Interview

OZG-Konto für juristische Personen?

[23.07.2021] Das Onlinezugangsgesetz (OZG) betrifft auch juristische Personen. Inwiefern es für diese ein eigenes Organisationskonto braucht und warum eine offene Standardisierung wichtig ist, erläutert procilon-Geschäftsführer Jürgen Vogler.

Herr Vogler, das Bundesministerium des Innern, für Bau und Heimat (BMI) hat eine Rechtsverordnung zum Onlinezugangsgesetz (OZG) als Drucksache 369/21 veröffentlicht. Hierin werden neben den geplanten privaten Bürgerkonten auch juristische Personen – also Unternehmen, Vereinigungen und Verbände – betrachtet. Ist das die Genese eines weiteren Kontos im OZG-Kontext? Eine gewisse Unsicherheit kann ich in meiner Antwort auf diese Frage nicht verbergen. Natürlich ist im Zusammenhang mit dem OZG die Schaffung eines Organisationskontos für juristische Personen ein begrüßenswerter und notwendiger Schritt. Auf der anderen Seite werden wir im elektronischen Rechtsverkehr mit dem besonderen elektronischen Bürger- und Organisationenpostfach eBO etwas ganz Ähnliches haben. Hier fehlt allerdings der rechtliche Rahmen und liegt zur Verabschiedung mit einer entsprechenden positiven Empfehlung des Rechtsausschusses noch beim Bundestag. Die Infrastruktur ist aber de facto vorhanden und mit dem Verzeichnisdienst SAFE existiert dort auch ein Vertrauensanker für bestätigte elektronische Identitäten. In der Vergangenheit sind neben natürlichen Personen bereits juristische, wie Behörden, Verwaltungen oder Körperschaften des öffentlichen Rechts erfasst. Mit der geplanten Gesetzesänderung wird dies nun auf Bürger und nichtöffentliche Organisationen ausgedehnt. Wir haben die Hoffnung, dass beide Systeme für Organisationskonten zusammenpassen. Worauf begründet sich die Hoffnung auf Kompatibilität? Die Fäden für die Organisationskonten laufen beim IT-Planungsrat zusammen. Wir gehen davon aus, dass es hier kein weiteres Produkt des IT-Planungsrats geben wird, sondern Schnittstellen und Standards festgelegt werden. Dadurch wird ganz automatisch Wettbewerb ermöglicht. Der Mittelstand in Deutschland wird unterstützt, Monopole werden vermieden. Das führt zu attraktiven Konditionen, gleichzeitig werden höchste Qualitätsansprüche gewahrt. Aus unserer Perspektive gilt dies analog für die Gewährleistung der IT-Sicherheit im genannten Kontext. Welche Rolle spielt die IT-Sicherheit in diesem Gefüge und wie kann sie hergestellt werden? Nur wenn die verarbeiteten Daten, egal ob von Bürgerinnen und Bürgern oder von Organisationen vor Manipulation, Verlust und unbefugter Offenbarung nach dem Stand der Technik geschützt sind, wird die Akzeptanz des Gesamtsystems zu den beabsichtigten positiven Nutzungseffekten führen. Auf der einen Seite sind Standards in Form von Schutzprofilen und Technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Servicekonten (BSI TR-03160), elektronische Identitäten (BSI TR-03107-1) oder auch für kryptografische Vorgaben für Projekte der Bundesregierung (BSI TR-03116-4) vorhanden. Auf der anderen Seite kann der IT-Planungsrat als so genannte verantwortlichen Stelle, den Stand der Technik auf andere Weise herbeiführen. Er trägt dann jedoch die Nachweispflicht über die Wirksamkeit der gewählten Maßnahmen. Ob dann noch Zeit für die Weiterentwicklung und Pflege von Applikationen bleibt, lasse ich einfach mal offen. „Verbindliche Standards schaffen eine sichere Infrastruktur, eine hohe Zahl individueller Fachanwendungen große Akzeptanz bei den Nutzern." Warum ist die offene Standardisierung ohne Beschränkungen wichtig? Im Umfeld der OZG-Umsetzung haben wir immer betont, dass ein One-Fits-All-Ansatz nicht zum Erfolg führt. Es existieren am Markt bereits viele bewährte Lösungen und Dienste. Wichtiger ist, auf Basis einer verbindlichen Normung dafür zu sorgen, dass Anfragen aus den entsprechenden Konten auch in den vielfältigen Fachverfahren beantwortet und verarbeitet werden können. Aus technischer Perspektive ist die

Art des Kontos erst einmal egal. Ob es sich um eine juristische oder natürliche Person handelt, hat primär nur Auswirkungen auf die Art und Weise der formalen Identitätsbestätigung. Das dann diese zuverlässigen elektronischen Identitäten mit vielfältigen Fachanwendungen verknüpft werden können, zeigt der elektronische Rechtsverkehr mit einer Vielzahl von Nutzern aus ganz unterschiedlichen Bereichen eindrucksvoll. Hier schaffen verbindliche Standards, eine sichere Infrastruktur und eine hohe Zahl individueller Fachanwendungen eine große Akzeptanz bei Nutzerinnen und Nutzern. Zusammengefasst: Was braucht es für eine erfolgreiche OZG-Umsetzung? Durch die Delegierung von Bundesaufgaben auf kommunale Ebenen ist Interoperabilität bei der OZG-Umsetzung eine zwingende Bedingung, damit Prozesse, von einem Antragsformular auf Bundesebene bis zur fachlichen Umsetzung im Fachverfahren einer Kommune durchgängig, sicher und vollständig funktionieren. Hier sind nicht nur technische Normierungen für die Zielerreichung nötig, sondern auch eine Harmonisierung der Begrifflichkeiten. Auch der Nationale Normenkontrollrat hat vor einem ganz anderen Hintergrund, nämlich der Initiative zur Registermodernisierung, eine Reform der IT-Fachverfahren angeregt. Ganz oben steht hier das Thema vernetzte Kommunikation. Hier spielen die oben genannten Aspekte der IT-Sicherheit natürlich wieder eine bestimmende Rolle. Wir sehen also: die Anwendung sicherer Identitäten und die Herstellung vertraulicher elektronischer Kommunikation werden letztendlich zu einem kritischen Erfolgsfaktor.

()

Stichwörter: Politik, procilon, BMI, OZG