Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 22.03.2017

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Haushaltsausschusses,

am 27. März 2017

zum Entwurfs eines Gesetzes zur Änderung des Grundgesetzes (Bundestags-Drucksache 18/11131) und Entwurf eines Gesetzes zur Neuregelung des bundesstaatlichen Finanzausgleichsystems ab dem Jahr 2020 und zur Änderung haushaltsrechtlicher Vorschriften (Bundestags-Drucksache 18/11135)

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Mit dem Thema Digitalisierung befassen sich zwei Artikel in den in Rede stehenden Gesetzentwürfen. Der mit Art. 1 Nr. 2. des Entwurfs eines Gesetzes zur Änderung des Grundgesetzes vorgeschlagene neue Art 91c Abs. 5 GG bestimmt die Zuständigkeit des Bundes bei der Regelung des Onlinezugangs zu Verwaltungsleistungen, Art. 9 des Entwurfs zur Neuregelung des bundesstaatlichen Finanzausgleichssystems ist der Entwurf einer solchen Regelung (Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz, OZG)).

Soweit mit dem Entwurf eines **Onlinezugangsgesetzes** der neu zu schaffende Artikel 91c Abs. 5 GG konkretisiert wird, nehme ich im Folgenden nur zu diesem Entwurf Stellung. **Wenn im Folgenden zur besseren Lesbarkeit von einem Gesetzentwurf die Rede ist, dann ist der Entwurf dieses Onlinezugangsgesetzes (OZG-E) gemeint.**

Mit dem OZG-E soll ein bundesweit einheitliches Online-Angebot für den Zugang zu Verwaltungsleistungen geschaffen werden, das den Nutzern zugleich ermöglichen soll, sämtliche Dienstleistungen von Bund, Ländern und Gemeinden über nur einen Zugang zu erreichen. Bund und Länder werden mit dem Entwurf verpflichtet, innerhalb von fünf Jahren sämtliche Verwaltungsleistungen auch online anzubieten, soweit die jeweilige Verwaltungsleistung digitalisierbar ist. Für auf einem Bundesgesetz beruhende Verwaltungsleistungen soll der Bund im Benehmen mit dem IT-Planungsrat und mit der Zustimmung durch den Bundesrat die Nutzung bestimmter IT-Komponenten per Rechtsverordnung bestimmen können. Standards für die IT-Sicherheit und den Austausch von Daten im Portalverbund soll der Bund insgesamt im Benehmen mit dem IT-Planungsrat und der Zustimmung des Bundesrats auf dem Verordnungsweg festlegen können. Art und Umfang der Verwaltungsleistungen bleiben in dem Entwurf unbestimmt.

Mit Blick auf das Ziel eines Zugangs zu allen elektronisch angebotenen Verwaltungsleistungen von nur einem Zugangspunkt aus wird angenommen, dass zur Identifizierung von Nutzern die Einrichtung von Nutzerkonten erforderlich sei, welche wiederum durch jeweils eine öffentliche Stelle des Bundes und der Länder angeboten werden sollen. Im Kern ist gemeint, dass sich Nutzer für den elektronischen Zugang zu Verwaltungsleistungen an nur einer Stelle identifizieren müssen, um dann flächendeckend Verwaltungsleistungen in Anspruch nehmen zu können. Nur in diesem Punkt werden datenschutzrechtliche Regelungen in den den Verwaltungsleistungen zugrunde liegenden Gesetzen explizit berührt. Betroffen ist der Umgang mit den zur Identifizierung erforderlichen Daten, der mit § 8 OZG-E so geregelt wird, dass diese bereits bei der Anmeldung an einem Portal für den Zweck

der Identifizierung zur Nutzung einer Verwaltungsleistung erhoben und an die Stellen übermittelt werden dürfen, die die jeweilige Verwaltungsleistung anbieten.

Die Regelung bewerte ich wie folgt:

Nach dem gegenwärtigen Stand der Dinge verbleibt mit diesem Entwurf die datenschutzrechtliche Verantwortlichkeit für die jeweiligen Verwaltungsverfahren bei den Stellen, die auch für deren Abwicklung zuständig sind. Ausgetauscht zwischen den Portalen und den Verwaltungsverfahren werden lediglich die zur Identifizierung erforderlichen Daten, deren maximaler Umfang durch § 8 Abs. 1 Ziff. 1 und 2 OZG-E abschließend geregelt wird. Datenschutzrechtlich verantwortliche Stelle dafür ist die durch § 7 OZG-E bestimmte Stelle, die Nutzerkonten anbietet. Weitere für die Abwicklung erforderliche Daten werden dann auch im Rahmen der Abwicklung erhoben und im Zuge der Verarbeitung ggf. gespeichert. Die datenschutzrechtlichen Regelungen der zugrunde liegenden Gesetze werden nicht berührt. Die Daten können den Zuständigkeitsbereich der jeweils verantwortlichen Stelle nur dann verlassen, wenn die der Verwaltungsleistung zugrunde liegende Regelung dies auch vorsieht. Der Gesetzentwurf greift an dieser Stelle nicht ein. Insbesondere bietet der Entwurf keine rechtliche Basis für den Aufbau eines zentralen Datenbestands unter der Verantwortung eines Portalbetreibers. Das begrüße ich ganz ausdrücklich.

Weiterhin begrüße ich, dass die Nutzung eines Onlinezugangs freiwillig bleibt und aufgrund des föderalen Prinzips die Vielfalt bei den Portalangeboten erhalten bleiben wird. Positiv werte ich auch, dass für den Nachweis der Identität nach § 8 Abs. 1 Satz 1 unterschiedliche Identifizierungsmittel genutzt werden können. Nur das für den jeweiligen Zweck erforderliche Vertrauensniveau ist ausschlaggebend für die Wahl des Identitätsnachweises. Etwa für die Anmeldung einer Mülltonne ist es nicht erforderlich, den Personalausweis als Identitätsnachweis zu nutzen.

Warum jedoch zur Identifizierung überhaupt ein Nutzerkonto erforderlich sein soll, ist für mich nach dem heutigen Stand der Technik nicht nachvollziehbar. Ein solches kann nur für den Fall einer häufigen Inanspruchnahme von Verwaltungsleistungen einen Mehrwert versprechen, dürfte für die große Mehrheit der Bürger und Bürgerinnen infolge dessen uninteressant sein und sollte deshalb nur ein Zusatzangebot zu dem grundsätzlich zu schaffenden einheitlichen und möglichst unkomplizierten Zugang zu Verwaltungsleistungen bilden. Der Charakter des Nutzerkontos als Zusatzangebot zum einheitlichen Zugang zu Verwaltungsleistungen wird mit dessen Definition in § 2 Abs. 5 OZG-E nicht deutlich. Erst mit § 8 Abs. 3 OZG-E wird klar, dass es sich bei dem Nutzerkonto zur einmaligen Identifizierung nur um ein temporäres Konto handeln kann, das automatisch erlischt, wenn der Identifizierungszweck erfüllt ist. Ich empfehle deshalb, die Begriffe

Identifizierungskomponente und Nutzerkonto getrennt zu definieren, damit klar wird, dass es sich bei einem letztendlich immer dauerhaft gedachten Nutzerkonto um ein Zusatzangebot handelt, das für die Nutzung einer Verwaltungsleistung nicht erforderlich ist.

Ein weiterer Kritikpunkt meinerseits betrifft § 8 Abs.1 Ziff. 2 Satz 2 OZG-E. Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identitätsnachweise zu nichtprivaten Zwecken bzw. zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können. Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann der Gebrauch von Nutzerkonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Nutzerkonten vollständig erfasst.

Im Weiteren darf ich noch auf zwei Vorschläge aus der Stellungnahme des Bundesrats (Bundesrats-Drucksache 814/16 (Beschluss)) eingehen, denen die Bundesregierung in ihrer Gegenäußerung (Bundestagsdrucksache 18/11185) zugestimmt hat.

Mit der Ziffer 29 der Stellungnahme des Bundesrats zum OZG-E wird ein neuer § 7 Absatz 2 OZG vorgeschlagen, mit welchem eine Registrierungsstelle eingeführt wird. Registrierungsstellen sollen die Aufgabe haben, Kontoanträge zu prüfen und Kontonutzer zu registrieren (Satz 1 und 2 der Begründung). Begründet wird dies damit (Satz 3 und 4 der Begründung), dass es ein möglichst breitflächiges Angebot zur Einrichtung von Nutzerkonten geben müsse.

Der Vorschlag erscheint sinnvoll vor dem Hintergrund, dass als Identitätsnachweis nicht notwendigerweise ein Personalausweis genutzt werden muss. Für die meisten Verwaltungsleistungen werden geringere Identitätsnachweise genutzt werden können. In diesem Fall müssen Behörden auch auf das jeweilige Identifizierungsmittel abgestimmte Prüfungen durchführen können, um die Identität des Nutzers auf Basis der genutzten Identifizierungsmittel zu bestätigen. Dies kann auch eine Überprüfung der Identität von Angesicht zu Angesicht einschließen. Dann ist es zweckmäßig, wenn diese Stelle Nutzer auch für die Kontonutzung registrieren kann.

Datenschutzrechtlich unbestimmt bleibt mit diesem Vorschlag allerdings das Verhältnis der Registrierungsstellen zu den Stellen, die die Konten anbieten. Handeln

die Registrierungsstellen im Auftrag der Kontoanbieter? In diesem Fall blieben die Kontoanbieter auch die datenschutzrechtlich verantwortliche Stelle für die Verarbeitung der personenbezogenen Daten, namentlich der zur Identifizierung erforderlichen Daten. Handeln die Registrierungsstellen jedoch in eigener datenschutzrechtlicher Verantwortung, so muss auch in den mit § 8 OZG-E bestimmten Rechtsgrundlagen der Datenverarbeitung zwischen der Rolle einer Registrierungsstelle und der Rolle des Anbieters unterschieden werden. Mindestens muss geregelt werden, wie lange Registrierungsstellen im Rahmen der Registrierung erhobene personenbezogene Daten aufbewahren dürfen.

Mit dem in Ziffer 32 der Stellungnahme des Bundesrats zum OZG-E vorgeschlagenen neuen § 8 Absatz 2a OZG wird der Rahmen der in einem Konto gespeicherten Daten ausgeweitet. Zusätzlich zu den Identitätsdaten sollen auch Dokumente und Verfahrensdaten im Konto gespeichert werden können. Aus der Begründung wird deutlich, dass ausschließlich Nutzer Zugriff auf diese Daten haben sollen. Leider wird dies nicht aus der Gesetzesformulierung selbst deutlich. Das darin formulierte Erfordernis eines Einverständnisses des Nutzers zur Speicherung im Konto legt vielmehr nahe, dass auch nicht durch Kontonutzer verursachte Datenverarbeitungen stattfinden könnten. Der Regelungsvorschlag sollte aber so gefasst werden, dass der Intention entsprechend deutlich wird, dass Nutzer über die zusätzlich gespeicherten Daten die volle Hoheit behalten.