Kompetenzzentrum Digitalisierung

Beweiskraft von Dokumenten in elektronischen Akten und der elektronischen Aktenführung

Empfehlungen zur Digitalisierung der Verwaltung

Nummer	Datum	Version	Änderung	Status
1	20.03.2020	1.0		fg.

i.B. = in Bearbeitung

vg. = vorgelegt

fg. = freigegeben

Inhaltsverzeichnis

1 Einleitung

Der Erstellung des vorliegenden Dokuments ist ein längerer Prozess vorangegangen. Im Frühjahr 2019 verzeichneten KDN-Mitglieder einen erhöhten Klärungsbedarf hinsichtlich der Beweiskraft von Dokumenten in eAkten. Der KDN unternahm daraufhin eine Mitgliederabfrage, um alle Fragen in einem Katalog zu erfassen. Die eAkten-Unterarbeitskreise des KDN haben diesen Fragenkatalog auf Vollständigkeit geprüft und ergänzt. Im nächsten Schritt wurde der Fragenkatalog von einer IT-Beratungsfirma durchgesehen und kommentiert. Außerdem wurden zwei gutachterliche Stellungnahmen des Fachanwalts für Informations-technologierecht Dr. Helmut Redeker eingeholt.

Das vorliegende Dokument soll den KDN-Mitgliedern und den ihnen angehörigen Kommunen als Orientierungshilfe für rechtliche Fragen zum Thema „Beweiskraft von Unterlagen in eAkten“ dienen. Dafür wurden in diesem Dokument alle vorhandenen Informationsquellen zusammengetragen.

Um die Navigation im vorliegenden Dokument zu erleichtern, verlinkt die Übersichtstabelle unter 2.1 die Fragen der KDN-Mitglieder mit den relevanten Textpassagen der jeweiligen Informationsquellen.

2 Gesammelte gutachterliche Stellungnahmen und weitere Dokumentation

2.1 Übersichtstabelle der behandelten Fragen

ID	Frage	Fragensteller	Link zur Textpassage
1	Möglichkeit des ergänzenden Scannens und Behalten des Originals?	KRZ Minden-Ravensberg/ Lippe	S. 19 aus Leitlinie zum ersetzenden Scannen in Kommunen nach TR RESISCAN 2017
2	Kann bei Einsatz revisionssicherer Speichersysteme (EMC Centera oder ECS, Hitachi Vantara, FAST LTA Silent Cubes, etc.) auf die Beweiswerterhaltung von qualifizierten elektronischen Signaturen verzichtet werden?	SIT	S. 4 Kommentar zu Nr. 5.1 aus Fragenkatalog zur Beweiserhaltung kommentiert
3	Wie ist der Beweiswert von „nur“ in einem DMS mit revisionssicheren Speichern abgelegten elektronisch erzeugten Dokumenten im Vergleich zu gescannten Dokumenten?	GKD Paderborn	S. 4 Kommentar zu Nr. 5.2 aus Fragenkatalog zur Beweiserhaltung kommentiert
4	Wie ist der Beweiswert von „nur“ in einem DMS mit revisionssicheren Speichern abgelegten elektronisch erzeugten Dokumenten im Vergleich zu gescannten Dokumenten?	GKD Paderborn	S. 5, 1. Frage aus Gutachtliche Stellungnahme 2019
5	Was muss von der Kommunikation zur Vollständigkeit der Aktenführung, aufbewahrt/veraktet werden, um z.B. die fristgerechte Einreichung zu dokumentieren?	KRZ	S. 6, 2. Frage aus Gutachtliche Stellungnahme
6	Was muss mit dem elektronischen Empfangsbekenntnis passieren?	KRZ	S. 7, 3. Frage aus Gutachtliche Stellungnahme
7	Wie genau hat die beweiskräftige Ablage des Formulars (in einem DMS) zu erfolgen? Genügt die Ablage des Formularfelds mit Antwort als xml oder PDFA?	Kreis Herford	S. 8, 4. Frage aus Gutachtliche Stellungnahme 2019
8	Welche Anforderungen bestehen hinsichtlich der Dokumentation der eingesetzten Hard- und Software sowie des Betriebs?	GKD Paderborn	S. 8, 5. Frage aus Gutachtliche Stellungnahme 2019

9	Welche Rechtsvorschriften und Richtlinien sind für die Kommunalverwaltung dabei zu beachten? (Bezieht sich auf die Frage: Welche Anforderungen bestehen hinsichtlich der Dokumentation der eingesetzten Hard- und Software sowie des Betriebs?)	GKD Paderborn	S. 9, 6. Frage aus Gutachtliche Stellungnahme 2019
10	Welche Verfahren (Spalten) erfüllen die Grundsätze der ordnungsgemäßen Aktenführung aus dem Rechtsstaatsprinzip (Zeilen) (Stichwort: Schriftgutverwaltung)?	Düsseldorf	S. 10 zur beigefügten Tabelle aus Gutachterliche Stellungnahme 2020; dazu auch S. 10, III. Gutachterliche Stellungnahme 2020 Gutachterliche Stellungnahme Tabelle
11	**Vergaberecht:** Im Vergaberecht reicht als Signaturniveau die Textform aus. Welche Unterlagen/Nachweise müssen im DMS abgelegt werden, um die Beweiskraft für die auf der Vergabeplattform eingereichten Unterlagen zu erhalten?	Stadt Bielefeld	S. 10, 2. Frage 1 aus Gutachtliche Stellungnahme 2019
12	**Vergaberecht:** Muss in jedem Fall das Prüfprotokoll angefordert und abgelegt werden oder sind die Details zum Angebot ausreichend?	Stadt Bielefeld	S. 11, 3. Frage 2 aus Gutachtliche Stellungnahme 2019
13	**Vergaberecht:** Hat es Auswirkungen auf die Beweiskraft, wenn die Angebotsunterlagen von der Vergabeplattform nicht direkt ins DMS abgelegt werden können, sondern erst auf einem Fileserver zwischengespeichert werden müssen?	Stadt Bielefeld	S. 10, 2. Frage 1 aus Gutachtliche Stellungnahme 2019
14	**Archivwesen:** Ist dieses Vorgehen ausreichend oder ist mit Blick auf die Beweiserhaltung eine Übernahme der Signatur ins Langzeitarchiv zwingend erforderlich, um die Integrität und Authentizität der Dokumente sicherzustellen?	Historisches Archiv Köln	S. 11, IV. Archivwesen aus Gutachtliche Stellungnahme 2019

15	**Archivwesen:** Ist im Fall, dass die Signaturübernahme im Langzeitarchiv zwingend erforderlich ist, auch die Nachsignatur (Auffrischung) zwingend erforderlich?	Historisches Archiv Köln	S. 11, IV. Archivwesen aus Gutachtliche Stellungnahme 2019
16	**Signatur:** Wann müssen qualifizierte elektronische Signaturen bei elektronischer Aktenführung inkl. dem Scannen eingesetzt werden?	SIT	S. 5 ff aus Gutachterliche Stellungnahme 2020
17	**Signatur:** Wann müssen qualifizierte elektronische Zeitstempel eingesetzt werden?	SIT	S. 5 ff aus Gutachterliche Stellungnahme 2020
18	**Signatur:** Wann müssen qualifizierte elektronische Signaturen zwingend bei elektronischer Aktenführung Beweiswert erhaltend gespeichert werden?	SIT	S. 5 ff aus Gutachterliche Stellungnahme 2020
19	**Signatur:** Wann sollten qualifizierte elektronische Signaturen bei elektronischer Aktenführung Beweiswert erhaltend gespeichert werden?	SIT	S. 5 ff aus Gutachterliche Stellungnahme 2020
20	**Signatur:** In welchen konkreten Anwendungsfällen muss die Kommune zwangsläufig qualifizierte elektronische Signaturen und qualifizierte elektronische Zeitstempel einsetzen?	GKD Paderborn	S. 5 ff aus Gutachterliche Stellungnahme 2020
21	**Signatur:** Wann müssen oder dürfen andere kryptographische Verfahren zum Einsatz kommen, wie z. B. die fortgeschrittene Signatur?	GKD Paderborn	S. 5 ff aus Gutachterliche Stellungnahme 2020
22	**Signatur:** Steigt durch den Verzicht auf kryptografische Sicherungen das konkrete Prozessrisiko signifikant?	GKD Paderborn	S. 5 ff aus Gutachterliche Stellungnahme 2020
23	**Siegel:** Inwieweit ist auch eine Nutzung von elektronischen Siegeln (eIDAS-Durchführungsgesetz) denkbar?	Herne	S. 5 ff aus Gutachterliche Stellungnahme 2020
24	**Archivwesen:** Wie geht das System mit digitalen Signaturen um?	Stadtarchiv Mülheim an der Ruhr	S. 7 f. aus Gutachterliche Stellungnahme 2020
25	**Archivwesen:** Wie können Akten aus DiPS.kommunal zur Vorlage bei Gericht gelangen?	Stadtarchiv Mülheim an der Ruhr	S. 7 f. aus Gutachterliche Stellungnahme 2020

26	**Signatur:** Wann müssen qualifizierte elektronische Signaturen bei elektronischer Aktenführung inkl. dem Scannen geprüft werden? (bei Eingang, bei Übernahme in Revisionssicheren Speicher, bei Versand an Dritte (Justiz, …)?	SIT	S. 7, Frage c) aus Gutachtliche Stellungnahme 2020
27	**Signatur:** Wann sollten qualifizierte elektronische Signaturen geprüft werden?	SIT	S. 7, Frage c) aus Gutachtliche Stellungnahme 2020
28	**Signatur:** Wann müssen qualifizierte elektronische Signaturen zwingend bei elektronischer Aktenführung Beweiswert erhaltend gespeichert werden?	SIT	S, 5, II.1.a. aus Gutachterliche Stellungnahme 2020
29	**Signatur:** Wann sollten qualifizierte elektronische Signaturen bei elektronischer Aktenführung Beweiswert erhaltend gespeichert werden?	SIT	S. 5, II.1.a aus Gutachterliche Stellungnahme 2020
30	**Signatur:** Ablage des Prüfungsdokuments in der eAkte?	KRZ Minden-Ravensberg/Lippe)	S. 5 II.1.a aus 2020 Gutachterliche Stellungnahme 2020
31	Wie ist der Beweiswert von „nur“ in einem DMS mit revisionssicheren Speichern abgelegten elektronisch erzeugten Dokumenten im Vergleich zu solchen, die mit kryptischen Verfahren behandelt wurden?	GKD Paderborn	S. 7, d. aus Gutachterliche Stellungnahme 2020
32	Ändern sich durch die GoBD die Regelungen zur elektronischen Signatur, zum OZG etc. die Anforderungen an konventionell erzeugte Dokumente im Rahmen der Speicherung/Aufbewahrung (z.B. Nutzung von zusätzlichen Qualitätskriterien wie Hash-Werte, qualifizierte Zeitstempel etc.)?	civitec	S. 8, Nr. 3 aus Gutachterliche Stellungnahme 2020
33	**Signatur:** Wann ist es zwingend, dass bei einer Anmeldung einer bestimmten Vertrauensstufe (z. B. Name Passwort (Stufe 1) oder elektronischer Personalausweis (Stufe 4)) auch jedes abgelegte Dokument digital signiert wird?	civitec	S. 9, Nr. 4 aus Gutachterliche Stellungnahme 2020

34	**Signatur:** Ist es zwingend, um die Sicherheit elektronischer Signaturen langfristig aufrechtzuerhalten, eine Signaturerneuerung nach § 17 Signaturverordnung (SigV) durchzuführen?	civitec	S. 4f., Nr. I.4, 9, Nr. 4 aus Gutachterliche Stellungnahme 2020

2.2 Gutachterliche Stellungnahme zu Fragen der Beweiskraft von Dokumenten in elektronischen Akten und der elektronischen Aktenführung 12.01.2020

Gutachterliche Stellungnahme

zu Fragen der Beweiskraft von Dokumenten in elektronischen Akten und der elektronischen Aktenführung

vorgelegt von

Rechtsanwalt und Fachanwalt für Informationstechnologierecht Dr. Helmut Redeker, Bonn

Heinle Redeker und Partner Rechtsanwälte mbB, Am Schaumburger Hof 10, 53175 Bonn

Vorbemerkung

In dieser gutachterlichen Stellungnahme geht es um den Beweiswert elektronischer Dokumente. Die Stellungnahme baut auf der früheren Stellungnahme zum gleichen Problemkreis vom 04.10.2019 auf und beantwortet eine Reihe weiterer, in diesem Zusammenhang aufgeworfener Fragen.

I. Gesetzliche Regelungen

Zu den gesetzlichen Grundlagen wird zunächst auf die entsprechenden Ausführungen unter I. in der früheren Stellungnahme verwiesen. Die dortigen Ausführungen zur qualifizierten elektronischen Signatur und zur elektronischen Aktenführung gelten auch hier. Es gibt aber einige zusätzliche Fragestellungen, die zu betrachten sind.

1. Qualifizierte elektronische Siegel und qualifizierte elektronische Zeitstempel

In mehreren in der Folge beantworteten Fragestellungen werden qualifizierte elektronische Siegel und qualifizierte elektronische Zeitstempel erwähnt.

Dabei wird ein qualifiziertes elektronisches Siegel in Art. 3 Nr. 27 eIDAS-VO als ein fortgeschrittenes elektronisches Siegel iSv Art. 36 eIDAS-VO definiert, das von einer qualifizierten elektronischen Siegelerstellungseinheit erstellt wird und auf einem qualifizierten Zertifikat für elektronische Siegel beruht. Die Definition ist mit der der qualifizierten elektronischen Signatur vergleichbar. Ein elektronisches Siegel dient dabei allerdings nach Art. 3 Nr. 25 eIDAS-VO nur dazu, den Ursprung und die Unversehrtheit von Daten in elektronischer Form sicherzustellen. Nach Art. 35 Abs. 2 eIDAS-VO gilt für ein qualifiziertes elektronisches Siegel die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen es verbunden ist. Diese Regelung führt im Ergebnis wohl wie § 371a Abs. 1 ZPO zu einem Anscheinsbeweis im Sinne des Prozessrechts (TR-RESICAN, Anwendungshinweise R – Unverbindliche rechtliche Hinweise, Stand 15.6.2018, S. 46f.). Werden also Daten mit einem elektronischen Siegel versehen, kann man davon ausgehen, dass sie authentisch sind und aus der angegebenen Quelle, in der Regel von einer Behörde oder einem Unternehmen, stammen, das oder die als Quelle der Daten bezeichnet wird. Im Unterschied zur qualifizierten elektronischen Signatur werden die Daten aber keinem persönlichen Verfasser zugeordnet. Letztendlich geht es um eine qualifizierte elektronische Signatur für juristische Personen (näher dazu TR-RESICAN, Anwendungshinweise R – Unverbindliche rechtliche Hinweise, Stand 15.6.2018, S. 45f.).

Ein qualifizierter elektronischer Zeitstempel ist ein elektronischer Zeitstempel, der bestimmte Anforderungen erfüllt (Art. 3 Nr. 34 i. Vbdg. m. Art. 42 eIDAS-VO). Ein elektronischer Zeitstempel verknüpft Daten in elektronischer Form mit einem bestimmten Zeitpunkt und erbringt dadurch den Nachweis, dass diese Daten zu diesem Zeitpunkt vorhanden waren (Art. 3 Nr. 33 eIDAS-VO). Bei einem qualifizierten elektronischen Zeitstempel werden Datum und Zeit so mit diesen Daten verknüpft, dass die Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist. Außerdem beruht einer auf einer Zeitquelle, die mit der koordinierten Weltzeit beruht. Er muss nicht mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel unterzeichnet werden. Es reichen eine fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel eines qualifizierten Vertrauensdienstanbieters. Trotz dieser nicht so strengen Voraussetzung wird bei ihm nach Art. 41 Abs. 2 eIDAS-VO vermutet, dass Datum und Zeit richtig und die mit Datum und Zeit verbundenen Daten unversehrt sind. Auch hier ergibt sich daraus wohl ein Anscheinsbeweis dafür, dass das Datum und die Zeit, die im elektronischen Siegel angegeben sind, stimmen (vgl. TR-RESICAN, Anwendungshinweise R – Unverbindliche rechtliche Hinweise, Stand 15.6.2018, S. 47).

2. Formanforderungen im VwVfG NRW

Eine Reihe weiterer Fragen beschäftigt sich mit dem Problem, ob bestimmte Sicherheitsmittel wie z.B. qualifizierte elektronische Signaturen verwendet werden müssen oder sollen.

Bestimmte Sicherheitsmittel müssen nur verwendet werden, wenn sie durch ein Gesetz vorgeschrieben werden. Im allgemeinen Verwaltungsrecht gibt es aber keine generellen Anforderungen, nach denen Begehren von Bürgern oder sogar Verwaltungsakte der Schriftform bedürfen. § 37 Abs. 2 S. 1 VwVfG NRW lässt sogar ausdrücklich mündliche Verwaltungsakte zu. Aber selbst dort, wo es formale Anforderungen gibt, gibt es keine Regelung, nach der z.B. zwingend eine qualifizierte elektronische vorgeschrieben wird. Wo vom Gesetz die Schriftform verlangt wird, kann diese durch nach § 3a Abs. 2 VwVfG NRW durch die elektronische Form ersetzt werden. Die elektronische Form kann zwar mithilfe der qualifizierten elektronischen Signatur gewahrt werden (§ 3a Abs. 2 S. 2 VwVfG NRW), es gibt aber noch vier andere Möglichkeiten, u.a. durch Abgabe einer Erklärung in einem von einer Behörde zur Verfügung gestellten elektronischen Formular oder durch die Versendung eines elektronischen Dokuments über DE-Mail mit Bestätigung gem. § 5 Abs. 5 DE-Mail-G (§ 3a Abs. 2 S. 4 VwVfG NRW). Wird ein elektronisches Formular verwendet, muss bei einer Eingabe über öffentliche Netze ein sicherer Identitätsnachweis nach § 18 PAuswG oder § 78 Abs. 5 AufenthG erfolgen (§ 3a Abs. 2 S. 5 VwVfG). Hier ist eine Verwendung einer qualifizierten elektronischen Signatur nicht vorgeschrieben. Erfolgt die Eingabe innerhalb des nicht öffentlich zugänglichen Behördennetzwerks, muss keine solche Identifizierung erfolgen. Aus alledem ergibt sich, dass die Verwendung einer qualifizierten elektronischen Signatur im allgemeinen Verwaltungsrechts nirgends vorgeschrieben ist.

Etwas Anderes kann sich nur aus Vorschriften in Einzelnormen ergeben.

Eine Besonderheit weist das VwVfG für Verwaltungsakte (und nur für diese) auf: Nach § 37 Abs. 2 S. 2 VwVfG müssen mündliche Verwaltungsakte schriftlich oder elektronisch bestätigt werden, wenn ein Bürger dies verlangt und daran ein berechtigtes Interesse hat. Für die Form gilt hier auch § 3a Abs. 2 VwVfG, sodass ein Zwang zur Verwendung der qualifizierten elektronischen Signatur auch hier besteht. Nach § 37 Abs. 2 S. 3 VwVfG kann ein Bürger sogar verlangen, dass ein elektronischer Verwaltungsakt ihm gegenüber schriftlich bestätigt wird, wenn er daran ein berechtigtes Interesse hat. An dieser Stelle ist die herkömmliche Schriftform verlangt – also ein Medienbruch vorgesehen. Aber auch das führt naturgemäß nicht dazu, dass bestimmte elektronische Sicherungsmittel vorgeschrieben werden.

3. Das Konzept der Vertrauensniveaus

Für viele, wenn nicht für die meisten Anwendungsszenarien gibt es daher keine gesetzlichen Formanforderungen. Die Behörden müssen dann entscheiden, welche elektronischen Sicherungsmittel sie einsetzen. In diesen Fällen wird – auch im Rahmen des OZG – dringend empfohlen, die Frage, welche Mittel zur Sicherheit von Identität von Absendern oder der Unverfälschtheit von Inhalten eingesetzt werden, von dem jeweiligen Sicherheitsniveau (so Art. 8 eIDAS-VO) oder Vertrauensniveau (so § 8 Abs. 1 S. 1 OGV) abhängig zu machen. Unterschieden wird dabei zwischen drei Sicherheits- bzw. Vertrauensniveaus. Dies geschieht eingeschränkt auf elektronische Identifizierungsmittel in Art. 8 Abs. 2 eIDAS-VO und umfassender auch in der

einschlägigen Technischen Richtlinie TR-03107-1 Elektronische Identitäten und Vertrauensdienste im E-Government des BSI, Teil 1, Punkt 1.3 (derzeit Version 1.1.1 v. 7.5.2019).

Die drei Niveaus werden in der Richtlinie des BSI unter 2.3 wie folgt beschrieben:

- **normal**: Die Schadensauswirkungen bei einer Kompromittierung sind begrenzt und überschaubar.
- **substantiell**: Die Schadensauswirkungen bei einer Kompromittierung sind substantiell.
- **hoch**: Die Schadensauswirkungen bei einer Kompromittierung können beträchtlich sein.

Bei Formvorschriften, die darüber hinausgehen, wird das Niveau auch als hoch+ bezeichnet.

Aufgrund dieses Konzepts können Anforderungen bei jeder Anwendung bewertet und ausgewählt werden: Zunächst muss das der Anwendung angemessene Vertrauensniveau ermittelt werden. Danach sind die notwendigen Sicherungsmaßnahmen auszuwählen. Bei einem normalen Vertrauensniveau ist weniger zu fordern als bei einem hohen. Neben den in den Fragestellungen genannten Sicherungsmitteln sowie weiteren kryptographischen Verfahren wie der fortgeschrittenen elektronischen Signatur kommt auch ein Verfahren mit Zwei-Wege-Authentifizierung wie im electronic banking oder der Einsatz des elektronischen Identitätsnachweises iSd§ 18 PersAuswG (z.B. beim Einsatz elektronischer Formulare in Portalen in § 3a Abs. 2 S. 5 VwVfG vorgesehen) in Betracht. Die BSI-Richtlinie bewertet eine Fülle in der Praxis üblicher Verfahren und Sicherungsmittel. Sie sollte daher bei der Verfahrensgestaltung im Einzelfall herangezogen werden, weil die gesetzlichen Vorschriften (auch § 8 OZG) den Verwaltungen hier meist viel Spielraum lassen (so auch Denkhaus/Richter/Bostelmann, EGovG; OZG, § 8 OZG Rn. 3). Es ist nur jeweils im Einzelfall zu prüfen, ob es für das jeweilige Fachverfahren spezielle gesetzliche Regelungen gibt, die den Einsatz bestimmter Sicherungsmittel verlangen.

Zu beachten ist, dass auch bei einem hohen Vertrauensniveau nicht notwendig ein kryptographisch sehr sicheres Mittel wie die qualifizierte elektronische Signatur verlangt wird (vgl. z.B. die Kriterien unter 7.2 der BSI-Richtlinie). Es können auch andere geeignete organisatorische Maßnahmen getroffen werden. Dies entspricht auch den gesetzlichen Anforderungen in § 3a Abs. 2 VwVfG NRW, den Regeln zum elektronischen Zeitstempel oder den im früheren Gutachten unter III. dargestellten Anforderungen der VgV.

4. Zur langfristigen Sicherheit kryptographischer Verfahren

Technisch beruhen die unter 2. genannten qualifizierten elektronischen Siegel ebenso wie auch die qualifizierten elektronischen Signaturen auf kryptographisch nach dem derzeitigen Stand von Wissenschaft und Technik sicheren Verfahren. Diese Situation kann sich freilich in der Zukunft aufgrund technologischer Fortschritte jederzeit ändern. Wenn man die Nachweisfunktionen dieser Verfahren langfristig sichern will, muss auf solche Situationen technologisch reagiert werden. Dazu sollen die in Art. 34 eIDAS-VO genannten Bewahrungsdienste dienen. Sie sollen gewährleisten, dass qualifizierte elektronische Siegel oder Signaturen auf Dauer prüfbar und sicher bleiben. Einzelheiten dazu werden in der Technischen Richtlinie 03125 Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR) v. 2.5.2019 dargestellt.

Es wird z.B. empfohlen, für die langfristige Aufbewahrung elektronischer Dokumente nur wenige und einheitliche Datenformate zu nutzen (BSI TR-ESOR, 6.2, S. 39). Soweit derzeit ersichtlich, gibt es aber noch keine zertifizierten Bewahrungsdienstanbieter. Es ist allerdings zu empfehlen, bei der langfristigen Aufbewahrung von elektronischen Dokumenten die vom BSI dargestellten Empfehlungen zu berücksichtigen.

II. Zu den einzelnen Fragestellungen

1. Einsatz von elektronischen Signaturen, Siegeln bzw. Zeitstempeln

In den ersten acht Fragen geht es darum, wann qualifizierte elektronische Signaturen, Siegel bzw. Zeitstempel bei einer elektronischen Aktenführung eingesetzt werden müssen bzw. sollen. Ferner geht es um andere kryptografische Verfahren wie die fortgeschrittene elektronische Signatur. Auch die Fragen 11 – 16 beziehen sich auf diesen Problemkomplex. Die Fragestellungen sollen jetzt zusammenhängend beantwortet werden.

a. Eine Pflicht zum Einsatz von qualifizierten elektronischen Signaturen, Siegeln bzw. Zeitstempeln besteht in erster Linie dann, wenn sie gesetzlich gefordert sind. Dies ist – wie unter I.2 erwähnt – im allgemeinen Verwaltungsrecht nirgends der Fall. Auch die Schriftform lässt sich elektronisch nicht nur durch qualifizierte elektronische Signaturen ersetzen. Etwas Anderes kann in einzelnen Gesetzen angeordnet werden. Dies muss aber im konkreten Anwendungszusammenhang geprüft werden. Es dürfte sich um seltene Ausnahmen handeln.

   Ferner gibt es einen Zwang zur Verwendung qualifizierter elektronischer Signaturen dann, wenn eine zivilrechtliche Erklärung in gesetzlich vorgeschriebener elektronischer Form angegeben werden soll. In diesem Fall verlangt § 126a BGB den Einsatz von qualifizierten elektronischen Signaturen. Praktische Fälle gibt es kaum – der Schriftform bedürfen z.B. langfristige Mietverträge über Immobilien nach §§ 550, 578 BGB oder die private Bürgschaft gem. § 766 BGB. Auch diese Fälle dürften kaum vorkommen. Nur dann, wenn langfristige Mietverträge elektronisch geschlossen werden sollen, ist auf die Einhaltung der Schriftform (einschließlich aller Anlagen) zu beachten.

   Ist eine qualifizierte elektronische Signatur aufgrund gesetzlicher Vorschriften zu verwenden, so muss – wie schon in der ersten Stellungnahme auf S. 7 unter II. 2.Frage dargestellt – auch die Signatur nebst Prüfdokumenten in der elektronischen Akte gespeichert werden und muss dort so lange bleiben, wie das Dokument noch Teil einer elektronischen Akte und nicht nur noch zur Archivierung im Sinne eines historischen Gedächtnisses der Stadt dient. Dafür sind die Voraussetzungen der BSI TR-ESOR zu berücksichtigen (oben 1-3).

   Für qualifizierte elektronische Siegel oder Zeitstempel gibt es keine entsprechenden Vorschriften.

b. In allen anderen Fällen, in denen es keine bindenden gesetzlichen Vorschriften zum Einsatz von qualifizierten elektronischen Signaturen, qualifizierten elektronischen Siegeln oder qualifizierten elektronischen Zeitstempeln gibt, muss auf Basis des oben unter I.2 dargestellten

Konzepts abgestufter Sicherheit zunächst ermittelt werden, welches Vertrauensniveau erforderlich ist. Danach müssen geeignete Maßnahmen zur Sicherheit gewählt werden. Dabei sollte auch beachtet werden, dass bei der Verwendung qualifizierter elektronischer Signaturen die Beweisvermutungen der ZPO (dazu frühere Stellungnahme S. 2) bzw. bei der Verwendung von elektronischem Siegel bzw. elektronischem Zeitstempel die im Ergebnis wohl gleichwertigen Vermutungen nach Art. 35 Abs. 2 bzw. 41 Abs. 2 eIDAS-VO (dazu oben I.1) gelten. Allerdings werden qualifizierte elektronische Signaturen auch in der Geschäftspraxis nicht genutzt. Selbst im Bereich des elektronischen Bankverkehrs gibt es andere Sicherungsmittel, die auch laufend an neue Bedrohungsszenarien angepasst werden. Zu diesen Sicherungsmitteln gehören auch andere kryptographische Verfahren wie die fortgeschrittene Signatur. Dies dürfte auch in den meisten Anwendungsszenarien im Verwaltungsbereich dazu führen, dass der Einsatz qualifizierter elektronscher Signaturen nicht zwingend ist.

Qualifizierte elektronische Zeitstempel sind gesetzlich – soweit ersichtlich – nirgends vorgeschrieben. Sie stellen aber ein zuverlässiges Mittel dar, um nachzuweisen, wann ein Dokument in einer elektronischen Akte vorhanden ist. Außerdem haben sie nach Art. 41 Abs. 2 eIDAS-VO die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben ist, für sich. Aus diesen Gründen ist die Verwendung qualifizierter elektronischer Zeitstempel ein wichtiges Mittel, um den Zeitpunkt zu belegen, zu dem ein Dokument etwa durch Scannen in eine elektronische Akte gelangt ist oder wann es gescannt wurde. In solchen Fällen ist die Verwendung qualifizierter elektronischer Zeitstempel auf den ersten Blick sinnvoll. Dennoch sollte auch vor ihrem Einsatz eine Risikobetrachtung unter Einbeziehung notwendiger Sicherheitsniveaus erfolgen. Die in der Fragestellung zitierte Vitako-Leitlinie zum ersetzenden Scannen in Kommunen nach TR-RESISCAN gibt hier auf die Kommunalverwaltung bezogene ergänzte Leitlinien. Zu beachten ist, dass dort das Schutzniveau von Papierdokumenten weitgehend als „normal“ gekennzeichnet wird. Aber auch aus dieser Leitlinie ergeben sich keine konkreten Empfehlungen für den Einsatz konkreter Sicherheitsmittel.

Insgesamt gilt daher: Außer in wenigen Fällen gesetzlicher Formvorgaben müssen in der elektronischen keine qualifizierten elektronischen Signaturen, qualifizierte elektronische Siegel oder qualifizierte elektronische Zeitstempel verwendet werden. Über ihre Anwendung in konkreten Verwendungszusammenhängen muss anhand des üblichen Vorgehens auf der Basis von Vertrauensniveaus unter Berücksichtigung dort einsetzbarer Sicherungsmittel entschieden werden. Eine darüberhinausgehende allgemeine Aussage, wo sie eingesetzt werden sollen, ist nicht möglich.

c. Gefragt wird ferner, wann qualifizierte elektronische Signaturen geprüft werden sollen oder müssen. Dazu gilt folgendes: Soweit es um die Authentifizierung eines Absenders geht, ist es dringend anzuraten, die Korrektheit der Signatur bei Eingang zu prüfen. Wenn das Mittel qualifizierte elektronische Signatur zur Absicherung eines Verfahrens eingesetzt wird, sollte ebenfalls geprüft werden, ob die jeweils verwendete Signatur korrekt ist. Diese Prüfung kann auch bei weiteren Prüfschritten widerholt werden, wenn dies notwendig erscheint. Dies

hängt aber von der Sicherheit etwa der internen Vorgänge ab. Ist die Gefahr einer nachträglichen unerkannten Verfälschung von Dokumenten gering, muss eine einmal geprüfte Signatur nicht nochmals geprüft werden. Dies kann aber nur im Einzelfall entschieden werden. Eine Prüfung einer neu erzeugten Signatur vor Versenden ist im Übrigen auch nicht üblich.

d. Eine letzte Frage bezieht sich auf den Beweiswert von mit kryptografischen Verfahren behandelten Dokumenten im Verhältnis von nur in einem DMS mit revisionssicheren Speichern abgelegten elektronisch erzeugten Dokumenten.

Hier muss man unterscheiden: Soweit ein Dokument mit einer qualifizierten elektronischen Signatur versehen ist, gelten die schon geschilderten besonderen Beweisregeln der ZPO, die auch in Verwaltungsprozessen Anwendung finden. Für die qualifizierten elektronischen Siegel und Zeitstempel gelten die faktisch gleichwertigen Beweisregeln Art. 35 Abs. 2 bzw. 41 Abs. 2 eIDAS-VO. Das erhöht ihren Beweiswert in der Praxis deutlich, weil die Beweiseignung des für die Sicherheit des Dokuments gewählten Verfahrens nicht im Einzelfall belegt werden muss, sondern schon vom Gesetz vermutet wird. Wie schon ausgeführt, kann es aber je nach gewähltem Verfahren auch andere Mittel geben, mit denen der Beweiswert von Dokumenten gesichert werden kann. Allerdings müsste die Sicherheit des Verfahrens im Einzelfall ggf. konkret dargelegt werden. In der Gerichtspraxis wird allerdings bei eingeführten Verfahren oft von der Sicherheit ausgegangen, wenn diese schon in geeigneter Form an anderer Stelle dargelegt wurde und der Gegner keine substantiierten Einwände gegen die Sicherheit des Verfahrens erhebt.

2. Zu den Fragen der Stadt Mülheim

Zwei Fragen der Stadt Mülheim beziehen sich auf ein System DiPS.

Die erste Frage bezieht sich auf den Umgang mit digitalen Signaturen. Diese werden offenbar vor dem Abspeichern ins Langzeitarchiv durch Klartextinformationen ersetzt. Der Begriff digitale Signatur ist dabei unklar. Vermutlich sind elektronische Signaturen gemeint. Dann ist jedenfalls die Entfernung qualifizierter elektronischer Signaturen so lange rechtlich bedenklich, wie die archivierten Dokumente noch zu Beweiszwecken benötigt werden. Nach Entfernen einer qualifizierten elektronischen Signatur geht der Beweiswert verloren. Die prozessualen Vorschriften zur Beweiswirkung qualifizierter elektronischer Signaturen gelten nicht mehr, weil ein qualifiziert signiertes elektronisches Dokument nicht mehr vorliegt. Das gleiche gilt für die Entfernung eines qualifizierten elektronischen Siegels oder eines qualifizierten elektronischen Zeitstempels. Die Entfernung anderer digitaler Signaturen ist nicht von so großer Bedeutung.

Wieweit eine geänderte Abspeicherung der Dokumente ohne digitale Signaturen zu Archivzwecken sinnvoll ist, ist juristisch nicht ohne weiteres zu entscheiden. Dort gibt es keine konkreten Vorgaben zu diesen Fragen. Allerdings ist Archivgut nach § 5 Abs. 2 S.2 ArchivG NRW

in seiner Entstehungsform zu erhalten und ggf. nach archivfachlichen Erkenntnissen zu bearbeiten. Die Entfernung der Signatur ist eine Veränderung. Ob diese Änderung archivfachlich sinnvoll ist, ist keine juristische Frage.

3. Zu den Anforderungen an die Aufbewahrung von Papierdokumenten

Eine Anfrage der civitec beschäftigt sich damit, ob sich durch die GoBD die Regelungen zu elektronischen Signaturen, dem OZG oder weitere Änderungen die Anforderungen an die Speicherung/Aufbewahrung konventionell erstellter Dokumente ändern.

Dazu ist Folgendes auszuführen: Änderungsanforderungen ergeben sich dann, wenn statt der konventionellen Aufbewahrung solcher Dokumente in herkömmlichen Akten die Aktenführung nur noch elektronisch erfolgen soll. In einem solchen Verfahren müssen auch die konventionellen Papierdokumente elektronisch aufbewahrt werden. Bleibt es demgegenüber bei der bisherigen Aktenführung, ändert sich nichts.

Insoweit ergeben sich Änderungsnotwendigkeiten für die Mitglieder des KDN derzeit nicht. § 9 Abs. 3 EGovG NRW, der eine Pflicht zur Führung einer elektronischen Akte vorsieht, gilt nur für Landesbehörden. Er gilt nicht für kommunale Behörden, selbst dann nicht, wenn sie als untere staatliche Verwaltungsbehörde tätig werden (§ 9 Abs. 3 S. 3 EGovG NRW).

Die GoBD sind in diesem Zusammenhang in aller Regel nicht direkt anwendbar. Anderes gilt nur für kommunale Tochtergesellschaften in Form von Handelsgesellschaften und u.U. einzelne Teile kommunaler Verwaltungen, die z.B. Stadthallen bewirtschaften.

Führt eine Behörde freiwillig die elektronische Akte ein, müssen konventionelle Dokumente in ein elektronisches Format übernommen werden. Dies geschieht durch (in der Regel ersetzendes) Scannen. Die dabei zu beachtenden Regelungen sind schon auf S. 3 der ersten Stellungnahme dargestellt. Die TR-RESICAN und die Vitako-Leitlinie geben dazu Hinweise. Im Übrigen entsprechen die GoBD weitgehend den Grundsätzen ordnungsgemäßer Aktenführung (vgl. S. 4 der ersten Stellungnahme). Die dort genannten allgemeinen Anforderungen an eine ordnungsgemäße Aktenführung entsprechen den allgemeinen Anforderungen der GoBD. Es fehlt nur der Grundsatz der Vertraulichkeit, der in der Privatwirtschaft keine handels- oder steuerrechtliche Anforderung darstellt. Allerdings ist die Vertraulichkeit auch dort zum Schutz der eigenen Betriebsgeheimnisse und auch aus datenschutzrechtlichen Gründen zu wahren. Im Übrigen galt dieser Grundsatz für die öffentliche Verwaltung auch bislang. Ich gehe daher davon aus, dass ein abgenommener GoBD-Prozess in aller Regel unverändert bleiben kann.

Zentral dürfte hier aber sein, ob der jeweilige Scanprozess den genannten Anforderungen der TR-RESISCAN und der Vitako-Leitlinie entspricht.

4. Zu den letzten Fragestellungen:

In den beiden letzten Punkten greift civitec schon erörterte Fragen auf:

Zunächst geht es darum, wann es zwingend ist, bei einer bestimmten Vertrauensstufe Dokumente digital zu signieren. Dazu besagt die in der Antwort genannte Richtlinie TR-ESOR 3125 nichts: Diese Richtlinie befasst sich nur dem Erhalt des Beweiswerts von Dokumenten, die vor der Speicherung zum Zwecke der Aufbewahrung bereits digital signiert waren, z.B. um den Absender und den Inhalt einer Nachricht zu authentifizieren oder den Zeitpunkt eines Scan-Vorgangs durch einen qualifizierten elektronischen Zeitstempel zu dokumentieren. Sie beschäftigt sich nicht mit der Frage, ob die auch ohne einen solchen kryptographischen Vorgang als sicher betrachteten Dokumente durch eine Signatur ergänzt werden können. Möglich ist es natürlich, den Zeitpunkt der Einspeicherung eines Dokuments durch einen qualifizierten elektronischen Zeitstempel zu belegen und das Dokument zusätzlich gegen Veränderung zu sichern. Dadurch wird auch eine kryptographische Sicherheit geschaffen. Dies kann auch auf anderem Wege geschehen, wenn nur gesichert bleibt, dass das ursprüngliche Dokument unverändert gespeichert wird. Eine zwingende Vorgabe zu einem solchen Verfahren ist den gesetzlichen Vorgaben und auch den verschiedenen Richtlinien juristisch nicht zu entnehmen. Sie lassen dem Anwender hier viel Spielraum. Auch die TR-RESISCAN führt in ihren unverbindlichen rechtlichen Hinweisen auf S. 7 aus, dass dazu keine generellen Vorgaben gemacht werden können.

Die letzte Frage beschäftigt sich mit dem Beweiserhalt von elektronischen Signaturen. Dazu ist auf die Ausführungen unter I.3 zu verweisen. Anzumerken ist ferner, dass die SigV am 29.07.2017 außer Kraft getreten ist.

III. Zur beigefügten Tabelle

Zur beigefügten Tabelle sind folgende Hinweise notwendig:

Wie oben ausgeführt, sind in der Regel für jedes eingesetzte Verfahren eigene Bewertungen vorzunehmen. Daher sind allgemeine Bewertungen wie sie sich aus der Tabelle ergeben, schon prinzipiell sehr fragwürdig.

Zum zweiten sind die in der Tabelle aufgeführten Differenzierungen aus Sicht des Unterzeichners nur bedingt zielführend. Insbesondere wird bei den elektronischen Dokumenten zwischen Dokumenten, die von Dritten stammen (Posteingang) und eigenen Dokumenten („digital born“) unterschieden, nicht aber nach der Qualität der eingehenden Dokumente. Die technischen Sicherungsmaßnahmen beziehen sich auf den Speichervorgang und nicht auf das vorher vorhandene Dokument. Das macht eine generelle Bewertung sehr schwierig. Die Antworten können sich außerdem insbesondere in der letzten Zeile nur auf den Zeitraum ab Aufnahme der Dokumente in die elektronische Akte beziehen.

Ferner entspricht die Terminologie teilweise nicht der in der TR-RESISCAN, die aber auch sonst üblich ist. Ich habe daher das Wort Transferbericht durch das Wort Transfervermerk ersetzt. Wichtig ist im Übrigen gerade für den Nachweis der Vollständigkeit der Akte und der Aktenwahrheit auch die Dokumentation des Zeitpunkts, zu dem ein Dokument in die Akte gelangt ist. Dies ist durch die Verwendung von Zeitstempeln möglich. Darauf habe ich im Text verwiesen.

Ferner verlangt aus meiner Sicht die der Grundsatz der Aktenmäßigkeit im Falle einer elektronischen Akte keine Schriftlichkeit, sondern eine geeignet organisierte und technisch gestaltete elektronische Aktenführung.

Insgesamt glaube ich nicht, dass diese Tabelle für die praktische Arbeit geeignet ist und rate daher von ihrer Nutzung ab. Ich habe sie dennoch wunschgemäß ausgefüllt. Die sehr holzschnittartigen Antworten sind aber allenfalls vage Anhaltspunkte für die praktische Anwendung.

Bonn, 12.01.2019
gez. Helmut Redeker

Welche Verfahren (Spalten) erfüllen die Grundsätze der ordnungsgemäßen Aktenführung aus dem Rechtsstaatsprinzip (Zeilen) (Stichwort: Schriftgutverwaltung)?

	Posteingang						„digital born“		
	Papierdokument			Elektronische Datei (z.B. E-Mail, DE-Mail, Dateianlage)			Elektronische Datei (z.B. E-Mail, Verwaltungsakt in Word-Datei)		
	Ohne weitere technische Maßnahmen gescannt und im DMS abgelegt	Gescannt mit technischen Maßnahmen und im DMS abgelegt		Ohne weitere technische Maßnahmen im DMS abgelegt	Mit technischen Maßnahmen im DMS abgelegt		Ohne weitere technische Maßnahmen im DMS abgelegt	Mit technischen Maßnahmen im DMS abgelegt	
		Qualifizierte elektronische Signatur + Transfervermerk	Qualifiziertes elektronisches Siegel + Transfervermerk		Qualifizierte elektronische Signatur	Qualifiziertes elektronisches Siegel		Qualifizierte elektronische Signatur	Qualifiziertes elektronisches Siegel
Aktenmäßigkeit[1]	ja	ja	ja	ja	ja	ja	ja	ja	ja
Aktenvollständigkeit und	nein	Nicht vollständig	Nicht vollständig	nein	Nicht vollständig	Nicht vollständig	nein	Nicht vollständig	Nicht vollständig

[1] = Pflicht Akten zur führen; aus der Akte ergibt sich jederzeit der Stand und die Entwicklung der Vorgangsbearbeitung. (Schriftlichkeit)

Aktenklarheit[2]		(Zeitstempel?)	(Zeitstempel?)		(Zeitstempel?)	(Zeitstempel?)		(Zeitstempel)	(Zeitstempel)
Aktenwahrheit[3]	nein	ja	ja	Eher nein (Dokument abhängig)	ja	ja	nein	ja	ja

2.3 Gutachterliche Stellungnahme 10.05.2019

Gutachterliche Stellungnahme

zu Fragen der Beweiskraft von Dokumenten in elektronischen Akten und der elektronischen Aktenführung

vorgelegt von

Rechtsanwalt und Fachanwalt für Informationstechnologierecht Dr. Helmut Redeker, Bonn

Heinle Redeker und Partner Rechtsanwälte mbB, Am Schaumburger Hof 10, 53175 Bonn

Vorbemerkung

In der gutachterlichen Stellungnahme geht es um den Beweiswert elektronischer Dokumente, insbesondere darum, in welchem Umfang bewiesen werden kann, dass in einem Verwaltungsverfahren oder auch einem Verwaltungsprozess vorgelegte elektronische Dokumente in dem Sinne echt sind, dass sie mit dem vorgelegten Inhalt vom angegebenen Verfasser stammen und ggf. auch beim Adressaten eingegangen sind. Dies ist primär eine technische Frage. Ihre Beantwortung hängt davon ab, wie sicher Mittel zur Identifizierung von Absendern und zur Feststellung der Authentizität von Texten sind und ob auch ein Zugang beim Empfänger so ausgeführt und dokumentiert wird, dass der Absender Sicherheit hat, dass das Dokument

[2] = Pflicht, alle wesentlichen Verfahrenshandlungen vollständig und nachvollziehbar in den Akten abzubilden. (Integrität der gesamten Akte)

[3] = Pflicht, alle wesentlichen Verfahrenshandlungen wahrheitsgemäß aktenkundig zu machen. (Integrität und Authentizität der einzelnen Dokumente in einer Akte)

auch wirklich beim Adressaten angekommen ist. Die Frage wird daher im Streitfall oft der Beweiswürdigung durch einen IT-technischen Sachverständigen unterliegen. Sie ist nicht primär rechtlicher, sondern tatsächlicher Natur.

Dennoch gibt es eine Reihe rechtlicher Vorgaben, die diese Beweisführung betreffen und Grundregeln für eine solche Beweiswürdigung aufstellen. Diese werden in der Folge dargestellt. In einem zweiten Schritt werden dann die einzelnen unter 1.2 aufgeworfenen Fragen beantwortet. Zuletzt geht es um besondere Fragestellungen im Vergabeverfahren und im Archivwesen.

I. Gesetzliche Regelungen

1. Qualifiziert elektronisch signierte Dokumente

Im Verwaltungsrecht gibt es keine konkreten Vorschriften zum Beweiswert elektronischer Dokumente. Allerdings enthält § 371a ZPO, der nach § 98 VwGO auch im Verwaltungsgerichtsprozess und nach § 118 SGG auch im Sozialgerichtsverfahren gilt, besondere Regelungen über die Beweiskraft elektronischer Dokumente.

Zunächst stellt § 371a Abs. 1 ZPO qualifiziert elektronisch signierte Dokumente privater Privaturkunden gleich (§ 371a ZPO). Dies bedeutet nach § 416 ZPO, dass sie den Beweis dafür bieten, dass die in dem elektronischen Dokument enthaltene Erklärung auch wirklich von dem Erklärenden abgegeben wurde. Nicht qualifiziert signierte private elektronische Dokumente sind dagegen nur Augenscheinobjekte und unterliegen der freien Beweiswürdigung. Wann eine qualifizierte elektronische Signatur vorliegt, richtet sich nach Art. 3 Nr. 12 eIDAS-VO.

Sehr viel weiter geht der Beweiswert elektronischer Dokumente, die von einer öffentlichen Behörde ausgestellt wurde. Nach § 371a Abs. 3 ZPO, der nach § 98 VwGO ebenfalls im Verwaltungsgerichtsprozess gilt, gelten für alle elektronischen Dokumente, die von einer Behörde im Rahmen ihrer Amtsbefugnisse in der vorgeschriebenen Form erstellt wurden, die Regelungen über die Beweiskraft öffentlicher Urkunden Anwendung. Diese Norm bezieht sich damit nicht nur auf qualifiziert signierte öffentliche Dokumente, sondern auf jedes elektronische Dokument, unabhängig von der konkreten Form. Allerdings muss diese elektronische Form gesetzlich vorgeschrieben sein. Der Beweis erstreckt sich dann auf den jeweils beurkundeten Vorgang, also eine von einem Bürger abgegebene Erklärung, einen erlassenen Verwaltungsakt oder ähnliches (§ 415 ZPO). Auch diese Norm dürfte im Verwaltungsverfahren oft gelten.

§§ 3a und 26 VwVfG NRW enthalten keine vergleichbaren Regelungen für elektronische Dokumente. Sachlich dürfte sich eine Beweiswürdigung im Verwaltungsverfahren aber nach ähnlichen Regeln wie im Gerichtsverfahren richten. Teilweise wird sogar eine analoge Anwendung dieser Normen im Verwaltungsverfahren befürwortet (Mann u.a./Engel/Pfau, § 371a 26 VwVfG, Rn. 44). Unabhängig von der rechtsdogmatischen Begründung wird man für die Praxis § 371a ZPO auch im Verwaltungsverfahren berücksichtigen müssen.

2. Grundsätze der ordnungsgemäßen Aktenführung

Der Beweiswert elektronischer Dokumente ergibt sich allerdings oft auch daraus, dass sie einer ordnungsgemäß geführten Akte entnommen sind. Auch Vorschriften zur Aktenführung sind daher für den Beweiswert wichtig. Insbesondere sind sie dann wichtig, wenn es um den Beweiswert gespeicherter Dokumente dahingehend geht, dass sie während der Speicherdauer nicht verändert wurden.

Erste, noch sehr rudimentäre Regelungen enthält das VwVfG NRW. So lässt § 3a VwVfG NRW die elektronische Kommunikation zu und erlaubt in § 3a Abs. 2 VwVfG auch den Ersatz der Schriftform nicht nur durch qualifiziert elektronisch signierte Dokumente (§ 3a Abs. 2 S. 1 u. 2 VwVfG), sondern auch durch den Einsatz elektronischer Formulare (§ 3a Abs. 2 S.4 Nr. 1 VwVfG NRW). Soweit solche Formulare über öffentliche Netze versandt werden, muss allerdings vom Nutzer der Formulare ein sicherer Identitätsnachweis nach § 18 PAuswG beigefügt werden (§ 3a Abs. 2 S. 5 VwVfG NRW). Ferner lässt § 35a VwVfG NRW auch vollständig automatisierte Entscheidungen in bestimmten Fällen zu.

Beide Vorschriften regeln aber nichts zu der Frage, wie die Akten in den geregelten Fällen der elektronischen Kommunikation oder bei vollständig automatisiert ergehenden Entscheidungen geführt werden sollen.

Mehr Regelungen enthält dann schon das EGovG NRW. Nach § 5 Abs. 1 EGovG NRW sollen Behörden bis spätestens zum 1.1.2021 die Durchführung ihrer Verwaltungsverfahren auch auf elektronischem Weg anbieten. In solchen Verfahren sollen auch notwendige Nachweise elektronisch eingereicht werden können (§ 8 Abs. 1 EGovG). Nach § 8 Abs. 1 EGovG können Akten auch elektronisch geführt werden. Ab dem 1.1.2022 sollen die Akten bei Landesbehörden sogar elektronisch geführt werden (§ 9 Abs. 3 S. 1 EGovG). Nach § 10 Abs. 1 eGoVG sollen die Behörden bei elektronischer Aktenführung an Stelle von Papierdokumenten deren elektronische Wiedergabe in der Akte führen. Nach heutigem Stand der Technik bedeutet dies das Scannen der Vorlagen. Dabei ist nach dem Stand der Technik sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen und dass nachvollzogen werden kann, wann und durch wen die Unterlagen übertragen wurden. Im Normalfall ist das gescannte Dokument nach dem Scannen zu vernichten oder zurückzugeben (§ 10 Abs. 2 eGoVG). Einzelheiten dazu regelt die nach § 23 Abs. 2 Nr. 5 eGoVG erlassene Verwaltungsvorschrift zum ersetzenden Scannen in der Landesverwaltung v. 31.1.2018. Diese verweist unter Nr. 3.1 auf die „Technische Richtlinie Ersetzendes Scannen (TR-RESISCAN)“ des BSI in der jeweils geltenden Fassung. Nach 3.2 Buchst. c ist neben den im Gesetz geregelten Anforderungen sicherzustellen, dass das elektronische Abbild des Papierdokuments unverändert bleibt. Nach 7.1 ist das Dokument nach dem Scanvorgang in der Regel zu vernichten. Es gibt dazu keine Ausnahme aus Beweisgründen.

Generell muss ferner bei der Führung elektronischer Akten gemäß § 8 Abs. 2 EGovG nach dem Stand der Technik sichergestellt werden, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden. Worin diese Grundsätze bestehen, ist an dieser Stelle nicht geregelt.

Allerdings besteht eine Ermächtigung, nach der das für Informationstechnik zuständige Ministerium Einzelheiten über die Anwendung der Grundsätze ordnungsgemäßer Aktenführung in Verwaltungsvorschriften regeln kann (§ 23 Abs. 2 Nr. 6 EGovG). Dies ist auch durch einen Runderlass des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie vom 2.8.2018 geschehen. Dieser gilt für alle dem EGovG unterfallenden Behörden und damit auch für Gemeinden und Gemeindeverbände (§ 1 Abs. 2 EGovG). Erst dieser Erlass, der zwar für die Behörden bindend ist, aber keine Gesetzeskraft hat, regelt Detaillierteres.

Nach diesem Erlass gehören zu diesen Grundsätzen ordnungsgemäßer Aktenführung (2.1 Erlass):

- das Gebot der Aktenmäßigkeit: Das Handeln der Verwaltung ist im Regelfall durch die elektronische Aktenführung zu dokumentieren.
- das Gebot der Vollständigkeit und Nachvollziehbarkeit: Alle wesentlichen Verwaltungshandlungen müssen vollständig und nachvollziehbar abgebildet werden. Hierzu sind alle entscheidungsrelevanten Unterlagen und Bearbeitungsschritte zu dokumentieren und im Sach- und Zeitzusammenhang abzulegen. Der Stand und die Entwicklung der Vorgangsbearbeitung müssen aus den elektronisch geführten Akten nachvollziehbar sein.
- das Gebot der wahrheitsgemäßen Aktenführung: Der Inhalt der Akten muss das Verwaltungshandeln korrekt abbilden.
- das Gebot der Integrität und Authentizität: Die physische und logische Unversehrtheit der Akteninhalte muss jederzeit gewahrt sein. Zulässige Veränderungen müssen grundsätzlich so angebracht werden, dass sie erkennbar und nachvollziehbar sind.
- das Gebot der Vertraulichkeit: Es ist sicherzustellen, dass ausschließlich die Personen Zugriff auf Akten, Vorgänge und Dokumente erhalten, die deren Inhalt zur rechtmäßigen Aufgabenerfüllung benötigen. Die Anforderungen des Datenschutzes sind zu beachten.
- das Gebot der langfristigen Sicherung: Der Aktenbestand ist entsprechend den Aufbewahrungs- und Dokumentationspflichten langfristig zu sichern. Hierzu sollen langzeitstabile Datenformate verwendet werden. Soweit Rechts- oder Verwaltungsvorschriften keine bestimmten Aufbewahrungsfristen vorsehen, sind diese in der behördlichen Aktenordnung festzulegen. Alle Unterlagen, die zur Aufgabenerfüllung nicht mehr erforderlich sind, insbesondere diejenigen, deren Aufbewahrungsfrist abgelaufen ist, sind dem jeweils zuständigen Archiv anzubieten.

Nach Punkt 3. sollen elektronische Akten, Vorgänge und Dokumente während der gesamten Aufbewahrungsfrist auffindbar und lesbar zu halten. Unberechtigte Zugriffe und Veränderungen sind zu verhindern.

Wie diese doch recht allgemeinen Anforderungen konkret umgesetzt werden soll, regelt der Erlass nicht. Insoweit ähnelt der den im Handels- und Steuerrecht geltenden Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen

in elektronischer Form sowie zum Datenzugriff (GoBD). Es liegt daher in der Verantwortung der einzelnen Behörden, die elektronische Aktenführung so zu organisieren, dass sie die Anforderungen erfüllt.

Von den oben aufgeführten Geboten sind für den Beweiswert insbesondere das Gebot der Vollständigkeit und Nachvollziehbarkeit und das Gebot der Integrität und Authentizität wichtig. Bei Erklärungen Dritter ist es auch wichtig, dass zuverlässig festgestellt werden kann, dass die Erklärung auch von dem Dritten stammt, von dem sie nach ihrem Inhalt stammen soll.

3. Zusammenfassung

Zusammenfassen kann festgestellt werden:

Für qualifiziert elektronisch signierte Dokumente gibt es gesetzliche Regelungen und damit konkrete Möglichkeiten, die Authentizität übermittelter Inhalte und die Identität von Verfassern elektronischer Dokumente sicher festzustellen. Die Identität von Verfassern kann ferner durch den Einsatz des Identitätsnachweises nach § 18 PAuswG sichergestellt werden. Auch beim Einsatz von gesicherter DE-Mail gibt es gesetzlich abgesichert gute Beweismöglichkeiten für sichere Beweise mittels elektronischer Dokumente.

In allen übrigen Fällen ist die Beweislage schwierig. Rechtliche Vorgaben für konkret einzusetzende technische Verfahren gibt es nicht.

Wichtig ist allerdings in allen Fällen, dass im Rahmen einer elektronischen Aktenführung die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden. So kann ein guter Beweis dafür geführt werden, dass die in der Akte geführten elektronischen Dokumente unverändert genau die sind, die zur Akte gelangt sind. Wichtig ist auch, dass alle zur Akte gelangten Dokumente auch in die Akte aufgenommen und gespeichert werden, weil so die Vollständigkeit des in der Akte dokumentierten Verwaltungsvorgangs belegt werden kann. Wo es konkrete gesetzliche Regelungen für den konkreten Anwendungsvorgang gibt – wie etwa im Vergabeverfahren –, sind auch diese Regeln zu beachten.

II. Zu den allgemeinen Fragestellungen

1. Frage

Die erste Frage beschäftigt sich mit dem Beweiswert von nur in einem DMS mit revisionssicheren Speichern abgelegten elektronisch erzeugten Dokumenten im Vergleich zu eingescannten Dokumenten.

Wird nach den Vorgaben des Erlasses bzgl. des ersetzenden Scannens verfahren, dürfte zunächst die Übereinstimmung des abgebildeten Dokuments mit der Papiervorlage sicher beweisbar sein. Eine förmliche Beweisregel wie § 371a in Vbdg. mit § 416 ZPO gibt es aber nicht. Das abgebildete Originaldokument ist jedoch in der Regel nicht sofort oder gar nicht mehr verfügbar. Wird nun von einem Betroffenen behauptet, das Originaldokument (oder z.B. seine Unterschrift darauf) sei gefälscht, kann darüber bei eingescannten Dokumenten nicht mehr

Beweis erhoben werden. Bewiesen werden kann nur, dass das Dokument bildlich und textlich unverändert wiedergegeben wird. Zur Echtheit des Originaldokuments ergibt sich nichts.

Demgegenüber sind die in einem DMS abgelegten elektronischen Dokumente die „Originale". Bei solchen elektronischen Dokumenten hängt die Frage des Beweiswerts zunächst von der verwendeten Form ab. Ist es qualifiziert elektronisch signiert, ist zunächst die Echtheit dahingehend bewiesen, dass die darin erhaltene Erklärung von Inhaber der elektronischen Signatur abgegeben wurde. Ist das nicht der Fall, ist der Beweis nicht so einfach. Sollte das Dokument über DE-Mail versendet worden sein, kann eine Zustellung beim Empfänger mittels eines De-Mail-Einschreibens nach § 5 Abs. 9 DeMailG bewiesen werden (Spindler/Schuster/Spindler, Recht der elektronischen Medien, § 126a BGB, Rn. 15). U.U. können auch sicher gestaltete Passwortsysteme helfen (dazu Redeker, IT-Recht, Rn. 906). Unabhängig davon gibt es u.U. auch sonstige Möglichkeiten, das Dokument dem Aussteller zuzuordnen oder festzustellen, dass es eine Fälschung ist. In diesem Punkt ist der Beweiswert des elektronischen Dokuments also besser.

In vielen Fällen kommt es ferner darauf an, dass sichergestellt ist, dass das gespeicherte (original elektronische oder eingescannte) Dokument während der Speicherzeit nicht verändert wurde. In der Frage ist von revisionssicherem Speichern die Rede. Dies dürfte bedeuten, dass beim Speichern und Aufbewahren die GoBD eingehalten sind. Damit dürfte das technisch Mögliche getan sein, um Manipulationen zu vermeiden, sodass zumindest ein Beweis des ersten Anscheins dafürspricht, dass das zum relevanten Zeitpunkt in den Speichern vorhandene elektronische Dokument dem ursprünglich gespeicherten entspricht. Förmliche Beweisregeln gibt es gleichwohl nicht. Dies gilt für beide Formen von Dokumenten.

Insgesamt dürfte daher wegen des Problems, die Echtheit des Originals zu beweisen, das gespeicherte von vornherein elektronische Dokument einen höheren Beweiswert haben als das gespeicherte eingescannte Dokument.

2. Frage

In der zweiten Frage soll geklärt werden, was von der vollständigen Kommunikation aufbewahrt bzw. veraktet werden muss, um die Akte vollständig zu führen und z.B. die fristgerechte Einreichung von Unterlagen zu dokumentieren.

Die Frage ergibt sich aus einer interpretierbaren Formulierung in Nr. 2.1 des oben erwähnten Erlasses. Danach müssen alle wesentlichen Verwaltungshandlungen vollständig und nachvollziehbar abgebildet werden. Es sind alle entscheidungsrelevanten Unterlagen und Bearbeitungsschritte zu dokumentieren und im Sach- und Zeitzusammenhang abzulegen. Der Stand und die Entwicklung der Vorgangsbearbeitung müssen jederzeit aus den elektronisch geführten Akten nachvollziehbar sein. Nimmt man den Text wörtlich, muss nicht alles, sondern nur das Wesentliche und Entscheidungsrelevante aufbewahrt werden. Es ist nicht recht erklärbar, warum es zu dieser Einschränkung kommt. Denn niemand weiß, was in einer Akte irgendwann einmal entscheidungsrelevant sein kann. Es kann für Vorgesetze, höhere Dienststellen, Be-

troffene und Gerichte wichtig und evtl. sogar entscheidend sein, zu wissen, was zu einem Verwaltungsvorgang wann von wem beigetragen wurde, auch wenn der Erstentscheider etwas nicht für wichtig hielt. Daher dürfte die Regel sein, dass alles aufzubewahren ist. Angesichts der Speicherkapazitäten moderner IT-Anlagen sollte das auch technisch unproblematisch sein. Ausnahmen gelten nur für erkennbar nicht zur Akte gehörige Vorgänge wie z.B. falsch zugeordnete Schreiben oder Zufallsfunde mit Beziehung zu anderen Vorgängen. Ferner müssen persönliche Notizen von Sachbearbeitern nicht zwingend in die Akte aufgenommen werden. In diesem Punkt unterscheiden sich elektronisch geführte Akten nicht von herkömmlichen Papierakten.

Was das konkrete Beispiel betrifft, so muss schon bei Eingang nach den Grundsätzen ordnungsgemäßer Aktenführung dokumentiert werden, wann eine Unterlage eingegangen ist. Soweit möglich, sollte auch geprüft werden, ob die Eingabe tatsächlich von demjenigen stammt, von dem sie kommen soll. Dies ist bei einer qualifizierten Signatur durch Prüfung der Echtheit des Zertifikats der Ausstellersignatur (ggf. auch des Zertifikats des Zertifizierungsanbieters und sogar des Wurzelzertifikats) möglich (dazu ausgiebig Müller-Wrede/Grünhagen, § 10 VgV Rn. 41ff.). Bei anderen Dokumenten ist das schwieriger. Wird geprüft, sollten auch Prüfvorgang und Prüfergebnis ordnungsgemäß gespeichert werden. Wird nicht geprüft, sollten alle Angaben gespeichert werden, die bei einem Streit zum Nachweis hilfereich sein können (z.B. der Header des E-Mails).

Insgesamt ist es sinnvoll, alle Eingänge möglichst vollständig zu speichern und aufzubewahren.

3. Frage

Die dritte gestellte Frage betrifft das elektronische Empfangsbekenntnis. Solche Empfangsbekenntnisse sind nicht anders zu behandeln als alle anderen Bestandteile der elektronischen Akte. Gehen Sie ein, ist – soweit möglich – zu prüfen, ob sie echt sind und vom angegebenen Absender stammen. Dies ist bei qualifiziert signierten Empfangsbekenntnissen und auch bei Empfangsbekenntnissen, deren Zugang nach § 5 Abs. 9 DE-Mail bestätigt wird, leicht. Ferner wird ein Beweis bei Verwendung des Identitätsnachweises nach § 18 Abs. 1 u. 2 PAuswG möglich sein. In den anderen Fällen gelten die oben auf S. 5 dargestellten Probleme. Nach der Prüfung sind elektronische Empfangsbekenntnisse nach den Grundsätzen ordnungsgemäßer Aktenführung der Akte beizufügen und aufzubewahren. Auch die Prüfergebnisse sind zur Akte zu nehmen. Soweit die Verwaltung solche Empfangsbekenntnisse z.B. in einem Verwaltungsgerichtsverfahren selbst versendet, ist auch dieser Vorgang entsprechend zur elektronischen Akte zu nehmen.

4. Frage

Die 4. Frage beschäftigt sich damit, wie vom Bürger eingereichte ausgefüllte Formulare iSv § 3a Abs. 2 S. 4 Nr. 1 iVm S. 5 VwVfG NRW sicher aufbewahrt werden können. Hier ist im Wesentlichen auf das schon Gesagte zu verweisen.

Zunächst ist das ausgefüllte Formular so zu speichern, dass festgestellt werden kann, welchen Inhalt es hatte, und zwar sowohl hinsichtlich des von der Behörde vorgegebenen Inhalts als auch hinsichtlich der vom Bürger eingesetzten Inhalte. Ferner ist der Identitätsnachweis (dazu oben 3. Frage) zu speichern ebenso wie die Ergebnisse von Prüfungen, mit denen seine Korrektheit geprüft wurde. Die Speicherung hat so zu erfolgen, dass sie den Anforderungen des Erlasses vom 02.08.2018 genügen. Insbesondere ist zu sichern, dass der Akteninhalt langfristig gesichert ist und keine Zweifel am Inhalt des Formulars und der Identität des Verwenders bestehen. Wie dies geschehen soll, ist weder in einem Gesetz noch in einem Erlass geregelt.

5. Frage

Die nächste allgemeine Fragestellung betrifft die Dokumentation der eingesetzten Hard- und Software sowie des Betriebs des für die elektronische Akte verwendeten IT-Systems. Dazu sind weder dem eGovG noch den dazu ergangenen Erlassen Regelungen zu entnehmen. Der Erlass vom 02.08.2018 erwähnt Dokumentationen noch nicht einmal. Nr. 3 Abs. 1 S. 3 des Erlasses führt lediglich aus, dass die korrekte Aufbewahrung des Akteninhalts während der Aufbewahrungsfrist durch die aktenführende Stelle sicherzustellen ist.

Für die elektronische Führung von Büchern nach Handels- und Steuerrecht enthält dagegen die GoBD als Verwaltungsvorschrift unter 10.1 einige auch recht allgemeine Regeln zur Verfahrensdokumentation. U.a. sollen sich aus der Verfahrensdokumentation Inhalt, Aufbau, Ablauf und Ergebnisse des DV-Verfahrens vollständig und schlüssig ergeben (Rn. 151 GoBD). Für elektronische Dokumente soll z.B. der organisatorisch und technisch gewollte Prozess von der Entstehung der Informationen über die Indizierung, Verarbeitung und Speicherung, dem eindeutigen Wiederfinden und der maschinellen Auswertbarkeit, der Absicherung gegen Verlust und Verfälschung und der Reproduktion beschrieben werden (Rn. 152 GoBD). Ferner muss für den Zeitraum der Aufbewahrungsfrist gewährleistet und nachgewiesen werden, dass das in der Dokumentation beschriebene Verfahren dem in der Praxis eingesetzten Verfahren entspricht (Rn. 154 GoBD). Die Verfahrensdokumentation muss ferner verständlich und damit für einen sachverständigen Dritten in angemessener Zeit nachprüfbar sein (Rn. 151 GoBD). Diese Vorschrift ist zwar für Verwaltungsakten nicht anwendbar. Die dargestellten Grundsätze bilden aber die Anforderungen ab, die auch für die Dokumentation eines Verfahrens aus juristischer Sicht im Rahmen ordnungsgemäße Aktenführung gelten. Es muss dargestellt werden, was geschieht und wie dadurch die Anforderungen der Grundsätze zur ordnungsgemäßen Aktenführung eingehalten werden sollen und auch tatsächlich eingehalten werden. Dadurch wird auch die Beweissicherheit elektronische Dokumente gesichert. Konkretere Anforderungen gibt es auch juristischer Sicht nicht.

6. Frage

Die letzte allgemeine Frage betrifft die Rechtsvorschriften und Richtlinien, die zu beachten sind. Die allgemeinen, für alle geltenden Vorschriften sind unter I. dargestellt. Viele in den Kommunen geführten Akten und Fachverfahren unterliegen allerdings verschiedenen Spezialgesetzen wie dem BMG, dem PAuswG, dem PStG oder dem SGB VIII. Hier gibt es oft spezielle

Anforderungen und Erlasse, die in diesen Spezialbereichen zu beachten sind. Hier ist im Einzelfall zu überprüfen, ob dazu auch spezielle Anforderungen an die elektronische Aktenführung gehören. Dies kann aber in einem allgemeinen Gutachten nicht geschehen.

Hinsichtlich der konkret nachgefragten Fragen zum Vergabe- und Archivrechts folgt eine Darstellung.

III. Teil Vergaberecht

1. Allgemeine Bemerkungen

Für das Vergaberecht enthält die VgV eine Reihe konkreter Vorgaben über im Vergabeverfahren verwendete Mittel. So verlangt § 10 Abs. 1 S. 2 VgV von eingesetzten elektronischen Mitteln, zu gewährleisten, dass

1. die Uhrzeit und der Tag des Datenempfangs genau zu bestimmen sind,
2. kein vorfristiger Zugriff auf die empfangenen Daten möglich ist,
3. der Termin für den erstmaligen Zugriff auf die empfangenen Daten nur von den Berechtigten festgelegt oder geändert werden kann,
4. nur die Berechtigten Zugriff auf die empfangenen Daten oder auf einen Teil derselben haben,
5. nur die Berechtigten nach dem festgesetzten Zeitpunkt Dritten Zugriff auf die empfangenen Daten oder auf einen Teil derselben einräumen dürfen,
6. empfangene Daten nicht an Unberechtigte übermittelt werden und
7. Verstöße oder versuchte Verstöße gegen die Anforderungen gemäß den Nummern 1 bis 6 eindeutig festgestellt werden können.

§ 11 Abs. 2 VgV verlangt den Einsatz solcher elektronischen Mittel, die die Unversehrtheit, Vertraulichkeit und Echtheit der Daten gewährleisten.

Welches Sicherheitsniveau beim Einsatz solcher Systeme erforderlich ist, kann die Vergabestelle selbst festlegen (§ 10 Abs. 1 S. 1 VgV). Hier muss eine Abwägungsentscheidung zwischen Risiken für insbesondere Unversehrtheit und Absenderidentifizierung einerseits gegen ein praktikables und zügiges Vergabeverfahren andererseits erfolgen (dazu Müller-Vrede/Grünhagen, § 10 VgV Rn. 16ff.), dass auch für den Mittelstand nutzbar ist.

Dabei gilt die Verwendung einer fortgeschrittenen oder qualifizierten elektronischen Signatur schon als erhöhte Anforderung (Müller-Vrede/Grünhagen, § 10 VgV, Rn. 27ff.). Gegebenenfalls kann zur Sicherheit von Vertraulichkeit und/oder Unversehrtheit auch eine Verschlüsselung eingesetzt werden (dazu Müller-Vrede/Grünhagen, § 11 VgV, Rn. 60ff.). Konkrete technische Anforderungen nennt das Gesetz nicht. Die Bundesregierung kann aber nach § 13 VgV allgemeine Verwaltungsvorschriften über die zu verwendenden elektronischen Mittel und die einzuhaltenden technischen Standards erlassen. Soweit ersichtlich, sind solche Verwaltungsvorschriften zu den hier interessierenden Themen derzeit nicht erlassen worden.

Es bleibt also bei allgemeinen Vorgaben, die inhaltlich aber denen im allgemeinen Verwaltungsverfahren ähneln. Die allgemeinen Anforderungen, insbesondere an die sichere Identifikation der Teilnehmer, scheinen aber nicht allzu hoch zu sein, da noch nicht einmal konsequent eine fortgeschrittene elektronische Signatur verlangt wird. Dennoch wird verlangt, dass zweifelsfrei nachgewiesen werden kann, dass die verwendeten Daten von der angegebenen Datenquelle stammen (Müller-Vrede/Grünhagen, § 11 VgV Rn. 59 unter Verweis auf die Verordnungsbegründung, BR-Drs. 87/16, S. 166). Angesichts der vom Gesetz vorgesehenen unterschiedlichen Sicherheitsniveaus kann die ohnehin nie vollständig zu gewährleistende Zweifelsfreiheit des Nachweises nur so verstanden werden, dass sie gefahrenabhängig unterschiedlich hoch ist. Dies gilt es bei der Beantwortung der Fragen zu beachten.

2. Frage 1

In der ersten Fragestellung wird danach gefragt, welche Unterlagen/Nachweise im DMS abgelegt werden müssen, um die Beweiskraft für die auf der Vergabeplattform eingereichten Unterlagen zu erhalten. Im Prinzip ergeben sich hier die gleichen Anforderungen wie sonst auch. Es sind die Unterlagen abzulegen, aus denen sich der Ablauf und Inhalt des Vergabeverfahrens ergibt. Dabei ist insbesondere alles abzulegen, was nachweist, dass die Anforderungen des § 10 Abs. 1 S. 2 VgV erfüllt sind. Ferner muss alles abgespeichert werden, aus dem sich ergibt, dass eine Unterlage tatsächlich von der Quelle stammt, die angegeben ist. Ggf. sind auch Prüfergebnisse abzuspeichern. Insoweit gelten die Grundsätze ordnungsgemäßer Aktenführung auch im Vergabeverfahren. Insbesondere ist auch sicherzustellen, dass die Daten während der Aufbewahrungsfrist unverändert zugänglich bleiben. Konkrete technische Vorgaben, wie das geschehen kann, enthalten die Vorschriften nicht. So wäre es zu einer sicheren Identifizierung neben der Verwendung fortgeschrittener oder qualifizierter elektronischer Signaturen ggf. auch möglich, auf einer Vergabeplattform ein PIN-/TAN-System zur Identifizierung einzusetzen, das den von den Banken im Zahlungsverkehr eingesetzten Systemen vergleichbar ist. Ggf. hilft auch die Verwendung einer De-Mail mit sicherem Zugang nach § 4 Nr. 1 DeMailG. Die Verwendung schlichter E-Mails dürfte nicht ausreichen.

3. Frage 2

Die zweite vergaberechtliche Prüfung beschäftigt sich mit einem sog. Prüfprotokoll. Es bleibt hier unklar, was gemeint ist. Der Begriff wird in der VgV nicht verwendet. Allerdings ergeben sich vergaberechtliche Prüfergebnisse aus dem Vergabevermerk (§ 8 VgV). Dieser ist auf jeden Fall abzulegen, um die Ordnungsgemäßheit der Vergabeentscheidung darlegen und ggf. beweisen zu können.

Vermutlich ist aber ein Protokoll einer Prüfung entweder der Echtheit von Signaturen, der Verwendung von sicheren Übermittlungssystemen oder der Korrektheit des verwendeten IT-Systems gemeint. Wenn es solche Prüfprotokolle gibt, sollten sie auf jeden Fall dokumentiert und aufbewahrt werden, um bei Auseinandersetzungen die Beweissituation zu verbessern.

IV. Archivwesen

Die letzte Frage betrifft das Archivwesen. Konkret geht es darum, ob die Verwendung bestimmter technischer Verfahren für das Archivwesen ausreichend ist. Konkret genannt sind bestimmte Algorithmen zur Erzeugung von Hash-Werten.

Zur Gesetzeslage kann festgestellt werden, dass über die in der Fragestellung bereits genannten Regelungen im ArchivG NRW (§ 2 Abs. 7 und § 5 Abs.) keine weiteren Normen existieren, die sich mit den technischen Anforderungen an die Archivierung elektronischer Dokumente beschäftigen. Grundsätzlich dürfen allerdings auch bei Archiven die Anforderungen an den Nachweis der Identität des Verfassers/der Verfasser einzelner Dokumente und an ihre Echtheit den bislang dargestellten Anforderungen entsprechen. Dazu können auch die genannten Hashwertverfahren beitragen, wenn sie z.B. sicherstellen, dass ein ihnen zugeordnetes Dokument unverändert bleibt. Ob dies der Fall ist, ist eine technische und keine juristische Frage.

Das Archivwesen weist allerdings einige Besonderheiten gegenüber der allgemeinen Aktenführung auf. So kann es sein, dass nicht komplette elektronische Akten, sondern nur einzelne in ihnen enthaltene Dokumente archivwürdig sind und in ein Archiv übernommen werden. Insoweit wird der Grundsatz der Aktenvollständigkeit nicht gelten. Ähnliches mag für andere Grundsätze der ordnungsgemäßen Aktenführung gelten. Hier dürfte die Aufgabenstellung des Archivs als Gedächtnis einer Kommune andere Anforderungen stellen als der Nachweis eines ordnungsgemäßen Verwaltungsverfahrens und einer rechtmäßigen Entscheidung, auf Grund derer eine ordnungsgemäße Aktenführung erforderlich ist.

Der wichtigste Unterschied besteht allerdings in der Dauer der Aufbewahrung. Archive verfolgen das Ziel, Unterlagen auf Dauer zeitlich unbegrenzt aufzubewahren. Einzelne Archivunterlagen sind daher auch mehrere hundert oder gar 1000 Jahre alt. Eine wissenschaftliche oder sonstige Nutzung ist ohnehin erst nach 30 Jahren möglich (§ 7 Abs. 1 S. 1 ArchivG NRW). Dieses Ziel der unbegrenzten Aufbewahrung erfordert insbesondere eine langfristige Speicherung, während derer das einzelne Dokument lesbar und nachweisbar authentisch bleibt. Neben der Frage, welche Trägermedien über einen so langen Zeitraum überhaupt lesbar bleiben, werden mit Zeitablauf oft auch Datenformate unlesbar, so dass umgespeichert werden muss. Dies sieht § 11 Abs. 1 S. 1 eGovG NRW auch vor. Dabei muss – ähnlich wie beim ersetzenden Scannen – gesichert werden, dass das neu gespeicherte Dokument gegenüber früher inhaltlich unverändert auf dem Bildschirm dargestellt wird und nachvollzogen werden kann, wann und durch wen die Unterlagen übertragen wurden (§ 11 Abs. 1 S. 2 i Vbdg. mit § 10 Abs. 1 S. 2 eGovG NRW). Diese Regelung dürfte auch für Archive gelten, obwohl das eGovG NRW die Regelungen des ArchivG NRW unberührt lässt (§ 11 Abs. 2 eGovG NRW). Darüber kann es sein, dass im Laufe der Zeit sichere Echtheitsnachweise (z.B. zugeordnete Hashwerte) unsicher werden. In diesem Fall müssen unabhängig vom Umspeichern des Dokuments neue Sicherungsmittel verwendet werden. Dann kann auch eine Nachsignatur in dem Sinne erfolgen, dass das gesamte Dokument einschließlich der ursprünglichen Signatur und der Prüfergebnisse neu sig-

niert wird. Wichtig ist nur, dass die Authentizität des Originaldokuments erhalten und die sichere Identifizierung des Autors möglich bleibt. Gesetzliche Vorgaben gibt es im Archivwesen dazu nicht.

Insgesamt sind die in der Fragestellung genannten Verfahren auf den ersten Blick technisch sinnvoll. Konkrete rechtliche Vorgaben dazu, ob sie für Archivzwecke ausreichend sind, existieren jedoch nicht. Es muss daher technisch und nicht juristisch geprüft werden, ob sie ausreichen, um eine Langzeitarchivierung von Archivmaterial zu sichern.

Bonn, 04.10.2019
gez. Helmut Redeker

2.4 KDN Fragenkatalog: Beweiskraft von Dokumenten in eAkten

KDN Fragenkatalog:
Beweiskraft von Dokumenten in eAkten – kommentiert

Inhalt

1. Einsatz/Nutzung von qualifizierten elektronischen Signaturen und qualifizierten elektronischen Zeitstempeln

Kommentar: Gegebenenfalls beantwortet im Dokument "Leitlinie zum ersetzenden Scannen in Kommunen nach TR RESICAN"

Vorsitzender Richter Finanzgericht Berlin-Brandenburg: Barbelege haben Vertrauensniveau hoch https://www.datev.de/web/de/m/presse/im-fokus/aktuelle-themen/ersetzendes-scannen/statement-ulrich-schwenkert-finanzgericht-berlin-brandenburg.html

1.1. Wann müssen qualifizierte elektronische Signaturen bei elektronischer Aktenführung inkl. dem Scannen eingesetzt werden?

1.2. Wann müssen qualifizierte elektronische Zeitstempel eingesetzt werden?

1.3. Wann sollten qualifizierte elektronische Signaturen eingesetzt werden?

Am besten nach hinten stellen, weil bezogen auf die Kryptographie Vereinfachungen durch eIDAS zu erwarten sind.

1.4. Wann sollten qualifizierte elektronische Zeitstempel eingesetzt werden?

1.5. In welchen konkreten Anwendungsfällen muss die Kommune zwangsläufig qualifizierte elektronische Signaturen und qualifizierte elektronische Zeitstempel einsetzen? Wann müssen oder dürfen andere kryptographische Verfahren zum Einsatz kommen, wie z. B. die fortgeschrittene Signatur?

1.6. Steigt durch den Verzicht auf kryptografische Sicherungen das konkrete Prozessrisiko signifikant?

1.7. Inwieweit ist auch eine Nutzung von elektronischen Siegeln (eIDAS-Durchführungsgesetz) denkbar?

2. Prüfung von qualifizierten elektronischen Signaturen und qualifizierten elektronischen Zeitstempeln

Kommentar: Gegebenenfalls beantwortet im Dokument "Leitlinie zum ersetzenden Scannen in Kommunen nach TR RESICAN"

Vorsitzender Richter Finanzgericht Berlin-Brandenburg: Barbelege haben Vertrauensniveau hoch https://www.datev.de/web/de/m/presse/im-fokus/aktuelle-themen/ersetzendes-scannen/statement-ulrich-schwenkert-finanzgericht-berlin-brandenburg.html

Kommentar: Am besten nach hinten stellen, weil bezogen auf die Kryptographie Vereinfachungen durch eIDAS zu erwarten sind.

2.1. Wann müssen qualifizierte elektronische Signaturen bei elektronischer Aktenführung inkl. dem Scannen geprüft werden? (bei Eingang, bei Übernahme in revisionssicheren Speicher, bei Versand an Dritte (Justiz, …)?

2.2. Wann sollten qualifizierte elektronische Signaturen geprüft werden?

3. Beweiswerterhaltung

Kommentar: Gegebenenfalls beantwortet im Dokument "Leitlinie zum ersetzenden Scannen in Kommunen nach TR RESICAN"

Vorsitzender Richter Finanzgericht Berlin-Brandenburg: Barbelege haben Vertrauensniveau hoch https://www.datev.de/web/de/m/presse/im-fokus/aktuelle-themen/ersetzendes-scannen/statement-ulrich-schwenkert-finanzgericht-berlin-brandenburg.html

Anmerkung: Am besten nach hinten stellen, weil bezogen auf die Kryptographie Vereinfachungen durch eIDAS zu erwarten sind.

3.1. Wann müssen qualifizierte elektronische Signaturen zwingend bei elektronischer Aktenführung Beweiswert erhaltend gespeichert werden?

3.2. Wann sollten qualifizierte elektronische Signaturen bei elektronischer Aktenführung Beweiswert erhaltend gespeichert werden?

3.3. Ablage des Prüfungsdokuments in der E-Akte?

3.4. Möglichkeit des ergänzenden Scannens und behalten des Originals?

Kommentar: Der Datensatz muss mit dem Nachweis des Authentifizierungsniveaus gespeichert werden.

4. Vergaberecht

4.1. Im Vergaberecht reicht als Signaturniveau die Textform aus.

4.2. Welche Unterlagen/Nachweise müssen im DMS abgelegt werden, um die Beweiskraft für die auf der Vergabeplattform eingereichten Unterlagen zu erhalten.

4.3. Muss in jedem Fall das Prüfprotokoll angefordert und abgelegt werden oder sind die Details zum Angebot ausreichend?

4.4. Hat es Auswirkungen auf die Beweiskraft, wenn die Angebotsunterlagen von der Vergabeplattform nicht direkt ins DMS abgelegt werden können, sondern erst auf einem Fileserver zwischengespeichert werden müssen?

5. Revisionssichere Speicherung

5.1. Kann bei Einsatz revisionssicherer Speichersysteme (EMC Centera oder ECS, Hitachi Vantara, FAST LTA Silent Cubes, etc.) auf die Beweiswerterhaltung von qualifizierten elektronischen Signaturen verzichtet werden?

Kommentar: In der Regel ja.

5.2. Welche Voraussetzungen müssen beim Betrieb eines leistungsfähigen DMS (bei uns d.3) und einer revisionssicheren Speicherung (bei uns FAST LTA Silent Bricks) erfüllt werden, um insgesamt die Anforderungen an eine vollständige Substituierung eines Papierarchivs erfüllen zu können?

Kommentar: Ist nur eine Güter-/Risikoabwägung, weil freie richterliche Beweiswürdigung.

5.3. Welche Anforderungen bestehen hinsichtlich der Dokumentation der eingesetzten Hard- und Software sowie des Betriebs? (Wünschenswert wäre hier eine Muster-Betriebsdokumentation, nach Umfragen bei anderen Rechenzentren ist das bei vielen ein wunder Punkt).

Kommentar: ZP Verfahrensdoku.

5.4. Welche Rechtsvorschriften und Richtlinien sind für die Kommunalverwaltung dabei zu beachten?

6. Langzeitarchivierung

Kommentar: Einige Annahmen sind nicht korrekt.

6.1. Weiterhin würden wir gerne die Frage prüfen lassen, ob das bisherige Vorgehen bei der Langzeitarchivierung rechtlich in Ordnung ist. Siehe auch Anhang (Schäfer zum „Ius Archivi“).

Zurzeit wird bei einer Übernahme in die Langzeitarchivierungslösung DiPS.kommunal geprüft, ob Objekte signiert waren und dieses Kennzeichen wird als Metadatum gespeichert. Die Signatur an sich wird allerdings nicht übernommen, da eine Signatur im Langzeitarchiv nicht gewünscht ist.

Kommentar: Wenn Signatur nicht gewünscht ist – wofür ich Verständnis habe – ist das ganze Konzept der Nachsignatur nicht notwendig.

Im Langzeitarchiv wird technisch und organisatorisch sichergestellt, dass die Daten unveränderbar sind – somit ist eine Signatur aus der aktuellen, archivarischen Sicht nicht mehr notwendig.

Kommentar: OK für uns (kenne natürlich das System nicht).

Außerdem ist es bei Dokumenten, die in das Langzeitarchivformat PDF/A umgewandelt werden, technisch nicht möglich, die Signatur beizubehalten.

Kommentar: Doch mit PDF/A 3 würde das gehen (Seit 2012).

Daher ist unsere Frage: Ist bei einer Übernahme von Objekten mit einer qualifizierten digitalen Signatur in eine Langzeitarchiv-Lösung die Speicherung ohne diese Signatur möglich, wenn gleichzeitig gespeichert wird, dass eine solche qualifizierte elektronische Signatur zum Zeitpunkt der Übernahme vorhanden war?

Kommentar: Wenn Signatur und Dokument getrennt aufbewahrt werden ist das möglich. Anders funktioniert auch die Nachsignatur nach ArchiSig nicht.

Rein akademisch: Die Signatur – und die Nachsignatur – erlauben die mathematische Prüfbarkeit der lückenlosen Unveränderbarkeit. Eine Aussage derartig, dass die Signatur zum Zeitpunkt tt.mm.JJJJ gültig und ungebrochen war, sagt a) nicht darüber aus, dass sie nicht nachträglich gebrochen wurde und b) die Aussage selbst kann – da sie selbst nicht signiert ist – manipuliert sein.

Wenn es nicht möglich ist, dieses Verfahren beizubehalten, werden enorme organisatorische und finanzielle Probleme auf die Archive zukommen. Zum einen muss eine Alternative für das aktuelle Langzeitarchivierungsformat von Dokumenten (PDF/A) gefunden werden, bei dem die qualifizierte digitale Signatur übernommen werden kann. Weiterhin sind umfangreiche Änderungen an der Software

DiPS.kommunal erforderlich, auch der Aufwand, die Signaturen in regelmäßigen Abständen zu aktualisieren, ist riesig und als Archiv nicht zu leisten.

6.2. Wie geht das System mit digitalen Signaturen um?

Digitale Signaturen werden nicht ins Langzeitarchiv übernommen, da sie i.d.R. nur für den Außenkontakt des Registraturbildners relevant waren.

Kommentar: Ich denke, im Workshop kann man erarbeiten, dass eine Beweisbelastbarkeit für alle Unterlagen die nicht bei IHRER GEBURT qualifiziert signiert wurden auch ohne QES erreicht werden kann.

Vor dem Ingest ins Langzeitarchiv sollten diese Signaturen durch Klartextinformationen (z.B. elektronische Stempel) ersetzt werden.

Kommentar: Das ist kein Ersatz. Eine Signatur beinhaltet eine mathematische Funktion, die durch visuelle Unterschrift nicht ersetzt werden kann. Unserer Meinung nach aber nicht notwendig.

Diese Funktionalitäten sind Sache des Exporters aus dem produzierenden System. Ein langfristiger Erhalt der nur zeitlich befristet gültigen Signaturen ist für Archive nicht leistbar. Es findet stattdessen eine detaillierte Protokollierung der Arbeitsschritte im AIP statt (vgl. nächster Punkt).

6.3. Wie können Akten aus DiPS.kommunal zur Vorlage bei Gericht gelangen?

Kommentar: Keine Kenntnisse bei uns.

DiPS.kommunal dokumentiert den Übernahmeprozess und alle Bearbeitungsschritte am Archivgut im internationalen Standard PREMIS und speichert die Informationen im AIP. Dieses AIP (TAR-Container) kann exportiert und in Drittsystemen (z.B. auch bei Gericht) nachverwendet werden. Die Daten haben zwar keinen Urkundscharakter, dürfen aber ein hohes Maß an Glaubwürdigkeit durch diese Art der Verarbeitung für sich beanspruchen.

Kommentar: Ja, sehe ich auch so.

Einen speziellen „Gerichtsexport“, wie er in manchen DMS eingebaut ist (z.B. als Gesamt-PDF mit durchlaufender Seitenzählung), ist derzeit in DiPS.kommunal nicht implementiert.

Quelle bzw. nähere Infos hierzu: https://www.lwl-archivamt.de/de/Fachinformationen/Archiv_IT/langzeitarchivierung/ und unter: https://www.lwl-archivamt.de/de/Fachinformationen/Archiv_IT/DMS/

7. Formanforderungen

Die Einführung von elektronischem Rechtsverkehr und eAkte dürfte die grundlegendste Veränderung der Arbeitsweise der öffentlichen Verwaltung darstellen, seitdem überhaupt rechtsstaatliche und bürokratische Systeme erfunden und eingeführt wurden. Daher ist aus unserer Sicht auch eine grundlegende Betrachtung und Beantwortung der entsprechenden Fragen notwendig. Das Stellen von Detailfragen und entsprechende Antworten zu Problemen des Einzelfalls führen nur zu punktuellen Lösungen. Die Umstellung der Verwaltungspraxis von einer papiergebundenen zu einer digitalen Arbeitsweise erfordert daher eine Fragestellung, die dazu führt, dass wir wissen: Welche grundlegenden Anforderungen bringt die Tätigkeit einer öffentlichen Verwaltung mit sich und durch welche digitalen Werkzeuge können diese Anforderungen erfüllt werden?

Die Vorgaben für die öffentliche Verwaltung bzw. für ihr Handeln ändern sich mit der Digitalisierung nicht. Es ändert sich lediglich die Arbeitsweise. Es stellen sich jedoch weiterhin dieselben Fragen zu Themen wie Nachvollziehbarkeit der Verwaltungsverfahren, Transparenz der Verfahren, Beweiswert von Akten und Dokumenten usw. Im zivilrechtlichen Rechtsverkehr, an dem die Verwaltung wie jeder andere teilnimmt, stellen sich ebenso die gleichen Fragen zu Formerfordernissen und dem Be- bzw. Nachweis bestimmter Tatsachen.

All diese Fragen sind gesetzlich geregelt, für das öffentliche Recht im allgemeinen Verwaltungsrecht, im privatrechtlichen Bereich durch das allgemeine Zivilrecht, sowie durch das jeweilige Prozessrecht. Die Umstellung der Verwaltung von einer papiergebundenen auf eine digitale, papierlose Arbeitsweise führt zu keiner Veränderung bei diesen Vorgaben, sondern zu der Frage, wie können diese Vorgaben, die ich bislang auf dem papiergebundenen Weg erfüllt habe, zukünftig ohne Papier und rein digital erfüllt werden.

Mit einer Fragestellung, die systematisch ergründet, welche Formanforderungen sich in der öffentlichen Verwaltung stellen und einer Antwort, welche dementsprechend einen Katalog auswirft, aus welchem ersichtlich ist, welche Formanforderung mit welchem digitalen Werkzeug (nicht) erfüllt werden kann, kann die Verwaltung bzw. jedes Fachamt selbst überprüfen, welche Werkzeuge notwendig sind.

7.1. Welche „Formanforderungen“ (klassische Formerfordernisse wie z.B. Schriftform; Anforderungen an Verfahren wie z.B. Aktenführung; Anforderungen, die gewisse

Zwecke wie Beweiskraft, Warnfunktion, Transparenz, etc. erfüllen) stellt das Gesetz an das Handeln der öffentlichen Verwaltung?

Kommentar: Zu wenig Informationen bei uns in der Schublade. Müssten wir erstmal recherchieren.

7.1.1 im Bereich des öffentlich-rechtlichen Handelns?

Bsp. Akte: Die Verwaltung ist im Rahmen ihrer Verwaltungsverfahren zur Aktenführung verpflichtet. § 29 VwVfG. Aktenführung bedeutet: Gebot der Aktenmäßigkeit, Gebot der Vollständigkeit, Gebot der Führung wahrheitsgetreuer Akten (vgl. Kopp/Ramsauer VwVfG 8. Aufl. § 29 Rn. 11). Zweck dieser Formanforderung ist es, dass das Verwaltungsverfahren transparent und nachvollziehbar ist. Diese Erfordernisse ergeben sich aus dem Rechtsstaatsprinzip, da ein wirksamer Rechtsschutz gegen den Staat nur möglich ist, wenn dessen Verwaltungsverfahren, welche überprüft werden sollen, auch nachvollzogen und so nachgeprüft werden können. Diese Formvorgaben werden dadurch erfüllt, dass die Verwaltung zu einem Verfahren zunächst eine Akte anlegt, in dieser Akte alle wesentlichen Verfahrensschritte aktenkundig macht bzw. ablegt und diese Akte nachträglich nicht verfälscht wird bzw. nicht verfälscht werden kann (Blattzahlen), also den tatsächlichen Ablauf des Verfahrens widerspiegelt und schlussendlich auch dem Bürger bzw. dem Gericht zur Verfügung gestellt wird. In der praktischen Papierarbeit erfolgt dies durch chronologisches Ablegen und Nummerieren der zum Verfahren gehörenden Dokumente und Schriftstücke u.Ä. zwischen zwei Aktendeckel.

Die Antwort zum Stichwort Akte wäre daher: § 29 VwVfG, Verpflichtung zur Aktenführung.

Diese ergibt folgende Formanforderungen:

- Gebot der Aktenmäßigkeit (keine unmittelbare Frage der Form, eher des systematischen Aufbaus und der Erfassung einzelner Verfahren in einem Datenmanagementsystem)
- Aktenvollständigkeit (Integrität der gesamten Akte)
- Aktenwahrheit (Integrität und Authentizität der einzelnen Dokumente in einer Akte). Bsp. Zustellung eines Verwaltungsaktes: Zustellung mittels PZU § 3 LZG NRW, definiert die Zustellung mittels PZU unter Verwies auf § 177 ff. ZPO

7.1.2 im Bereich des privatrechtlichen Handelns?

Bsp. Schriftform nach § 126 BGB

7.2. Wie können diese Formanforderungen digital/elektronisch umgesetzt werden?

7.2.1 welche digitalen "Werkzeuge/Verfahren" gibt es?

Aufführen und definieren der verschiedenen digitalen Werkzeuge, also einfache E-Mail, Versenden über spezielle Behörden-/Anwalts-/Gerichtspostfächer, qualifizierte elektronische Signatur, qualifiziertes elektronisches Siegel, einfaches Scannen, Scannen mit Transfervermerk, PDF-Dokument usw.

Kommentar: am besten nach hinten stellen, weil bezogen auf die Kryptographie Vereinfachungen durch eIDAS zu erwarten sind.

7.2.2 welche der unter 7.1 definierten Formanforderungen können mit welchem Werkzeug (nicht) erfüllt werden?

Stichwort Akte:

- Aktenmäßigkeit: erfordert ein Datenmanagementprogramm, bei welchem ein bestimmter Verwaltungsvorgang identifizierbar ist und sodann ersichtlich ist, welche Daten/Dokumente zu diesem Vorgang gehören. Hier könnten weiterhin Datenmanagementsysteme genannt werden, welche diese Anforderungen erfüllen.
- Aktenvollständigkeit (Integrität der gesamten Akte): Erfordert ein Datenmanagementsystem, bei welchem erkennbar ist, wann und in welcher Reihenfolge Dokumente einem Vorgang zugeordnet wurde und ob zwischenzeitlich/nachträglich aus diesem Vorgang einzelne Dokumente entfernt oder verändert wurden. Hier könnten weiterhin Datenmanagementsysteme genannt werden, welche diese Anforderungen erfüllen.
- Aktenwahrheit: Integrität der einzelnen Dokumente: hier ist für die unter 2a definierten Werkzeuge anzugeben, ob mit diesen die Formanforderung erfüllt werden kann, z.B. für Posteingänge: einfaches Scannen nein, Scannen mit Transfervermerk ja; oder bei eigenen Dokumenten: einfaches Word-Dokument nein, PDF nein, PDF mit elektronischer Signatur ja, Behördensiegel ja, Zeitstempel nein usw.
- Authentizität der einzelnen Dokumente: hier ist für die unter 2a definierten Werkzeuge anzugeben, ob mit diesen die Formanforderung erfüllt werden kann, z.B. für Posteingänge: einfaches Scannen nein, Scannen mit Transfervermerk ja; oder bei eigenen Dokumenten: einfaches Word-Dokument mit Namensunterschrift nein, PDF mit Namensunterschrift nein, elektronische Signatur ja usw.

Es handelt sich lediglich um Beispielantworten, die die Zielrichtung der Fragen vorgeben, ohne Gewähr auf inhaltliche Richtigkeit. Von Seiten der IT bitte ich das qualifizierte elektronische Siegel in die Fragestellungen einzubeziehen. Beispielhafte Darstellung der Beantwortung (Ziel der Fragestellung). Die „Antwortmatrix“ sollte nicht zu abstrakt sein. Eine rein theoretische Abhandlung würde nicht helfen.

8. Dokumentarten

8.1 Grundsätzlich wird technisch unterstellt, dass in einem technischen Prozess zwei grundsätzliche Dokumentarten unterschieden werden müssen:

- Konventionell erstellte und unterschriebene Dokumente
- Elektronisch signierte Dokumente
- Konventionelle Dokumente

Kommentar: Die Liste umfasst 3 Arten. Aber wir würden generell anders gliedern:

1. Dokumente, die die Schriftform erfordern und für die auch die QES kein zulässiger Ersatz ist. Das sind eigenhändig unterschriebene Papier-Dokumente

2. Dokumente, die die Schriftform erfordern und für die die QES ein zulässiger Ersatz der Unterschrift nach 126 BGB ist. Letzteres kommt in der Praxis bis auf wenige Ausnahmen kaum vor, die Signaturfunktion hat sich nach über 20 Jahren Signaturgesetz und SigV in Deutschland nicht durchgesetzt. Wenige Ausnahmen: bEA für Anwälte, in Planung: Gesundheitskarte (Einführung derzeit nicht bekannt)

3. Elektronisch geborene Dokumente mit einer freiwilligen Unterschrift (keine Schriftformerfordernisse) in analoger (Unterschreiben nach Ausdruck) oder elektronischer Form

4. Dokumente mit Namenszeichen (Das sind KEINE Unterschriften)

5. weitere

Frage: Ändern sich durch die GoBD, die Regelungen zur elektronischen Signatur, das OZG etc. die Anforderungen an konventionell erzeugte Dokumente im Rahmen der Speicherung/Aufbewahrung (z.B. Nutzung von zusätzlichen Qualitätskriterien wie Hash-Werte, qualifizierte Zeitstempel etc.)?

Erwartung ist nein (vgl. BSI Technische Richtlinie TR-RESISCAN 3138 Ersetzendes Scannen), obwohl die technischen Eigenschaften an z.B. eine fotografierte Unterschrift des Kunden wesentlich geringer sind als bei elektronischen Unterschriften (Fälschungssicherheit). Hier wird unterstellt, dass ein abgenommener GoBD-Prozess aus juristischer Sicht unverändert bleiben kann. Der Beweiswert von konventionellen GoBD-konform gespeicherten Dokumenten ändert sich nicht. Risikobetrachtung: Sofern der Bestand bestehender Prozesse nicht gewährleistet wird, sind auch bestehende Fachprozesse in Hinblick auf erweiterte Anforderungen zu untersuchen und zu ergänzen. Sofern bei Umsetzung des OZG einzelne elektronische Dokumente in einem Prozess nicht verarbeitet werden können, würde hier auch die Umgehungslösung „Erstellen eines konventionell unterschriebenen Bestätigungsdokuments beim Kunden“ o.ä. erschwert.

8.2 Elektronisch signierte Dokumente

Unter anderem im Zuge des OZG sind mehrstufige Lösungen denkbar. Dabei ist es dem Kunden (Organisation/Bürger) auch möglich, im Rahmen einer Anmeldung am Servicekonto ein Formular auszufüllen und zu versenden.

Kommentar: Gegebenenfalls beantwortet im Dokument "Leitlinie zum ersetzenden Scannen in Kommunen nach TR RESICAN"

Vorsitzender Richter Finanzgericht Berlin-Brandenburg: Barbelege haben Vertrauensniveau hoch https://www.datev.de/web/de/m/presse/im-fokus/aktuelle-themen/ersetzendes-scannen/statement-ulrich-schwenkert-finanzgericht-berlin-brandenburg.html

Anmerkung zu Signaturen: am besten nach hinten stellen, weil bezogen auf die Kryptographie Vereinfachungen durch eIDAS zu erwarten sind.

Frage: Wann ist es zwingend, dass bei einer Anmeldung einer bestimmten Vertrauensstufe (z. B. Name Passwort (Stufe 1) oder Elektronischer Personalausweis (Stufe 4)) auch jedes abgelegte Dokument digital signiert wird?

Erwartung ist, dass bei einer Anmeldung der höchsten Vertrauensstufe durch ein GoBD-konformes Verfahren die erstellten Dokumente durch eine elektronische Signatur ergänzt werden können. Damit wäre eine Dokumentenweitergabe in weitere GoBD-konforme Verfahren möglich, bei der nur die Dokumentenprüfung erfolgen muss (E-Akte, DMS) (vgl. hierzu die Vorgaben BSI Technische Richtlinie TR-ESOR 3125 Beweiswerterhaltung kryptographisch signierter Dokumente). Risiko-

betrachtung: Sofern eine enge Kopplung der elektronischen Signatur an das Dokument gegeben ist, ist eine dokumentenbezogene Verarbeitung möglich. Ansonsten entstehen Prozessabhängigkeiten.

8.3 Ablauffristen für elektronische Signaturen

Anmerkung zu Signaturen: am besten nach hinten stellen, weil bezogen auf die Kryptographie Vereinfachungen durch eIDAS zu erwarten sind.

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.

Frage: Ist es zwingend, um die Sicherheit elektronischer Signaturen langfristig aufrechtzuerhalten, eine Signaturerneuerung nach § 17 Signaturverordnung (SigV), durchzuführen?

Risikobetrachtung: 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, das die Übersignierung im Sinne des § 17 SigV gewährleistet.

2.5 Auszug aus „Leitlinie zum ersetzenden Scannen in Kommunen nach TR RESISCAN“2017

4.4.1 Verbleib des Papierguts regeln

Ein weiterer Punkt, der im Rahmen der organisatorischen Scanstrategie zu klären ist, ist die Frage, wie mit den Papieroriginalen zu verfahren ist, nachdem sie gescannt wurden. Diese Frage ist insbesondere relevant, wenn in einer zentralen Poststelle oder von einem externen Dienstleister gescannt wird. Es gibt u.a. die nachfolgenden Varianten:

Fachliche Scanstrategie	Umgang mit Papieroriginalen nach dem Scannen
Ersetzend Scannen	**Zentral:** Werden Dokumente an zentraler Stelle ersetzend gescannt, sind diese für einen definierten Zeitraum (z.B. vier Wochen) weiterhin aufzubewahren. Das eröffnet die Möglichkeit, im Bearbeitungsprozess noch zu einem späteren Zeitpunkt auf die Papieroriginale zuzugreifen. Auslöser kann z.B. ein fehlerhafter Scan oder ein Dokument sein, das nicht ersetzend gescannt werden durfte. Nach Ablauf dieser Aufbewahrungszeit werden die eingescannten Dokumente datenschutzkonform vernichtet. **Dezentral:** Beim Ersetzenden Scannen im Fachbereich werden die Dokumente nach der Digitalisierung durch den Mitarbeiter in das Dokumentenmanagementsystem (DMS) überführt und dann in der Regel sofort vernichtet.
Kopierend Scannen	**Zentral:** Wird an zentraler Stelle kopierend gescannt, werden die Originale an den für den Vorgang verantwortlichen Sachbearbeiter bzw. an die verantwortliche Organisationseinheit weitergeleitet. **Dezentral:** Der Sachbearbeiter entscheidet, ob die Originale dem Absender zurückgegeben, in einer hybriden Akte abgelegt oder vernichtet werden.

Von der zentralen Poststelle nicht gescannte Dokumente gehen an den verantwortlichen Sachbearbeiter bzw. die fachlich verantwortliche Organisationseinheit. Hier wird über das weitere Verfahren (Veraktung, Vernichtung, nachträgliches Scannen) entschieden.

Das vollständige Dokument kann hier abgerufen werden:

https://www.vitako.de/Publikationen/Leitlinie%20zum%20ersetzenden%20Scannen%20in%20Kommunen%20nach%20TR%20RESISCAN.pdf

3 Impressum

KDN Dachverband kommunaler IT-Dienstleister

Kompetenzzentrum Digitalisierung

Mühlenstraße 51

53721 Siegburg

E-Mail: ccdigitalisierung@kdn.de

Telefon: 02241/999-1186