

Dr. Wolfram Viefhues (Hrsg.)

# Elektronischer Rechtsverkehr

**Ausgabe 4:**

Endlich: Das beA ist gestartet!

eBroschüre

# Elektronischer Rechtsverkehr

Endlich: Das beA ist gestartet!

---

Hrsg. von

Aufsicht führender Richter am Amtsgericht Oberhausen a. D.

**Dr. Wolfram Viefhues**

Gelsenkirchen

**Zitiervorschlag:**

*Viefhues*, Elektronischer Rechtsverkehr Ausgabe 4/2016, Rn 1

Copyright 2016 by Deutscher Anwaltverlag, Bonn  
ISBN 80007785

# Endlich: Das beA ist gestartet!

## Inhalt

	Rdn		Rdn
<b>A. Einleitung</b> . . . . .	1	10. Inkrafttreten . . . . .	32
<b>B. Das Elektronische Urkundenarchiv der Notare</b> . . . . .	5	III. Weitere Regelungen des Gesetzentwurfs . . . . .	33
I. Hintergrund . . . . .	5	IV. Ausblick und Fazit . . . . .	34
II. Eckpunkte des Gesetzentwurfs zum Elektronischen Urkundenarchiv . . . . .	10	<b>C. Die Ende-zu-Ende-Verschlüsselung im beA</b>	35
1. Grundsätze der elektronischen Verwahrung . . . . .	11	<b>D. Nachlässigkeit bei der Passwortvergabe.</b>	48
2. Neue Aufgaben für die Notarkammern . . . . .	13	<b>E. Ausgewählte Rechtsprechung zum ERV</b> . . . . .	50
3. Neue Aufgaben für die Bundesnotarkammer . . . . .	15	I. Einfache E-Mail kein Antrag im Sinne des Unterhaltsvorschussgesetzes . . . . .	50
4. Neue Akten und Verzeichnisse für die Notare . . . . .	17	II. Akte muss nicht aus Originaldokumenten bestehen . . . . .	51
a) Elektronische Urkundensammlung . . . . .	18	III. Keine Mitbestimmung bezüglich Dienst-anweisung zum Umgang mit privaten E-Mails. . . . .	52
b) Urkundenverzeichnis . . . . .	19	VI. Keine Wiedereinsetzung in den vorigen Stand bei Fehlen eines Hinweises auf Unzulässigkeit der Klageerhebung per einfacher E-Mail . . . . .	53
c) Verwahrungsverzeichnis . . . . .	21	V. Unvollständigkeit der elektronischen Akte begründet keine Rechtswidrigkeit des angefochtenen Bescheides . . . . .	54
5. Nähere Regelungen über die Aktenführung . . . . .	22		
6. Elektronischer Notaraktenpeicher . . . . .	24		
7. Erstellung der elektronischen Fassung der Urschrift. . . . .	25		
8. Auswirkungen auf die Praxis . . . . .	28		
9. Sicherheitsarchitektur des Elektronischen Urkundenarchivs . . . . .	30		

## A. Einleitung

*Verfasser: Dr. Wolfram Viefhues*

*weitere Aufsicht führender Richter am Amtsgericht a.D.*

Die gute Botschaft zuerst: Das beA ist seit dem 28.11.2016 freigeschaltet.

1

Es ist das glückliche Ende eines Trauerspiels, das viel zu lange gedauert hat und die ganz große Mehrheit der Anwältinnen und Anwälte über Monate daran gehindert hat, das beA zu nutzen, sich mit dem beA praktisch vertraut zu machen und ihre kanzleiinterne Organisation Schritt für Schritt den neuen Techniken und den damit verbundenen Abläufen anzupassen.

Aber wie konnte es dazu kommen? In unserer letzten Ausgabe der eBroschüre ERV (3/2016 vom Oktober) hatte ich sehr nachdrücklich meine Meinung zu der Entscheidung des Anwaltsgerichtshofes (AGH) vom 6.6.2016 sowie zum weiteren Verfahrensablauf geäußert. Dabei hatte ich die Hoffnung zum Ausdruck gebracht, dass der AGH in einer Angelegenheit, die letztlich nur noch marginal die Interessen der beiden Antragsteller des Verfahrens betrifft, nunmehr durch eine zeitnahe Entscheidung auch den schutzwürdigen Interessen der überwiegenden Mehrheit der Anwältinnen und Anwälte Rechnung tragen wird, die freiwillig ihr beA nutzen und den auf jeden Fall kommenden elektronischen Rechtsverkehr mit den Gerichten endlich praktisch üben wollen. Leider hat der zuständige Senat des Anwaltsgerichtshofes nach seiner Entscheidung vom 6.6.2016 nicht umgehend einen Termin zur Verhandlung in der Hauptsache anberaumt. Auch über den von der BRAK gestellten Antrag auf Aufhebung der einstweiligen Anordnung hat der Senat erst nach einer sehr langen Überlegungszeit jetzt entschieden.

Wegen dieser Hängepartie haben wir bei der Vorbereitung dieser Ausgabe darauf verzichtet, weitere konkrete Hinweise zur künftigen Arbeit mit dem beA zu geben. Wir werden dies in den nächsten Ausgaben nachholen, nachdem der AGH jetzt endlich den Weg zur freiwilligen Nutzung des beA für alle Anwältinnen und Anwälte freigemacht hat. Eine Starthilfe für die Anmeldung und Inbetriebnahme des beA mit entsprechenden Schaubildern können Sie jedoch schon der eBroschüre ERV 3/2016 entnehmen. Sofern Sie also über eine beA-Karte verfügen, können Sie Ihr Postfach ab sofort aktivieren und erkunden.

Abseits der juristischen und technischen Anlaufschwierigkeiten des beA gibt es zwischenzeitlich auch positive Entwicklungen im ERV. Wir berichten in der aktuellen Ausgabe in dem Beitrag „Das **Elektronische Urkundenarchiv der Notare**“ über den bereits weit fortgeschrittenen Einsatz der modernen Informationstechnik im Notariat und die schon im Gesetzgebungsverfahren eingeleiteten Bestrebungen, diesen Einsatz weiter auszuweiten. Es zeigt sich an dieser Stelle wieder einmal, dass die Notarinnen und Notare durchaus als „Speerspitze des elektronischen Fortschritts“ bezeichnet werden, die die Chancen der Digitalisierung nicht nur erkannt haben, sondern auch eine sichere und inzwischen bewährte technische Basis entwickelt haben und diese Fortschritte konsequent vorantreiben, anstatt sich in sinnlosen Abwehrkämpfen verschleifen.

2

In der Diskussion über das besondere elektronische Anwaltspostfach wird vielfach über dessen Sicherheit gestritten, wobei sich die schärfsten Kritiker oftmals durch die geringste Sachkenntnis auszeichnen scheinen. Vor allem in den Internetforen der Kritiker des beA ist zu sehen, dass sich die Teilnehmer gerne gegenseitig argumentativ bestätigen, sich sozusagen verbal „auf die Schulter klopfen“. Je heftiger und drastischer eine Behauptung aufgestellt wird, desto weniger muss man sich offenbar um deren Wahrheitsgehalt kümmern. Sachliche Argumente der wenigen Teilnehmer, die sich trauen, eine andere Meinung zu äußern, werden dreist niedergemobbt. Dass man dabei jedes Augenmaß verliert, wird offensichtlich hingegenommen. So werden z.B. allen Ernstes Probleme mit dem beA als Grundlage für Aufrufe genommen,

3

die BRAK gänzlich abzuschaffen. Leider sind auch Anwälte gegen solche Verhaltensweisen nicht gänzlich gefeit.

Zur Versachlichung der Diskussion greifen wir daher im zweiten Beitrag dieser Ausgabe das Thema Sicherheit des beA noch einmal auf. Darin wird das Prinzip der **Ende-zu-Ende-Verschlüsselung** näher erläutert, die einer der Sicherheits-Eckpfeiler des beA ist und die – anders als viele andere praktisch genutzte Kommunikationsformen wie E-Mail und Fax – die Einhaltung der anwaltlichen Verschwiegenheitsverpflichtungen auf technischem Wege tatsächlich sicherstellt.

Ein weiterer Kurzbeitrag befasst sich mit der **Nachlässigkeit bei der Passwortwahl**. Und wie in jeder Ausgabe gibt RA *Kuntz* abschließend einen Überblick über die für den Themenbereich ERV relevante **aktuelle Rechtsprechung**. 4

## B. Das Elektronische Urkundenarchiv der Notare

*Verfasser: Matthias Frohn*

*Notarassessor, Mitglied der Geschäftsführung der Bundesnotarkammer*

### I. Hintergrund

Nach einem Gesetzentwurf der Bundesregierung wird die Bundesnotarkammer ein Elektronisches Urkundenarchiv einrichten, das die sichere Aufbewahrung der notariellen Urkunden für 100 Jahre ermöglicht. 5

Die Notare gehören seit Langem zu den Vorreitern im elektronischen Rechtsverkehr. Seit nunmehr fast zehn Jahren reichen sie **Anmeldungen zum Handelsregister** ausschließlich in elektronischer Form ein. Auch in Grundbuchsachen hat der elektronische Rechtsverkehr inzwischen in mehreren Bundesländern begonnen. In Baden-Württemberg, Sachsen, Schleswig-Holstein und Rheinland-Pfalz werden die **Grundbuchämter** nach und nach für den elektronischen Rechtsverkehr freigeschaltet. Die Notare sind dort verpflichtet, Anträge und weitere erforderliche Unterlagen elektronisch einzureichen und zusätzliche Strukturdaten zu übersenden, die eine automatisierte Datenübernahme durch die Fachverfahren der Justiz ermöglichen. 6

Die für den elektronischen Rechtsverkehr geschaffenen Rechtsgrundlagen ermöglichen es den Notaren, elektronisch beglaubigte Abschriften zu erstellen, die den Anforderungen des Handelsregister- und des Grundbuchverfahrens gerecht werden: Die öffentlichen elektronischen Dokumente stehen in ihren Rechtswirkungen den öffentlichen Urkunden gleich. Das Beurkundungsgesetz sieht dabei sowohl eine Umwandlung von Papierurkunden in die elektronische Form als auch den umgekehrten Weg vor, also die Erstellung von Papierabschriften von elektronischen Dokumenten. Dies verdeutlicht die Rolle der Notare als „Medienbruchstelle der Justiz“: Solange nicht sämtliche Stellen, mit denen die Notare typischerweise im Rahmen der Abwicklung von Amtsgeschäften kommunizieren, elektronische Akten führen und elektronische Dokumente erstellen, kann und wird der Notar die Unterlagen in ihrer jeweiligen Form für die Beteiligten sammeln, ordnen und dann entweder in Papierform oder, ggf. nachdem er sie digitalisiert hat, elektronisch bei den Gerichten einreichen. 7

Die Bundesnotarkammer hat die Notare von Anfang an dabei unterstützt, den von der Justiz gestellten Anforderungen, insbesondere die Erstellung von Strukturdaten, gerecht zu werden. Das von der NotarNet GmbH angebotene **Programm XNotar** wird in der überwiegenden Mehrzahl der Notariate für die Erstellung von elektronischen Anträgen zum Handelsregister und, soweit erforderlich, zum Grundbuch einge- 8

setzt. Die NotarNet GmbH ist eine hundertprozentige Tochtergesellschaft der Bundesnotarkammer. Zudem betreibt die Bundesnotarkammer eine akkreditierte Zertifizierungsstelle nach dem Signaturgesetz und ist auch bereits als **qualifizierter Vertrauensdiensteanbieter** gemäß der eIDAS-Verordnung in die sog. Trusted List der Bundesnetzagentur eingetragen. Das bedeutet, dass die Notare bei der Bundesnotarkammer Signaturkarten für die Erstellung qualifizierter elektronischer Signaturen beziehen können. Über eine Verbindung zum ebenfalls von der Bundesnotarkammer betriebenen **elektronischen Notarverzeichnis** ist sichergestellt, dass nur Notare ein Zertifikat mit einem Amtsträgerattribut erhalten. Da das Signaturzertifikat unverzüglich gesperrt wird, sobald der Inhaber nicht mehr Notar ist, ist gewährleistet, dass nur amtierende Notare öffentliche elektronische Dokumente nach dem Beurkundungsgesetz errichten können. Die Zertifikate werden von der Bundesnotarkammer dauerhaft prüfbar gehalten und sind dadurch auch nach langer Zeit noch für eine Beweisführung in gerichtlichen Verfahren geeignet.

### *Hinweis*

Die Verwendung **qualifizierter elektronischer Signaturen** durch Notare ist inzwischen seit vielen Jahren Alltag. Da auch mehrere Dokumente durch eine PIN-Eingabe signiert werden können, benötigt die elektronische Signatur bei einer entsprechenden Organisation der Arbeitsabläufe im Ergebnis weniger Zeit als eine handschriftliche Unterschrift. Etwaige Befürchtungen in der Justiz und der Anwaltschaft, die qualifizierte elektronische Signatur sei in ihrer Handhabung kompliziert, dürften daher aufgrund der gegenteiligen praktischen Erfahrungen der Notare unbegründet sein.

Die Bundesnotarkammer betreibt schließlich das **Zentrale Vorsorgeregister (seit 2005)** und das **Zentrale Testamentsregister (seit 2012)**. Insofern hat der Gesetzgeber ihr als Registerbehörde staatliche Aufgaben übertragen. Das Vorsorgeregister sorgt dafür, dass Vorsorgevollmachten und Betreuungsverfügungen von den Betreuungsgerichten gefunden und dadurch überflüssige Betreuungen verhindert werden. Im Zentralen Testamentsregister sind die Aufbewahrungsorte sämtlicher amtlich verwahrter erbfolgerrelevanter Urkunden registriert. In jedem von den Standesämtern beurkundeten Sterbefall wird das Zentrale Testamentsregister automatisch benachrichtigt sowie das Nachlassgericht und die Verwahrstelle informiert. Dies hat zu Effizienzsteigerungen und Beschleunigungen in den Nachlassverfahren geführt. Die Gerichte sind über ein speziell gesichertes Netzwerk und das System SAFE (Secure Access to Federated E-Justice) mit den Systemen der Bundesnotarkammer verbunden.

## **II. Eckpunkte des Gesetzentwurfs zum Elektronischen Urkundenarchiv**

Zu diesen vielfältigen Aufgaben der Bundesnotarkammer im elektronischen Rechtsverkehr wird ab dem Jahr 2020 eine weitere hinzutreten: Sie wird als „Urkundenarchivbehörde“ das Elektronische Urkundenarchiv einrichten, in dem jeder Notar die ab einem Stichtag neu errichteten Urkunden in digitalisierter Form verwahren wird. Daneben ist zunächst eine 30-jährige parallele Verwahrung der Papierurkunden, gerechnet ab dem Zeitpunkt der Digitalisierung, vorgesehen. Dieser Zeitraum kann bei erfolgreichem Betrieb des Elektronischen Urkundenarchivs zu gegebener Zeit verkürzt werden. Der Gesetzentwurf wurde von einer Bund-Länder-Arbeitsgruppe unter Beteiligung der Bundesnotarkammer erarbeitet und im Oktober 2016 vom Bundeskabinett beschlossen. Eine Verabschiedung des Gesetzes noch in der laufenden Legislaturperiode ist geplant.

### **1. Grundsätze der elektronischen Verwahrung**

Der Gesetzentwurf enthält umfangreiche Änderungen der Bundesnotarordnung und des Beurkundungsgesetzes. Die Bundesnotarkammer wird durch die Neuregelungen nicht selbst zur Verwahrstelle von Urkunden, sondern stellt lediglich die Infrastruktur für die Verwahrung zur Verfügung. Jeder Notar wird in

Zukunft jede ab einem Stichtag errichtete Urkunde digitalisieren und in „seiner“ elektronischen Urkundensammlung, die im Elektronischen Urkundenarchiv bei der Bundesnotarkammer geführt wird und individuell verschlüsselt ist, verwahren. Darüber hinaus können die Notare wahlweise die alten Urkunden nachdigitalisieren. Das Gleiche gilt auch für die Amtsgerichte und die zukünftig ebenfalls Urkunden verwahrenden Notarkammern.

#### *Hinweis*

Das im elektronischen Urkundenarchiv gespeicherte Dokument wird per Legaldefinition zur „elektronischen Fassung der Urschrift“. **Notarielle Urkunden** können somit **medienbruchfrei im elektronischen Rechtsverkehr** verwendet werden.

Die elektronischen Fassungen eignen sich darüber hinaus zukünftig ganz allgemein zum **Nachweis gegenüber Gerichten, Ämtern, Banken** und anderen Stellen, die die Echtheit und Unversehrtheit des Dokuments aufgrund der elektronischen Signatur des Notars überprüfen können. Diese Stellen müssen dann ihrerseits keine Papierurkunden mehr archivieren und können notarielle Dokumente in elektronischen Aktensystemen weiterverarbeiten, ohne diese erst einscannen zu müssen. **12**

## 2. Neue Aufgaben für die Notarkammern

Den Notarkammern wird nach dem Gesetzentwurf ab dem Jahr 2022 die Aufgabe zugewiesen, die **Akten und Verzeichnisse ausgeschiedener Notare** zu übernehmen, sofern die Landesjustizverwaltung die Verwahrung nicht einem Notar überträgt. Die Notarkammern treten damit hinsichtlich der Verwahrung an die Stelle der Amtsgerichte. Von der Möglichkeit der Übertragung der Verwahrung auf einen Notar wird heute regional in sehr unterschiedlichem Umfang Gebrauch gemacht. Im hauptberuflichen Notariat ist die Verwahrung durch den sog. „Amtsnachfolger“ die Regel. Hieran soll sich durch den Gesetzentwurf nichts ändern. **13**

Aber auch **im Anwaltsnotariat** werden die Urkunden keinesfalls überall durch die Amtsgerichte – und damit zukünftig durch die Notarkammern – verwahrt, sondern teilweise ebenfalls durch Notare, z.B. solche, die mit dem ausgeschiedenen Notar in Sozietät verbunden waren oder in der anwaltlichen Tätigkeit weiter verbunden sind. Für die neue Aufgabe müssen die Notarkammern geeignete Räumlichkeiten und Strukturen für die Aufbewahrung der Papierurkunden und einen Zugang zum Elektronischen Urkundenarchiv einrichten. **14**

## 3. Neue Aufgaben für die Bundesnotarkammer

Die Bundesnotarkammer ist zukünftig „**Urkundenarchivbehörde**“. Dadurch wird sie aber nicht zur Verwahrstelle der Notarurkunden. Die neue Aufgabe verpflichtet sie vielmehr lediglich zur Bereitstellung der technischen Infrastruktur für die eigentlichen Verwahrstellen, nämlich insbesondere die Notare und die Notarkammern. Das Elektronische Urkundenarchiv wird ein zentrales elektronisches Archiv sein, in dem die Notare ihre elektronische Urkundensammlung, ihr Urkundenverzeichnis und ihr Verwahrungsverzeichnis führen. **15**

Die Bundesnotarkammer wird darüber hinaus nach dem Gesetzentwurf auch einen **Elektronischen Notaraktenpeicher** betreiben. Der Elektronische Notaraktenpeicher stellt im Gegensatz zum Urkundenarchiv ein optionales Angebot an die Notare bzw. Notarkammern dar und wird daher von der Bundesnotarkammer nicht als Behörde, sondern in ihrer Funktion als Selbstverwaltungskörperschaft eingerichtet. **16**

#### 4. Neue Akten und Verzeichnisse für die Notare

Im Elektronischen Urkundenarchiv wird künftig jeder Notar verbindlich die **elektronische Urkundensammlung**, das **Urkundenverzeichnis** und das **Verwahrungsverzeichnis** führen. Zusätzlich ermöglicht der Gesetzentwurf es den Notaren erstmals, für die Bearbeitung ihrer Vorgänge **elektronische Akten** zu führen. Die hierbei einzuhaltenden Standards wird das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) noch durch eine Rechtsverordnung festlegen. Es wird also das bisher in der Dienstordnung verankerte Prinzip aufgegeben, wonach sämtliche Akten zwingend in Papierform zu führen sind und die Elektronik dafür lediglich ein „Hilfsmittel“ darstellt. Stattdessen wird in Zukunft differenziert, es gibt dann **drei Arten von Akten und Verzeichnissen**: Nämlich solche, die ausschließlich in Papier zu führen sind (das sind die Urschriften), solche, die ausschließlich elektronisch geführt werden (das sind die elektronische Urkundensammlung und die beiden genannten Verzeichnisse) und solche, bei denen der Notar die Wahl hat, ob er sie (ganz oder teilweise) in Papier oder elektronisch führt (das sind die übrigen Akten, insbesondere die Nebenakten).

17

##### a) Elektronische Urkundensammlung

Die Bedeutung der elektronischen Urkundensammlung erschließt sich von selbst: Sie wird das Pendant zur Urkundensammlung sein, in der die elektronischen Fassungen der Urschriften verwahrt werden. Hier-von ausgenommen sind nur Verfügungen von Todes wegen, bei denen aufgrund der Besonderheiten des Nachlassverfahrens weiter allein die Papierfassung maßgeblich bleibt und von denen statt einer elektronischen Fassung der Urschrift eine elektronisch beglaubigte Abschrift in der elektronischen Urkundensammlung aufbewahrt wird.

18

##### b) Urkundenverzeichnis

Das Urkundenverzeichnis wird im Beurkundungsgesetz künftig legal definiert. Es **ersetzt** die **Urkundenrolle**, stellt also gewissermaßen das Inhaltsverzeichnis der elektronischen Urkundensammlung dar. Weil man ein elektronisches Verzeichnis ganz einfach nach unterschiedlichen Kriterien durchsuchen kann, ersetzt es gleichzeitig auch das **Namensverzeichnis zur Urkundenrolle**. Durchsucht werden kann dieses Verzeichnis ausschließlich von der zuständigen Verwahrstelle, also in der Regel vom Notar und seinen Mitarbeitern bzw. den Mitarbeitern der verwahrenden Notarkammer. Die Daten sind so verschlüsselt, dass eine Suche durch die Urkundenarchivbehörde und ihre Mitarbeiter nicht ohne die Mitwirkung der verwahrenden Stelle möglich ist.

19

##### *Hinweis*

Vom Urkundenverzeichnis wird es **keine Papierversion** geben, es existiert ausschließlich elektronisch.

Im Urkundenverzeichnis werden künftig auch wichtige Informationen zur Urkunde eingetragen, die heute auf der Urschrift zu vermerken sind, so etwa, wem und an welchem Tag eine **Ausfertigung der Urkunde** erteilt wurde. Diese Eintragungen könnten zukünftig möglicherweise auch das Problem der fehlenden elektronischen Ausfertigung lösen. Da sich „Original“ und „Kopie“ bei elektronischen Dokumenten nicht unterscheiden, sind Ausfertigungen, die gerade aufgrund ihrer körperlichen Einmaligkeit mit bestimmten Legitimationswirkungen ausgestattet sind, nicht möglich. Ein zentrales Verzeichnis über die erteilten Ausfertigungen und deren Status könnte dieses Problem lösen.

20

##### *Hinweis*

Im Hinblick auf **vollstreckbare Ausfertigungen** wäre ein solches Verzeichnis ein „Titelregister“, das auch vollständig elektronische Zwangsvollstreckungsverfahren ermöglichen würde.

**c) Verwahrungsverzeichnis**

Ebenfalls im Beurkundungsgesetz legal definiert wird das Verwahrungsverzeichnis. Es **ersetzt die Masse- und Verwahrungsbücher** und die dazu gehörigen Namensverzeichnisse, betrifft also vor allem die Notaranderkonten. Lesen können das Verzeichnis grundsätzlich ebenfalls nur der Notar und seine Mitarbeiter. Vom Verwahrungsverzeichnis wird es ebenfalls keine Papierversion geben, es existiert wie das Urkundenverzeichnis **ausschließlich elektronisch**.

21

**5. Nähere Regelungen über die Aktenführung**

Über die elektronische Urkundensammlung, das Urkundenverzeichnis und das Verwahrungsverzeichnis hinaus enthält der Gesetzentwurf keine Definition von Akten und Verzeichnissen. Hierfür ist vielmehr eine Rechtsverordnung vorgesehen, in der auch die Einzelheiten über die Art und Weise der Aktenführung zu regeln sind. Die Verordnungsermächtigung legt als Maßstäbe die Verfügbarkeit, Transparenz, Integrität und Vertraulichkeit der Akten und Verzeichnisse fest. Darüber hinaus können Regelungen zu den erlaubten Datenformaten getroffen und die Rahmenbedingungen über den Inhalt der Akten und die Aufbewahrungsfristen festgelegt werden.

22

Auch hier wird sich also Grundsätzliches ändern: Ein großer Teil der heute in der Dienstordnung enthaltenen Vorschriften wird in dieser Rechtsverordnung aufgehen und die Dienstordnung insoweit ablösen. Daher hat die Justizministerkonferenz die bestehende Bund-Länder-Arbeitsgruppe, die den Gesetzentwurf erstellt hat, bereits mit der Erarbeitung eines Entwurfs dieser Rechtsverordnung beauftragt. Ausgangspunkt für die Regelungen in der Rechtsverordnung werden sicher die bewährten Inhalte der DONot sein. Gleichzeitig wird es aber erforderlich sein, diese Inhalte ihrem Regelungszweck entsprechend auf die elektronische oder hybride Aktenführung zu übertragen. Das ist eine spannende und herausfordernde Aufgabe, der sich derzeit auch die Justiz bei ihren Überlegungen zur Einführung der elektronischen Gerichtsakte stellen muss. Die Bundesnotarkammer steht in einem engen Austausch mit den Arbeitsgruppen der Justiz, um so die jeweiligen Überlegungen gegenseitig nutzbar zu machen und bestehende Gemeinsamkeiten, aber natürlich auch Unterschiede, herauszuarbeiten.

23

**6. Elektronischer Notaraktenspeicher**

Da notarielle Akten amtliche Unterlagen sind, die stets in der Verfügungsgewalt des Notars bleiben müssen, trifft der Gesetzentwurf auch eine Regelung zum Speicherort der elektronischen Akten. Die Idee hinter dem Elektronischen Notaraktenspeicher ist, dass die Sicherheit des Elektronischen Urkundenarchivs auch für eine zentrale elektronische **Nebenaktenführung** genutzt werden kann. Der Notar kann seine elektronischen Nebenakten aber auch auf lokalen Servern in der Geschäftsstelle führen. Zu einer Nutzung des Elektronischen Notaraktenspeichers ist er nicht verpflichtet. Die Akten müssen in beiden Fällen jederzeit für eine Prüfung durch die Aufsichtsbehörden zugänglich sein. Hierfür muss der Notar dem Prüfer ggf. einen Arbeitsplatz zur Verfügung stellen und ihm die erforderlichen Einblicke in die Akten und Verzeichnisse ermöglichen.

24

**7. Erstellung der elektronischen Fassung der Urschrift**

Künftig wird es eine „elektronische Fassung der Urschrift“ geben. Die Einzelheiten zur Erstellung der elektronischen Fassung der Urschrift werden im Beurkundungsgesetz geregelt sein. Denn das in der elektronischen Urkundensammlung hinterlegte elektronische Dokument wird rechtlich der Urschrift gleichgestellt. Um diese Gleichstellung zu rechtfertigen, bedarf es verfahrensrechtlicher Vorgaben für die Überführung der Papierurschrift in die elektronische Form. Insbesondere ist die **bildliche und inhaltliche**

25

**Übereinstimmung der Urschrift mit ihrer elektronischen Fassung** zu gewährleisten. Die Umwandlung eines elektronischen Dokuments, z.B. der Textdatei des Urkundenentwurfs, in ein für die langfristige Archivierung geeignetes Format (PDF/A) reicht also nicht aus. Vielmehr muss die bildliche Übereinstimmung, z.B. mit den bei der Beurkundung handschriftlich eingefügten Vermerken des Notars und den Unterschriften der Beteiligten und des Notars, feststehen. Das Dokument ist also einzuscannen. Dies schließt die zusätzliche Hinterlegung auch einer elektronischen Reinschrift als Lesefassung im Elektronischen Urkundenarchiv nicht aus.

Um unbemerkte Veränderungen durch die beim **Scannen** eingesetzten Geräte oder andere Sicherheitslücken möglichst auszuschließen, wird das Gesetz anordnen, dass die Übertragung „nach dem Stand der Technik“ erfolgen soll. Die Bundesnotarkammer arbeitet bereits daran, in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Musterscanprozess zu entwickeln und geeignete Scanner, möglicherweise in Verbindung mit einer speziellen Software, für das Verfahren zu ermitteln. Sie wird sich dabei an der Technischen Richtlinie RESISCAN des BSI orientieren, die Empfehlungen für die rechtssichere Übertragung von Papierdokumenten in die elektronische Form enthält. 26

Nach dem Scannen der Urschrift, das in der Regel von den Mitarbeitern des Notars vorgenommen werden wird, hat der Notar persönlich die bildliche und inhaltliche Übereinstimmung der Urschrift mit ihrer elektronischen Fassung in einem elektronischen Vermerk zu bestätigen. Das Dokument und die **Bestätigung sind mit einer qualifizierten elektronischen Signatur des Notars** zu versehen. Im Moment der Speicherung des Dokuments in der elektronischen Urkundensammlung entsteht die elektronische Fassung der Urschrift. Ab diesem Zeitpunkt kann die elektronische Fassung der Urschrift auch verwendet werden, um Ausfertigungen und Abschriften in Papierform zu erteilen. 27

#### *Hinweis*

Im elektronischen Rechtsverkehr (beispielsweise mit den Handelsregistern und Grundbuchämtern) reicht es hingegen aus, eine Kopie der elektronischen Fassung der Urschrift zu versenden. Denn diese hat aufgrund des Übereinstimmungsvermerks automatisch auch die rechtliche Qualität einer elektronisch beglaubigten Abschrift.

## 8. Auswirkungen auf die Praxis

Das Elektronische Urkundenarchiv wird spürbare **Veränderungen für die praktischen Abläufe** an jeder einzelnen Notarstelle mit sich bringen. Zukünftig müssen alle Urkunden digitalisiert werden und verbindliche Eintragungen in elektronische Verzeichnisse vorgenommen werden. Bei den Nebenakten wird der Notar wählen können, ob er weiterhin auf die Papieraktenführung setzt oder ganz oder teilweise auf eine elektronische Aktenführung umstellt. Möglich sein wird insofern insbesondere auch eine „hybride“ **Aktenführung** aus Papier und Elektronik. 28

Auch für die Softwarehäuser bedeutet dies neue Herausforderungen, denn das, was bislang nach der Dienstordnung lediglich ein „Hilfsmittel“ für die verbindlich auszudruckende Papierakte darstellt, kann zukünftig die „echte“ elektronische Akte werden. Auch mit den Herstellern von **Notarsoftware** steht die Bundesnotarkammer deshalb in engem Austausch und wird diesen in den kommenden Jahren während der Realisierung des Elektronischen Urkundenarchivs und des Elektronischen Notaraktenspeichers noch weiter intensivieren. 29

#### *Hinweis*

Im Gegensatz zu den Gerichtsakten, die von der „Medienbruchfunktion“ des Notars profitieren, werden die notariellen Akten voraussichtlich zunächst weiterhin teilweise aus Papier und teilweise aus elektronischen Dokumenten bestehen.

## 9. Sicherheitsarchitektur des Elektronischen Urkundenarchivs

Das Elektronische Urkundenarchiv wird sich von den Rechenzentren der Bundesnotarkammer bis in das Notarbüro erstrecken. Den lokalen Eintrittspunkt wird die **sog. Archivbox** darstellen, die in jedem Notarbüro, ähnlich den heutigen Registerboxen, aufgestellt werden wird. Die Archivbox wird einen zentralen Bestandteil der Sicherheitsarchitektur des Elektronischen Urkundenarchivs darstellen, da sie das **Elektronische Urkundenarchiv vom Internet abschirmt**. Zudem werden bestimmte kryptographische Funktionen über die Boxen ausgeführt. Diese Verschlüsselungsfunktionen werden zur Erstellung der elektronischen Fassung der Urschrift benötigt. Sie dienen der Datensicherheit und der Erhaltung des Beweiswerts der Dokumente.

30

Es muss technisch und organisatorisch sichergestellt sein, dass nur der jeweilige Notar und die von ihm hierzu berechtigten weiteren Personen Zugriff auf die Akten und Verzeichnisse haben. Dies kann durch entsprechende sichere **Verschlüsselungsverfahren** erreicht werden. In diesem wichtigen Punkt arbeitet die Bundesnotarkammer eng mit Sicherheitsexperten zusammen und wird sich bei der technischen Umsetzung des Projekts auch von externen Fachleuten beraten lassen. Das BMJV wird im Wege einer Rechtsverordnung die Leitlinien für die technische Umsetzung vorgeben.

31

Trotz der erforderlichen aufwändigen individuellen Verschlüsselung muss aber auch jede nachfolgende Verwahrstelle in die Lage versetzt werden können, die ihr zur Verwahrung übertragenen Unterlagen im Elektronischen Urkundenarchiv finden und lesen zu können. Dies muss umgesetzt werden, ohne dass es einen Generalschlüssel gibt, der es z.B. der Urkundenarchivbehörde ermöglichen würde, ebenfalls „mitzulesen“. Einen solchen Generalschlüssel darf und wird es nicht geben. Daher werden die **Schlüssel für die einzelnen sog. Archivräume der Notare** von der jeweils zuständigen Notarkammer verwaltet und von dieser in jedem einzelnen Fall im Mehraugenprinzip für die jeweils neu zu berechtigende Stelle freigeschaltet. Auch für die Notarkammern besteht dabei keine Einsichtsmöglichkeit, soweit sie nicht selbst Verwahrstelle der Unterlagen werden.

Das Gleiche gilt auch für den einzelnen Notar als Verwahrstelle: Sobald ihm von der Notarkammer die Berechtigung zum Zugriff auf einen oder mehrere Archivräume erteilt wurde, kann er „Unterberechtigungen“ für seine Mitarbeiter vergeben. Diese leiten sich immer von der Berechtigung des Notars ab und erlöschen auch mit dieser wieder.

## 10. Inkrafttreten

Der Gesetzentwurf sieht eine **gestaffelte Einführung** des Elektronischen Urkundenarchivs vor. Die Führung des Urkundenverzeichnisses und des Verwahrungsverzeichnisses soll mit dem 1.1.2020 zeitlich bereits vor der Führung der elektronischen Urkundensammlung beginnen. Diese wird dann ab dem 1.1.2022 verpflichtend. Dies soll eine reibungslose Einführung des gesamten Elektronischen Urkundenarchivs erleichtern.

32

Die zeitliche Staffelung bietet zudem den Notaren und ihren Mitarbeitern die Möglichkeit, sich an die Führung originär elektronischer Verzeichnisse zu gewöhnen, ohne bereits eine elektronische Urkundensammlung führen zu müssen. Der Übergangszeitraum ermöglicht schließlich insbesondere auch die Ausstattung der Notarstellen mit den erforderlichen technisch geeigneten Scannern, soweit solche noch nicht vorhanden sind, und die notwendigen Schulungen. Neuanschaffungen von Scannern sollten Notare zunächst soweit möglich zurückstellen, bis klar ist, welche Anforderungen an die Scanner für das Elektronische Urkundenarchiv gestellt werden.

### III. Weitere Regelungen des Gesetzentwurfs

Der Gesetzentwurf enthält neben den Vorschriften zum Elektronischen Urkundenarchiv auch eine Regelung zum besonderen elektronischen Notarpostfach und zum Notarverzeichnis. 33

#### *Hinweis*

Angelehnt an die Vorschriften zum „beA“ wird die Bundesnotarkammer zum 1.1.2018 für jeden Notar ein **besonderes elektronisches Notarpostfach („beN“)** einrichten. Technisch ist dies im Grundsatz bereits geschehen, und zwar dadurch, dass die Bundesnotarkammer die EGVP-Postfächer der Notare auf einen eigenen Intermediär „migriert“ und dabei jedem Postfach eine eindeutige Nummer (SAFE-ID mit der Kennung „ben“) zugeteilt hat.

Die Nummer des Postfachs wird im Notarverzeichnis beim jeweiligen Notar vermerkt, sodass die Gerichte über das Verzeichnis das eindeutige beN eines jeden Notars ermitteln und Nachrichten in das Postfach zustellen können. Aufgrund des Gesetzes wird das beN nunmehr in den Kreis der „sicheren Übermittlungswege“ nach den Verfahrensordnungen (z.B. § 130a ZPO in der ab 1.1.2018 geltenden Fassung) aufgenommen.

### IV. Ausblick und Fazit

Das Elektronische Urkundenarchiv bietet Strukturen und Ordnung bei der elektronischen Organisation der Arbeitsabläufe im Notariat und kann insbesondere durch die Einbindung des Programms XNotar und der jeweiligen Notarsoftware zu einer weiteren Effizienzsteigerung im elektronischen Rechtsverkehr beitragen. Denkbar ist auch eine Verknüpfung der elektronischen Aktensysteme der Justiz mit dem Elektronischen Urkundenarchiv, die insbesondere für das Handelsregister und das Grundbuch, in denen Dokumente dauerhaft aufzubewahren sind, Effizienz- und Kostenvorteile mit sich bringen kann. Eine Über-sendung von Dokumenten an die Gerichte könnte entbehrlich sein, wenn der Notar stattdessen einen Link auf das im Elektronischen Urkundenarchiv beweiswerterhaltend gespeicherte Dokument verschickt. 34

Das Elektronische Urkundenarchiv schafft die strukturellen Voraussetzungen, damit der einzelne Notar seine Rolle als Teil der Justiz und der vorsorgenden Rechtspflege auch in der digitalen Welt weiterhin effizient und umfassend wahrnehmen kann.

## C. Die Ende-zu-Ende-Verschlüsselung im beA

*Verfasser: Dr. Wolfram Viefhues*

*weitere Aufsicht führender Richter am Amtsgericht a.D.*

Die Frage der Sicherheit der elektronisch übertragenen Dokumente und der Schutz gegen unbefugte Einsichtnahme werden – zu Recht – im Hinblick auf die anwaltlichen Verpflichtungen zur Verschwiegenheit beim elektronischen Rechtsverkehr besonders intensiv diskutiert. Dabei fällt allerdings auf, dass der elektronischen Kommunikation auch hier mit oft nur sehr pauschalen Vorwürfen Unsicherheiten und Risiken unterstellt werden, ohne die technischen Gegebenheiten überhaupt zur Kenntnis zu nehmen. Daher soll die Gelegenheit genutzt werden, die Einzelheiten der sicheren sog. **Ende-zu-Ende-Verschlüsselung im besonderen elektronischen Anwaltspostfach beA** näher darzustellen. 35

Bei herkömmlicher Kommunikation durch Papier und Postversand erfolgt der Schutz gegen unbefugte Einsichtnahme dadurch, dass der Brief in einem verschlossenen Umschlag transportiert wird. Hier soll 36

nicht weiter thematisiert werden, wie wirksam ein solcher Schutz tatsächlich ist, da ein Umschlag ohne große Probleme, und oft auch ohne Spuren zu hinterlassen, leicht geöffnet werden kann, so dass das darin abgelegte Schriftstück keinesfalls wirksam davon geschützt ist, von Unbefugten gelesen zu werden.

Genauso problematisch sind in diesem Zusammenhang auch offene Gerichtspostfächer, auf deren Inhalt eine größere Zahl von Personen ungehindert und meist auch unbemerkt Zugriff haben kann.

In der elektronischen Welt kann ein sehr wirksamer Schutz gegen unbefugte Einsichtnahme durch **elektronische Verschlüsselung** erreicht werden. Eine solche elektronische Verschlüsselung kann dadurch erfolgen, dass **jedes einzelne Dokument verschlüsselt** wird. Einen recht einfachen Schutz kann man z.B. auch schon in dem Textverarbeitungsprogramm Word realisieren, indem man das Dokument beim Speichern mit einem Passwort versieht. Damit ist das elektronische Dokument bei der Übertragung vor unbefugter Lektüre geschützt. Allerdings kann das Dokument dann auch vom Empfänger nur geöffnet werden, wenn er das Passwort kennt und eingibt. Auch eine andere Person, die das Dokument irgendwie in ihre Verfügung bekommt, kann das Dokument nicht einsehen, da ihr das Passwort ja nicht bekannt ist. (Wie sicher ein solch einfacher Schutz durch ein Word-Passwort gegen Angriffe durch professionelle Hacker ist, soll hier nicht diskutiert werden).

37

Problematisch ist allerdings, dass der Empfänger eben dieses Passwort zur Kenntnis bekommen muss, damit er das Dokument öffnen und den Text lesen kann. Möglich ist dies z.B., indem man auf gesondertem Weg das Passwort übermittelt oder vorher mit bestimmten Kommunikationspartnern bestimmte, ggf. zeitlich geltende Passwörter vereinbart. Vergleichbar ist dies mit dem aus dem Online-Banking bekannten Verfahren, für eine erfolgte Transaktion eine Kontrollziffer – die iTan – auf einem anderen Wege, nämlich über das Handy, zu übermitteln, um Missbrauch zu verhindern. Eine andere Möglichkeit ist das früher übliche Verfahren, dem Kunden eine durchnummerierte Liste mit Tan-Zahlen zur Verfügung zu stellen, aus der er dann nach Anforderung durch die Bank eine Tan mit einer bestimmten laufenden Nummer heraussuchen musste. Nur wer diese Tan (Kontrollziffer) kennt, kann also die Transaktion abschließen.

38

Der Vorgang der Verschlüsselung eines einzelnen Dokumentes kann auch mit bestimmten, am Markt verfügbaren Verschlüsselungsprogrammen durchgeführt werden. Ein solches Verfahren, bei dem man jedes einzelne Dokument mit einem Passwort verschlüsselt, ist daher bei gelegentlicher elektronischer Kommunikation in der Praxis sicherlich einsetzbar.

39

Im anwaltlichen und gerichtlichen Alltag erfolgt jedoch die **Kommunikation im Massenbetrieb**. Dabei zeigt sich sehr schnell, dass durch die Verschlüsselung eines jeden einzelnen Dokumentes erheblicher Zusatzaufwand ausgelöst wird: Die Passwörter müssen bei der Verschlüsselung eingegeben und auf einem gesonderten Weg an den Kommunikationspartner übermittelt werden. Außerdem müssen die Passwörter intern verwaltet werden, um die verschickten Dokumente selbst noch einmal lesen zu können. Denn selbst der Absender kann sein verschlüsseltes Dokument nicht mehr öffnen, wenn er das Passwort vergessen hat.

An dieser Stelle ist ein Hinweis zur **elektronischen Signatur** erforderlich, da hier gedanklich vielfach eine Verwechslung bzw. Vermischung zwischen Signatur und Verschlüsselung erfolgt. Die – personenbezogene – **qualifizierte elektronische Signatur** ist ein elektronischer Unterschriftenersatz, der nachvollziehbar macht, dass dieses konkrete Dokument von dem Aussteller – dem Inhaber der Signaturkarte – elektronisch „unterschrieben“ worden ist. Rechtliche Folge ist, dass dieser Signierende sich den Inhalt des signierten Dokumentes entgegenhalten lassen muss – wie bei einer Unterschrift unter einem Papierdokument.

40

*Hinweis*

Auch nach dem Anbringen dieser qualifizierten elektronischen Signatur bleibt das Dokument weiterhin uneingeschränkt lesbar; es erfolgt **keine Verschlüsselung!**

Technisch wird das Dokument beim Signieren lediglich mit einer Art Kontrollzahl – dem sog. „**Hashwert**“ – versehen. Wird das Dokument inhaltlich verändert, kann man durch eine Prüfprozedur feststellen, dass der dann gebildete Hashwert (die Kontrollzahl) nicht mehr mit dem ursprünglichen Inhalt übereinstimmt. Ebenso wird bei einer Signaturprüfung überprüft, ob die Signatur des Inhabers der Signaturkarte noch gültig ist.

41

*Hinweis*

Die Signatur schützt also nicht unmittelbar vor inhaltlichen Veränderungen, sondern macht es nur möglich, durch eine Signaturprüfung eine Veränderung festzustellen. Nicht festgestellt werden kann dabei, welcher Art die Veränderung war.

So führt z.B. die schlichte Korrektur eines Kommafehlers in einem qualifiziert signierten Dokument dazu, dass die Signaturprüfung einen Fehler meldet und das Dokument damit aus rechtlicher Sicht „wertlos“ geworden ist.

Man kann sich das bildlich etwa so vorstellen, dass ein **gedruckter Brief** zum Transport in eine **Klarsichthülle eingeschweißt** wird. Ist diese Klarsichthülle unbeschädigt, lässt dies den Schluss zu, dass ist auch das darin eingeschweißte Dokument unverändert übertragen worden ist. Das Dokument ist aber durch die Klarsichthülle jederzeit uneingeschränkt lesbar. Damit ist also keinerlei Verschlüsselung gegeben. Eine solche Verschlüsselung, die den Blick auf den Inhalt des Dokumentes verwehrt, müsste also bei jedem Dokument immer zusätzlich zur qualifizierten elektronischen Signatur erfolgen, um den anwaltlichen Verschwiegenheitspflichten in ausreichendem Maße zu genügen.

Das besondere elektronische Anwaltspostfach beA bietet dagegen eine sog. **Ende-zu-Ende-Verschlüsselung**, die ohne jeden Zusatzaufwand **vollautomatisch** eine durchgehende Verschlüsselung vom Absender bis hin zum Empfänger sicherstellt. Hierfür wird eine Technik nach dem sog. OSCI-Standard verwendet. Während die zuvor geschilderten Verschlüsselungsarten die Verschlüsselung eines jeden einzelnen Dokumentes durch den Anwender selbst verlangen, bietet das beA eine Art „Leitungsver Schlüsselung“ an. Jedes Dokument, das vom Absender in seinem Machtbereich in das beA gegeben wird, wird automatisch hier noch verschlüsselt und dann durch eine durchgängig geschützte Leitung bis hin in den Machtbereich des Empfängers verschlüsselt übertragen und dort erst für den Empfänger automatisch entschlüsselt.

42

*Hinweis*

Weder der Absender noch der Empfänger müssen hier Hand anlegen und sich selbst um Verschlüsselung oder Entschlüsselung kümmern.

Die hierfür verwendete Technik nach dem sog. **OSCI-Standard** kann man sich vereinfachend mit einem **doppelten Briefumschlag** veranschaulichen. Das Dokument wird automatisch verschlüsselt, also bildlich gesprochen in einem Briefumschlag sicher verschlossen. Dieser Briefumschlag wird in einen zweiten verschlossenen Briefumschlag gelegt, in dem nur die Daten von Absender und Empfänger enthalten sind. Diese Informationen werden benötigt, um den elektronischen Transportweg vom Absender zum Empfänger zu steuern. Nur dieser Umschlag wird auf dem Transport von den Stellen, die den elektronischen Transport abwickeln, geöffnet. Der innere Umschlag aber mit dem Dokument selbst bleibt während des gesamten Transportweges verschlossen – also sicher verschlüsselt und von niemandem einsehbar.

43

Damit unterscheidet sich das beA auch deutlich von dem heute noch gängigen Kommunikationsmittel des **Fax**. Denn dort werden die Informationen völlig offen ohne jegliche Verschlüsselung durch die Leitung übertragen. Das Argument, es sei kaum möglich, ein einzelnes Fax gezielt aus dem Strom der täglich übertragenen Faxesendungen herauszuholen, ist sicherlich richtig, geht aber an der Kernfrage vorbei. Denn schon ein schlichter Zahlendreher in der Fax-Nummer des Empfängers führt schon mal dazu, dass eine hoch brisante Anklageschrift aus dem Büro des Strafverteidigers nicht beim Beschuldigten landet, sondern bei einem Pizza-Bäcker, der sich dann damit mit einer riesigen Schlagzeile in der Bild-Zeitung ablichten lässt. So geschehen im Jahre 2010 mit der von seinem Verteidiger per Fax verschickten Anklageschrift wegen Drogenmissbrauchs gegen einen namhaften Fernsehmoderator. Erstaunlich war damals, dass hier weder die Anwaltskammer noch der sonst immer sehr aktive Datenschützer tätig geworden ist. Wenn es dagegen nicht um Kommunikation mittels Fax, sondern um „echte“ elektronische Kommunikation geht, muss man damit rechnen, dass regelmäßig eine weitaus höhere Sensibilität und ein deutlich größeres Misstrauen an den Tag gelegt werden. **44**

Zweifel an der Einhaltung der anwaltlichen Verschwiegenheitspflicht gelten auch für die **einfache E-Mail**, die ebenfalls als praktikabler elektronischer Kommunikationsweg in den Anwaltsalltag weitgehend Einzug gehalten hat. Ob die gängige Argumentation, es reiche aus, dass der Mandant sich mit dieser Kommunikationsform einverstanden erklärt hat, tatsächlich greift, mag offenbleiben. Man denke hier auch daran, dass jedenfalls der Verfahrensgegner, dessen Daten auch in vielen Schriftsätzen enthalten sind, die per E-Mail übertragen werden, dieser Art der Kommunikation nicht zugestimmt hat. Auch diesen kritischen Bereich haben die sonst so aktiven Verfechter des Datenschutzes allerdings bislang noch ignoriert. **45**

Soweit in der Diskussion als Alternative zum beA auf den elektronischen Transport über **DE-Mail** verwiesen wird, ist jedenfalls festzuhalten, dass sich sowohl die Bundesrechtsanwaltskammer (BRAK) als auch der Deutsche Anwaltverein (DAV) gegen diesen Weg ausgesprochen haben, weil die anwaltliche Verschwiegenheitspflicht dabei nicht gewahrt werde. Denn anders als beim beA ist bei DE-Mail – jedenfalls ohne Zusatzprogramm – eben keine Ende-Zu-Ende-Verschlüsselung gewährleistet. Vielmehr wird auf dem Transportweg das Dokument selbst vom DE-Mail-Provider entschlüsselt und wieder verschlüsselt. **46**

**Fazit:** Das beA bietet ohne jeden Zusatzaufwand den Komfort einer echten Ende-zu-Ende-Verschlüsselung mit der damit verbundenen Sicherheit. Wer sich gegen das beA wehrt, verkennt also einen entscheidenden Vorteil, den diese Ende-zu-Ende Verschlüsselung gegenüber anderen Systemen bietet. Wer dann auch noch in Unkenntnis oder bewusster Verkenntnis der Sachlage Sicherheitsaspekte als Grundlage für seine Abwehrhaltung gegen das beA vorbringt, macht sich gänzlich unglaubwürdig. **47**

## D. Nachlässigkeit bei der Passwortvergabe

*Verfasser: Dr. Wolfram Viefhues*

*weitere Aufsicht führender Richter am Amtsgericht a.D.*

Nach einer repräsentativen Untersuchung des Branchenverbandes Bitkom verwendet mehr als ein Drittel aller Internetnutzer in Deutschland ein- und dasselbe Passwort für mehrere Online-Zugänge. Nach dem Ergebnis der Umfrage nutzen rund 50 % der Teilnehmer der Befragung zwischen 1 bis 10 verschiedenen Online-Diensten, die einen Login mit Benutzernamen und Passwort erfordern. Ein Drittel der Befragten **48**

benutzt sogar 11 bis zu 20 Online-Dienste dieser Art. Nur etwas mehr als die Hälfte der Befragten gibt an, für jedes Online-Konto ein gesondertes Passwort zu nehmen.

Nachlässigkeiten bei der Passwortvergabe sind aber nach Einschätzung von Experten besonders gefährlich, denn damit macht man es professionellen kriminellen Hackern sehr leicht, in das System einzudringen und Schaden anzurichten.

Hilfestellung bieten kann laut Bitkom bei der Verwaltung der Flut von Passwörtern ein **Passwort-Manager**. Dieser Manager speichert alle Passworte und Benutzernamen in einer sicher verschlüsselten Datei. Die Anwender müssen sich dann nur noch das Master-Passwort für diesen Passwort-Manager merken.

49

#### *Hinweis*

Für die **Erstellung neuer Passwörter** gilt generell der Grundsatz: Je komplexer das Passwort ist, desto besser ist der Schutz gegen Hackerangriffe.

Leider wird gegen diesen Grundsatz immer wieder verstoßen, denn angeblich soll das am häufigsten verwendete Passwort die Zahlenfolge „1234“ sein, die man sich ja leicht merken und auf der Tastatur auch schnell eingeben kann.

## E. Ausgewählte Rechtsprechung zum ERV

*Autor: Wolfgang Kuntz*

*Rechtsanwalt und Fachanwalt für IT-Recht, Saarbrücken*

### I. Einfache E-Mail kein Antrag im Sinne des Unterhaltsvorschussgesetzes

#### ■ VG Berlin, Urt. v. 2.8.2016 – 21 K 432.15

50

**Eine E-Mail erfüllt nicht die Anforderungen an einen Antrag im Sinne des Unterhaltsvorschussgesetzes.**

Der Kläger begehrt eine frühere Bewilligung von Unterhaltsvorschuss.

Die Mutter des Klägers hatte mit einem (Formular-)Antrag vom 26.4.2015 die Bewilligung von Unterhaltsvorschuss für den am 5.3.2015 geborenen Kläger, der (auch) die deutsche Staatsangehörigkeit hat, beantragt. Dabei fügte sie die Kopie ihrer nicht unterschriebenen E-Mail vom 14.3.2015 an den „Briefkasten SenBJW“ bei, mit der sie erklärte, sie beantrage für das Kind Unterhaltsvorschuss und bitte um Übersendung der Antragsformulare, sowie die Antwort-E-Mail, wonach sie sich an das bezirkliche Jugendamt in Spandau wenden solle. Das Jugendamt bewilligte dem Kläger mit Bescheid vom 15.7.2015 Unterhaltsvorschuss in gesetzlicher Höhe ab April 2015. Gegen die Bewilligung von Unterhaltsvorschuss erst ab April 2015 legte der Kläger Widerspruch mit der Begründung ein, es sei bereits am 5.3.2015 formlos Unterhaltsvorschuss beantragt worden; über den Widerspruch ist nicht entschieden worden.

Das Gericht führt aus, die Klage wäre auch dann unbegründet gewesen, wenn alleine auf den Einwand des Klägers abgestellt würde, er habe mit der E-Mail seiner Mutter vom 14.3.2015 einen für die Unterhaltsvorschussbewilligung ausreichenden Antrag gestellt. Die E-Mail erfüllte nicht die Anforderungen an einen Antrag im Sinne des Unterhaltsvorschussgesetzes. Nach § 9 Abs. 1 S. 1 des Gesetzes zur Sicherung des Unterhalts von Kindern alleinstehender Mütter und Väter durch Unterhaltsvorschüsse oder -ausfallleistungen i.d.F. v. 17.7.2007 (BGBl I 1446), zuletzt geändert mit Gesetz v. 16.7.2015 (BGBl I 1202) – UVG –, wird über die Zahlung der Unterhaltsleistung auf **schriftlichen** Antrag des Elternteils, bei dem

der Berechtigte lebt, entschieden. Mangels näherer Bestimmung zur Schriftlichkeit im UVG oder im SGB I und SGB X ist auf § 126 BGB („Schriftform“) zurückzugreifen. Danach muss, wenn durch Gesetz schriftliche Form vorgeschrieben ist, die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden. Dies ist bei der E-Mail der Mutter des Klägers nicht der Fall. Nach § 126 Abs. 3 BGB kann zwar die schriftliche Form durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt, jedoch schreibt § 126a S. 1 BGB („Elektronische Form“) vor, dass, wenn die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden soll, der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen muss. Auch hieran fehlt es. Der Einwand des Klägers, § 9 Abs. 1 UVG sei nur für die Entscheidung in der Sache maßgeblich, nicht aber für die Frage, wann eine Leistung einsetze, was sich allein aus § 4 UVG ergebe, überzeugt nicht. § 4 UVG stellt entscheidend auf den Monat ab, „in dem der Antrag gestellt“ wird, und steht damit im Zusammenhang mit § 9 Abs. 1 UVG, der das „Verfahren“, insbesondere die Art des Antrags und den Antragsberechtigten regelt. Beide Vorschriften gehören zusammen. Entsprechend hält auch die Kommentarliteratur einen (schriftlichen) Antrag i.S.v. § 9 Abs. 1 UVG konstitutiv für das Einsetzen der Leistung nach § 4 UVG.

## II. Akte muss nicht aus Originaldokumenten bestehen

### ■ OLG Koblenz, Beschl. v. 6.9.2016 – 1 OWi 3 SsRs 93/16

51

**Der Eintritt einer Verjährungsunterbrechung nach § 33 Abs. 1 Nr. 10 OWiG setzt nicht voraus, dass die dem Amtsgericht zugeleitete Akte aus Originaldokumenten besteht.**

Das OLG Koblenz stellte in einer Art obiter dictum fest, dass gegen die Verwendung von Kopien bzw. Ausdrucken auch im gerichtlichen Verfahren grundsätzlich nichts einzuwenden ist (BGH v. 5.1.1999 – 3 StR 550/98, NSZ-RR 1999, 176). Es könne inzwischen als offenkundig (allgemeinkundig) i.S.d. § 244 Abs. 2 S. 2 StPO angesehen werden, dass die heute verwendete Technik dann, wenn es nicht zu manipulativen Eingriffen kommt, gewährleistet, dass sich der Inhalt eines Dokuments auf dem Weg vom Scannen über das Speichern bis zum Drucken nicht verändert; auch eine versehentlich unrichtige Übertragung des Inhalts auf eine Fotokopie könne ausgeschlossen werden. Es gebe grundsätzlich auch keinen Anlass, ernsthaft in Betracht zu ziehen, Mitarbeiter staatlicher Stellen hätten bereits beim Scannen bzw. Kopieren manipuliert oder nachträglich Datensätze verändert. Folglich kann der Tatrichter mangels entgegenstehender konkreter Anhaltspunkte auch davon ausgehen, dass die von einer Bußgeldstelle hergestellten und in die Akte gehefteten Ausdrucke oder Kopien von Eichschein, Schulungsnachweis und Messprotokoll mit dem jeweiligen Original übereinstimmen (s. auch Thür. OLG v. 16.1.2008 – 1 Ss 284/07, VRS 114, 453).

## III. Keine Mitbestimmung bezüglich Dienstanweisung zum Umgang mit privaten E-Mails

### ■ OVG Berlin-Brandenburg, Beschl. v. 29.9.2016 – OVG 60 PV 10.15

52

In dem gegenständlichen Verfahren möchte der Antragsteller festgestellt wissen, dass der Beteiligte durch den Erlass der „Dienstanweisung zum Umgang mit privatem E-Mail-Verkehr und Zugriffsregelungen auf E-Mail-Postfächer“ (DA E-Mail) vom 6.1.2015 ohne Zustimmung des Antragstellers dessen Mitbestimmungsrechte verletzt. Die Dienstanweisung hat u.a. folgenden Wortlaut:

*„Die Nutzung des dienstlichen E-Mail-Accounts zu privaten Zwecken wird allen Dienstkräften untersagt. Das bedeutet, dass sie selbst keine privaten E-Mails versenden dürfen und dafür Sorge zu tragen*

*haben, dass sie auch keine privaten E-Mails erhalten. Erhalten sie dennoch private E-Mails, haben sie diese sofort und endgültig zu löschen.“*

Nach § 85 Abs. 1 S. 1 Nr. 6 PersVG Berlin bestimmt die Personalvertretung, soweit keine Regelung durch Rechtsvorschrift oder Tarifvertrag besteht, ggf. durch Abschluss von Dienstvereinbarungen mit über die Regelung der Ordnung in der Dienststelle und des Verhaltens der Dienstkräfte. Der Antragsteller kann dieses Mitbestimmungsrecht für das Verbot der privaten Nutzung dienstlicher E-Mail-Accounts in Ziffer 1 der DA E-Mail nicht für sich in Anspruch nehmen. Die Bestimmung von dienstlichen Gegenständen, wozu auch die hier in Rede stehenden dienstlichen E-Mail-Accounts gehören, zu alleinigem dienstlichem Gebrauch ist mitbestimmungsfrei.

Da die Verteilung der E-Mail-Posteingänge ungeachtet einer etwaigen (unerwarteten) Abwesenheit des zuständigen Mitarbeiters erfolgt, will (und muss) der Beteiligte sicherstellen, dass auf das E-Mail-Postfach des betreffenden Mitarbeiters zugegriffen werden kann. Diesem Zweck dient ersichtlich das Verbot der privaten Nutzung dienstlicher E-Mail-Accounts in der DA E-Mail, indem damit u.a. zum Schutz des Persönlichkeitsrechts des Beschäftigten sichergestellt wird, dass der zugreifende Vertreter keinen Einblick in die private E-Mail-Korrespondenz des zu vertretenden Beschäftigten erhält. Dieser Zweck lässt sich unschwer den Einleitungssätzen der Dienstanweisung entnehmen. Das Verbot der privaten Nutzung dienstlicher E-Mail-Accounts stellt sich somit als Regelung dar, mit der die Erbringung der den Beschäftigten obliegenden Arbeitsleistungen konkretisiert wird.

Abgesehen davon hat das Verwaltungsgericht zutreffend darauf hingewiesen, dass die Anordnung in der DA etwas im Grunde Selbstverständliches regelt, nämlich die Nutzung eines dienstlichen „Gegenstandes“ ausschließlich zu dienstlichen Zwecken, unabhängig davon, ob die private Nutzung zuvor geduldet wurde. Etwas anderes mag gelten, wenn der Dienststellenleiter an dienstlichen Gegenständen die private (Mit-)Nutzung gestattet und in einer Dienstanweisung Art und Umfang der privaten Nutzung regelt. An einer solchen Abspaltung der Regelung von der Dienstaufgabe fehlt es hier aber.

## **VI. Keine Wiedereinsetzung in den vorigen Stand bei Fehlen eines Hinweises auf Unzulässigkeit der Klageerhebung per einfacher E-Mail**

### **■ LSG Rheinland-Pfalz, Urt. v. 4.8.2016 – L 5 SO 130/15**

53

Zwischen den Beteiligten ist streitig, ob die per E-Mail erhobene Klage die Klagefrist gewahrt hat und, falls dies nicht der Fall ist, ob der Klägerin Wiedereinsetzung in den vorigen Stand zu gewähren war. In der Sache ist streitig, ob die Klägerin einen Anspruch auf höhere Unterkunftskosten hat.

Mit Bescheid vom 30.6.2014 und Widerspruchsbescheid vom 13.5.2015 lehnte die Beklagte einen Antrag der Klägerin auf höhere Unterkunftskosten teilweise ab. Der Widerspruchsbescheid wurde am 15.5.2015 an die Prozessbevollmächtigten der Klägerin, die die Klägerin auch im Widerspruchsverfahren vertreten haben, zum Zweck der Zustellung gegen Empfangsbekanntnis zur Post gegeben. Mit Telefax vom 18.5.2015 beantragten die Prozessbevollmächtigten der Klägerin unter Bezugnahme auf den Widerspruchsbescheid bei der Beklagten Kostenerstattung für das Verwaltungsverfahren. Am 18.6.2015 um 10.53 Uhr haben die Prozessbevollmächtigten per E-Mail (ohne elektronische Signatur) eine PDF-Datei mit eingescannter, unterschriebener Klageschrift an das Sozialgericht Speyer übersandt und vorgetragen, eine Übertragung des Schriftsatzes per Telefax sei aufgrund einer Störung des Empfangsgeräts nicht möglich gewesen. Die Verwaltung des Sozialgerichts hat bestätigt, dass es Leitungsprobleme gegeben habe. Am 19.6.2015 ging die Klageschrift auf dem Postweg ein.

Das Gericht lehnte eine Wiedereinsetzung in den vorigen Stand ab. Diese sei auch nicht deshalb zu gewähren, weil das Sozialgericht es unterlassen hätte, rechtzeitig auf die Unwirksamkeit der Klageerhebung

per einfache E-Mail hinzuweisen. Nach § 65a Abs. 2 S. 3 SGG ist, wenn das Dokument nicht den Anforderungen des § 65a SGG genügt, dies dem Absender unter Angabe der für das Gericht geltenden technischen Rahmenbedingungen unverzüglich mitzuteilen. Die Mitteilungspflicht erstreckt sich auch auf das Erfordernis einer qualifizierten elektronischen Signatur. Unverzüglich ist eine Mitteilung, wenn sie ohne schuldhaftes Zögern erfolgt. Da die einfache E-Mail mit der Klageschrift am 18.6.2015 um 10.53 Uhr einging, wäre eine Wahrung der Klagefrist für die Klägerin nur möglich gewesen, wenn das Sozialgericht noch am selben Tag auf die für das Gericht geltenden technischen Rahmenbedingungen hingewiesen hätte. Das Sozialgericht war jedoch nicht verpflichtet, am letzten Tag der Klagefrist zu prüfen, ob die Klage ordnungsgemäß eingegangen war, um erforderlichenfalls sofort durch entsprechende Hinweise auf die Behebung der Mängel hinzuwirken. Ein Beteiligter kann nicht erwarten, dass die Prüfung der Formvorschriften unmittelbar nach Eingang eines Schriftstücks erfolgt. Im Hinblick auf den übrigen Geschäftsanfall ist es nicht zu beanstanden, wenn diese Prüfung erst bei der Bearbeitung des Falls und damit nach Ablauf der Frist für die Zulässigkeit des Antrags erfolgt (zum Ganzen LSG Berlin-Brandenburg 12.11.2015 – L 25 AS 1511/14, juris Rn 46 m.w.N.; BGH 16.3.2015 – NotSt (Brfg) 7/14, juris Rn 14 m.w.N.). Es lagen auch keine besonderen Umstände vor, die das Gericht verpflichtet hätten, durch eine frühere Reaktion einem drohenden Fristversäumnis bei der Klageerhebung entgegenzuwirken. Selbst wenn dem Sozialgericht am Eingangstag bekannt war, dass die Telefaxverbindung des Gerichts gestört war, war es nicht verpflichtet, E-Mail-Eingänge auf Einhaltung von Formvorschriften zu überprüfen. Die Prozessbevollmächtigten der Klägerin haben in ihrer E-Mail selbst darauf hingewiesen, dass eine Übertragung des Schriftsatzes per Fax nicht möglich gewesen sei. Ihnen war daher bei Übersendung der E-Mail bekannt, dass die Telefax-Verbindung zum Sozialgericht gestört war. Die Prüfung formwirksamer alternativer Übermittlungsmöglichkeiten oblag damit zunächst ihnen. Eine gesteigerte Hinweispflicht des Gerichts bestand unter diesen Umständen nicht.

## V. Unvollständigkeit der elektronischen Akte begründet keine Rechtswidrigkeit des angefochtenen Bescheides

### ■ VG Düsseldorf, Beschl. v. 28.9.2016 – 13 L 1014/16.A

54

**Eine etwaige Unvollständigkeit der elektronischen Akte des Bundesamtes und gegenüber dem Asylbewerber unterbliebene Informationen haben nicht per se Rechtswidrigkeit des angegriffenen Bundesamtsbescheides zur Folge.**

Das Gericht führt aus, dass es die vom Verwaltungsgericht Wiesbaden (vgl. VG Wiesbaden, Urt. v. 28.2.2014 – 6 K 152/14.WI.A) geäußerten Bedenken gegen die Vollständigkeit der elektronischen Akte des Bundesamtes in dem vorliegenden Verfahren nicht teile. Im Übrigen sei nicht ersichtlich, inwieweit eine etwaige Unvollständigkeit der elektronischen Akte des Bundesamtes sich auf die Rechtmäßigkeit des angegriffenen Bescheides auswirken könne, zumal zumindest die Möglichkeit bestünde, die Dokumentenmappe beizuziehen.

### **Anmerkung:**

55

Diese Begründung des Gerichts ist fragwürdig, denn sie setzt das Vorhandensein einer Papierakte neben der elektronischen Akte voraus. Was geschieht aber, wenn die Behörde (künftig) die Akten ausschließlich elektronisch führt? Es muss für diesen Fall m.E. gewährleistet werden, dass die elektronische Akte vollständig vorliegt und alle Dokumente des Verfahrens enthält.