STAATSMINISTERIUM
DER JUSTIZ
UND FÜR EUROPA

Freistaat
SACHSEN

# Handreichung zur rechtssicheren Aufbewahrung von elektronischen Dokumenten

Sächsisches Staatsministerium der Justiz und für Europa
Projektgruppe EU-Dienstleistungsrichtlinie

Version: 1.0
Stand: 16.11.2009

# Inhalt

# 1 Einleitung

Am 12. Dezember 2006 wurde die EU-Dienstleistungsrichtlinie (EU-DLR) verabschiedet. Diese Richtlinie hat das Ziel, die Beschränkungen der Niederlassungsfreiheit von Dienstleistungserbringern in den Mitgliedstaaten und des freien Dienstleistungsverkehrs im Binnenmarkt zu beseitigen und dadurch eine Liberalisierung des Binnenmarktes zu erreichen.

Die Bestimmungen der EU-DLR müssen bis zum 28.12.2009 von den Mitgliedsstaaten umgesetzt werden. Betroffen davon sind neben den Einheitlichen Ansprechpartnern (EA) in den einzelnen Bundesländern auch die Kommunen als zuständige Behörden nach der EU-DLR.

Eine wesentliche Forderung der EU-DLR ist die in Artikel 8 definierte elektronische Verfahrensabwicklung. Danach soll es möglich sein, „dass alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch über den betreffenden einheitlichen Ansprechpartner oder bei der betreffenden zuständigen Behörde abgewickelt werden können.“[1]

Aus der Notwendigkeit der elektronischen Verfahrensabwicklung ergibt sich, dass Formulare elektronisch bereitgestellt werden müssen und ein Zugang für die elektronische Kommunikation zu eröffnen ist, über den auch signierte und verschlüsselte Dokumente bzw. E-Mails übertragen werden können[2]. Weiterhin ergibt sich die Anforderung der rechtssicheren Aufbewahrung elektronischer Dokumente. Dabei entstehen für elektronisch signierte Dokumente mit Urkundenqualität besondere Anforderungen, um sicherzustellen, dass es sich um die jeweiligen Originaldokumente handelt. Insbesondere in Gerichtsverfahren kann es erforderlich sein, Dokumente in unveränderbarer Form vorzuhalten.

Die vorliegende Handreichung skizziert die Mindestanforderungen zur rechtssicheren elektronischen Speicherung von Dokumenten und soll die Kommunen bei der Umsetzung einer rechtssicheren Speicherung unterstützen.

Es sei darauf hingewiesen, dass unter dem Begriff „Kommunen“ die Städte, Gemeinden und Landkreise verstanden werden.

---

[1] Artikel 8 Absatz 1 der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates 12. Dezember 2006 über Dienstleistungen im Binnenmarkt

[2] vgl. Mindestanforderungen an die Kommunen bei der Umsetzung der EU-Dienstleistungsrichtlinie im Freistaat Sachsen

# 2 Aufbewahrung elektronischer Dokumente

## 2.1 Aktenrelevanz und Aufbewahrungspflicht

Bei den im Rahmen der Umsetzung der EU-DLR zu bearbeitenden und zu speichernden elektronischen Dokumenten ist zunächst zu prüfen, ob sie als behördliches Schriftgut (d.h. als aktenrelevant) einzuordnen sind. Falls ja, ist das Dokument durch die zuständige Behörde zu den Akten zu nehmen und aufzubewahren. Ein Dokument ist dann aktenrelevant, wenn sich dies unmittelbar aus geltenden Rechts- und Verwaltungsvorschriften ergibt oder das Dokument eine hohe Relevanz besitzt. Eine solche Relevanz ergibt sich insbesondere nach den folgenden Kriterien:

- Eingriffe in Rechte Dritter
- Prozessrisiko
- Haushalterische bzw. finanziell wirksame Maßnahmen
- Nachweis der ausgeübten und tradierten Verwaltungspraxis
- Dokumentation und Rechtfertigung des Handelns der Beschäftigten gegenüber Vorgesetzten und Dritten

Daraus kann folgender Grundsatz abgeleitet werden: Dokumente (sowie die zugehörigen entscheidungserheblichen Bearbeitungsschritte) sind dann aktenrelevant, wenn sie zum späteren Nachweis der Vollständigkeit, zur Nachvollziehbarkeit und für die Transparenz des Verwaltungshandelns innerhalb der Verwaltung oder gegenüber Dritten beweisfest vorzuhalten sind. Das gilt zum Beispiel für Antragsunterlagen und ihre Anlagen. Unter Beweisfestigkeit wird hierbei die langfristige, unveränderliche Les- und Nutzbarkeit verstanden. Die Dauer der Aufbewahrung richtet sich nach den ggf. gesetzlich geregelten Aufbewahrungspflichten.

Für elektronische Dokumente bedeutet dies, dass für die Dauer der Aufbewahrungspflicht die Speicherung rechtssicher erfolgen muss. Eine rechtssichere Speicherung liegt vor, wenn Dokumente revisionssicher gespeichert werden und der Beweiswert von angebrachten Signaturen durch Mechanismen der Übersignierung sichergestellt ist. Diese Aufbewahrung erfolgt sinnvoller Weise in einem revisionssicher betriebenen Dokumentenmanagement- bzw. Vorgangsbearbeitungssystem. **Bei nicht signierten Dokumenten ist es grundsätzlich möglich, die Dokumente auszudrucken und in einer Papierakte aufzubewahren,** aber bei signierten elektronischen Dokumenten besteht diese Möglichkeit nicht, da das elektronische Original aufzubewahren ist. Für diese Fälle ist zumindest eine rechtssichere Aufbewahrung der signierten elektronischen Dokumente sicherzustellen. Es kann somit festgestellt werden, dass als Mindestanforderung die aktuellen Formen der Aktenführung als Ausgangsbasis zunächst beibehalten werden können.

## 2.2 Revisionssichere Speicherung von Dokumenten

Der Begriff Revisionssicherheit für die Speicherung von Dokumenten im Bereich der öffentlichen Verwaltung baut auf den Festlegungen zur revisionssicheren Archivierung von Dokumenten auf, welche im industriellen und handelsrechtlichen Bereich verwendeten werden. In der Zusammenfassung ergeben sich aus diesen rechtlichen Anforderungen folgende Grundsätze zur revisionssicheren Aufbewahrung von Dokumenten:

- Jedes Dokument wird unveränderbar gespeichert.
- Es darf kein Dokument auf dem Weg in den Speicher oder im Speicher selbst verloren gehen.
- Jedes Dokument muss mit geeigneten Techniken wieder auffindbar sein.
- Es muss genau das Dokument wiedergefunden werden, das gesucht worden ist.
- Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.
- Jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können.
- Alle Inhalte müssen zeitnah wiedergefunden werden können.
- Alle Aktionen im Speicher, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist.
- Elektronische Langzeitspeicher sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.
- Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer sicherzustellen.

Zusammengefasst bedeutet dies, dass eine revisionssicherere Speicherung von Dokumenten unter folgenden Voraussetzungen möglich ist:

- Die Daten werden in einem Dokumentenmanagementsystem gespeichert, welches Informationen datenbankgestützt wieder auffindbar, nachvollziehbar, unveränderbar und verfälschungssicher bereitstellen kann.
- Der ordnungsgemäße Betrieb des Systems ist sichergestellt.
- Das System und die Vorgaben zur Nutzung des Systems sind dokumentiert.
- Das System wird ordnungsgemäß genutzt.

Für die Verwaltungspraxis ergeben sich daraus folgende Anforderungen an die revisionssicherere Speicherung von elektronischen Dokumenten:

- Aktenrelevante Dokumente sind frühzeitig, vollständig und richtig in einem System zur revisionssicheren Speicherung elektronischer Akten abzulegen. Dabei ist sicherzustellen, dass der Sachzusammenhang (Akte, Vorgang) erkennbar ist.
- Die Veränderungen an Dokumenten, Vorgängen und Akten sowie die Bearbeitung eines Vorgangs müssen für berechtigte Personen vollständig nachvollziehbar dokumentiert sein. Das bedeutet, dass Protokoll- und Bearbeitungsinformationen (geordnete Darstellung der

Entstehung und Abwicklung der Vorgangsbearbeitung = Protokollierung) erfasst, gepflegt und automatisch generiert werden.

- Berechtigte Personen müssen jederzeit Zugriff auf die Daten haben. Nichtberechtigte Personen dürfen keinen Zugriff haben.
- Für das System zur revisionssicheren Speicherung elektronischer Akten sowie für dessen Nutzung muss eine aktuelle, verständliche und nachvollziehbare Dokumentation existieren, die regelmäßig fortgeschrieben wird. Dabei müssen der Stand des Systems und die Dokumentation jederzeit übereinstimmen.
- Die Einhaltung der technischen und organisatorischen Anforderungen ist regelmäßig zu prüfen.

## 2.3 Beweiswerterhalt von signierten Dokumenten

Bei Papierdokumenten wird die Echtheit (Authentizität) durch eine Unterschrift gewährleistet. Die Unverfälschtheit (Integrität) wird meist durch bloßes Ansehen des Dokumentes geprüft. Bei elektronischen Dokumenten besteht die Möglichkeit und Notwendigkeit, die Integrität und Authentizität durch elektronische Signaturen zu sichern. Elektronische Signaturen können insofern das elektronische Äquivalent zur handschriftlichen Unterschrift sein.

Die rechtlichen Rahmenbedingungen zur Nutzung elektronischer Signaturen regeln in Deutschland das „Gesetz über Rahmenbedingungen für elektronische Signaturen“ (SigG oder SigG 2001) vom 16. Mai 2001 sowie die Signaturverordnung (SigV). Das Signaturgesetz unterscheidet folgende Formen der elektronischen Signatur:

- allgemeine (einfache) elektronische Signatur
- fortgeschrittene elektronische Signatur und
- qualifizierte elektronische Signatur

Lediglich die letztgenannte kann gemäß § 2 Nr. 3 SigG eine per Gesetz geforderte Schriftform ersetzen, da nur die qualifizierte elektronische Signatur zum Zeitpunkt ihrer Erzeugung auf einem gültigen qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit erstellt wurde. Anbieter von qualifizierten elektronischen Signaturen können sich zudem hinsichtlich der Sicherheit des betriebenen Rechenzentrums durch die Bundesnetzagentur bewerten und akkreditieren lassen. Damit entsteht in der Praxis eine vierte Form der elektronischen Signatur, die qualifizierte elektronische Signatur mit Anbieterakkreditierung.

Durch die Verwendung einer qualifizierten elektronischen Signatur entsteht aus einer Datei ein Dokument, das einem unterzeichneten Papierdokument rechtlich gleichwertig ist. Die qualifizierte elektronische Signatur sichert vorrangig die Integrität des Dokumentes sowie die Authentizität des Unterzeichners.

Ein solch qualifiziert elektronisch signiertes Dokument kann im Falle einer gerichtlichen Auseinandersetzung als Beweis herangezogen werden. Im Unterschied zu Papierdokumenten kann die Beweiseignung elektronisch signierter Dokumente jedoch mit der Zeit abnehmen. Ursachen hierfür sind insbesondere, dass die verwendeten kryptografischen Algorithmen und Schlüssel im Laufe der Zeit ihre Sicherheitseignung verlieren, und dass nicht gewährleistet ist, dass die für die Überprüfung von Zertifikaten notwendigen Verzeichnisse und Unterlagen über 30 Jahre und mehr verfügbar sind. Dies würde bedeuten, dass z.B. bei signierten Anträgen nicht mehr geprüft werden kann, ob der Antrag vom Berechtigten unterschrieben oder seit der Unterschrift verändert wurde.

Um die Sicherheit elektronischer Signaturen langfristig aufrechtzuerhalten, muss daher eine Signaturerneuerung nach § 17 Signaturverordnung (SigV), durchgeführt werden.

Ziel der Signaturerneuerung nach § 17 SigV ist es, die Integrität der mit einer qualifizierten elektronischen Signatur versehenen Daten auch dann noch feststellen zu können, wenn eine Signaturprüfung aufgrund mangelnder Sicherheitseignung der verwendeten Algorithmen nicht mehr geeignet ist, um die Integrität der signierten Daten zu belegen. Die Authentizität der Signatur muss dadurch gewährleistet werden, dass die für eine Signaturprüfung erforderlichen Prüfmittel jederzeit in geeigneter Form verfügbar sind.

Vor diesem Hintergrund ergibt sich für die Kommunen die Anforderung, ein qualifiziert elektronisch signiertes Dokument in einem Speichersystem abzulegen, welches einerseits die Unveränderbarkeit der enthaltenen Daten sicherstellt und anderseits über ein Softwaremodul verfügt, dass die Übersignierung im Sinne des § 17 SigV gewährleistet.

## 2.4 Dateiformate

Bei Papierdokumenten ist in der Regel eine Sichtung des Dokuments auch nach Jahrzehnten problemlos möglich. Bei elektronischen Dokumenten kann dies durch besondere Verfahrensweisen ermöglicht werden. Zum einen ist schon in technischer Hinsicht die Lesbarkeit älterer elektronischer Dokumente gefährdet, wenn die ursprüngliche Hard- und Software aufgrund der technischen Entwicklung nicht mehr verfügbar ist. Notwendig ist daher die regelmäßige Datenaufbereitung, um überhaupt die Lesbarkeit zu gewährleisten.

In der Folge sind besondere Vorkehrungen nötig, um bei dieser Umformatierung die ggf. vorhandene Urkundenqualität eines Dokumentes beizubehalten, vgl. § 33 Abs. 4 Nr. 4 b VwVfG. Hierbei spielt die Verwendung und die Auswahl geeigneter Formate und elektronischer Signaturen schon bei der Erstellung der Dokumente eine wichtige Rolle.

Da auch für die im Rahmen der EU-DLR elektronisch eingehenden Dokumente Aufbewahrungspflichten von mehreren Jahren gelten können, ergibt sich die Anforderung, aktenrelevante Dokumente (spätestens nach Abschluss der aktiven Sachbearbeitung) in ein Langzeitspeicherformat zu überführen.

Vor diesem Hintergrund wird zur (langfristigen) Speicherung elektronischer Dokumente das PDF/A-Format empfohlen[3]. PDF/A ist der internationale ISO-Standard[4] (ISO 19005-1:2005) für die Langzeitspeicherung und Archivierung. PDF/A unterstützt die Anforderungen an die Barrierefreiheit sowie die authentische Darstellung der Inhalte. In eine PDF/A-Datei lassen sich rechtssicher Signaturen einbetten.

[3] Neben PDF/A ist auch TIFF ein Langzeitspeicherformat.

[4] International Organization for Standardization

# 3 Leitlinien zur Speicherung elektronischer Dokumente

Nach Umsetzung der EUDLR kann es in allen Kommunen zur Abgabe elektronischer Anträge kommen. Gemäß den Anforderungen an die behördliche Schriftgutverwaltung sind diese elektronisch eingegangenen Dokumente rechtssicher aufzubewahren. Eine besondere Herausforderung stellen in diesem Zusammenhang die Dokumente dar, die (z.B. auf Grund eines vorliegenden Schriftformerfordernisses) qualifiziert elektronisch signiert wurden.

Bei der Sicherstellung der rechtssicheren Speicherung dieser elektronischen Dokumente sind folgende Leitlinien zu beachten:

- Elektronische Dokumente unterliegen den Anforderungen an die behördliche Schriftgutverwaltung und sind daher auf Aktenrelevanz zu prüfen. Bei vorliegender Aktenrelevanz sind diese Dokumente zur Akte zu nehmen.
- Zur Sicherstellung der Revisionssicherheit sind aktenrelevante Dokumente in einem dafür geeigneten System zu speichern. Dateiserver und E-Mail-Systeme erfüllen diese Anforderungen nicht. Daher ist der Einsatz eines Dokumentenmanagement- bzw. Vorgangsbearbeitungssystems (DMS/VBS) zu empfehlen. Bei der Speicherung muss der Aktenzusammenhang erkennbar sein. Sollte es neben der elektronischen Akte auch eine den Fall betreffende Papierakte geben, so sind in beiden Akten entsprechende Verweise anzubringen.
- Nicht signierte elektronische Dokumente mit Aktenrelevanz können behelfsweise auch ausgedruckt und zur Papierakte genommen werden (Mindestanforderung!).
- Für signierte elektronische Dokumente mit Aktenrelevanz ist zwingend die Speicherung in einem System notwendig, welches über ein Softwaremodul verfügt, dass die Übersignierung im Sinne des § 17 SigV gewährleistet. Allerdings ist es auch für diese Dokumente möglich, Bearbeitungskopien in einer Papierakte aufzubewahren. Bei der elektronischen Version eines solchen Dokumentes und auch bei der Bearbeitungskopie muss nachvollziehbar dokumentiert sein, wo elektronisches Original und Bearbeitungskopie aufbewahrt werden. (Mindestanforderung!).
- Mittelfristig wird empfohlen, für die relevanten Verwaltungsprozesse eine elektronische Akte einzuführen. Das dabei einzuführende System (DMS/VBS) sollte die Anforderungen zur revisionssicheren Speicherung erfüllen können. Weiterhin sollte dieses System signierte Daten in einem Speicherbereich ablegen, in dem eine Übersignierung nach § 17 SigV möglich ist.
- Für die Sicherstellung der Langzeitspeicherfähigkeit der elektronischen Dokumente ist (möglichst mit der Erzeugung) ein entsprechendes Format (PDF/A oder TIFF) zu wählen. Diese Forderung sollte zumindest bei den selbsterstellten Dokumenten umgesetzt werden.

# 4 Ansprechpartner

Herr Nicol Feske
Sächsisches Staatsministerium der Justiz und für Europa
Hospitalstraße 7, 01097 Dresden

E-Mail: Nicol.Feske@smi.sachsen.de
***Ab 30.11.2009 neue E-Mailadresse:***
Nicol.Feske@smj.justiz.sachsen.de
Tel.: 0351 564 – 1966
Fax.: 0351 564 - 1959