

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)303 I



FITKO | Zum Gottschalkhof 3 | 60594 Frankfurt

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1

11011 Berlin

Ihre Ansprechperson:

Jörg Kremer
Kommissarischer Leiter
Leitung | Föd. IT-Architekturmanagement,
Projekte und Standards
+49 (69) 401270-103
joerg.kremer@fitko.de

Aktenzeichen: [xxx]

Frankfurt am Main, 8. Oktober 2023

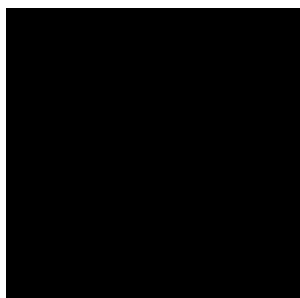
Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Online-Zugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (BT-Drucksache 20/8093) und zum Antrag der Fraktion der CDU/ CSU „Mehr Tempo bei digitaler Verwaltung: Onlinezugangsgesetz fortführen, Nutzungslücken schließen, Rechtsanspruch einführen“ (BT-Drucksache 20/4313)

Sehr geehrter Herr stellvertretender Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

aufgrund Ihrer Einladung vom 02.10.2023 darf ich Ihnen beigefügt meine Stellungnahme zu dem im Betreff genannten Gesetzesentwurf übersenden.

Ich hoffe, die aufgeführten Punkte können einen Beitrag zu den parlamentarischen Diskussionen leisten.

Mit freundlichen Grüßen



Jörg Kremer
(Kommissarischer Leiter)



Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Online-Zugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (BT-Drucksache 20/8093) und zum Antrag der Fraktion der CDU/ CSU „Mehr Tempo bei digitaler Verwaltung: Onlinezugangsgesetz fortführen, Nutzungslücken schließen, Rechtsanspruch einführen“ (BT-Drucksache 20/4313)

Vorbemerkung:

Das vorliegende Änderungsgesetz enthält einige wichtige Änderungen gegenüber dem Onlinezugangsgesetz. Dennoch gibt es nach Meinung der FITKO Optimierungspotentiale, die noch gehoben werden könnten. Dementsprechend werden Empfehlungen zu Identifizierungs- und Authentifizierungsverfahren, dem Einsatz von Open Source-Software sowie dem Aspekt der Kommunikation der Verwaltung mit Bürgerinnen und Bürgern formuliert.

Daneben soll an dieser Stelle auf einen weiteren Aspekt hingewiesen werden, der neben den gesetzlichen Änderungen ebenfalls unbedingt Beachtung finden sollte.

Die digitale Transformation der öffentlichen Verwaltung stellt einen umfassenden Veränderungsprozess dar, dessen Steuerung bislang unterschätzt wurde. Ein solcher Veränderungsprozess muss durch strukturelle Veränderungen initiiert und gezielt gesteuert werden.

Die derzeit praktizierten Entscheidungsprozesse stammen aus einer Zeit, in der Digitalisierung noch keine wahrnehmbare Rolle gespielt hat. Für diese Zeit waren diese Prozesse passend und zielführend.

Die Digitalisierung verändert die Geschwindigkeit von Veränderungen enorm. Vor etwa zwei Jahren beispielsweise waren KI-Anwendungen zwar im Gespräch, echte Nutzungsszenarien gerade in der öffentlichen Verwaltung jedoch in scheinbar weiter Ferne. ChatGPT hat dies in kürzester Zeit geändert. Gleiches gilt, wenn auch nicht in dieser ausgeprägten Form, für Cloud-Technologien: Was vor drei Jahren noch „State of the Art“ war, ist es heute nicht mehr bzw. gibt es heute Lösungen, die vor wenigen Jahren keine Rolle spielten.

In dieser Zeit stoßen etablierte Governanceprozesse an ihre Grenzen: Sie können mit der Geschwindigkeit der Digitalisierung und der sich daraus ergebenden Entscheidungsbedarfe oft nicht mithalten.

Um daher die Digitalisierung der öffentlichen Verwaltung gezielt zu verbessern, müssen die grundlegenden Governancestrukturen überarbeitet werden. Die Änderung des Onlinezugangsgesetzes ist wichtig für die Behandlung der Symptome – die Ursachen kann es nicht beseitigen.

Empfehlungen zu einzelnen gesetzlichen Vorschriften

Zu §3 Abs. 1

Mit dem Gesetzesentwurf wird das Nutzerkonto Bund (BundID) verpflichtend für die Identifizierung und Authentifizierung natürlicher Personen bei der Inanspruchnahme von Verwaltungsleistungen vorgeschrieben (§ 3 Abs. 1). Eine Nutzung der eID-Funktion ohne BundID, wie es bisher möglich war, ist demnach nicht mehr möglich. Lediglich der Nachweis der Identität des Nutzers im Bürgerkonto selbst erfolgt mittels eID (§ 3 Abs. 4 Nr. 1).

Dabei ist problematisch, dass die BundID eine zentral betriebene Komponente ist. Beeinträchtigungen im Betrieb der BundID haben mit dieser Neuregelung zwangsläufig Auswirkungen auf alle Verwaltungsleistungen im Portalverbund. Im Falle eines Ausfalls der BundID wären deutschlandweit keine Verwaltungsleistungen mehr nutzbar. Zudem ist die dezentrale, direkte Nutzung der eID-Funktion des elektronischen Personalausweises (ePA) durch die zuständige Fachbehörde auch unter Datenschutzaspekten deutlich näher am Stand der Technik anzusehen (Art. 25 DSGVO: Datenschutz durch Technikgestaltung; Privacy-by-Design-Ansatz), da hierbei keine Metadaten über Identifizierungs- und Authentifizierungsvorgänge an zentraler Stelle anfallen. Die aktuelle Umsetzung der BundID erlaubt technisch hingegen eine Profilbildung über alle Identifizierungs- und Authentifizierungsvorgänge aller Bürger:innen in allen Verwaltungsleistungen, die nur durch juristische Mittel unterbunden werden kann.

Die folgende Formulierung könnte das Problem lösen:

„Die Identifizierung und Authentifizierung der Nutzer im Sinne des § 2 Absatz 4 Nummer 1 für die Inanspruchnahme elektronischer Verwaltungsleistungen im Portalverbund erfolgt, soweit nicht durch Bundesgesetz etwas anderes bestimmt ist, über ein zentrales Bürgerkonto, das der Bund bereitstellt, [und / oder] nach einem der in Absatz 4 Nummer 1 genannten Verfahren.“

Zu §4 Abs. 3

Die Formulierung „dort, wo es technisch möglich und wirtschaftlich ist“ lässt einen breiten Interpretationsspielraum. Die Neuregelung zielt lediglich auf den Einsatz von Open-Source-Software, nicht jedoch auf die Lizenzierung der IT-Komponenten unter einer freien Softwarelizenz selbst, ab.

Die folgende Formulierung könnte das Problem lösen:

„Bei der Bereitstellung der IT-Komponenten im Sinne des Absatzes 1 soll unter einer freien Softwarelizenz lizenzierte Software vorrangig vor solcher Software eingesetzt werden, deren Quellcode nicht öffentlich zugänglich ist oder deren Lizenz die Verwendung, Weitergabe und Veränderung einschränkt. Eigenentwicklungen sind unter einer freien Softwarelizenz zu veröffentlichen.“

§8 Abs. 3 und 5

Grundsätzlich werden die Neuregelungen begrüßt, insb. die bidirektionale Kommunikation über das Postfach sowie die Neuregelung zur Kommunikation mit den Nutzern über dritte Kommunikationsmittel.

Wünschenswert wäre noch eine Öffnungsklausel für andere Kommunikationsdienste, die nicht auf einer E-Mail-Adresse oder Telefonnummer basieren (technologieoffenheit).

Der folgende Formulierungsvorschlag könnte das Problem lösen (§8 Abs. 3):

„Zur Kommunikation mit dem Nutzer können zusätzlich folgende Daten verarbeitet werden: Anrede, weitere Anschriften, De-Mail-Adresse oder vergleichbare Adresse eines Zustelldienstes eines anderen EU-/EWR-Staates nach der Verordnung (EU) Nr. 910/2014, E-Mail-Adresse, Telefon- oder Mobilfunknummer, Nutzerkennungen weiterer Kommunikationsinfrastrukturen im Einklang mit den Vorgaben nach der Verordnung (EU) Nr.2016/679.“

§9

Die aktuelle Regelung über die Bekanntgabe eines Verwaltungsaktes schreckt vor der Nutzung eines Nutzerkontos ab. Aufgrund der Regelung, dass der Verwaltungsakt am dritten Tag nach der Bereitstellung zum Abruf als bekannt gegeben gilt, führt bei Nutzern zu der Annahme, ihr Postfach ständig im Blick haben zu müssen, um z.B. keine wichtigen Fristen zu versäumen. Diese Verpflichtung könnte zu einer geringen Akzeptanz des Postfachs führen.

Der folgende Vorschlag könnte das Problem lösen:

Die Regelung sollte ersetzt werden durch die Regelung des § 41 Verwaltungsverfahrensgesetz (VwVfG).

§9a Abs. 5

Die Vorschrift ermöglicht eine schriftformersetzende Wirkung eines Identitätsnachweises über ein Nutzerkonto. Sie schließt eine schriftformersetzende Wirkung der eID-Funktion ohne Nutzung der BundID aus. Wünschenswert wäre, die schriftformersetzende Wirkung auch auf die direkte, dezentrale Nutzung der eID-Funktion durch die zuständige Fachbehörde auszudehnen.

Der folgende Formulierungsvorschlag könnte das Problem lösen:

„Hat der Nutzer über ein in § 3 Absatz 4 genanntes Verfahren den Identitätsnachweis erbracht und gibt er über ein Verwaltungsportal mittels Online-Formular eine Erklärung ab, für die durch Rechtsvorschrift die Schriftform angeordnet ist, so wird dadurch zugleich die Schriftform ersetzt.“

§13 Abs. 2

Die Nutzung des ELSTER-Zertifikates auf dem Vertrauensniveau „substantiell“ wird bis zum 30.06.2026 verlängert. Gleichzeitig werden das Bundesministerium des Innern und für Heimat sowie das Bundesministerium für Finanzen ermächtigt, diese Frist erneut beliebig zu verlängern. Dies schwächt die Nutzung des elektronischen Personalausweises. Bürgerinnen und Bürger verlangen jedoch eine von Seiten des Staates zur Verfügung gestellte digitale Identität, die höchsten Sicherheitsanforderungen genügt.

Dass darüber hinaus auch weitere Identifikations- und Authentifizierungslösungen angeboten werden können, erscheint sinnvoll. Dazu müssen diese die jeweiligen, für das beabsichtigte Einsatzszenario relevanten Anforderungen des gewünschten Sicherheitsniveaus, technisch und organisatorisch erfüllen.

Folgender Vorschlag könnte das Problem lösen:

Angesichts der noch nicht sehr weit verbreiteten Nutzung des elektronischen Personalausweises erscheint es zunächst sinnvoll, ELSTER als eine weitere Identifikationslösung vorzusehen. Eine weitere Fristverlängerung zur Nutzung des ELSTER-Zertifikates für das Vertrauensniveau „substantiell“ über den 30.06.2026 hinaus sollte jedoch entfallen.