BUNDESNOTARKAMMER
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

Referentenentwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften

Stellungnahme der Bundesnotarkammer

3. März 2023

Zusammenfassung:

Die Bundesnotarkammer begrüßt das Ziel des Referentenentwurfs, die Digitalisierung der Verwaltung voranzutreiben. Bürgerinnen und Bürger können durch ein einheitliches Nutzerkonto maßgebliche Leistungen einfacher auffinden und niederschwellig in Anspruch nehmen. Gleichzeitig darf eine Modernisierung bestehender Abläufe auch im Bereich der Verwaltung nicht dazu führen, dass Effizienzgewinne durch Digitalisierung der Prozesse zulasten der Integrität des rechtsstaatlichen Verwaltungsverfahrens gehen. Stellenweise lässt dies der Referentenentwurf allerdings befürchten. Wir regen daher an, einzelne verfahrensrechtliche Vorschriften anzupassen, um das bisherige Maß an Rechtssicherheit auch im Rahmen eines elektronischen Verfahrens aufrechtzuerhalten.

Die Anforderungen an eine Ersetzung der Schriftform sind derzeit systematisch missverständlich und uneinheitlich geregelt (A. I.). Überdacht werden sollte ferner, bei Organisationen das ELSTER-Softwarezertifikat zur Identifizierung ausreichen zu lassen (A. II.). Darüber hinaus regen wir an, die weitergehenden Anforderungen an die Identifizierung zu spezifizieren (A. III.) und Bescheide zwingend mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel zu verknüpfen (A. IV.). Schließlich sollte die Möglichkeit, Nachweise im Original zu verlangen, aus Gründen der Rechtssicherheit verfahrensbezogen und abstrakt geregelt werden (B.).

Im Einzelnen:

A. Anforderungen an den elektronischen Schriftformersatz (§ 9a OZG-E)

§ 9a OZG-E überführt das analoge Schriftformerfordernis in das digitale Verwaltungsverfahren. Da Formvorschriften zu einem rechtsstaatlichen Verfahren beitragen und das Verfahren absichern, sollen diese nicht ersatzlos abgeschafft werden.[1] Vielmehr sieht der Referentenentwurf einheitliche Anforderungen vor, insbesondere um den unterschiedlichen Formvorschriften im elektronischen Verwaltungsverfahren Rechnung zu tragen. Hierfür differenziert der Entwurf zwischen drei Modellen: Eine Antragsstellung ist möglich entweder nach bloßer Anlegung eines Nutzerkontos (I.), nach Anlegung eines Nutzerkontos einschließlich Identifikation des Nutzenden (II.) oder nach Anlegung eines Nutzerkontos einschließlich der Einhaltung fachspezifischer, über die vorstehenden Voraussetzungen hinausgehender Anforderungen (III.).

I. Nutzerkonto ohne Identifizierung

Auf einer ersten Stufe genügt eine einfache Anmeldung am Nutzerkonto ohne Identifizierung des Nutzers sowie die Einhaltung von § 9a Abs. 3 bis Abs. 5 OZG-E.[2] Hiernach ist den

[1] Entwurfsbegründung, S. 32.
[2] Entwurfsbegründung, S. 34.

Nutzenden vor dem Absenden der Erklärung lediglich Gelegenheit zu geben, die Erklärung zu prüfen. Dies soll vor einer übereilten Abgabe schützen. Ferner muss eine dauerhafte und lesbare Kopie der Erklärung zur Verfügung gestellt werden.

Diese Basisvoraussetzungen sollen nach der Entwurfsbegründung nur „ausnahmsweise" ausreichen, wenn die Behörde einen Identitätsnachweis nicht für notwendig erachtet. Aufgrund des erhöhten Missbrauchsrisikos digitaler Verwaltungsleistungen sei „für jede elektronische Abwicklung […] – unabhängig vom Vorliegen eines Schriftformerfordernisses – eine elektronische Identifizierung [erforderlich]".[3] Dieser Ausnahmecharakter kommt im Wortlaut der Vorschrift allerdings nicht zum Ausdruck. Im Gegenteil: Die derzeitige Formulierung „Soweit für die Inanspruchnahme einer Verwaltungsleistung und der sonstigen elektronischen Kommunikation ein Nachweis der Identifizierung erforderlich ist, […]" legt nahe, dass eine Identifikation den Ausnahmefall darstellte und im Regelfall eine bloße Registrierung genüge. Dies erscheint vor dem in der Entwurfsbegründung zutreffend aufgezeigten Missbrauchspotenzial digitaler Verwaltungsleistungen widersprüchlich.[4]

Daher wird angeregt, § 9a Abs. 2 OZG-E wie folgt zu formulieren:

„Der Nachweis der Identifizierung erfolgt [es folgen die derzeitigen Nummern 1 und 2]. Von den Anforderungen kann abgesehen werden, wenn nach der Art der Verwaltungsleistung eine Identifizierung nicht erforderlich ist."

Gleichzeitig sollte in der Begründung klargestellt werden, dass das Absehen von einer Identifizierung keine Entscheidung im Einzelfall darstellt, sondern nach abstrakten Gesichtspunkten – orientiert am jeweiligen Formzweck – zu erfolgen hat. Der Wortlaut lässt bisweilen die Auslegung zu, dass die für die Entscheidung zuständige Stelle in jedem einzelnen Verfahren darüber entscheiden könne, ob eine Identifizierung erforderlich ist oder nicht. Unabhängig von der für die Bürgerinnen und Bürger damit einhergehenden Rechtsunsicherheit widerspricht dies auch dem Zweck der Formvorschriften. Auch der Entwurfsbegründung liegt hinsichtlich der Formzwecke eine abstrakte Sichtweise zugrunde.[5]

II. Nutzerkonto mit Identifizierung

Auf einer zweiten Stufe ist eine Identifizierung der antragstellenden Person nach § 9a Abs. 2 OZG-E erforderlich. Das Gesetz differenziert insoweit zwischen natürlichen Personen und Vereinigungen (z.B. Personengesellschaften, juristische Personen) bzw. Behörden: Im Bürgerkonto erfolgt dies durch einen elektronischen Identitätsnachweis („eID"). Im Organisationskonto erfolgt die Identifizierung durch ein ELSTER-Softwarezertifikat oder durch ein anderes elektronisches Identifizierungsmittel, das mit dem Sicherheitsniveau „hoch" i.S.d. Verordnung

[3] Entwurfsbegründung, S. 34.
[4] Entwurfsbegründung, S. 34.
[5] Vgl. etwa Entwurfsbegründung, S. 33 f.

(EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung) notifiziert worden ist.

Die Anforderungen für das Sicherheitsniveau „hoch“ i.S.d. eIDAS-Verordnung sind in der Durchführungsverordnung (EU) 2015/1502 vom 8. September 2015 konkretisiert. Danach ist insbesondere bei der Identitätsprüfung von juristischen Personen eine Prüfung anhand anerkannter Beweismittel erforderlich, vgl. hierzu die Tabelle in Abschnitt 2.1.3. der Durchführungsverordnung. Hinsichtlich der Merkmale und Gestaltung des Identifizierungsmittels wird sowohl eine Zwei-Faktor-Authentisierung als auch ein Schutz des Identifizierungsmittels vor Duplizierung und Fälschung und auch vor Angreifern mit hohem Angriffspotenzial verlangt sowie die Möglichkeit der berechtigten Person, das Identifizierungsmittel zuverlässig vor einer Benutzung durch andere zu schützen. Diesen Anforderungen entsprechen vor allem qualifizierte elektronische Signaturen und qualifizierte elektronische Siegel.

Obgleich eine Identifizierung mittels ELSTER-Zertifikatsdatei als „sicheres Verfahren“ i.S.v. § 87a Abs. 6 Satz 1 AO gilt, entspricht dies nicht den Anforderungen des Sicherheitsniveaus „hoch“ i.S.d. eIDAS-Verordnung. Für den Erhalt der ELSTER-Zertifikatsdatei ist es lediglich erforderlich, sich mit persönlichen Daten (insbesondere Steuernummer und E-Mail-Adresse) zu registrieren. Anschließend ist die angegebene E-Mail-Adresse über einen zugesendeten Link zu bestätigen. Nach Bestätigung der E-Mail-Adresse werden die Aktivierungsdaten auf dem Postweg an die bei der Finanzverwaltung gespeicherte Anschrift übermittelt. Der letztgenannte Schritt soll sicherstellen, dass ausschließlich berechtigte Personen einen Zugang für eine Organisation erstellen können. Nach Abschluss der Registrierung kann die Zertifikatsdatei heruntergeladen werden.[6]

Für eine erfolgreiche Identitätstäuschung müsste also lediglich die Steuernummer bekannt sein und die Post an die bei der Finanzverwaltung hinterlegte Anschrift abgefangen werden. Darüber hinaus handelt es sich bei den ELSTER-Zertifikatsdateien um bloße Softwarezertifikate, die leicht kopiert werden können, ohne dass dies für den Zertifikatsinhaber bemerkbar wäre. Zwar ist das Zertifikat durch ein persönliches Passwort geschützt. Dieses kann allerdings umgangen werden, beispielsweise unter Einsatz von „Brute-Force-Angriffen“.

Vor diesem Hintergrund wird angeregt, von der Identifizierung im Organisationskonto mittels ELSTER-Softwarezertifikats grundsätzlich abzusehen. Eine Identifizierung sollte vielmehr durch elektronische Identifizierungsmittel mit dem Sicherheitsniveau „hoch“ i.S.d. eIDAS-Verordnung erfolgen (insbesondere qualifizierte elektronische Signatur oder qualifiziertes elektronisches Siegel).

[6] Vgl. zur Registrierung im Einzelnen die Anleitung der Finanzverwaltung zur Login-Option Zertifikatsdatei, abrufbar unter https://www.elster.de/eportal/helpGlobal?themaGlobal=help_registrierung#c3867, zuletzt abgerufen am 3.3.2023.

III. Weitergehende fachspezifische Anforderungen

Auf einer dritten Stufe sollen gemäß § 9a Abs. 7 OZG-E weitergehende, über § 9a Abs. 2 Nr. 1 OZG-E hinausgehende Anforderungen an die Identifizierung einer Person unberührt bleiben, wenn diese zur Durchführung eines Verwaltungsverfahrens erforderlich sind. Dadurch sollen in bestimmten Verwaltungsverfahren weitergehende Anforderungen an die Identifizierung zulässig sein – etwa im Personenstandswesen.[7]

Insoweit ist nicht verständlich, warum die Möglichkeit, weitergehende Anforderungen zu stellen, nicht auch für das Organisationskonto nach § 9a Abs. 2 Nr. 2 OZG-E gegeben sein soll. Das gilt umso mehr, als für das Organisationskonto mit dem ELSTER-Softwarezertifikat eine niedrigere Stufe der Identifikation ausreichen soll. Selbst § 87a Abs. 6 Satz 1 AO lässt eine Identifizierung mittels ELSTER-Zertifikatsdatei nur genügen, „soweit nichts anderes bestimmt ist".

Darüber hinaus fehlen auch hier im Wortlaut oder in der Begründung der Vorschrift abstrakt formulierte Voraussetzungen, bei deren Vorliegen weitergehende Anforderungen gestellt werden müssen, sowie eine nähere Konkretisierung, welcher Art diese weitergehenden Anforderungen sein können. Dies der Einzelfallentscheidung der Behörden zu überlassen, führt zu einer uneinheitlichen Rechtsanwendung und damit letztlich zu Rechtsunsicherheit.

IV. Sonderregelung für behördliche Bescheide

§ 9a Abs. 6 OZG-E enthält schließlich eine Sonderregelung insbesondere für behördliche Bescheide. Danach „können" Behörden ihren Bescheid mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel verknüpfen, wenn die Erklärung beweissicher außerhalb der Nutzerkonten eingesetzt werden soll. Gegen diese Regelung bestehen erhebliche Bedenken.

Zunächst ist nicht nachvollziehbar, warum die Vorschrift lediglich als „Kann"- und nicht als „Muss"-Vorschrift ausgestaltet ist. Wie die Begründung des Referentenentwurfs zutreffend ausführt, betrifft die Norm öffentliche Urkunden i.S.d. §§ 415 ff. ZPO, die gegenüber Dritten den vollen Beweis ihres Inhalts erbringen sollen.[8] Der Beweiswert einer öffentlichen Urkunde kann nur erreicht werden, wenn sowohl für den Adressaten der Erklärung als auch für den Rechtsverkehr generell zuverlässig feststellbar ist, dass die Erklärung mit ihrem gegenwärtigen Inhalt (Integritätsschutz) von der aus ihr als Ersteller hervorgehenden Behörde (Authentizitätsschutz) abgegeben wurde.[9] Vor diesem Hintergrund sehen § 3a Abs. 2 Satz 2 VwVfG und – speziell für Verwaltungsakte – § 37 Abs. 3 Satz 2 VwVfG bislang zwingend das Anbringen einer qualifizierten elektronischen Signatur vor, wobei aus dem der Signatur zugrunde liegenden Zertifikat bei Verwaltungsakten die erlassende Behörde erkennbar sein muss. Signaturschlüssel- und Attribut-Zertifikate bilden Zuständigkeiten, Funktionen und Rechte von

[7] Entwurfsbegründung, S. 36.
[8] Entwurfsbegründung, S. 35.
[9] *Huber* in Musielak/Voit, ZPO, 19. Aufl. 2022, § 437 Rn. 1 m.w.N.

Behördenmitarbeitenden sowie Dienstsiegel im elektronischen Rechtsverkehr ab.[10] Mithilfe des Zertifikats lässt sich im Rahmen einer Signaturprüfung feststellen, wer das Dokument mit welchem Inhalt erstellt hat.[11] Sie bieten die Möglichkeit einer Echtheitskontrolle.[12] Diese Nachvollziehbarkeit rechtfertigt letztlich eine Gleichstellung des elektronischen Dokuments, insbesondere in Hinblick auf die Echtheitsvermutung, vgl. § 371a Abs. 3 Satz 2, § 437 ZPO.

Den erforderlichen, für jedermann nachprüfbaren Integritäts- und Authentizitätsschutz bieten letztlich nur eine qualifizierte elektronische Signatur und ein qualifiziertes elektronisches Siegel. Daher setzen das Grundbuchverfahren beispielsweise bei der Übermittlung elektronischer Dokumente (vgl. § 137 Abs. 2 Nr. 2 GBO) und die beurkundungsrechtlichen Vorschriften bei der Beglaubigung eines Ausdrucks bzw. einer Abschrift eines elektronischen Dokuments (vgl. § 42 Abs. 4 Satz 1 BeurkG) eine qualifizierte elektronische Signatur zwingend voraus.

Vor diesem Hintergrund wird dringend angeregt, § 9a Abs. 6 OZG-E als „Muss“-Vorschrift auszugestalten.

Zudem geht die im Entwurf vorgesehene Erweiterung um das qualifizierte elektronische Siegel damit einher, dass der Rechtsverkehr keinen sicheren Nachweis mehr darüber hat, von welchem Behördenmitarbeiter die Erklärung herrührt. Während die qualifizierte elektronische Signatur mit einem Behördenattribut im Signaturzertifikat einer konkreten Person zugeordnet werden kann, für die gleichzeitig die Behördenzugehörigkeit nachgewiesen ist, lässt sich das qualifiziert elektronische Siegel nur der Behörde als solcher zuordnen.[13] Übersetzt in die Papierwelt würde man also anstelle der Unterschrift des Sachbearbeiters das Behördensiegel genügen lassen. Das kann im Sinne einer erleichterten Digitalisierung unter Umständen zweckmäßig sein – zumal die Zuordnung der Erklärung zur Behörde für den Rechtsverkehr von größerer Bedeutung sein dürfte als die Zuordnung zu einem konkreten Sachbearbeiter. Jedenfalls sollten dann aber erweiterte Anforderungen an den Inhalt der Erklärung gestellt oder klargestellt werden, dass die Vorgabe des § 37 Abs. 3 Satz 1 VwVfG unberührt bleibt. Der mit einem qualifiziert elektronischen Siegel versehene Verwaltungsakt muss dann die Namenswiedergabe des Behördenleiters, seines Vertreters oder seines Beauftragten enthalten.

B. Elektronischer Nachweisabruf (§ 5 EGovG-E)

Nach § 5 Abs. 1 Satz 1 Nr. 2 EGovG-E sind vom Antragsteller in einem elektronischen Verwaltungsverfahren zu erbringende Nachweise grundsätzlich elektronisch einzureichen. Ausweislich der Entwurfsbegründung sind hierunter im Regelfall elektronische Kopien eines Nachweises zu verstehen.[14] Auf die Vorlage von Originalen soll im Regelfall verzichtet werden. Möglich bleibt die Einholung von Nachweisen im Original auf Grundlage des

[10] BT-Drs. 15/4067, S. 35.
[11] *Krafka* in BeckOK ZPO, 47. Edition, Stand: 1.12.2022, § 437 Rn. 7.
[12] Entwurfsbegründung, S. 35.
[13] Entwurfsbegründung, S. 35.
[14] Entwurfsbegründung, S. 39.

Amtsermittlungsgrundsatzes, § 5 Abs. 1 Satz 2 EGovG-E, § 24 VwVfG. Ausweislich der Begründung soll es sich hierbei um eine Entscheidung im Einzelfall handeln.[15]

Mit Blick auf die Gewährleistung der Authentizität und Integrität der Nachweise waren bislang regelmäßig Originaldokumente einzureichen. Inwieweit dies im Rahmen digitaler Verwaltungsverfahren pauschal nicht mehr erforderlich sein soll, ist nicht nachvollziehbar. Dies gilt umso mehr, als die Entwurfsbegründung elektronischen Verfahren an anderer Stelle eine erhöhte Missbrauchsanfälligkeit attestiert.[16] Dabei ist auch zu berücksichtigen, dass für viele zu erbringende Nachweise bereits originär elektronische Formen bestehen, die in der elektronischen Kommunikation mit der Verwaltung verwendet werden können.

Jedenfalls sollte die Frage, ob die elektronische Kopie eines analogen Nachweises genügt, nicht einer Einzelfallentscheidung überlassen werden. Die Frage, welche Anforderungen an einen Nachweis zu stellen sind, dürfte verfahrensbezogen und somit abstrakter Natur sein. Andernfalls wäre der bezweckte Schutz der Authentizität nicht gewährleistet und gleichzeitig eine uneinheitliche Rechtsanwendung sowie – damit einhergehend – eine entsprechende Rechtsunsicherheit in der Praxis die Folge.

Auch hier sollten die bisherigen Nachweispflichten kritisch hinterfragt und abstrakte, einheitliche und verfahrensbezogene Regelungen geschaffen werden.

* * *

[15] Entwurfsbegründung, S. 41.
[16] Entwurfsbegründung, S. 34.

Kontakt:

Bundesnotarkammer K.d.ö.R.

Mohrenstraße 34
10117 Berlin

Telefon: +49 30 383866 – 0
Telefax: +49 30 383866 – 66
E-Mail: bnotk@bnotk.de

Büro Brüssel:
Avenue de Cortenbergh 172
B-1000 Bruxelles

Telefon: +32 2 7379000
Telefax: +32 2 7379009
E-Mail: buero.bruessel@bnotk.de