Stellungnahme

Formulierungshilfe für einen Änderungsantrag zu einem Gesetzesentwurf – Änderung des Onlinezugangsgesetzes (OZG) und der Abgabenordnung (AO)

27. November 2018

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Rebekka Weiß, LL.M.
Bereichsleiterin
Datenschutz & Verbraucherrecht
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

A. Einleitung

Bitkom bedankt sich für die Gelegenheit zur Formulierungshilfe für einen Änderungsantrag zum Gesetzesentwurf zur Änderung des Onlinezugangsgesetzes (OZG) und der Abgabenordnung (AO) Stellung zu nehmen.

Die geplante Anpassung des OZG und Einführung eines Verfahrens auf dem Vertrauensniveau „substanziell" begrüßen wir. Jedoch sehen wir insbesondere Klarstellungsbedarf hinsichtlich der entsprechenden Anforderungen an das Verfahren und möchten unsere Position zunächst wie folgt zusammenfassen:

- Bitkom spricht sich für die Verwendung des ELSTER Zertifikats aus – wenn die Erfüllung der Anforderungen nach dem Vertrauensniveaus „substanziell" nachgewiesen wurden.
- Identifikationsverfahren sollten sich nach der eIDAS Verordnung[1] richten und die Kriterien/Vorgaben des Implementing Act (EU) 2015/1502 erfüllen.
- Sofern vom OZG Entwurf das ELSTER Zertifikat und entsprechend zugrundeliegende Verfahren in Bezug genommen werden, merken wir an, dass es ELSTER Varianten gibt, die das Vertrauensniveau „substanziell" nach eIDAS nicht erfüllen. Dies gilt insbesondere für das ELSTER Basic Zertifikat.
- Die Verfahrensbeschreibung für das ELSTER Basic Verfahren sollte aus dem Entwurf gestrichen werden und stattdessen offener die Anforderungen an das Vertrauensniveau „substanziell" in Bezug genommen werden. Andernfalls besteht die Gefahr, dass durch die Beschreibung eines Verfahrens, das die Anforderungen an „substanziell" gerade nicht erfüllt, ein neues Niveau eingeführt wird.
- Die voranstehende Problematik steht dem Vereinheitlichungsgedanken der eIDAS Verordnung entgegen. Deutsche Sonderwege sollten auch im Interesse der Gleichbehandlung innerhalb der EU unbedingt vermieden werden.

[1] EU Verordnung Nr. 910/2014.

- EU Ausländer die aufgrund fehlender Steuerpflichtigkeit hier im Inland kein ELSTER Zertifikat besitzen, können die Leistungen nicht in Anspruch nehmen; es sollte daher ohnehin ermöglicht werden, dass auch andere Verfahren auf dem Niveau „substanziell" zugelassen werden.
- Es besteht die Gefahr, dass der Vorschlag zu einer Diskriminierung von im deutschen Markt aktiven Drittanbietern für Authentifizierung und Identifizierung führt.
- Bitkom empfiehlt der Bundesregierung den Beschluss eines bei der EU notifizierten e-ID Schemas, gegen das Angebote des öffentlichen und des privaten Sektors gleichermaßen nach den eIDAS-Vertrauensniveaus geprüft und bestätigt werden können. Vorbild hierfür könnte das italienische Schema SPID sein.

Auf diese Aspekte möchten wir im Folgenden im Detail eingehen.

B. Anmerkungen zum Inhalt des Entwurfs

I. Vorbemerkungen

Mit der vorgelegten Formulierungshilfe soll ein Beitrag zu einer beabsichtigen Novelle des OZG geleistet werden. Der Schwerpunkt liegt dabei auf den Anpassungen zur Einführung des in der eIDAS Verordnung definierten Vertrauensniveaus „substanziell" und der Möglichkeit zur Übermittlung von Melde- und Identitätsdaten vom BZSt an Bürgerservicekonten. Laut dem vorgelegten Vorschlag soll der Bürger einer Nutzung der beim BZSt zum Zwecke der Steuererhebung von den Meldebehörden übernommene Bestand von Identitäts- und Meldedaten zustimmen können.
Für die Nutzung des Vertrauensniveaus „substanziell" sind entsprechende Identifizierungs- und Authentifizierungsmittel notwendig. In der Begründung wird erläutert, dass sich die Novelle dabei an der eIDAS Verordnung orientiert. Als Mittel der Identifizierung und Authentifizierung ist das ELSTER-Zertifikat vorgesehen.

Bitkom begrüßt die mit dem vorgelegten Textvorschlag verfolgte Anpassung des OZG an die eIDAS Verordnung und die Einführung des Vertrauensniveaus „substanziell". Bitkom weist jedoch gleichzeitig darauf hin, dass das in der Begründung des Gesetzes beschriebene ELSTER-Verfahren in wesentlichen Punkten die Anforderungen nach (EU) 2015/1502 an das angestrebte Vertrauensniveau „substanziell" nicht erfüllt (siehe unten). Bei Verwendung des ELSTER-Verfahrens in der beschriebenen Art würde somit ein neues Vertrauensniveau entstehen, das zwischen den eIDAS-Vertrauensniveaus „niedrig" und „substanziell" eingeordnet werden müsste. Bitkom kritisiert diese Neudefinition eines

Vertrauensniveaus und fordert – im Sinne der eIDAS Verordnung und zur Sicherstellung einer EU-weiten Interoperabilität – dass für das mit der OZG-Novelle eingeführte Vertrauensniveau „substanziell“ die in (EU) 2015/1502 aufgestellten Anforderungen nachgewiesen werden müssen. Das ELSTER-Zertifikat mit den heute betriebenen Verfahren kann diesen Nachweis nicht führen.

— Bitkom weist darauf hin, dass der beim BZSt geführte Datenbestand durch diese Novelle mittelfristig zu einer zentralen Verteilstation von Identitäts- und Meldedaten an Servicekonten und damit an alle für den Bürger relevanten öffentlichen Stellen entwickelt wird. Wegen des hohen Automatisierungsgrades und der Dauerhaftigkeit der Verknüpfungen ist dem Bürger die für eine tatsächliche Ausübung der Kontrolle über die persönlichen Daten somit ab dem Moment der (einmaligen) Zustimmung zur Datenübernahme nicht mehr möglich. Dies sollte auch aus Datenschutzgesichtspunkten noch einmal überprüft werden.

— Wir weisen nochmals darauf hin, dass in Abhängigkeit des jeweils benötigten Vertrauensniveaus „niedrig“, „substanziell“ und „hoch“ unterschiedliche formale, organisatorische und technische Vorgaben zu erfüllen sind. Aus Sicht des Bitkom kann weder der heutige Prozess bei der Identifizierung, noch das Sicherheitsniveau im Umgang mit dem ELSTER Basic Zertifikat selbst, ein Vertrauensniveau „substanziell“ erreichen.

In Anbetracht der besonderen Bedeutung der Nutzerkonten als zukünftig zentrales Element der elektronischen Verwaltungsdienstleistungen sollte kein so gravierender Verlust an Vertrauenswürdigkeit eingegangen werden.

II. Im Einzelnen: Anmerkungen zur Begründung der Formulierungshilfe – Anforderungen an das Vertrauensniveau „substanziell“

Bitkom weist darauf hin, dass das in der Begründung des Gesetzes beschriebene ELSTER-Verfahren in wesentlichen Punkten die Anforderungen nach (EU) 2015/1502 an das angestrebte Vertrauensniveau „substanziell“ nicht erfüllt.
Bei Verwendung des ELSTER-Verfahrens in der beschriebenen Art würde somit ein neues Vertrauensniveau entstehen, das zwischen den eIDAS-Vertrauensniveaus „niedrig“ und „substanziell“ eingeordnet werden müsste. Hierauf möchten wir in diesem Abschnitt im Detail eingehen.

1. Auszug aus dem Formulierungsvorschlag

„Einführende Erläuterungen

a) Sichere Identifikationsmittel als Grundlage digitaler Verwaltung

Nach § 3 Absatz 2 des Onlinezugangsgesetzes (OZG) sind Bund und Länder dazu verpflichtet, im Portalverbund Nutzerkonten bereitzustellen, über die sich Nutzer für elektronische Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können. Die eindeutige Identifizierung eines Bürgers oder eines Unternehmens als Nutzer ist eine grundlegende Voraussetzung dafür, dass Verwaltungsleistungen sicher elektronisch angeboten werden können.

Entsprechend den Vorgaben der Verordnung (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) sollen für eine elektronische Identifizierung unterschiedliche Sicherheitsniveaus angeboten werden können. Die eIDAS-Verordnung unterscheidet insoweit die Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“. Auf welchem Sicherheitsniveau der Nutzer sich identifizieren muss, um bestimmte Verwaltungsleistungen in Anspruch nehmen zu können, ist abhängig von der jeweiligen Verwaltungsleistung und ihren fachlichen Anforderungen.

Bislang können auf Grundlage des OZG nur zwei Sicherheitsniveaus angeboten werden: Dies ist zum einen eine Identifizierung auf dem Sicherheitsniveau „niedrig“ durch manuelle Eingabe von personenbezogenen Daten (in der Regel Benutzername/Passwort). Zum anderen ermöglicht das OZG schon jetzt die Verwendung der eID-Funktion des neuen Personalausweises für eine Identifizierung auf dem Niveau „hoch“. Es wird angestrebt, zur

Identifizierung auf dem Vertrauensniveau „substanziell“ künftig ELSTER-Zertifikate anzubieten. Hierzu soll im Sinne der Nutzerfreundlichkeit kein neues Identifizierungsmittel entwickelt und eingeführt werden, sondern es sollen die bereits im Steuerverfahren zur Identifizierung angebotenen und bei Bürgerinnen, Bürgern und Unternehmen weit verbreiteten ELSTER-Zertifikate zum Einsatz kommen. Dies wird durch die vorliegenden Gesetzesänderungen möglich. Zur Klarstellung wird darauf hingewiesen, dass in den ELSTER-Zertifikaten die eindeutige Steuer-ID von Bürgerinnen, Bürger und Unternehmen nicht gespeichert ist.“

Bitkom Anmerkung:

Das ELSTER-Zertifikat (Basis-Zertifikat) wurde ursprünglich als geheimer Schlüssel zur Verschlüsselung und zum Schutz der Integrität der übermittelten Steuerdaten konzipiert. Die Nutzung des geheimen Schlüssels wird durch eine vom Benutzer selbst gewählte PIN gegen unberechtigte Verwendung geschützt. Die Zertifikatsdatei ist nicht gegen die Anfertigung von Kopien geschützt. Sie kann parallel auf verschiedenen Rechnern und – wenn das Passwort oder die PIN bekannt ist – von mehreren Personen genutzt werden. (EU) 2015/1502 Punkt 2.2.1 legt für das Niveau "substanziell" fest: "Das elektronische Identifizierungsmittel ist so gestaltet, dass davon ausgegangen werden kann, dass es nur unter der Kontrolle oder im Besitz der Person, der es gehört, verwendet wird." Der Schutz des ELSTER-Basis-Zertifikats wird hinsichtlich seiner "Gestaltung" nur durch ein vom Nutzer selbst gewähltes Passwort oder eine PIN gewährleistet. Dieses Passwort oder die PIN ist das einzige technische Sicherheitsmerkmal des Zertifikats. Daneben existiert kein davon unabhängiger „zweiter Faktor“.

(EU) 2015/1502 Punkt 2.2.1 erfordert für das Niveau "substanziell" weiterhin: „Das elektronische Identifizierungsmittel benutzt mindestens zwei Authentifizierungsfaktoren unterschiedlicher Kategorien.“ Da das Passwort oder die PIN bereits als Nachweis der Berechtigung zum Besitz eines ELSTER-Zertifikats dient, existiert kein zweiter davon unabhängiger Faktor. Die Authentifizierung mit dem ELSTER Basic Zertifikat erfüllt somit nicht die Anforderungen an das Vertrauensniveau „substanziell“.

2. Auszug aus dem Formulierungsvorschlag

Funktionsweise der ELSTER-Zertifikate zum Zweck der Identifizierung

„Steuerpflichtige natürliche Personen haben über das Online-Portal der Steuerverwaltung („Mein ELSTER“) die Möglichkeit, sich ein ELSTER-Zertifikat erstellen zu lassen. Dazu muss sich

der Nutzer mit Aktivierungsdaten registrieren, die er zu einem Teil per E-Mail und zu einem weiteren Teil per Post vom Finanzamt erhält. Der Registrierungsprozess prüft durch diese Verknüpfung von E-Mail- und Postversand an den Nutzer implizit, ob der Nutzer Zugang zu der gemeldeten Adresse des Steuerpflichtigen hat.“

Bitkom Anmerkung:

Aus dem im Formulierungsvorschlag beschriebenen Prozess wird deutlich, dass für die Beantragung eines ELSTER-Nutzerkontos nur die Kenntnis der Steuer-ID eines Bürgers und der Zugriff auf den Briefkasten dieses Bürgers zur Entwendung eines Freischaltbriefes notwendig sind. Ein Angreifer kann mit dem so übernommenen Nutzerkonto im Namen des Bürgers ohne dessen Kenntnis handeln.

(EU) 2015/1502 Punkt 2.3.1 beschreibt für das Vertrauensniveau „substanziell“: „Im Authentifizierungsmechanismus sind Sicherheitskontrollen zur Überprüfung des elektronischen Identifizierungsmittels implementiert, so dass es höchst unwahrscheinlich ist, dass ein Angreifer mit mäßigem Angriffspotenzial durch Handlungen wie Erraten, Abhören, Replay oder Manipulation der Kommunikation den Authentifizierungsmechanismus aushebeln kann.“

Das vom Bürger selbst gewählte Passwort oder die PIN ist in der Zertifikatsdatei verschlüsselt gespeichert. Es ist dort nicht änderbar und nicht gegen Brute-Force-Offline-Angriffe geschützt. Ein Angreifer, der eine Kopie der Zertifikatsdatei besitzt, kann durch „automatisiertes Erraten“ das vom Bürger gewählte Passwort oder die PIN ermitteln und sich mit diesem Passwort oder der PIN und der Zertifikatsdatei im Nutzerkonto des Bürgers anmelden. Eine beim ELSTER-Zertifikat zulässige sechs-stellige PIN kann mit gebräuchlichen und frei erhältlichen Tools ohne besondere technische Kenntnisse innerhalb von maximal 30 Sekunden ermittelt werden. Die in eIDAS geforderte Gestaltung der technischen Sicherheit könnte z.B. durch einen Zähler für Fehl-eingaben und Mechanismen zur Sperrung bei einer Überschreitung der Fehlversuche erfüllt werden. Solche Mechanismen fehlen jedoch beim ELSTER Zertifikat. Die Anforderungen an das Vertrauensniveaus „substanziell“ sind somit nicht erfüllt.

(EU) 2015/1502 Punkt 2.1.1 fordert weiterhin für das Vertrauensniveau „substanziell“:

1. Es ist gewährleistet, dass der Antragsteller die Geschäftsbedingungen für die Benutzung des elektronischen Identifizierungsmittels kennt.

2. Es ist gewährleistet, dass der Antragsteller die empfohlenen Sicherheitsvorkehrungen im Zusammenhang mit dem elektronischen Identifizierungsmittel kennt.

Der Bitkom fordert daher eine ausführliche Information zu den mit der Nutzung des ELSTER Zertifikates verbundenen Vorkehrungen.

(EU) 2015/1502 Punkt 2.2.2 stellt für das Vertrauensniveau „substanziell“ die Anforderung auf: „Nach der Ausstellung wird das elektronische Identifizierungsmittel auf eine Weise ausgeliefert, bei der davon ausgegangen werden kann, dass es nur in den Besitz der Person gelangt, der es gehört.“

Die kombinierte Auslieferung der Aktivierungsdaten per einfacher E-Mail an eine beliebige Adresse und per Briefpost an den Haushaltsbriefkasten einer zur Steuer-ID bekannte Meldeadresse erfüllt die Anforderungen an eine Auslieferung „nur in den Besitz der Person“ nicht.

3. Auszug aus dem Formulierungsvorschlag

„Dadurch bewirkt der Prozess einen erhöhten Vertrauenstatbestand. Das sodann generierte ELSTER-Zertifikat wird auf dem Endgerät des Nutzers gespeichert (grundsätzlich ist dies ein PC oder ein Notebook; über die App ELSTERSmart ist dies aber auch über ein Smartphone oder Tablet möglich). Bisher ermöglicht das Zertifikat dem Nutzer eine eindeutige Identifizierung gegenüber den Finanzbehörden; künftig soll eine Identifizierung mit diesem Zertifikat auch gegenüber dem Nutzerkonto möglich werden. Dies soll wie folgt funktionieren:

Möchte der Nutzer sich gegenüber seinem Nutzerkonto mit einem ELSTER-Zertifikat identifizieren, wird er vom Nutzerkonto zu „Mein ELSTER“ weitergeleitet. Nachdem er sich dort mit seiner Zertifikatsdatei angemeldet hat, wird er im Online-Portal „Mein ELSTER“ gefragt, ob seine persönlichen Identifizierungsdaten an das Nutzerkonto übermittelt werden dürfen. Nach der Übermittlung an das Nutzerkonto kann der Nutzer selbst diesen Datensatz nicht mehr bearbeiten. Sofern der Nutzer im Folgenden gegenüber einer Behörde elektronisch eine Verwaltungsleistung beantragen möchte, die eine Identifizierung auf dem Sicherheitsniveau „substanziell“ voraussetzt, kann der Nutzer diese in seinem Nutzerkonto hinterlegten Daten an die für die Verwaltungsleistung zuständige Stelle übermitteln. Die Behörde kann dann davon ausgehen, dass die Identifizierungsdaten, die sie erhalten hat,

besonders vertrauenswürdig sind, da sie ursprünglich aus den Steuerdatenbanken stammen und vom Nutzer nicht verändert werden können."

Bitkom Anmerkung:

Hier wird dem Bürger die Möglichkeit zu einer Einwilligung zur Nutzung seiner Daten angeboten (Opt-In). Es fehlt die Erläuterung, ob und wie der Bürger die Zustimmung zur so hergestellten Verwendung durch ein Opt-Out wieder zurücknehmen kann.

4. Auszug aus dem Formulierungsvorschlag

„Für natürliche Personen werden die Daten aus der ID-Nummer-Datenbank des Bundeszentralamtes für Steuern (BZSt) bezogen (vgl. § 139b der Abgabenordnung - AO). Diese Datenbank wird tagesaktuell mit Daten der Meldebehörden befüllt. Da sich der Nutzer bei jedem Login mit seinem ELSTER-Zertifikat identifizieren muss, werden auch die entsprechenden Identifizierungsdaten bei jedem Login aktualisiert."

Bitkom Anmerkung:

Es ist fraglich, ob dem Bürger bewusst ist, dass das von ihm einmalig erteilte Opt-In zur dauerhaften Datenübermittlung vom BZSt zum Bürgerkonto verwendet wird.

Im Text wird erklärt, dass „*sich der Nutzer bei jedem Login mit seinem ELSTER-Zertifikat identifizieren muss*". Der Bitkom geht davon aus, dass der Bürger auch die Möglichkeit behält, sich mit Benutzernamen/Passwort auf niedrigem Niveau anzumelden und dass er sich nur dann auf dem Niveau substanziell anmelden muss, wenn dies für den beabsichtigten Vorgang notwendig ist. Hier ist eine Korrektur oder Ergänzung des Textes notwendig.

5. Auszug aus dem Formulierungsvorschlag

„Auch für Ehegatten, die ihre Steuererklärung gemeinsam in der Form abgeben, dass ein Ehepartner sich über einen Freischaltprozess die Steuerdaten des anderen Ehepartners freigeben lässt und dann mit seinem Zertifikat die gemeinsame Steuererklärung übermittelt, kann technisch gewährleistet werden, dass an das Nutzerkonto nur diejenigen Daten übermittelt werden, die sich auf den Inhaber des Zertifikats beziehen. Um ein Nutzerkonto

anlegen zu können, muss daher jeder Ehepartner ein auf sich bezogenes Zertifikat besitzen und verwenden."

Bitkom Anmerkung:

Für die Übermittlung einer Steuerklärung wird ein ELSTER-Zertifikat verwendet. Da viele Ehepaare eine gemeinsame Steuerklärung abgeben – unter Verwendung des ELSTER-Zertifikats eines der beiden Ehepartner - wird die Anforderung der getrennten Verwendung in diesem Fall häufig nicht erfüllt. Es ist unwahrscheinlich, dass eine Verpflichtung zur ständig wechselnden gemeinsamen und getrennten Verwendung des ELSTER-Zertifikats bei gemeinsam veranlagenden Ehepaaren praktikabel und vermittelbar ist.

III. weitere Inhalte der Regelungen

1. Unklare Begrifflichkeiten

Die „wirtschaftliche Tätigkeit" ist nicht definiert und wird vermengt mit gewerblicher Tätigkeit. Es bleibt dadurch zum Beispiel die Frage offen, wie Freiberufler einzuordnen sind. Wir halten daher eine Klarstellung und Ergänzung des Textes für erforderlich.

Die Begrifflichkeit der „natürlichen Person" bleibt ebenfalls uneindeutig. Es wird nur auf § 139b Abs. 3 AO verwiesen (Seite 5), aber in § 139c Abs. 3 AO wird auch die Begrifflichkeit der natürliche Personen mit wirtschaftlicher Tätigkeit verwendet.

Die erforderlichen Daten für das „Nutzerkonto" (entspricht dem Servicekonto des Portalverbunds) werden laut Begründung „aus den Steuerdaten" oder „aus den Steuerkonten" gewonnen oder entsprechen „dem Stand der letzten Steuererklärung oder einer zwischenzeitlichen Datenaktualisierung". Es gibt bei Unternehmen jedoch oftmals nicht „die" Steuerdaten oder „die" Steuererklärung. Insbesondere bei bestehenden Organschafts-verhältnissen können zwischen Umsatzsteuer und Körperschaftsteuer die Daten variieren, sofern die Wirtschafts-Identifikationsnummer auf USt IDNr aufbauen sollte. Unter-nehmen können unter Umständen mehrere Steuernummern haben.

2. Vertretung von Bürgern und Unternehmen durch Intermediäre (insbesondere Steuerberater, Anwälte)

Zu den Vertretungsrechten von Intermediären (insbesondere Steuerberater, Anwälte) finden sich im Entwurf keine Ausführungen. Im Sinne nutzenstiftender Lösungen für Bürger und Wirtschaft erscheint ein Vertretungsrecht unumgänglich. Ein Austausch

zwischen Betroffenen und Verwaltung wäre für die Konzeption tragfähiger und wertschaffender Lösungen an dieser Stelle angebracht.

3. Authentifizierung durch Drittanbieter

Es erscheint sinnvoll, im OZG die Nutzung von (bestehenden) ELSTER-Verfahren mit vorzusehen und zu unterstützen. Fraglich ist indes, warum dies ausschließlich für (echte) ELSTER-Zertifikate gelten soll, womit weitere bei ELSTER zugelassene Authentifizierungsverfahren, die die ELSTER Security Policy unterstützen und heute das selbe Sicherheitsniveau haben, nicht einbezogen sind. Damit würden weitere nutzenstiftende Szenarien für Bürger und Wirtschaft nicht ermöglicht.

Bei einer wachsenden Anzahl von Online-Diensten wird für eine Akzeptanz sowohl privatwirtschaftlicher als auch behördlicher Dienste ein bequemer und selbstbestimmter Zugang mit einer Nutzung der vom Nutzer hinterlegten Daten entscheidend sein. Bürger wollen ihre Identität einfach und sicher bei alltäglichen Dingen wie Einkäufen oder Bankgeschäften ebenso einsetzen, wie für die Verwaltung ihrer Privatsphäre wie Vertragsänderungen bei Versicherungen, Behördengängen oder die Ablage vertraulicher Informationen. Daher müssen privatwirtschaftliche und verwaltungstechnische Entwicklungen miteinander in Einklang gebracht werden. Dem dürfen keine Medien- und Technologiegrenzen entgegenstehen. Vielmehr muss durch eine Akzeptanz auch privatwirtschaftlicher Identitäten ermöglicht werden, Behördengänge gleichberechtigt zu anderen elektronischen Diensten online abzuwickeln. Aus diesem Grunde ist u. E. dringend anzustreben, neben (echten) ELSTER-Zertifikaten das Schutzniveau „substanziell“ ebenfalls zu gewährleisten, wenn bereits heute gleichberechtigte (privatwirtschaftliche) Authentifizierungsverfahren mit demselben Schutzniveau bestehen.

Auf Fremdidentitäten wird im Entwurf nicht eingegangen. Vielmehr lässt die Gesetzesbegründung den Schluss zu, dass es künftig erschwert bis unmöglich sein wird, dass private Anbieter überhaupt einen „substanziell“ vertrauenswürdigen Account erzeugen können. Die Verbindung digitaler Fremdidentitäten mit öffentlichen Dienstleistungen ist im Rahmen der Digitalisierung im Sinne der Nutzer unbedingt anzustreben.

Erläuterung: Der Nutzer wird im Falle des Einsatzes des Elster-Zertifikates gefragt, ob seine persönlichen Identifizierungsdaten an das Nutzerkonto übermittelt werden dürfen. Nach der Übermittlung an das Nutzerkonto kann der Nutzer selbst diesen Datensatz nicht mehr

bearbeiten. Das ist für das Sicherheitsniveau „substanziell“ vorteilhaft, da diese Daten dann tagesaktuell mit Daten der Meldebehörden befüllt werden. Ein tagesaktueller Abgleich mit den Daten der Meldebehörden steht privaten Anbietern vermutlich auch perspektivisch nicht offen. Im Ergebnis würden damit beide Sicherheitsniveaus „substanziell“ sowie „hoch“ (=nPA) aus-schließlich vom Staat bedient werden und für privatwirtschaftliche Anbieter verbliebe allenfalls nur noch das Sicherheitsniveau „einfach“ (=Benutzername + Passwort).

4. Wirtschafts-Identifikationsnummer

Es sollte nochmals überlegt werden, ob es der zielführende Weg ist, bei Unternehmensidentifikation auf die Wirtschafts-ID in der heute angestrebten Form zu setzen, da diese im Kern auf der USt IDNr basieren dürfte. Insbesondere bei bestehenden Organschaftsverhältnissen können zwischen Umsatzsteuer und Körperschaftsteuer die Daten variieren. Zu einer USt IDNr können unter Umständen mehrere Steuernummern gehören (keine Eineindeutigkeit). Eine belastbare Lösung für Freiberufler ist dem Entwurf nicht zu entnehmen.

5. Verwaltungsinterne Metastammdatenverwaltung“ zur Verknüpfung von Registern in Anlehnung an die Lösung in Österreich als mögliches Bild auch für Deutschland

Sofern die Einführung der Wirtschafts-Identifikationsnummer durch den Gesetzgeber „andere Nummernsysteme“ ersetzen soll, so stellt sich die Frage, ob es nicht eines umfassenderen Konzeptes zu einer Metastammdatenverwaltung bedarf.
In Österreich werden Register mit einer (neutralen) eindeutigen Nummer verknüpft, die jedoch keine inhaltliche Aussage über die Entität zulässt. In den jeweiligen Registern werden andere Nummern verwendet. Ein zentraler Dienst kann Verknüpfungsabfragen zwischen Registern ermöglichen, wodurch jedoch keine dauerhafte Verknüpfung der Register entsteht. Eine ähnliche Lösung könnte auch für Deutschland angestrebt werden. Dadurch könnte ein zentrales Portal für ein One-Stop-Government geschaffen werden, das dem Zensus-Urteil mit dem Verbot einer Verknüpfung aller Register mittels eines singulären Identifikationsmerkmals standhält. Ohne Anknüpfung an Steuerdaten könnte so eine standardisierte Schnittstelle zwischen Bürgern, Unternehmen, Verwaltung und Registern geschaffen werden.

IV. Änderungsvorschlag zu § 8 Absatz 1 OZG

lfd Nr.	Artikel/ Absatz	Art (K/R/T)	Kommentar	Änderungsvorschlag
1	§ 8 Abs. 1	R	Es sollte hier deutlich werden, dass eine Identifikation für die Nutzerkonten Verfahrensneutral möglich ist. Im Hinblick auf den Diskriminierungs- und Barrierefreien Zugang sollten hier, neben einer persönlichen Identifikation und einer mittels der eID Funktion des neuen deutschen Personalausweises, alle zulässigen Verfahren zur Identifikation, wie z.B. die Video Ident Verfahren und auch Verfahren, die auf einen bereits gesetzeskonform erhobenen Datensatz zurückgreifen, zulässig sein.	§ 8 Absatz 1 wird durch den folgenden Einschub ergänzt: „(1) Der Nachweis der Identität des Nutzers eines Nutzerkontos kann auf unterschiedlichen Vertrauensniveaus *unter Verwendung aller nach der eIDAS Verordnung bestätigten Identifizierungsmittel (unter nachgewiesener Erfüllung der in Implementing Act 2015/1502)* erfolgen und muss die Verwendung des für das jeweilige Verwaltungsverfahren erforderlichen Vertrauensniveaus ermöglichen. Zur Feststellung der Identität des Nutzers eines Nutzerkontos dürfen bei Registrierung und Nutzung die in den Absätzen 1a bis 1c genannten Daten verarbeitet werden.

Bitkom vertritt mehr als 2.600 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 400 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.