information zu den Signaturstufen: ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.5.1

¹³ Zu beachten ist, dass nur in seltenen Ausnahmefällen für Verwaltungsakte einer Behörde die Verwendung einer Signatur vorgeschrieben ist. Selbst wenn für einen Verwaltungsakt die Schriftform vorgeschrieben ist, so folgt § 37 VwVfG eigenen Regeln für die Formvorschriften; eine qualifizierte Signatur ist dafür in der Regel nicht erforderlich.

Grundsätzlich spricht somit nichts dagegen, für die Kommunikation mit der Verwaltung auch einfache Formen elektronischer Signaturen zu verwenden, wie etwa eine E-Mail, die zwar unter Umständen den Namen des Erstellers erkennen lässt, deren Integrität und Authentizität jedoch in der Regel nicht überprüft werden kann, so dass Manipulationen nicht ausgeschlossen werden können.

Die Formfreiheit besteht gemäß § 10 VwVfG nur insoweit, als keine besonderen Rechtsvorschriften für die Form des Verfahrens oder einzelne Handlungen bestehen. Eine nähere Regelung der elektronischen Kommunikation erfolgte insbesondere durch das 3. VwVf-ÄndG¹⁴ mit der Einführung des § 3a VwVfG, der an ein bestehendes Schriftformerfordernis anknüpft.¹⁵

Gemäß § 3a Abs. 2 VwVfG erfüllt ein elektronisches Dokument dann die Anforderungen eines gesetzlich bestehenden Schriftformerfordernisses, wenn es mit einer qualifizierten elektronischen Signatur versehen ist. Wie zuvor bereits im Privatrecht wurde die qualifizierte elektronische Signatur damit auch im öffentlichen Recht als elektronisches Pendant zur eigenhändigen Unterschrift anerkannt. Sofern ein Schriftformerfordernis für das Verwaltungshandeln oder Handlungen gegenüber einer Behörde besteht, ist grundsätzlich ein elektronisches Dokument mit qualifizierter elektronischer Signatur notwendig und hinreichend. Ausnahmen von diesem Grundsatz bedürfen einer ausdrücklichen Regelung durch den Gesetzgeber.

Der Gesetzgeber hat bereits durch das 3. VwVf-ÄndG ausdrückliche Regelungen in verschiedenen Fachgesetzen vorgenommen, soweit er eine abweichende Regelung für notwendig hielt. Soweit der elektronische Rechtsverkehr dadurch ausgeschlossen wird, ist dies häufig dadurch begründet, dass die technische Ausstattung der Behörden einen flächendeckenden elektronischen Rechtsverkehr zum Teil noch nicht gewährleisten kann.

¹⁴ Drittes Gesetz zur Änderung verwaltungsverfahrenrechtlicher Vorschriften vom 21. August 2002, Bundesgesetzblatt Jahrgang 2002 Teil I Nr. 60, ausgegeben zu Bonn am 27. August 2002

¹⁵ Weitergehende Informationen zu Formvorschriften im öffentlichen Recht und im Privatrecht: ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.3

Abweichende Regelungen sind aber auch dadurch begründet, dass teilweise die Signaturstufe „qualifizierte Signatur“ im Einzelfall als nicht angemessen erscheint.

Abweichende Regelungen von der Generalklausel des § 3a Abs. 2 VwVfG werden im Gesetzestext regelmäßig folgendermaßen zum Ausdruck gebracht:

- Das Begriffspaar „schriftlich oder elektronisch“ wird vom Gesetzgeber verwendet, wenn bei gesetzlich angeordneter Schriftform auch einfache Formen elektronischer Kommunikation ausreichen sollen. Eine qualifizierte elektronische Signatur ist hier nicht erforderlich.
- Soll die Generalklausel des § 3a Abs. 2 VwVfG überhaupt keine Anwendung finden und auch keine sonstige Form der elektronischen Kommunikation erfolgen, wird dies vom Gesetzgeber explizit mit den Formulierungen „die elektronische Form ist ausgeschlossen“ / „§ 3a VwVfG findet keine Anwendung“ zum Ausdruck gebracht.

Ferner hat der Gesetzgeber in Einzelfällen die Verwendung einer qualifizierten Signatur mit Anbieter-Akkreditierung angeordnet, soweit es um Handeln der Behörde geht (siehe hierzu Abschnitt 4.3).

4.2 Erfordernis hoher Beweissicherheit

Auch außerhalb des Bereichs, für den der Gesetzgeber ausnahmsweise die Schriftform für einzelne Schritte des Verfahrens angeordnet hat, kann es ein Bedürfnis nach einer hohen Beweissicherheit elektronischer Daten geben. Dabei sind die Konsequenzen einer möglichen Verfälschung von elektronischen Daten, insbesondere die Gefahr aufgrund einer eventuellen leichteren Abstreitbarkeit des Dokuments sorgfältig zu untersuchen. Die Verwendung qualifizierter elektronischer Signaturen kann demzufolge auch dann angezeigt sein, wenn hierfür keine explizite gesetzliche Vorgabe besteht.

Dabei ist allerdings zu beachten, dass von den Bestimmungen in § 3a Abs. 2 VwVfG sowie in abweichenden Fachgesetzen, die die elektronische Kommunikation mit dem Bürger betreffen, nicht ohne explizite gesetzliche Grundlage abgewichen werden darf. Ohne eine solche Grundlage darf die Verwaltung weder geringere noch höhere Ansprüche an die Signaturerfordernisse bei der elektronischen Kommunikation stellen. Sie muss elektronische

Eingänge ohne qualifizierte Signatur mithin auch dann als formgerecht annehmen, wenn der Inhalt des eingegangenen Dokumentes äußerst beweisrelevant ist.¹⁶ Sofern es um elektronische Dokumente der Behörde geht, ist ihr die Verwendung einer höheren als der vorgeschriebenen Signaturstufe natürlich frei gestellt.

Daneben stellt sich die Frage des Einsatzes qualifizierter elektronischer Signaturen zur Beweiskräftigen Dokumentation auch bei anwendungsabhängigen Datensammlungen der Verwaltung, z. B. bei elektronischen Vorgängen und Akten. Hier ist es ggf. nicht ausreichend, wenn sich die hohe Beweissicherheit nur auf einzelne Daten bezieht.¹⁷

4.3 Dauerhafte Überprüfbarkeit

Die Anforderungen an die Integrität und Authentizität elektronischer Daten können durch qualifizierte elektronische Signaturen in der Regel erfüllt werden. Ausnahmsweise kann jedoch eine höhere Signaturstufe gefordert werden. Hierzu bedarf es einer abweichenden gesetzlichen Regelung, in der die dauerhafte Überprüfbarkeit der elektronischen Signatur vorgeschrieben wird. Hierdurch soll z.B. sichergestellt werden, dass Verwaltungsakte mit besonderer Bedeutung (z. B. Dauerverwaltungsakte) auch über längere Zeit beweiskräftig bleiben.

Bei der Anordnung der dauerhaften Überprüfbarkeit ist allerdings § 1 Abs. 3 SigG zu beachten. Danach ist die Vorgabe einer höheren Signaturstufe als die der qualifizierten elektronischen Signatur in Übereinstimmung mit der EU-Signaturrichtlinie nur unter bestimmten restriktiven Voraussetzungen zulässig.

Bereits normiert wurde das Erfordernis der dauerhaften Überprüfbarkeit für einzelne Verwendungen von Signaturen seitens der Behörde, z. B. in § 33 Abs. 5 Nr. 2 VwVfG für elektronische Beglaubigungen und in § 69 Abs. 2 S. 2 VwVfG für elektronische

¹⁶ In diesem Fall stellt sich allerdings die Frage, ob die Eingänge durch eine Art „Eingangssignatur“ einen höheren Sicherheitsstandard erhalten sollen.

¹⁷ Im ArchiSig-Anforderungskatalog wurde die Anforderung erhoben, dass sich die hohe Beweissicherheit bei Bedarf auch auf gesamte Vorgänge und Akten zu erstrecken hat: ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.3.1.1.2

Verwaltungsakte bei Abschluss eines förmlichen Verwaltungsverfahrens i. S. v. § 63 Abs. 1 VwVfG. Darüber hinaus sieht § 37 Abs. 4 VwVfG vor, dass für Verwaltungsakte, die nach § 3a Abs. 2 VwVfG aufgrund eines gesetzlich bestimmten Schriftformerfordernisses einer qualifizierten elektronischen Signatur bedürfen, durch Rechtsvorschrift die dauerhafte Überprüfbarkeit vorgeschrieben werden kann.

Was unter „dauerhafter Überprüfbarkeit“ elektronischer Signaturen zu verstehen ist, bestimmt sich nach dem jeweiligen Stand der Technik. Eine qualifizierte elektronische Signatur gilt zur Zeit als dauerhaft überprüfbar, wenn der Zertifizierungsdiensteanbieter durch Organisation seiner technischen Infrastruktur sicherstellt, dass die von ihm ausgestellten qualifizierten Zertifikate für einen Zeitraum von 30 Jahren nach dem Ende des Jahres, indem der im Zertifikat angegebenen Gültigkeitszeitraum abläuft, in einem sicheren Verzeichnis führt. Diese Anforderung erfüllen akkreditierte Zertifizierungsdiensteanbieter gem. § 15 SigG i. V. m. § 4 Abs. 2 SigV.

5 Die Signaturerneuerung nach § 17 SigV

Die Verwendung elektronischer Signaturen ist in vielen Fällen nur dann sinnvoll – und auf Seiten der Behörde möglicherweise aus Gründen ihrer Dokumentationspflicht nur dann zulässig –, wenn die Signaturen einen langfristigen Schutz der Integrität und auch einen Nachweis der Authentizität der signierten Daten sicherstellen. Da signierte Daten eine dauerhafte beweissichere Dokumentation – anstelle der bisherigen „Papier-Dokumentation“ – gewährleisten müssen, müssen der Schutz der Integrität und der Nachweis der Authentizität dauerhaft sein. Dieser Anforderung wird durch das Signaturgesetz auf vielfältige Weise Rechnung getragen. Die durch das Signaturgesetz beschriebene Infrastruktur ist prinzipiell geeignet, die Beweiskraft qualifizierter elektronischer Signaturen langfristig sicherzustellen, sofern die dazu erforderlichen Sicherungsmaßnahmen ergriffen werden.

Zu den für die langfristige Sicherstellung der Beweiskraft erforderlichen Sicherheitsmaßnahmen gehört insbesondere auch die Signaturerneuerung nach § 17 SigV, die dem langfristigen Schutz der Integrität dient. Daneben muss auch der Schutz der Authentizität, also der Identifizierbarkeit des Ausstellers, langfristig gewährleistet sein.

Ohne diese Maßnahmen wäre das Ziel, die hohe Beweiskraft signierter Dokumente langfristig zu erhalten, nicht zu erreichen. Denn ein Dokument, dessen Integrität und Authentizität vor Gericht leicht abgestritten werden könnte, weil Manipulationen nicht ausgeschlossen werden können, wird aller Voraussicht nach einen nur einen geringen Beweiswert haben (zur Beweisführung mit qualifiziert signierten Dokumenten siehe Abschnitt 6).¹⁸

5.1 Obliegenheiten und Rechtspflichten

Gemäß § 17 SigV „sind“ Daten mit einer qualifizierten elektronischen Signatur neu zu signieren, wenn sie für längere Zeit benötigt werden, als der Signaturalgorithmus als geeignet (technisch sicher) beurteilt werden kann. § 17 SigV begründet allerdings keine

¹⁸ Weitergehende Informationen zu § 17 SigV: ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.5.2

Rechtspflicht. Der Zweck dieser technischen Vorschrift ist darauf beschränkt, ein geeignetes Verfahren für eine langfristige Datensicherung zu beschreiben. Ob der Empfänger signierter Daten eine solche Sicherung vornimmt, ist prinzipiell in sein Belieben gestellt, denn in der Regel trägt nur er die Konsequenzen des Verlustes einer beweiskräftigen Dokumentation

Der Zertifizierungsdiensteanbieter hat den Signaturschlüssel-Inhaber gemäß § 6 Abs. 1 S.2 SigG i. V. m. § 6 Nr. 5 SigV darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf gemäß § 17 SigV neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird. Die Anwendung des Verfahrens ist damit grundsätzlich als eine Obliegenheit im Umgang mit signierten Daten anzusehen. Die Obliegenheit besteht unabhängig vom Hinweis des Zertifizierungsdiensteanbieters.

Auch wenn § 17 SigV somit grundsätzlich lediglich eine Obliegenheit begründete, kann eine Rechtspflicht zur Anwendung des § 17 SigV bestehen. Diese muss sich dann jedoch aus anderen Gesetzen oder aus Vertrag ergeben.¹⁹ Eine Rechtspflicht zur Anwendung des § 17 SigV besteht immer dann, wenn sich auf Grund von Gesetzen oder Verträgen die Verpflichtung ergibt, den besonderen Beweiswert qualifizierter elektronischer Dokumente zu erhalten (siehe Abschnitt 6).

5.2 Sicherung der Integrität

Die Integrität einer elektronischen Signatur wird durch mathematische Algorithmen gesichert, die bei der Signaturbildung und Signaturprüfung verwendet werden. Bei der Signaturbildung müssen die Daten, auf die sich die Signatur bezieht, gemäß § 2 Nr. 2d SigG so mit der elektronischen Signatur verknüpft werden, dass jede Änderung der Daten oder der Signatur bei der Signaturprüfung erkennbar wird, da die Signatur für diese Daten in diesem Fall nicht gültig ist. Die Prüfung dieser Verknüpfung zwischen Daten und Signatur wird allgemein als mathematische Gültigkeitsprüfung bezeichnet.²⁰

¹⁹ Roßnagel, Fischer-Dieskau, Pordes, Brandner, CR 4/2004, S. 305

²⁰ Der Integritätsschutz wird technisch dadurch bewirkt, dass von dem zu signierenden Dokument ein Hashwert gebildet wird, auf den ein Signaturalgorithmus angewendet wird. Die Hashwert ist eine Art mathematischen Fingerabdruck der zu signierenden Daten. Der signierte Hashwert „in“ der
Seite 21 von 47
2005-09-04_Verwaltungsrechtliche_Rahmenbedingungen_V10.doc

Die Bundesnetzagentur (BNetzA)²¹ veröffentlicht im Bundesanzeiger jährlich die Algorithmen und deren Parameter, die als geeignet angesehen werden, die Integrität für die Dauer von mindestens 6 Jahren zu gewährleisten.²² Sobald die BNetzA ankündigt, dass sie einen Algorithmus bzw. einen zugehörigen Parameter ab einem bestimmten Zeitpunkt als nicht mehr sicher genug ansieht (Abkündigung des Algorithmus), sollte dieser Algorithmus danach nicht mehr verwendet werden, da die Integrität einer danach erzeugten Signatur und damit die Integrität der signierten Daten zweifelhaft sein könnte.

Bei bereits vorliegender qualifizierter elektronischer Signatur kann die Situation eintreten, dass der besondere Beweiswert einer qualifizierten elektronischen Signatur auch nach einer Abkündigung des verwendeten Algorithmus weiterhin erhalten bleiben muss. Falls in diesem Fall keine zusätzlichen Maßnahmen zur Sicherung der Integrität der Signatur ergriffen werden, könnte auch hier die Integrität der signierten Daten zweifelhaft werden. Als besondere Maßnahme zur langfristigen Sicherung der Integrität wurde das in § 17 SigV beschriebenen Verfahren konzipiert.

Das Ziel dieses Verfahrens ist es, die Integrität der mit einer qualifizierten elektronischen Signatur versehenen Daten auch dann noch feststellen so können, wenn die mathematische Signaturprüfung aufgrund mangelnder Sicherheitseignung der verwendeten Algorithmen nicht mehr geeignet ist, die Integrität der signierten Daten zu belegen. Falls der verwendete Hash-Algorithmus unsicher geworden ist, kann es gelingen, andere Daten zu präsentieren, die den gleichen Hashwert haben wie die tatsächlich signierten Daten.²³ Falls der Signaturalgorithmus unsicher geworden ist, kann es z. B. gelingen, den Signaturschlüssel aus dem öffentlich bekannten Prüfschlüssel zu berechnen.

Signatur wird bei der Verifikation mit dem Hashwert des signierten Dokuments verglichen. Ist der Hashwert identisch, ist dies der Beleg dafür, dass die signierten Daten nicht manipuliert worden sind.

²¹ Frühere Bezeichnung: RegTP

²² Die Überprüfung der Sicherheit der Algorithmen und deren Parameter obliegt dem BSI.

²³ Die Kryptographen nennen dies eine Kollision. Allgemein wird ein Hash-Algorithmus als kollisionsfrei bezeichnet, wenn es praktisch unmöglich ist, verschiedene elektronische Daten mit dem gleichen Hashwert zu produzieren.

Um sicherzustellen, dass die Integrität qualifizierter elektronischer Signaturen – trotz später möglicherweise bekannt werdender Sicherheitsmängel – auf Dauer nachweisbar ist, wird eine Integritätssicherung benötigt, die die Signaturen zu einem Zeitpunkt „konserviert“, zu dem diese Mängel in Nachhinein als noch nicht relevant anzusehen sind. Daher müssen Daten mit einer neuen qualifizierten Signatur nach den Vorgaben des § 17 SigV versehen werden, wenn die Daten nach Ablauf der Eignung der verwendeten Signaturalgorithmen noch benötigt werden.

5.3 Anforderungen an die erneute Signatur gemäß § 17 SigV

Die folgenden Vorgaben, die § 17 SigV für diese erneute Signierung macht, sind auslegungsbedürftig: Die Daten sind mit einer neuen qualifizierten Signatur zu versehen. Diese (qualifizierte Signatur) muss geeignete Signaturalgorithmen verwenden, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.

Ein qualifizierter Zeitstempel ist gemäß § 2 Nr. 14 SigG eine elektronische Bescheinigung eines Zertifizierungsdiensteanbieters darüber, dass ihm elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Nach dem Wortlaut des § 17 SigV wird eine qualifizierte Signatur mit einem qualifizierten Zeitstempel verlangt. Es stellt sich die Frage, ob § 17 SigV sowohl eine qualifizierte Signatur als auch einen qualifizierten Zeitstempel verlangt, wenn bereits ein qualifizierter Zeitstempel eine qualifizierte elektronische Signatur enthält. Alle technischen Spezifikationen für Zeitstempel sehen vor, dass elektronische Signaturen verwendet werden, um Daten so mit einer authentischen Zeitangabe zu verbinden, dass die Vorlage der Daten zu diesem Zeitpunkt belegt werden kann. Qualifizierte Zeitstempel sind somit technisch gesehen in der Regel ebenfalls qualifizierte elektronische Signaturen.

Überwiegend wird vor diesem Hintergrund davon ausgegangen, dass der Gesetzgeber „nur“ einen mit einer qualifizierten elektronischen Signatur verbundenen Zeitstempel verlangt. Da ein qualifizierter Zeitstempel eine qualifizierte Signatur voraussetzt, wird eine teleologische Reduktion vorgenommen um unsinnige Ergebnisse zu vermeiden.²⁴

²⁴ Roßnagel, Fischer-Dieskau, Pordes, Brandner, CR 4/2004, S. 304

Bereits in der amtlichen Begründung zur Signaturverordnung wurde darauf hingewiesen, dass neben dem Zeitstempel keine weitere Signatur, z. B. die eines Archivars, erforderlich ist. Diese weitere Signatur würde keinen zusätzlichen Sicherheitswert haben. Die sicherheitstechnische Zielsetzung des § 17 SigV lässt sich auch ohne diese weitere Signatur erreichen.

Eine unmittelbare Folge dieser teleologischen Reduktion ist, dass die Anwendung des in § 17 SigV beschriebenen Verfahrens nicht erforderlich ist, falls bereits ein qualifizierter Zeitstempel vorliegt. Solange dieser Zeitstempel geeignet ist, die Signatur zu konservieren, besteht für die Anwendung des Verfahrens kein Bedarf. Mit dem Zeitstempel hat bereits eine erste Signaturerneuerung stattgefunden.

Allerdings kann der Zeitstempel selbst im Laufe der Zeit seinen Sicherheitswert verlieren. Für ihn gilt insoweit dasselbe wie für qualifizierte Signaturen, da der qualifizierte Zeitstempel mittels einer qualifizierten Signatur erteilt wird. Die sicherheitstechnische Eignung eines Zeitstempels kann im Laufe der Zeit verloren gehen. Bevor dies geschieht, müssen diese Zeitstempel daher ebenfalls konserviert werden, indem ein erneuter Zeitstempel eingeholt wird.

Sicherheitstechnisch lässt sich eine weitere teleologische Reduktion des § 17 SigV begründen, die den Zeitstempel betrifft. § 17 SigV unterscheidet nicht danach, ob der Hash-Algorithmus, der Signatur-Algorithmus oder beide ihre Eignung verlieren. Der qualifizierte Zeitstempel muss sich aber nur dann sowohl auf die signierten Daten als auch auf die Signatur beziehen, wenn das verwendete Hash-Verfahren unsicher zu werden droht. Falls der Hash-Algorithmus noch geeignet ist, muss sich der zu bildende Zeitstempel nur auf die Signatur beziehen. Dies reicht aus, da die Daten weiterhin zuverlässig mit der alten Signatur verknüpft sind. Sicherheitstechnisch gesehen ist es nicht erforderlich, für die Daten einen neuen Hashwert zu bilden, um diesen dann neu zu signieren.²⁵

²⁵ Roßnagel, Fischer-Dieskau, Pordes, Brandner, CR 4/2004, S. 303

Erst diese teleologische Reduktion ermöglicht eine wirtschaftliche Signaturerneuerung im Falle großer Datenvolumina. Solange die verwendeten Hash-Algorithmen als geeignet angesehen werden, müssen bei der Signaturerneuerung nur relativ kleine Datenmengen verarbeitet werden. Die ursprünglich signierten Daten, die demgegenüber in der Regel deutlich umfangreicher sind, müssen in den Verarbeitungsprozess nicht einbezogen werden.

Um eine wirtschaftliche Signaturerneuerung zu ermöglichen, wird § 17 SigV darüber hinaus so ausgelegt, dass es nicht erforderlich ist, für jedes elektronische Datum, das erneut signiert werden muss, einen eigenen Zeitstempel einzuholen. Ein Zeitstempel darf sich vielmehr auf beliebig viele signierte Daten beziehen. Dies kann es zu erheblichen Kosteneinsparungen führen, da qualifizierte Zeitstempel in der Regel kostenpflichtig sind.

Sicherheitstechnisch gesehen ist dies ohne weiteres möglich. Die Wirkung eines Zeitstempels als Mittel zur Integritätssicherung ist nicht davon abhängig, wie viele Signaturen gleichzeitig konserviert werden. Auch wurde bereits in der amtlichen Begründung zu § 18 SigV 1997 ausgeführt, dass „für eine beliebige Anzahl signierter Daten eine (übergreifende) neue digitale Signatur ... angebracht werden kann“.

§ 17 Satz 3 SigV fordert, dass frühere Signaturen in die Integritätssicherung einzubeziehen sind. Dies bedeutet, dass sich der Zeitstempel neben der Ausgangssignatur auch auf alle weiteren (Zeitstempel-)Signaturen beziehen muss, die später zu Konservierungszwecken angebracht wurden. Durch den jeweiligen Einschluss aller früheren Signaturen ergibt sich eine geschachtelte Datenstruktur.

Die Verwendung des Plurals in § 17 Satz 3 SigV (frühere Signaturen) wird zum Teil auch so interpretiert, dass sich der Zeitstempel im Falle von Mehrfachsignaturen stets auf alle Signaturen beziehen muss. Dies führt im Ergebnis zu einer Beweiserhöhung gegenüber den Ausgangssignaturen. Bei Mehrfachsignaturen wird zwischen parallelen und sequenziellen Signaturen unterschieden. Bei parallelen Signaturen kommt es nicht darauf an, in welcher Reihenfolge die Daten signiert wurden. Durch das Signaturdatenformat ist in der Regel kein Schutz gegen das unerkannte Löschen einzelner Signaturen vorgesehen, d. h. die Tatsache, dass es zu den elektronischen Daten mehr als eine Signatur gibt, wird nicht durch das Signaturformat gesichert. Sequenzielle Signaturen sichern demgegenüber die Reihenfolge,

in der die Daten signiert wurden, indem die jeweils nächste Signatur die vorhergehenden umfasst. Im Falle von parallelen Mehrfachsignaturen kann ein Zeitstempel deshalb zu einer Beweiswerterhöhung führen, da er die Vollständigkeit aller Signaturen zu den signierten Daten langfristig sicherstellen kann. Es wird die Meinung vertreten, dass diese Beweiswerterhöhung durch § 17 Satz 3 SigV gefordert wird.²⁶

Es wird jedoch auch die Meinung vertreten, dass § 17 Satz 3 SigV nicht in diesem Sinne auszulegen sei.²⁷ Es müsse dem Aufbewahrer überlassen bleiben, eigene Zielsetzungen bei der Aufbewahrung zu verfolgen. Der Aufbewahrer müsse selbst entscheiden können, ob es ihm nur darauf ankommt, dass lediglich einzelne Signaturen langfristig gesichert aufbewahrt werden, oder ob auch der Zusammenhang zwischen mehreren Signaturen nachvollziehbar gemacht werden soll.

Dieser Ansicht ist aus sicherheitstechnischen Gründen zuzustimmen. Zweck des § 17 SigV ist es, den Sicherheitswert von Signaturen zu erhalten, nicht jedoch, ihn zu erhöhen. Im Einzelfall kann es zwar erforderlich sein, die Vollständigkeit aller Signaturen nachweisen zu können. Dieser Zweck kann jedoch auch durch andere Maßnahmen erreicht werden, die deutlich wirtschaftlicher sein können.

In der Regel lässt sich die Integritätssicherung durch eine erneute Signatur wirtschaftlich durchführen, wenn im Falle von Mehrfachsignaturen alle Signaturen auf einmal erneuert werden. Dies setzt jedoch voraus, dass alle Mehrfachsignaturen bereits durch die verwendete Datenstruktur zusammengefasst wurden. Allgemein sind Mehrfachsignaturen lediglich dadurch definiert, dass zu elektronisch signierten Daten mehrere Signaturen vorliegen. Diese müssen nicht notwendig in nur einer Datenstruktur enthalten sein. Wirtschaftlich keinesfalls sinnvoll wäre es in diesem Fall, den Langzeitspeicher auf das Vorhandensein von Signaturen zu bestimmten Daten durchsuchen zu wollen, um danach alle zugehörigen Signaturen mit einem Zeitstempel zusammenfassen zu können.²⁸ Das Ziel,

²⁶ Roßnagel, Rechtsgutachten zur „Signaturgesetzkonformität des Standardisierungsvorschlags ‘Long-Term Conservation of Electronic Signatures` für die ISIS-MTT Spezifikation vom 30. 06. 2004, Kassel, den 20. Juli 2004, Seite 8

²⁷ Roßnagel, Fischer-Dieskau, Pordes, Brandner, CR 4/2004, S. 304

²⁸ Bei verschlüsselten Daten könnte dies sogar unmöglich sein.

die Vollständigkeit der Signaturen nachweisen zu können, ließe sich auf einfachere Art und Weise erreichen.

§ 17 Satz 3 SigV bedarf hinsichtlich der Sicherheitsstufe des zu verwendenden Zeitstempels einer weiteren Interpretation. § 17 Satz 3 SigV enthält keine Regelung darüber, ob stets ein Zeitstempel eines qualifizierten Zertifizierungsdiensteanbieters genügt oder ob unter bestimmten Umständen auch ein Zeitstempel eines akkreditierten Zertifizierungsdiensteanbieters erforderlich ist.

Sofern in Rechtsvorschriften die dauerhafte Überprüfbarkeit einer qualifizierten elektronischen Signatur angeordnet wird (vgl. Abschnitt 4.3), muss das qualifizierte Zertifikat, auf dem die Signatur beruht, von einem akkreditierten Zertifizierungsdiensteanbieter gemäß § 15 SigG ausgestellt sein.²⁹ Die erneute Signatur muss aus Gründen der Erhaltung der Beweiskraft mindestens die gleiche Sicherheitsstufe haben, wie die der Ausgangssignatur. Wenn die Ausgangssignatur akkreditiert ist, muss die erneute Signatur ebenfalls dieser Signaturstufe entsprechen, d. h. es wird in diesem Fall ein „akkreditierter“ Zeitstempel benötigt.

5.4 Sicherung der Authentizität

Neben der Integrität muss auch die Authentizität qualifizierter elektronischer Signaturen gesichert werden. Es muss langfristig nachweisbar sein, wem die Signatur zugerechnet werden kann, d. h. der Urheber der signierten Daten muss eindeutig erkennbar sein. Die für eine langfristige Aufbewahrung elektronischer Daten erforderlichen Vorkehrungen zur Sicherung der Authentizität sind im Signaturgesetz nur zum Teil geregelt. Fehlende Vorkehrungen müssen aus einer sicherheitstechnischen Betrachtung und den beweisrechtlichen Anforderungen an eine Prüfung von Zertifikaten gemäß Signaturgesetz entwickelt werden.

Die Zurechnung einer qualifizierten Signatur zu einem bestimmten Signaturschlüssel-Inhaber erfolgt über qualifizierte Zertifikate mit dem in § 7 SigG bestimmten Inhalt. Die Ausstellung

²⁹ Die Signatur wird in diesem Fall als qualifizierte elektronische Signatur mit Anbieter-Akkreditierung oder kurz als „akkreditierte“ Signatur bezeichnet.

eines qualifizierten Zertifikats durch einen Zertifizierungsdiensteanbieter setzt voraus, dass der Signaturschlüssel-Inhaber (der stets eine natürliche Person ist) zuverlässig identifiziert werden konnte und über eine sichere Signaturerstellungseinheit verfügt (vgl. § 5 SigG). Der Zertifizierungsdiensteanbieter hat das Zertifikat ggf. unverzüglich zu sperren (vgl. § 8 SigG). Diese und weitere im Signaturgesetz getroffene Vorkehrungen lassen den Urheber einer Signatur jederzeit mit hinreichender Sicherheit erkennen, sofern eine Prüfung des Zertifikats gemäß Signaturgesetz erfolgreich verlaufen ist (vgl. Abschnitt 6.4.1).

Die Authentifizierung erfolgt im Wege einer Überprüfung der qualifizierten Signatur anhand der Daten des Zertifikats. Voraussetzung für diese Prüfung gemäß Signaturgesetz ist es, dass das Zertifikat überhaupt vorliegt bzw. die zugehörige Dokumentation eingesehen und geprüft werden kann. Nach den Regelungen des Signaturgesetzes ist dieses jedoch nur für einen begrenzten Zeitraum gewährleistet: Ein Zertifizierungsdiensteanbieter hat die von ihm ausgestellten Zertifikate gemäß § 5 Abs. 1 Satz 2 SigG über öffentlich erreichbare Kommunikationsverbindungen jederzeit abrufbar zu halten. Damit scheint die Vorlage des Zertifikates zum Zwecke der Prüfung jederzeit möglich zu sein. Allerdings ist diese Pflicht des Zertifizierungsdiensteanbieters zweifach beschränkt.

Zunächst kann der Signaturschlüssel-Inhaber gemäß § 5 Abs. 1 Satz 3 SigG bestimmen, dass sein Zertifikat nicht abrufbar sein soll. Dem Zertifizierungsdiensteanbieter ist in diesem Fall verboten, das Zertifikat zum Abruf bereitzustellen. Der Signaturschlüssel-Inhaber selbst muss das Zertifikat dem bestimmungsgemäßen Empfänger der von ihm signierten Daten auf andere Weise zur Verfügung stellen, in der Regel dadurch, dass das Zertifikat der Signatur beigelegt wird.

Die Verpflichtung des Zertifizierungsdiensteanbieters ist aber auch zeitlich begrenzt. Gemäß § 4 Abs. 1 SigV besteht die gesetzliche Verpflichtung zur Bereithaltung der Dokumentation nur für einen Zeitraum von bis zu fünf Jahren nach dem Schluss des Jahres, in dem die Gültigkeit des Zertifikats abläuft. Dieser Zeitraum umfasst 30 Jahre, falls der Zertifizierungsdiensteanbieter akkreditiert ist (vgl. § 4 Abs. 2 SigV).

Nur solange die Daten des Zertifikats anhand der Dokumentation des Zertifizierungsdiensteanbieters überprüft werden können, kann der Empfänger signierter Daten positiv feststellen,

dass es sich um eine gültige qualifizierte Signatur handelt. Denn er erhält zwar in aller Regel das Zertifikat – also eine Kopie der Bescheinigung eines Zertifizierungsdiensteanbieters über die Zuordnung eines Signaturschlüsselpaares – mit der Signatur mitgeschickt. Dies gibt ihm aber noch keinen Aufschluss darüber, ob das Zertifikat zum Zeitpunkt der Signaturerzeugung gültig war oder ob es z.B. wegen Verlustes der Signaturkarte gesperrt worden ist. Diese Prüfung kann nur anhand der Dokumentation des Zertifizierungsdiensteanbieters vorgenommen werden, nämlich entweder über eine OCSP-Anfrage (online certificate status protocol) oder über den Abgleich mit sog. CRLs (certificate revocation list).

Nach dem Ende der Aufbewahrungspflicht des Zertifizierungsdiensteanbieters kann diese Prüfung der Gültigkeit nicht mehr durchgeführt werden und das Zertifikat kann auch nicht mehr vom ausstellenden Zertifizierungsdiensteanbieter bestätigt werden. Deswegen muss (Obliegenheit) der Empfänger signierter Daten, selbst dafür zu sorgen, dass er das Zertifikat vorgelegen und die Gültigkeit zum Zeitpunkt der Signaturerzeugung belegen kann, wenn er ggf. den Nachweis erbringen muss, dass eine gültige qualifizierte Signatur vorliegt.³⁰

(1) Vorhalten des Zertifikats. Mit Hilfe des Zertifikats ist der verwendete Signaturschlüssel auf ein konkretes Individuum zuverlässig zurückführbar. In der Regel muss der Empfänger die Vorkehrung treffen, nicht nur die signierten Daten und die Signatur, sondern auch die erforderlichen Zertifikate zu speichern. Sofern ihm diese Zertifikate nicht bereits vorliegen, muss er sie sich beschaffen, solange sie noch verfügbar sind.

Falls die Beschaffung der Zertifikate nicht bereits zeitnah erfolgt, sollte der Empfänger der Signatur auch das mit der Zeit wachsende Risiko berücksichtigen, dass der Zertifizierungsdiensteanbieter seine Tätigkeit einstellt und nicht dafür sorgt, dass ein anderer Zertifizierungsdiensteanbieter die von ihm ausgestellten Zertifikate übernimmt. Darüber hinaus ist stets auch das – wenn auch geringe – Risiko zu berücksichtigen, dass der Zertifizierungsdiensteanbieter seinen Verpflichtungen nicht mehr nachkommen kann, da die Zertifikate verloren gegangen oder nicht auffindbar sind.

³⁰ Da sich aus dem Signaturgesetz keine Rechtspflichten für den Empfänger ableiten lassen, müsste sich diese aus anderen Gesetzen oder aus Verträgen ergeben (vgl. Abschnitt 5.1).

Vor diesen Risiken kann sich der Empfänger einer Signatur am besten dadurch schützen, dass er bereits beim Eingang signierter Daten eine Signaturprüfung durchführt und die dazu erforderlichen Zertifikate, die ihm zu diesem Zweck ohnehin vorliegen müssen, zusammen mit den Daten und der Signatur sowie ggf. zusammen mit dem Abfrageergebnis in der Auskunft des Zertifizierungsdiensteanbieters über die Gültigkeit des Zertifikats speichert.

(2) Prüfen des Zertifikats mittels „Abfrage“ beim Zertifizierungsdiensteanbieter. Eine weitere notwendige Voraussetzung für eine Prüfung eines Zertifikats gemäß Signaturgesetz ist, dass das Zertifikat nachprüfbar ist. Die Nachprüfbarkeit setzt voraus, dass das Zertifikat in dem vom Zertifizierungsdiensteanbieter gemäß § 4 Abs. 1 SigV zu führenden Zertifikatsverzeichnis vorhanden ist. Eine Signaturprüfung nach Signaturgesetz erfordert stets eine Abfrage beim Zertifizierungsdiensteanbieter, der eine entsprechende Auskunft zu erteilen hat. Der Zertifizierungsdiensteanbieter hat diese Auskunft gemäß § 5 Abs. 1 Satz 2 SigG über öffentlich erreichbare Kommunikationsverbindungen zu erteilen. Da die Authentizität der Auskunft nachweisbar sein muss, werden Auskünfte der Zertifizierungsdiensteanbieter stets mit einer qualifizierten elektronischen Signatur des Zertifizierungsdiensteanbieters versehen.

Für diese Auskünfte des Zertifizierungsdiensteanbieters gelten die gleichen zeitlichen Beschränkungen wie für die Abrufbarkeit von Zertifikaten, denn nach Ende der Dokumentationsfrist kann auch der Zertifizierungsdiensteanbieter die gewünschte Auskunft mangels nachprüfbarer Dokumentation nicht mehr geben. Die o. g. Risiken für den Abruf von Zertifikaten bestehen mithin auch für die Auskünfte. Auch hier kann sich der Empfänger einer Signatur am besten dadurch schützen, dass er die Auskünfte unverzüglich einholt, prüft und speichert.

Die Auskunft des Zertifizierungsdiensteanbieters enthält neben den Angaben darüber, ob das Zertifikat im Verzeichnis vorhanden ist, auch eine Information über den Status des Zertifikats, insbesondere über seine Gültigkeit. Sperrungen hat der Zertifizierungsdiensteanbieter gemäß § 7 Abs. 2 SigV im Zertifikatsverzeichnis mit Angabe von Datum und Uhrzeit kenntlich zu machen. Da der Sperrstatus für eine Prüfung eines Zertifikats nach Signaturgesetz benötigt wird, sollten die Auskünfte auch aus diesem Grund unverzüglich einholt, geprüft und gespeichert werden.



ArchiSafe



Mit der signierten Auskunft des Zertifizierungsdiensteanbieters hat der Empfänger einer signierten Nachricht zumindest eine Art „Sekundärbeweis“ in Form einer Art von antizipierter Aussage eines sachverständigen Zeugen darüber, dass die Voraussetzungen für eine qualifizierte Signatur erfüllt sind. Dieses Beweismittel muss der Empfänger nach den oben beschriebenen Prinzipien beweissicher konservieren, denn es handelt sich bei der Auskunft des Zertifizierungsdiensteanbieters ja ebenfalls um eine in elektronischer Form vorliegende signierte Erklärung.

6 Beweiskraft elektronischer Dokumente

6.1 Allgemeine Beweisregeln

Nach allgemeinen Beweisregeln hat jede Partei in einem Prozess sämtliche Tatsachen darzulegen und im Fall des Bestreitens durch den Prozessgegner auch zu beweisen, die ihren Anspruch begründen, d. h. sie trifft die Darlegungs- und Beweislast. Legt die beweisbelastete Partei ein elektronisches Dokument zum Beweis für eine behauptete Tatsache vor, so unterliegt dieses elektronische Dokument (als Augenscheinsobjekt, § 371 ZPO) grundsätzlich der freien richterlichen Beweiswürdigung; das Gericht ist nicht an Beweisregeln gebunden.

Dies ändert sich, wenn das zum Beweis vorgelegte elektronische Dokument eine qualifizierte Signatur des Ausstellers trägt. Seit der Neufassung der ZPO durch das Justizkommunikationsgesetz zum 01.04.2005 erklärt der neu gefasste § 371a ZPO auf solche signierten Dokumente **die Beweisregeln für Urkunden** für entsprechend anwendbar. Nach diesen Beweisregeln begründen (private) Urkunden den vollen Beweis für die sich aus der Urkunde ergebende Tatsache bzw. Erklärung, wenn sie vom Aussteller unterschrieben ist (§ 416 ZPO).

Der technische Sicherheitsstandard einer qualifizierten elektronischen Signatur, der im Signaturgesetz verankert ist, verleiht dem signierten elektronischen Dokument einen sehr hohen Beweiswert.

6.2 Besonderheiten im Verwaltungsprozess und bei der Beweisführung mit „öffentlichen“ Urkunden

Im Verfahren vor den Verwaltungsgerichten (die für Entscheidungen in Verwaltungsverfahren zuständig sind) sind die oben beschriebenen Beweisregeln grundsätzlich ohne Einschränkung anwendbar. Allerdings gilt im Verwaltungsprozess der sog. Amtsermittlungsgrundsatz, d.h. das Gericht erforscht den für relevant erachteten Sachverhalt unabhängig davon, ob sich eine der beteiligten Parteien auf diesen Sachverhalt beruft oder nicht. Daher gelten auch die Ausführungen zur „Beweisbelastung“ nur eingeschränkt.

Besonderheiten gelten weiterhin für die Beweiskraft „öffentlicher elektronischer Dokumente“ gemäß § 371a Abs. 2 ZPO. Öffentliche elektronische Dokumente sind „elektronische Dokumente, die von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind“. Auf solche öffentlichen elektronischen Dokumente finden gemäß § 371a Abs. 2 ZPO die **Beweisregeln für „öffentliche Urkunden“** uneingeschränkt Anwendung. Sie erbringen demnach vollen Beweis eines beurkundeten Vorgangs (§ 415 ZPO), vollen Beweis ihres Inhalts (§ 416 ZPO) oder anderer bezeugter Tatsachen (§ 418 ZPO). Ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen, hat es gemäß § 371a Abs. 2 ZPO die Vermutung der Echtheit für sich, denn § 437 ZPO bestimmt, dass „Urkunden, die nach Form und Inhalt als von einer öffentlichen Behörde oder von einer mit öffentlichem Glauben versehenen Person errichtet sich darstellen, [...] die Vermutung der Echtheit für sich [haben].“

6.3 Besondere Beweiskraft elektronischer Dokumenten mit qualifizierter Signatur

Elektronische Dokumente mit qualifizierter elektronischer Signatur erbringen Beweis wie eine Urkunde³¹. Die Echtheit des Dokuments hat die beweisbelastete Partei zu beweisen. Bei der Beweisführung hilft ihr der gesetzlich normierte Anschein der Echtheit der Signatur. Der Anschein der Echtheit ergibt sich bereits aus einer „Prüfung der Signatur nach dem Signaturgesetz“. Grund diesen gesetzlich normierten Anscheinsbeweis ist, dass nach der Auffassung des Gesetzgebers eine qualifizierte elektronische Signatur einen so hohen Fälschungsschutz bietet – und zwar Schutz vor Fälschung der Signatur ebenso wie Schutz vor nachträglicher Verfälschung –, dass es eines gesonderten Nachweises der Echtheit nicht mehr bedarf.

Nach den allgemeinen Regeln für Anscheinsbeweise, die auch im Rahmen von § 371a ZPO zu beachten sind, muss die beweisbelastete Partei die tatsächlichen Voraussetzungen

³¹ Dass elektronische Dokumente dennoch nicht im juristischen Sinne Urkunden sind, sondern nur ebenso behandelt werden, liegt daran, dass ihnen das Merkmal der „Verkörperung“ fehlt. Sie sind nur bildliche Darstellungen und daher Augenscheinsobjekte.

darlegen und ggf. beweisen, an die der Anscheinsbeweis anknüpft. Im Falle des § 371a ZPO ist darzulegen und ggf. zu beweisen, dass es sich um ein elektronisches Dokument mit einer qualifizierten Signatur handelt. Gelingt es der beweisbelasteten Partei der Beweis, dass es sich um eine qualifizierte elektronische Signatur handelt, ist von der Echtheit des elektronischen Dokumentes als Rechtsfolge des Anscheinsbeweises auszugehen.

Bereits der Nachweis, dass es sich bei der Signatur um eine qualifizierte Signatur i.S.d. SigG handelt, kann dem Beweisführer allerdings durchaus Schwierigkeiten bereiten. Dies wäre insbesondere dann der Fall, wenn von ihm der Nachweis des Vorliegens sämtlicher **Voraussetzungen einer qualifizierten Signatur** verlangt würde.

Gemäß § 2 Nr. 3 SigG³² sind nur solche elektronischen Signaturen auch qualifizierte elektronische Signaturen, die alle Eigenschaften einer fortgeschrittenen Signatur haben (§ 2 Nr. 2 SigG), nämlich

1. ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
2. die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
3. mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,
4. mit den Daten, auf die sie sich beziehen, derart verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,

und die zusätzlich (§ 2 Nr. 3 SigG)

5. auf einem im Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
6. mit einer sicheren Signaturerstellungseinheit erzeugt wurden.

Im Rahmen der Beweisführung können hier insbesondere die letzten beiden Punkte problematisch sein. Da die Signatur auf einem gültigen qualifizierten Zertifikat beruhen muss, ist ggf. die Einhaltung aller Anforderungen zu beweisen, die das Signaturgesetz an qualifizierte Zertifikate stellt. Qualifizierte Zertifikate sind gemäß § 2 Nr. 7 SigG aber nur solche Zertifikate, die von einem Zertifizierungsdiensteanbieter ausgestellt worden sind, der

³² § 2 Nr. 3 SigG:

Im Sinne dieses Gesetzes sind qualifizierte elektronische Signaturen elektronische Signaturen nach Nr. 2, die

- a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
- b) mit einer sicheren Signaturerstellungseinheit erzeugt werden.

eine Vielzahl von Anforderungen des SigG an den Betrieb des Zertifizierungsdienstes erfüllt. Es wird sich regelmäßig bereits der Kenntnis des Beweisführers entziehen, ob der Zertifizierungsdiensteanbieter alle seine Pflichten erfüllt hat oder nicht. Ohne Mithilfe des Zertifizierungsdiensteanbieters ist es deshalb in der Regel völlig ausgeschlossen, zu beweisen, dass der Zertifizierungsdiensteanbieter allen seinen Pflichten nachgekommen ist.

Der Zertifizierungsdiensteanbieter hat gemäß § 10 Abs. 2 SigG nur dem Signaturschlüssel-Inhaber, also typischerweise dem Beweisgegner (nämlich dem Absender des signierten Dokuments) Einblick in die Dokumentation zu gewähren, mit deren Hilfe der Beweis möglicherweise erbracht werden könnte. Ein Recht auf Einblick in die Dokumentation hat der Beweisführer (der Empfänger des signierten Dokuments) in der Regel nicht. Hier kann dem Beweisführer nur helfen, dass das Prozessgericht dem Zertifizierungsdiensteanbieter aufgibt, die bei ihm vorhandene Dokumentation vorzulegen.³³ Sollte die Dokumentation jedoch nicht mehr vorhanden sein, z. B. weil die gemäß Signaturgesetz vorgesehene Aufbewahrungsfrist abgelaufen ist, lässt sich der Beweis im Allgemeinen kaum noch erbringen.

Beruhet die verwendete qualifizierte Signatur auf einem qualifizierten Zertifikat, das ein akkreditierter Zertifizierungsdiensteanbieter ausgestellt hat (hier sog. „akkreditierte elektronische Signatur“) kann sich der Beweisführer allerdings auf die nachgewiesene Sicherheit berufen, die mit der Akkreditierung gemäß § 15 Abs. 1 S. 4 SigG der Nachweis der umfassend geprüften technischen und administrativen Sicherheit des Zertifizierungsdiensteanbieters verbunden ist. Die mit der Akkreditierung verbundene Bestätigung entsprechender organisatorischer und technischer Vorkehrungen durch den Zertifizierungsdiensteanbieter begründet eine Sicherheitsvermutung, auf die sich der Beweisführer berufen kann.³⁴ Es wird vermutet, dass der akkreditierte Zertifizierungsdiensteanbieter die erforderlichen Sicherheitsvorkehrungen tatsächlich ergriffen hat.

Ebenso problematisch kann sich der Nachweis gestalten, dass die Signatur mit einer sicheren Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG gebildet worden ist. Die Art und Weise der Bildung der Signatur wird sich ebenfalls regelmäßig der Kenntnis des

³³ Fischer-Dieskau, Gitter, Paul, Steindle: Elektronisch signierte Dokumente als Beweismittel, MMR 11/2002

³⁴ Roßnagel, MMR 2002, S. 218

Beweisführers entziehen. In der Regel wird gerade der Beweisgegner die Signatur erstellt haben. Auf die Hilfe des Beweisgegners bei der Beweisführung wird er sich deshalb kaum verlassen können.

Für den Beweisführer kann hier hilfreich sein, dass der Zertifizierungsdiensteanbieter gemäß § 5 Abs. 6 SigG und § 5 Abs. 1 S. 1 SigV Zertifikate nur für solche Antragsteller ausstellen darf, die im Besitz einer sicheren Signaturerstellungseinheit sind. Da sichere Signaturerstellungseinheiten die Signaturschlüssel gemäß § 15 Abs. 1 S. 2 SigV nicht preisgeben dürfen, ist es nahezu ausgeschlossen, dass die mit diesem Schlüssel generierte Signatur einer anderen Komponente entstammt, die nicht gesetzeskonform ist.

Für den Beweis dafür, dass der Zertifizierungsdiensteanbieter seinen Pflichten tatsächlich nachgekommen ist, kommt dem Beweisführer im Falle akkreditierter elektronischer Signaturen die o. g. Sicherheitsvermutung zugute. Andernfalls muss der Beweisführer bei Bedarf beweisen können, dass sich der Zertifizierungsdiensteanbieter tatsächlich davon überzeugt hat, dass der Antragsteller im Besitz einer sicheren Signaturerstellungseinheit war. Dazu wird er wiederum die Mithilfe des Zertifizierungsdiensteanbieters benötigen (s. o.)

6.4 Beweiserleichterung des § 371a ZPO

Die vorstehenden Ausführungen zeigen, dass es für den Beweisführer durchaus schwierig, wenn nicht gar unmöglich sein kann, das Vorliegen sämtlicher Voraussetzungen einer qualifizierten elektronischen Signatur zu beweisen. Es verwundert daher nicht, dass unter Juristen die Frage streitig ist, ob § 371a ZPO nicht auch insoweit eine Beweiserleichterung bietet.

Eine Regelung über den Anscheinbeweis für qualifizierte elektronische Signaturen ist durch das Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr (Formgesetz – FormG) vom 31. Juli 2001³⁵ in die

³⁵ Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001, Bundesgesetzblatt Jahrgang 2001 Teil I Nr. 35, ausgegeben zu Bonn am 18. Juli 2001

Zivilprozessordnung (ZPO) eingeführt worden, in § 292a ZPO³⁶. Ziel des Gesetzgebers war es dabei, die Rechtsstellung des Empfängers einer elektronischen Willenserklärung durch eine Beweiserleichterung im Prozess wesentlich zu stärken und im Hinblick darauf das Vertrauen in die Rechtssicherheit und die Verkehrsfähigkeit der elektronischen Form in besonderem Maße zu gewährleisten.

Durch das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG)³⁷ wurde § 292a ZPO zwischenzeitlich aufgehoben. Die Aufhebung erfolgte lediglich aus gesetzessystematischen Gründen. Der Regelungsgehalt des § 292a ZPO wurde unter Aufgabe der Beschränkung auf Willenserklärungen in die Generalvorschrift für die Beweiskraft privater elektronischer Dokumente als § 371a Abs. 1 Satz 2³⁸ überführt. Die Beweiserleichterung gilt nun für alle in elektronischer Form vorliegenden Erklärungen, auch für Wissenserklärungen wie beispielsweise Quittungen.

Die Vorschrift sieht eine Beweiserleichterung zugunsten des Empfängers einer in der elektronischen Form vorliegenden Erklärung vor. Entsprechend den für den Beweis des ersten Anscheins von der Rechtsprechung entwickelten Grundsätzen soll er den Beweis dafür, dass die Erklärung von dem Signaturschlüssel-Inhaber abgegeben worden ist (Echtheit), durch eine Überprüfung der Signatur nach dem Signaturgesetz erbringen können.³⁹ Der Beweisgegner soll den Beweis nur durch Tatsachen erschüttern können, die

³⁶ § 292a ZPO:

Der Anschein der Echtheit einer in elektronischer Form (§ 126a des Bürgerlichen Gesetzbuches) vorliegenden Willenserklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.

³⁷ Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) vom 22. März 2005, Bundesgesetzblatt Jahrgang 2005 Teil I Nr. 18, ausgegeben zu Bonn den 20. März 2005

³⁸ § 371a Abs. 1 Satz 2:

Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.

³⁹ Weitere Informationen zur Bedeutung des Anscheinsbeweises: ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.5.2

es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.

Diese in der ZPO geregelte Beweiserleichterung gilt nicht nur für den Zivilprozess, sondern für alle deutschen Prozessordnungen, in denen auf die ZPO verwiesen wird. Für die Verwaltungsgerichtsbarkeit findet sich diese Verweisung z. B. in § 173 VwGO. Auch § 202 SGG und § 155 FGO verweisen auf die ZPO.

6.4.1 Voraussetzungen der Beweiserleichterung

Gemäß § 371a Abs. 1 ZPO ergibt sich der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung „auf Grund einer Prüfung nach Signaturgesetz“. Wenn diese Prüfung zu einem positiven Prüfergebnis führt, erbringt das signierte Dokument vollen Urkundsbeweis.

Durch die Prüfung nach dem Signaturgesetz wird nachgewiesen, dass die Erklärung integer und authentisch ist. Eine Prüfung nach Signaturgesetz setzt voraus, dass eine „Signaturanwendungskomponente“ mit den in § 17 Abs. 2 S. 2 und 3 SigG beschriebenen Eigenschaften verwendet wird, mit deren Hilfe eine gesetzeskonforme Verifikation der Signatur nebst Überprüfung der Zertifikate vorgenommen wird.

Der Beweis kann gemäß § 371 Abs. 1 S. 2 ZPO dadurch angetreten werden, dass der Beweisführer dem Gericht die in einer Datei enthaltene elektronische Erklärung übermittelt. Das Gericht – oder ein vom Gericht bestellter Gutachter – wird die Datei dann unter Verwendung einer geeigneten Signaturanwendungskomponente prüfen. Falls die Signaturanwendungskomponente ein positives Prüfergebnis anzeigt, ist der Anscheinsbeweis gelungen, falls er vom Beweisgegner nicht erschüttert werden kann.

Tatbestandsvoraussetzung des § 371a Abs. 1 S. 2 ZPO ist, dass es sich um eine qualifizierte elektronische Signatur handelt. Dadurch wird klargestellt, dass die Beweiserleichterung bei einfachen oder fortgeschrittenen Signaturen nicht in Betracht kommt. Strittig ist, ob der Beweisführer zunächst ggf. alle der in Abschnitt 6.3 beschriebenen

Voraussetzungen einer qualifizierten elektronischen Signatur nachweisen muss, damit er überhaupt in den Genuss der Beweiserleichterung kommen kann.

Die oben beschriebene Prüfung nach Signaturgesetz ist nicht nur Voraussetzung für den Anscheinsbeweis, sie erbringt zugleich den Beweis für das Vorliegen einiger aber nicht aller der Abschnitt 6.3 beschriebenen Voraussetzungen einer qualifizierten elektronischen Signatur. Durch eine Prüfung nach Signaturgesetz steht bei negativem Ergebnis fest, dass keine qualifizierte elektronische Signatur vorliegt. Ein positives Ergebnis der Prüfung nach Signaturgesetz bedeutet jedoch nicht zwangsläufig, dass tatsächlich alle Voraussetzungen einer qualifizierten elektronischen Signatur vorliegen. Durch eine Prüfung nach Signaturgesetz kann insbesondere nicht positiv festgestellt werden, dass das Zertifikat, auf dem die Signatur beruht, tatsächlich alle Eigenschaften erfüllt, die das SigG an ein qualifiziertes Zertifikat stellt oder dass eine sichere Signaturerstellungseinheit verwendet wurde (s. Abschnitt .6.3).

Durch eine Prüfung nach Signaturgesetz kann positiv festgestellt werden, dass das verwendete Zertifikat als qualifiziertes Zertifikat *ausgewiesen* ist. Gemäß § 7 Abs. 1 Nr. 8 SigG muss die Angabe, dass es sich um ein qualifiziertes Zertifikat handelt, im Zertifikat vermerkt sein. Falls diese Angabe nicht im Zertifikat enthalten ist, kann es sich nicht um ein qualifiziertes Zertifikat handeln. Bei einer Prüfung nach Signaturgesetz verwendet der Prüfende zudem eine Auskunft des Zertifizierungsdiensteanbieters, durch die dieser bestätigt, dass es sich um ein gültiges Zertifikat handelt (vgl. Abschnitt 5.4).

Es stellt sich somit die Frage, ob der Beweisführer die weiteren Voraussetzungen einer qualifizierten elektronischen Signatur beweisen muss oder ob die Beweiserleichterung dem Beweisführer bereits dann zugute kommen soll, wenn eine Prüfung nach Signaturgesetz zu einem positiven Ergebnis geführt hat.

Es wird die Meinung vertreten, dass eine insoweit erfolgreiche Prüfung nach Signaturgesetz ausreichend sei, um den Beweisführer die Beweiserleichterung zugute kommen zu lassen. Die Beweiserleichterung solle den Beweisführer gerade von der Obliegenheit entbinden, das Vorliegen aller Voraussetzungen einer qualifizierten elektronischen im Detail beweisen zu müssen. Entsprechend den für den Beweis des ersten Anscheins von der Rechtsprechung

entwickelten Grundsätzen soll er den Beweis, dass die Erklärung von dem Signaturschlüssel-Inhaber abgegeben worden ist, grundsätzlich schon durch eine Überprüfung der Signatur nach dem Signaturgesetz (durch Überprüfung der Zuordnung des Signaturprüfchlüssels) erbringen können.⁴⁰

Der Tatbestand des § 371a Abs. 1 S. 2 ZPO und damit das Eingreifen des Anscheinsbeweises der Echtheit setzt nach dieser Interpretation allein voraus, dass die Prüfung nach Signaturgesetz zu einem positiven Ergebnis geführt hat. Ob die Signatur auf einem qualifizierten Zertifikat beruht, ist dann allein den Angaben im Zertifikat bzw. der Auskunft des Zertifizierungsdiensteanbieters bei der Zertifikatsabfrage zu entnehmen.⁴¹ Der Beweisführer muss nicht etwa beweisen, dass tatsächlich alle Eigenschaften einer qualifizierten Signatur (einschließlich eines qualifizierten Zertifikats) vorliegen.

Es wird allerdings auch die Gegenansicht vertreten, nach der der Beweisführer alle in Abschnitt 6.3 genannten Voraussetzungen der qualifizierten elektronischen Signatur beweisen muss, bevor er überhaupt in den Genuss der Beweiserleichterung kommen kann.⁴² Dabei wird richtigerweise erkannt, dass der Beweisführer dann, wenn er das Vorliegen aller Voraussetzungen der qualifizierten elektronischen Signatur beweisen kann, auf den Anscheinsbeweis des § 371a Abs. 1 S. 2 ZPO nicht mehr angewiesen ist.⁴³ Nach dieser Ansicht wäre § 371a Abs. 1 S. 2 ZPO an sich überflüssig. Wenn es dem Beweisführer gelingt, alle Voraussetzungen der qualifizierten elektronischen Signatur zu beweisen, benötigt er die Beweiserleichterung nicht mehr und, falls ihm dies nicht gelingt, hilft sie ihm nicht.

Die Gegenansicht entspricht somit in keiner Weise dem erklärten Ziel des Gesetzgebers, die Rechtsstellung des Empfängers einer elektronischen Willenserklärung durch eine Beweiserleichterung im Prozess wesentlich zu stärken und im Hinblick darauf das Vertrauen

⁴⁰ Begründung zum Entwurf des Formgesetzes vom 6. September 2000, S. 49

⁴¹ Jungermann, DUD 2003, S. 71

⁴² So auch ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.6.3

⁴³ Roßnagel, MMR 8/2000, S. 459

in die Rechtssicherheit und die Verkehrsfähigkeit der elektronischen Form in besonderem Maße zu gewährleisten, und ist daher abzulehnen.

6.4.2 Rechtsfolgen der Beweiserleichterung

Die Rechtsfolgen des § 371 Abs. 1 S. 2 ZPO beziehen sich auf den gesetzlich begründeten Anschein, dass

- die Erklärung echt ist,
- die Erklärung vom Signaturschlüsselinhaber abgegeben wurde und
- die Erklärung willentlich abgegeben wurde.

Sofern es dem Beweisführer gelungen ist, den Anscheinsbeweis zu erbringen, muss der Beweisgegner den Anschein der Echtheit zu erschüttern versuchen, wenn er den Inhalt oder die Echtheit des elektronischen Dokuments abstreitet. Der Beweisgegner soll den Anscheinsbeweis dabei nur durch Tatsachen erschüttern können, die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit dem Willen des Signaturschlüsselinhabers abgegeben worden ist, etwa durch den Nachweis, die Signaturkarte sei ihm abhanden gekommen o.ä.⁴⁴

Der Beweisgegner muss nicht etwa den Beweis des Gegenteils in Sinne des § 292 ZPO erbringen. Die Rechtsfolgen des § 371a Abs. 1 S. 2 ZPO sind damit als reduzierte Beweislastumkehr zu qualifizieren.

Sofern es dem Beweisgegner gelingt, den Anschein zu erschüttern, ist wiederum der Beweisführer am Zug. Ohne die Beweiserleichterung des § 371 Abs. 1 S. 2 ZPO muss er dann nach den allgemeinen Beweisregeln beweisen, dass die in Abschnitt 6.3 genannten Voraussetzungen der qualifizierten elektronischen Signatur vorliegen.

⁴⁴ Begründung zum Entwurf des Formgesetzes vom 6. September 2000, S. 49-50

6.5 Verlust des Anscheinsbeweises mit Ablauf der Dokumentationsfrist

Die Prüfung nach dem Signaturgesetz, die Voraussetzung für den Anscheinsbeweis nach § 371a ZPO ist, ist nur solange möglich, wie die Daten, anhand derer die Signatur überprüft wird, verfügbar sind. Der Zeitraum, für den der Zertifizierungsdiensteanbieter Daten zu einem Zertifikat vorhalten muss, ist begrenzt (siehe oben Abschnitt 5.4). Nach Ablauf dieses Zeitraums darf der Zertifizierungsdiensteanbieter seine gesamte Dokumentation für das Zertifikat löschen. Der Zertifizierungsdiensteanbieter ist danach nicht mehr in der Lage Auskunft über das Zertifikat zu geben.

Auch nach Ablauf der Dokumentationsfrist ist eine Prüfung nach dem Signaturgesetz möglich, wenn eine Auskunft vorliegt die z.B. bereits zum Zeitpunkt des Eingangs der signierten Nachricht eingeholt wurde. Da diese Auskunft mit einer qualifizierten elektronischen Signatur versehen ist und sich ihre Echtheit deshalb jederzeit prüfen lässt, führt der Ablauf der Dokumentationspflicht nicht zwingend zum Verlust des Anscheinsbeweises.

Dies ist jedoch nicht unumstritten. Es wird die Ansicht vertreten, dass der Anscheinsbeweis des § 371a Abs. 1 ZPO die Möglichkeit einer erneuten Prüfung anhand der Dokumentation des Zertifizierungsdiensteanbieters voraussetzt.

Auch wenn überwiegend die Ansicht vertreten wird, dass der Ablauf der Dokumentationsfrist keine direkte Auswirkung auf den Anscheinsbeweis hat, sollten nach Möglichkeit akkreditierte Signaturen verwendet werden, bei denen diess Problem frühestens nach mehr als 30 Jahren auftreten kann.

6.6 Erhaltung der Beweiskraft durch Signaturerneuerung

Wie gezeigt, haben elektronische Dokumente mit qualifizierter Signatur einen hohen Beweiswert. Dieser Beweiswert kann verloren gehen, wenn die qualifizierte Signatur keinen ausreichenden technischen Schutz vor Manipulationen mehr bietet. Dies soll durch die Signaturerneuerung gemäß § 17 SigV verhindert werden. Der hohe Beweiswert einer

qualifizierten elektronischen Signatur soll nicht dadurch wegfallen, dass die bei der Signaturbildung verwendeten Algorithmen oder Schlüssellängen im Lauf der Zeit als nicht mehr geeignet angesehen werden. Sobald die zuständige Behörde ankündigt, dass sie einen Algorithmus ab einem bestimmten Zeitpunkt als nicht mehr sicher genug ansieht, ist vorher eine erneute Signatur anzubringen.

Falls das Versäumnis, die erneute Signatur rechtzeitig anzubringen, bei der Prüfung nach Signaturgesetz erkannt wird, ist die Prüfung fehlgeschlagen und dem Beweisführer kommt die Beweiserleichterung nicht zugute. Möglicherweise würde das Versäumnis, die erneute Signatur rechtzeitig anzubringen, bei einer Prüfung nach Signaturgesetz nicht erkannt.⁴⁵ Jedenfalls würde aber eine Tatsache vorliegen, die geeignet ist, den durch § 371a Abs. 1 S. 2 ZPO gesetzten Anschein zu erschüttern.

Zwar bedeutet die Einstufung der zuständigen Behörde nicht automatisch, dass der Algorithmus bzw. die Schlüssellänge tatsächlich so unsicher sind, dass das Auftreten von Fälschungen unmittelbar zu befürchten ist. Aufgrund der Sicherheitsreserve, die von der zuständigen Behörde bei der Prognose der Eignung der Algorithmen und Schlüssellängen berücksichtigt wird, kann die Sicherheit tatsächlich auch dann noch ausreichen, wenn die zuständige Behörde die Eignung bereits verneint. Für § 371a Abs. 1 S. 2 ZPO ist dies jedoch irrelevant, d.h. die Sicherheitsreserve kann sich nicht zugunsten des Beweisführers auswirken, der die Beweiserleichterung in Anspruch nehmen will.

Wenn ein Algorithmus durch die zuständige Behörde abgekündigt worden ist und der Beweisführer es unterlassen hat, rechtzeitig eine erneute Signatur anzubringen, muss er ggf. nachweisen, dass die Signatur tatsächlich keine Fälschung ist.

Wurde die Signatur entsprechend den in § 17 SigV genannten Vorgaben rechtzeitig erneuert, bleibt die Beweiskraft jedoch voll erhalten. Dem Beweisführer kommt die Beweiserleichterung des § 371 Abs. 1 S. 2 ZPO in diesem Fall auch dann zugute, wenn die

⁴⁵ Im Rahmen von ArchiSig wurde ein Konzept erstellt, nach dem die zuständige Behörde eine Datenstruktur bereitstellt, die durch Signaturanwendungskomponenten ausgewertet und bei der Signaturprüfung berücksichtigt werden kann (vgl. Frye, Pordesch, DUD 2003, S. 73 ff.). Dies Konzept wurde jedoch noch nicht umgesetzt.



ArchiSafe



Algorithmen bzw. Parameter, die bei der Signaturerstellung verwendet wurden, nicht mehr geeignet sind.⁴⁶

⁴⁶ Roßnagel, Fischer-Dieskau, Pordes, Brandner, CR 4/2004, S. 305

7 Aufbewahrungsfristen

Aufbewahrungsfristen haben sich immer am Aufbewahrungszweck zu orientieren, der sich aus Rechtspflichten oder Obliegenheiten der Behörde ergibt. Die Aufbewahrungsfristen der jeweiligen Aktenordnungen bzw. Aktenplänen innerhalb der Verwaltung dienen hier in der Regel lediglich dem Zweck, eine gewisse Vereinheitlichung herbeizuführen, d. h. eine Regelfrist vorzugeben.

Die verschiedenen Interessen, die mit der Aufbewahrung verbunden sein können, sind ggf. gegeneinander abzuwägen.⁴⁷

7.1 Mindestaufbewahrungsfristen

Aufbewahrungsfristen sind in der Regel als Mindestfristen ausgestaltet. Dies gilt insbesondere für die Aufbewahrung zum Zwecke der Revisionsicherheit.

Dokumente werden in eine Akte aufgenommen und in diesen aufbewahrt, bis die Akte dem Bundesarchiv angeboten und vollständig übergeben wird (§ 21 Abs. 1 RegR).

7.2 Höchstaufbewahrungsfristen

Höchstaufbewahrungsfristen bestehen dort, wo eine strikte Zweckbindung gesetzlich vorgesehen ist oder das Ziel verfolgt wird, die Anzahl der Akten zu reduzieren.

7.2.1 Datenschutzrecht

Im Datenschutzrecht gelten die Grundsätze der strikten Zweckbindung personenbezogener Daten sowie der Datenvermeidung bzw. Datensparsamkeit. Personenbezogene Daten sind daher grundsätzlich sofort zu löschen, wenn sie nicht mehr benötigt werden.⁴⁸

⁴⁷ Weitergehende Informationen zu Aufbewahrungsfristen: ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.1

⁴⁸ Weitere Informationen zum Datenschutz: ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.4.1

7.2.2 Bundesarchivgesetz

Das Bundesarchivgesetz ist ein Spezialgesetz des Datenschutzes. Es geht dem Bundesdatenschutzgesetz vor.⁴⁹ Das bedeutet auch im Hinblick auf § 3a BDSG, der Regelungen zur Datenvermeidung und Datensparsamkeit enthält, dass dort, wo eine Anbietepflicht nach Bundesarchivgesetz besteht, eine Anonymisierung und Pseudonymisierung nicht möglich ist..⁵⁰

7.2.3 RegR

§ 19 Abs. 1 RegR schreibt vor, dass Aufbewahrungsfristen von mehr als 30 Jahren auf den Ausnahmefall zu begrenzen sind.

⁴⁹ § 1 Abs. 3 BDSG: „Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten ... anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.“

⁵⁰ Weitere Informationen zum Datenschutz im Archivrecht: ArchiSig, Anforderungskatalog, Version 2.0, Dezember 2002, Abschnitt 2.1.4.2

8 Aufbewahrungsmodalitäten zur Sicherung des Daten- und Geheimnisschutzes

8.1 Sicherung der datenschutzrechtlichen Ansprüche des Betroffenen

Auch wenn die datenschutzrechtlichen Ansprüche des Betroffenen hinter den Interessen des Archivs zurückstehen müssen (vgl. Abschnitt 7.2.2), kann er gegenüber der Behörde jedoch ggf. Ansprüche auf Berichtigung, Sperrung und Gegendarstellung geltend machen. Außerdem sind die datenverarbeitenden Stellen verpflichtet, Schutzvorkehrungen zu treffen, um die Rechte des Betroffenen zu wahren. Dazu gehört insbesondere der Schutz des Datengeheimnisses.

8.2 Geheimschutz

Neben dem Datengeheimnis ist auch der Geheimschutz zu wahren.