DATABUND
Bundesverband der mittelständischen IT- Dienstleister und Softwarehersteller für den öffentlichen Sektor e. V.

Europaplatz 2
10557 Berlin

Tel.: +49 30 220 661 600
Fax: +49 30 220 661 609
E-Mail: info@databund.de
www.DATABUND.de

Stellungnahme zum Gesetz zur Änderung des Onlinezugangsgesetzes (OZG-ÄndG)

Der DATABUND nimmt zu den Gesetzesänderungen hier insgesamt Stellung und geht auf die Details der jeweiligen Gesetzes-Änderungen, soweit diese aus unserer Sicht zu kommentieren sind, in den Anhängen 1 und 2 ein:

Der vorliegende Gesetzentwurf OZG 2.0 ist eine logische Fortsetzung des Onlinezugangsgesetzes. Er sollte die Ursache für die nicht vollständige Umsetzung des ursprünglichen OZG beheben und die Weichen stellen für eine permanente und nachhaltige Digitalisierung in der deutschen Verwaltung.
Leider wurde erneut, wie schon zu Beginn des OZG, auf eine umfassende Analyse der realen IST-Gegebenheiten verzichtet.
Als Ursache wurde u.a. die unzureichende Zusammenarbeit zwischen Bund und Ländern ausgemacht. Diese mag nicht optimal gewesen sein, doch die wirklichen Ursachen für das nichtbefriedigende Gesamtergebnis des OZG sind andere – fehlender Wettbewerb, fehlende Standards, fehlende Infrastrukturen und ganz wichtig eine fehlende digitale Identität.

Darüber hinaus ist die Summe der Verwaltungsleistungen so komplex, dass die Komplexität nicht mit einem politischen Lösungsansatz realisiert werden kann und die Entwicklung in der IT so speziell und dynamisch ist, dass eine Fixierung von Technologien in langlebigen Gesetzen nicht zielführend ist.
Eine mögliche Lösung besteht in Ökosystemen, die fachlich und technisch Besonderheiten eines bestimmten Verwaltungssegments abbilden.

Ferner wurde die Erwartungshaltung des Bürgers nicht hinreichend in die Betrachtung einbezogen. Für den Bürger ist es wichtig, nicht wochenlange Antragsprozesse digital abzubilden, sondern mit einer einzigen Aktion höchst kompetent und komplett den Verwaltungsvorgang auszuführen.
Dabei sind die Hürden, die der Bürger nehmen muss, ein entscheidendes Kriterium. Die Einstiegshürde, d.h. die Identifizierung und Authentifizierung muss einfach und effizient im Sinne einer häufigen Nutzbarkeit, auch für Nichtverwaltungsprozesse, geplant werden.

Im vorliegenden Entwurf wurden aber die Anforderungen bzw. Erwartungshaltungen der Behördenmitarbeiter nicht berücksichtigt. Digitalisierung soll deren Arbeitsprozesse ebenfalls vereinfachen. Es ist notwendig, weil sich in der Übergangsphase sowohl herkömmliche als auch neue Arbeitsweisen etablieren. Das bedeutet eine duale Arbeitsweise und erhöhte Anforderungen bei gleichzeitigen Problemen bei der Personalbeschaffung. Einziger Ausweg ist hier, dass möglichst schnell, möglichst viele

digitale Prozesse herkömmliche Prozesse ablösen, die dabei aber effizient und qualitativ besser sind. Das ist mit den komplexen (angedachten) Strukturen (Servicekonto, Portal, …) schwer möglich.

Ein allgemeines und einheitliches Bürgerkonto, wie es derzeit angedacht ist, ist zweckmäßig. Besser, als ein Servicekonto beim Bund vorzugeben ist es, wenn eine genaue minimale Funktionsbeschreibung (um weitere Nutzungsmöglichkeiten offen zu lassen), eine maximale Sicherheitsanforderung und eine Beschreibung des Zusammenwirkens als Leitplanken festgelegt werden. Der Bürger hat dann die Auswahl und kann frei entscheiden. Mit einer solchen Herangehensweise würde sich die Umsetzung definitiv beschleunigen.

Darüber hinaus ist es nicht erforderlich, ja sogar abzulehnen, dass Daten im Portal zwischengespeichert werden. Dadurch entstehen neue, absolut datenschutzrelevante Datenbestände, die zwangsläufig zu Problemen führen werden.
Es ist verständlich, dass Kriterien wie „Auskunft zum Bearbeitungsstand“, „Änderung der Anträge“ zur Servicebereitstellung für den Bürger als Information dazugehören, doch sowohl der Bearbeitungsstand als auch eventuelle Änderungen müssen in der Verwaltung selbst beauskunftet oder umgesetzt werden. Dort erfolgt letzten Endes die Verarbeitung.

Absolut zu begrüßen ist die Bereitstellung deutschlandweit verwendbarer weiterer Komponenten, wie z.B. ein gängiges Bezahlverfahren (was allerdings alle dem Bürger bekannten Verfahren inkludieren muss) oder der zwingend erforderliche Siegeldienst.

Kritisch ist aber das Fehlen weiterer Infrastrukturkomponenten zu sehen. Dazu zählen die nicht hinreichend definierte Standardisierung als auch die fehlenden digitalen Identitäten. Der Eindruck, dass dieses Problem über die Servicekonten gelöst werden kann, ist falsch. Bei wesentlichen, die Person betreffenden Vorgängen wird das Sicherheitsniveau „hoch“ verlangt. Das ist durchaus richtig, aber erreicht wird das Sicherheitsniveau nur durch Nutzung des Personalausweises. Bei den relevanten Online-Vorgängen muss der Bürger somit sowohl ein Servicekonto als auch den Ausweis nutzen können. Das bedeutet: Er muss zwei Hürden überspringen. Wichtig ist aber, dass diese Art des Zuganges ausschließlich bei Verwaltungsvorgängen bzw. Anträgen nutzbar ist. Die Erfahrungen anderer Länder (z.B. Dänemark) lehren aber, dass möglichst viele verschiedene Online-Aktionen, nicht nur für interne Prozesse der öffentlichen Verwaltung, mit der digitalen Identität nutzbar sein müssen. Es ist daher anzustreben, dass alternativ eine einfache und sichere „Zwei-Wege“-Authentifizierung (analog den Banken) als zulässig erarbeitet und eingestuft wird.

Extrem unbefriedigend ist im Gesetzentwurf der Umgang mit dem Thema Standardisierung geregelt. Wenn es keinerlei Wettbewerb um die beste Lösung gibt und wenn jeweils eine Lösung im Sinne des EfA-Prinzips gelten soll, dann bedarf es keiner Standardisierung! Standardisierung braucht es, wenn verschiedene Lösungen (im Falle der IT) über die gleichen Schnittstellen funktionieren sollen! In diesem Sinne ist Standardisierung unerlässlich! Für eine professionelle Standardisierung müssen aber klare und kompetente Verantwortlichkeiten benannt und entsprechende Mittel bereitgestellt werden. Es muss eine unabhängige Instanz, zusammen mit den

entsprechenden Nutzern des Standards, fachlich ausgereifte, leicht pflegbare, aber auch allgemeingültige und übergreifende Festlegungen treffen. Das „DIN-Whitepaper zur Normung und Standardisierung bei der Digitalisierung der öffentlichen Verwaltung“ vom 18.01.2023 bietet einen allgemein akzeptierten Ansatz und sollte in das OZG 2.0 Eingang finden.

Der Entwurf enthält eine ganze Reihe wichtiger Forderungen, die dringend für eine erfolgreiche Digitalisierung der deutschen Verwaltung umgesetzt werden müssen. Dazu zählen die Barrierefreiheit, die Nutzerfreundlichkeit und der Umgang mit dem Schriftformerfordernis.

Alles in allem ist das OZG 2.0 zu sehr auf die geradlinige Fortsetzung des OZG ausgerichtet. Es wird zu sehr auf eine Lösung aus eigenen Kräften, d.h. auf verwaltungsinternes Handeln gesetzt, Wettbewerb und Wirtschaft werden nicht hinreichend in die zwingend notwendige Digitalisierung einbezogen. Es fehlt an Innovationspotentialen, zu viele technische Vorgaben sind bereits nicht mehr der neueste Stand der Technik (Portale, Nutzerkonten, …), wenn das Gesetz verabschiedet wird.

Generell sollte der Gesetzentwurf in wesentlichen Punkten grundsätzlich überarbeitet werden, um mittels einer klaren Zieldefinition ein Umfeld für Innovation und letztendlich für einen permanenten und dauerhaften Digitalisierungsprozess zu bilden.

Zu den einzelnen Gesetzen:
Anhang 1 – Stellungnahme zum OZG-ÄndG und ITNetzG
Anhang 2 – Stellungnahmen zum eGovernment-Gesetz (EGovG)

DATABUND
Bundesverband der mittelständischen IT- Dienstleister und Softwarehersteller für den öffentlichen Sektor e. V.

Europaplatz 2
10557 Berlin

Tel.: +49 30 220 661 600
Fax: +49 30 220 661 609
E-Mail: info@databund.de
www.DATABUND.de

Anhang 1 zur Stellungnahme zum Referentenentwurf „Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften (OZG-Änderungsgesetz – OZG-ÄndG)

Wir bedanken uns für die Gelegenheit einer Stellungnahme und gehen wie folgt auf die einzelnen Teile des Entwurfes bzw. farblich und kursiv kenntlich gemachten Passagen ein:

Onlinezugangsgesetz

1 Anwendungsbereich

Es wird die Geltung explizit auch für die Städte und Gemeinden festgelegt.

Eine solche Regelung bedarf der Zustimmung aller Bundesländer, oder zumindest des Bundesrates, weil diese für die Kommunen zuständig sind. Inwieweit es verfassungsrechtlich im Rahmen der kommunalen Selbstverwaltung zulässig ist, in ein Bundesgesetz Detail-Vorgaben für die Kommunen zu schreiben, wird juristisch aufzuarbeiten sein.

(1) Portalverbund

Obwohl inzwischen technisch veraltet, bleibt der Begriff des Portalverbunds im Gesetz und wird sogar noch verstärkt. Gesetze sollten aber keine Vorgaben von kurzer bis mittlerer Halbwertzeit beinhalten. Gerade IT-Technologie ändert sich so schnell, dass jede technische Festlegung im Gesetz rückwärtsgewandt sein muss. Gerade ChatGPT hat jetzt gezeigt, wie die Zukunft aussehen wird. Wenn in zwei Jahren klassische Suchmaschinen und Portale kaum mehr genutzt werden, stehen diese noch immer als Muss-Vorschrift im Gesetz und bewirken damit eine technologische Vollbremsung.

Stattdessen sollte nur die Zieldefinition festgelegt werden, dass ein barriere- und medienbruchfreier Zugang zu elektronischen Verwaltungsleistungen geschaffen werden soll.

(2) Suchdienst

Es mag aus Souveränitätsgründen legitim sein, einen eigenen staatlichen Suchdienst aufzubauen. Jedoch ist davon auszugehen, dass dieser nie genutzt werden wird, da Bürger/innen eher die ihnen bekannte allgemeine Suchmaschine nutzen werden. Außerdem entwickelt sich gerade im Internet eine umgangssprachliche Suche, die auch mit gesprochenem Wort interagieren kann. Diese ist allerdings durch die eingesetzte KI so aufwendig, dass der Staat diese nie wird nachbauen können. Dies führt dazu, dass in naher Zukunft eine Suchmaschine des Bundes daherkommt, wie aus einer längst vergangenen Welt.

Aus unserer Sicht ist Souveränität deutlich besser zu erreichen, indem mehrere privatwirtschaftliche Suchmaschinen unterstützt werden, idealerweise aus verschiedenen Ländern, unter anderem aus der EU. Diese lassen sich oft auch in eigene Angebote integrieren und ersetzen somit kostengünstig eigene Entwicklungen. Damit wären die staatlichen Angebote immer auf dem Stand der Technik, was die Suchtechnologien betrifft.

(3) Festlegung der Pflicht zum Datenaustausch

Der Bund möchte die Länder und Kommunen zum Datenaustausch verpflichten, dort wo es jeweils zur Umsetzung einer EU-Verordnung nötig ist. Dies ist grundsätzlich richtig, da ohne Datenaustausch keine Umsetzung der EU-Vorgaben zum SDG möglich ist.

Es muss jedoch dringend auch die Ende-zu-Ende-Digitalisierung als Ziel festgeschrieben werden. Diese bewusst nicht aufzunehmen, um die Kosten nach dem Konnexitätsprinzip zu sparen, führt zu einer halbherzigen und für die Kommunen nutzlosen Digitalisierung. Damit wird die Motivation der Kommunen zur Digitalisierung weiterhin gering bleiben, wenn überwiegend andere föderale Ebenen den Nutzen daraus ziehen. Da die Kommunen 80% der Leistungen erbringen, kann so keine signifikante Flächendeckung bei der Digitalisierung erreicht werden.

Ein reines Anhörungsrecht für die kommunalen Spitzenverbände, ohne über ihre eigenen Belange wirklich mitbestimmen zu dürfen, wird daran nichts ändern.

(4) Antragsassistent

Der Bund räumt sich das Recht ein, Antragsassistenten für Bundes-Angelegenheiten zu entwickeln und verbindlich vorzugeben.

Eine reine Fokussierung auf Antragsassistenten kann dem Anspruch einer durchgängigen Digitalisierung jedoch nicht gerecht werden. Bei komplexen Prozessen, online angeboten durch die Fachverfahren selbst, könnten Daten bereits während der Eingabe durch das entsprechende Fachverfahren geprüft und ggf. auch ermittelt werden, mit einem live-Feedback an die Bürger/innen. Das reine Ausfüllen und Absenden eines Antrages bietet in solchen komplexen Fällen ein deutlich schlechteres Nutzer/innen-Erlebnis und damit Akzeptanz. Für einfache Anträge können sich Antrags-Assistenten dagegen gut eignen.

Es steht nach den Erfahrungen der letzten Jahre zu befürchten, dass hier Lösungen auf der Bundesebene in völliger Unkenntnis der Verhältnisse in den Kommunen entwickelt werden und diese zumindest teilweise unbrauchbar oder mit deutlichem Mehraufwand für die Kommunen verbunden sind. Die per Antrags-Assistent eingehenden Daten müssen von den Kommunen dann manuell in ihre Fachverfahren abgetippt werden, was eine deutliche Verschlechterung gegenüber der aktuellen Situation darstellt und vor dem Hintergrund des allgemeinen Personalmangels zum Zusammenbruch einiger Verwaltungen führen könnte.

Grundvoraussetzung für die unter (4) genannten Maßnahmen ist die Definition von offenen Daten- und Datenübermittlungsstandards gemeinsam mit den betroffenen Fachverfahren. Die Existenz eines solchen Standards muss zwingende Voraussetzung für die verbindliche Nutzungsfestschreibung von Angeboten des Bundes sein, um die oben genannten Probleme zu vermeiden.

(6) Nutzerkonto

Es wird ein zentrales Bürgerkonto auch für Organisationen und Unternehmen durch den Bund bereitgestellt.

Insgesamt ist die Vereinheitlichung hier zu begrüßen, auch wenn wir der Meinung sind, dass ein Nutzerkonto nicht benötigt wird, wenn eine zentrale digitale Identität bereitgestellt wird. Selbst das Postfach wäre nicht zwingend notwendig, da bei entsprechender Rechtsänderung die Email-Adressen der Bürger/innen gespeichert werden können, über die dann eine Benachrichtigung über eine neue Nachricht (in einem geschlossenen System) als Link geschickt werden kann. Durch ein vorgeschaltetes Login mit der digitalen Identität des/der Nutzer/in bei Abruf der Nachricht, wäre die Sicherheit hier sogar noch höher als bei einem Nutzerkonto.

(8) Postfach

Unabhängig davon, dass ein Postfach nicht zwingend notwendig wäre, stellt sich die Frage, warum dies nur für an den Portalverbund angebundene Stellen verwendet werden soll. Warum soll nicht auch eine Stelle, die nicht an den Portalverbund angebunden ist, weil sie keine staatliche Dienstleistung erbringt, ein Postfach nutzen? In viele Prozesse sind neben den staatlichen auch nicht-staatliche Stellen eingebunden, wie Krankenkassen, IHKs, HWKs und weitere. Bei der aktuellen Regelung findet an dieser Stelle ein Medienbruch statt. Bei einer Gewerbeanmeldung beispielsweise muss in einigen Fällen die IHK zustimmen bzw. angehört werden, bei Handwerksbetrieben die Innung. Auch Bauanträge sind komplex und binden zahlreiche Akteure ein. Hier wäre es sinnvoll das Postfach auch für die Kommunikation mit dritten Stellen zu nutzen.

§3

(1) Bürgerkonto

Auch wenn Bürgerkonten als solches bei Nutzung der eID des Personalausweises oder einer anderen digitalen Identität nicht notwendig wären, ist die Vereinheitlichung der Bürgerkonten insgesamt zu begrüßen. Dies erleichtert und beschleunigt die Implementierung von Bürgerkonten in die Dienste, bei flächendeckenden Rollouts. Ansonsten verweisen wir auf unsere Ausführungen unter §2 (8).

§3 a

Die Bereitstellung eines Nutzer/innen-Supports für die digitalen Leistungen ist ein wichtiger Schritt. Es kann jedoch bei einer Vielzahl von komplexen Leistungen eine logistische Herausforderung darstellen, für jedes Problem ad hoc das passende Knowhow vorzuhalten und abzurufen.

§4 Elektronische Abwicklung von Verwaltungsverfahren; Verordnungsermächtigungen

(1) Ermächtigung

Die Ermächtigung des Bundes, ohne Einfluss der Länder oder gar der Kommunen, IT-Verfahren für den Gebrauch durch die Kommunen festzulegen, ist ein starker Eingriff in die kommunale Selbstverwaltung und die dort eingesetzte IT. Dies kann ohne abgestimmte Vorgehensweisen in dem komplexen Zusammenspiel der Fachverfahren in den Kommunalverwaltungen zu großen Störungen führen. Dies sollte nur mit Zustimmung der kommunalen Spitzenverbände möglich sein.

§6 Kommunikationsstandards

(1) Ermächtigung

Auch hier verweisen wir auf die gleichen Bedenken wie zu §4 (1).

§ 7 Für die Nutzerkonten zuständige Stelle

Die Fokussierung auf eine Akzeptanz der angebotenen Online-Dienste bei den Nutzer/innen ist sehr zu begrüßen, da die Zielgruppe die Dinge nur umfangreich nutzen wird, wenn eine ausreichender Nutzen und Einfachheit in der Bedienung gegeben ist.

§ 8 Rechtsgrundlagen der Datenverarbeitung

Ein Ersatz der bisherigen Einwilligung durch eine Veranlassung durch Nutzer/innen stellt richtigerweise klar, dass der Impuls von den Nutzer/innen ausgeht und nicht von den Behörden oder IT-Systemen. Diese Änderung und zugleich erfolgte Klarstellung ist zu begrüßen.

(1) Identitätsfeststellung

2. Juristische Personen

Die hier zu erhebenden Daten sind teilweise identisch mit den Daten des Transparenzregisters. Eine Doppelhaltung der Daten wird zu Inkonsistenzen und Mehraufwänden führen. Auch ist es im Sinne der Datensparsamkeit geboten und im Sinne des Once-Only-Prinzips gefordert, Daten nur einmal zu erheben. Hier eine Doppelerhebung in ein neues Gesetz zu schreiben konterkariert dagegen das gewünschte Once-Only-Prinzip und belastet Unternehmen zusätzlich, vor allem bei komplexen Unternehmensstrukturen.

(5) Elektronische Identifizierung und Speicherung der Kommunikationsdaten

Unter der Speicherung von „Kommunikationsdaten“ dürften die meisten Leser/innen etwas anderes verstehen. Daher sollte der Begriff anders gewählt werden. „Antragsdaten“ wäre hier sicher treffender und verständlicher.

Die Weitergabe von Daten durch Behörden, welche diese auf Veranlassung der Nutzer/innen erhalten haben, erscheint undurchsichtig und wird dazu führen, dass Nutzer/innen deutlich weniger Daten freigeben werden, als mit einer vollen Steuerung über die Datenverwendung. Nach dem Gesetzentwurf verlieren Nutzer/innen, einmal aus der Hand gegeben, die Kontrolle über ihre Daten.

§ 8a Rechtsgrundlage der Datenverarbeitung in einem Antragsassistenten

Der EfA-Online-Dienst soll nicht Teil des Fachverfahrens und diesem gegenüber auch nicht weisungsgebunden sein.

Dies ist zwar nachvollziehbar, jedoch erscheint es wenig hilfreich, wenn an zwei Seiten begonnen wird aufeinander zuzuarbeiten, ohne sich jedoch abzusprechen, damit sich die beiden Arbeitsergebnisse auch treffen und Anschlussfähig sind. Es muss ein Kooperationsgebot des Betreibers des EfA-Dienstes geben, damit EfA-Dienste nicht wie bisher Daten nur an der Rathaustür abgeben, sondern diese nach gemeinsam entwickelten Standards in die Fachverfahren übertragen und auch die Rückmeldungen dieser entgegennehmen und weiterleiten.

(1) Offenlegung der Daten

Es wird in der Synopse darauf hingewiesen, dass die Verarbeitung der Daten in einem Antragsassistenten zwingend erforderlich sei.

Dem möchten wir vehement widersprechen. Es gibt inzwischen modernere Ansätze, die ohne solche Assistenten auskommen und das User-Interface zum Bürger direkt in das Fachverfahren integrieren, wodurch eine zusätzliche Datenverarbeitung in einer Dritten Software entfällt und darüber hinaus auch die Zahl der Schnittstellen drastisch sinkt, genauso wie der Rollout-Aufwand. Diese Möglichkeit sollte zumindest berücksichtigt werden, um den Eindruck einer dargestellte Alternativlosigkeit des Antragsassistenten zu vermeiden.

(3) Löschung der Daten

Eine vorherige Benachrichtigung über den Löschzeitraum ist sicher wichtig, jedoch erscheint es genauso wichtig, die Nutzer/innen direkt vor und nach dem Löschen der Daten zu informieren.

(4) Datenschutzrechtliche Verantwortlichkeit

Die Klarstellung der datenschutzrechtlichen Verantwortlichkeit ist ein wichtiger Schritt zur Kapselung von Aufgaben. Jedoch wird es für Bürger/innen zunehmend schwieriger in solch einem aufgeteilten Prozess die datenschutzrechtlich Verantwortlichen zu erkennen. Es sollte daher festgelegt werden, dass zum Beginn des Prozesses alle datenschutzrechtlich verantwortlichen Stellen mit ihrem jeweiligen Verantwortungsbereich im Rahmen des Prozesses benannt werden.

§ 9 Bekanntgabe des Verwaltungsaktes

(1) Um eine elektronische Abwicklung einer Verwaltungsleistung zu ermöglichen wird mit der Ergänzung des § 9a „eine durch Rechtsvorschrift angeordnete Schriftform elektronisch ersetzt."

(2) Beim Bürgerkonto (eID-Funktion Personalausweis) und beim Organisationskonto (Elster-Zertifikat) wird dies einschließlich des Sicherheitsniveau „hoch" ermöglicht.

(3) Den Nutzer:innen wird vor dem Versenden die Möglichkeit der Prüfung eingeräumt.

(4) Um übereilten Handlungen der Nutzer:innen vorzubeugen wird eine Warnfunktion implementiert.

(5) Den Nutzer:innen wird anschließend eine Kopie des Verwaltungsaktes zur Verfügung gestellt.

(6) Um die Beweissicherheit eine Bescheides sicherzustellen können Behörden zusätzlich eine Dokument mit einer „qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel" versehen.

(7) Da in bestimmten Fällen zusätzliche „Nachweise der Identifizierung zur Identitätsfeststellung" über Absatz 2 Nummer 1 erforderlich sein können bleibt dies bei Notwendigkeit weitere Anforderung an eine Identifizierung zu fordern möglich.

Das Ermöglichen eines elektronischen Schriftformersatzes ist sehr zu begrüßen, da die Schriftformerfordernis einer Nutzung digitaler Verwaltungsleistungen als Hürde entgegensteht. Der Abbau von unnötigen Schriftformerfordernissen und wenn notwendig Ersatz durch komfortabel nutzbare elektronische Varianten ist sicherzustellen. Die eID-Funktion des Personalausweises für das Bürgerkonto, sowie das ELSTER-Softwarezertifikat für das einheitliche Organisationskonto, die in der EU das Sicherheitsniveau „hoch" garantieren, sind für die Fachverfahrenshersteller sinnvolle und empfehlenswerte Lösungen.

(3) (4) Erklärungen

Die technologieoffenen Definitionen zur Abwicklung von Erklärungen sind zu begrüßen, da sie Spielraum für den technischen Fortschritt lassen.

(5) Dauerhafte und lesbare Speicherung

Die dauerhafte und lesbare Speicherung der Erklärungen ist eine wichtige und hohe Anforderung, da sie über Jahrzehnte umgesetzt werden muss, bei allem technischen Fortschritt, den es in der Zeit geben wird. Es muss damit gerechnet werden, dass es außer den elektronischen Fassungen keine gedruckten Kopien mehr gibt. Hier ist vom Staat entsprechend Vorsorge zu treffen, dass diese Daten in keinem Fall verloren gehen können.

(6) Qualifizierte elektronische Signaturen und Siegel

Bei den Signaturen und Siegeln ist sicherzustellen, dass diese auch nach Jahrzehnten noch gelesen und vor allem geprüft werden können. Dazu müssen die ausstellenden Behörden verbindlich verpflichtet werden.

§ 10 Datenschutzcockpit

Bei Nutzung und vorheriger Registrierung mit einem Nutzerkontos des Portalverbundes beim Datenschutzcockpit, soll zukünftig die dem „Nutzerkonto zuständige Stelle das dienste- und kartenspezifischen Kennzeichen an die für das Datenschutzcockpit zuständige Stelle übermittelt“ werden.

Um Daten im Sinne des Once-Only-Prinzips zur Verfügung zu stellen und um gleichzeitig die notwendige Transparenz für den Bürger herzustellen (welche Behörde wann auch welche Daten zugegriffen hat), ist die Nutzung eines Datenschutzcockpits eine gangbare Lösung. Dies ermöglicht Verwaltungsdigitalisierung und das verfügbarmachen von Daten bei gleichzeitiger Wahrung des Datenschutzes und der informationellen Selbstbestimmung. Die Weiterleitung des dienste- und kartenspezifischen Kennzeichen ist hierbei ein Weg um einen Datenzugriff bei Nutzung eines Nutzerkontos des Portalverbundes zu ermöglichen. Dafür ist die unter (2) festgelegte Löschung der Daten

bei Beendigung des jeweiligen Nutzungsvorgangs im Datenschutzcockpit zwingend sicherzustellen.

Die Fachverfahrenshersteller weisen aber darauf hin, dass ein Datenschutzcockpit ohne Auskunftsrechte und Sanktionen für festgestellte unrechtmäßige Datenabrufe völlig sinnlos ist und sehr große Aufwände auf ihrer Seite produzieren, denen kein entsprechender datenschutzrechtlicher Nutzen gegenübersteht.

§ 11 Übergangsregelung zum Einsatz des Datenschutzcockpits

Um Nutzer/innen schon vor Inkrafttreten des § 10 Datenschutzcockpit eine Nutzung im Pilotverfahren zu gewährleisten soll dies mit Zustimmung des BMI ermöglicht werden. Dies geschieht unter der Voraussetzung, dass der/die Nutzer/in eine Einwilligung erteilt „dass erforderliche Nachweise durch einen automatisierten Datenaustausch beigebracht werden."

Da erfolgreiche Verwaltungsdigitalisierung sich an Nutzerzahlen misst, sollten funktionierende Leistungen den Early Adopter unter den Bürger:innen zeitnah zur Verfügung gestellt werden. Für die meisten Bürger:innen ist es vermutlich sinnvoll, dass zum Start bereits einige Leistungen verfügbar sind, um keine Frustrationen auszulösen.

§ 12 Evaluierungsklausel

„Mit der Evaluierungsklausel soll ein kontinuierlich wirkendes qualitatives Überprüfungsinstrument etabliert werden."

Grundsätzlich ist eine Evaluierung sinnvoll, um Erfolge und Defizite bei der Umsetzung zu erfassen und im laufen Prozess ggf. notwendige Änderungen zu tätigen, um die Ziele der OZG-Nachfolgegesetzgebung bestmöglich zu erreichen. Dies ist zu begrüßen. Jedoch muss sich die Evaluierung an klar identifizierbaren und nutzerorientierten Indikatoren festmachen, die in der Visualisierung keine falschen Eindrücke erwecken.

§ 13 Übergangsregelung zu § 3

Mit der Übergangsregelung die bisherigen Nutzerkonten der Länder bis zu zwei Jahre im Portalverbund zu belassen, wird ein vorläufiger Weiterbetrieb ermöglicht. Dies sollte allen Beteiligten genug Zeit geben, die Landes-OZG-Nutzerkonten abzulösen und ggf. notwendige Anpassungen vorzunehmen.

Aus Sicht des DATABUND ist diese Übergangsregelung zu begrüßen. Dabei ist es wichtig, dass notwendige Standards im Bereich Schnittstellen zur Anbindung des Nutzerkonto Bund frühzeitig definiert werden und entstehende Kosten im Backend einkalkuliert und finanziert werden.

Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – (IT-NetzG)

§ 3 Datenaustausch; Verordnungsermächtigung

Mit § 3 Datenaustausch; Verordnungsermächtigung soll zusätzlich im Anwendungsbereich des Onlinezugangsgesetzes ermöglicht werden, dass zwischen Bund und Ländern ein Datenaustausch neben dem Verbindungsnetz auch über weitere Netze des Bundes erfolgen kann. Das BMI soll mit dem Koordinierungsgremium ohne Zustimmung des Bundesrates entsprechende IT-Sicherheitsstandards festlegen können.

Die Ausweitung der Übertragungsnetz-Möglichkeiten ist zu begrüßen, da diese digitale Souveränität und Ausfallsicherheit schaffen können. Festlegungen sollten anhand des Standes der Technik erfolgen, um die IT-Sicherheit zu gewährleisten. Hierfür sind die allgemeingültigen technischen Standards anzuwenden.

Es wird in der Synopse Bezug darauf genommen, dass die Fachverfahren die Sicherheitsanforderungen der anderen Netze bestimmen. Auf der anderen Seite wird festgelegt, dass ausschließlich das BMI mit dem Koordinierungsgremium die Sicherheitsstandards festlegt. In Anbetracht der formulierten Erkenntnis muss es daher heißen „in Abstimmung mit den Fachverfahrensherstellern“.

DATABUND
Bundesverband der mittelständischen IT- Dienstleister und Softwarehersteller für den öffentlichen Sektor e. V.

Europaplatz 2
10557 Berlin

Tel.: +49 30 220 661 600
Fax: +49 30 220 661 609
E-Mail: info@databund.de
www.DATABUND.de

Anhang 2 zur Stellungnahme zum Referentenentwurf „Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften (OZG-Änderungsgesetz – OZG-ÄndG)

eGovernment-Gesetz des Bundes

§ 2 Elektronischer Zugang zur Verwaltung

In § 2 Elektronischer Zugang zur Verwaltung soll der flächendeckende Einsatz des (1) qualifizierten elektronischen Siegels und die Nutzung der qualifizierten elektronischen Signatur ermöglicht werden. Dabei wird die Prüfung der Signatur durch die betraute Behörde verbindlich vorgeschrieben. Um einen elektronischen Identitätsnachweis zu erbringen soll das jeweilige (3) Fachverfahren an das Bürgerkonto angebunden werden, um diese Voraussetzung zu erfüllen. Eine Bundesbehörde muss weiterhin einen De-Mail-Dienste anbieten, wenn Zugang zum IT-Verfahren besteht.

Um dies zu gewährleisten sollten klare Standards für Schnittstellen definiert sein, damit Fachverfahrensherstellen hier systematisch und mit klaren Vorgaben agieren können. Dabei entstehen bei Fachverfahrensherstellern, kommunalen IT-Dienstleistern und Kommunen Aufwände. Hierfür ist eine Finanzierung zu planen und sicherzustellen.

De-Mail hat sich in Deutschland nicht durchgesetzt und sollte bald möglichst abgeschafft werden. Der Absatz (2) ist daher insofern zu ändern, als dass die Verpflichtung in eine Soll-Bestimmung umgewandelt wird, um jederzeit den DE-Mail-Dienst beenden zu können, zumal er eine Doppelstruktur zum Postfach im Bürger- und Unternehmenskonto des OZG darstellt.

§ 3 Information zu Behörden und über ihre Verfahren in öffentlich zugänglichen Netzen

Mit dem Föderalen Informationsmanagement (FIM) „werden zu neuen oder zu ändernden leistungsbegründenden Gesetzen und Verordnungen des Bundes allgemeine Leistungsinformationen nach einem festgelegten Standard zur Verfügung“ gestellt.

Das im Absatz (3) FIM nicht direkt benannt wird, ist zu begrüßen. Damit kann das erklärte Ziel im Rahmen der Innovationsoffenheit auch durch andere Entwicklungen erreicht werden. Dies halten wir vor allem deshalb für wichtig, weil FIM sich nicht einmal in den meisten Bundesländern so durchgesetzt hat, das dies benutzbar und verlässlich wäre. Die kommunale Ebene ist bei FIM kaum vertreten. Aus Sicht der Fachverfahren ist eine Doppel-Datenstruktur in Konkurrenz zu XöV-Standards eher behindernd für die Digitalisierung als fördernd. Entscheidend ist die digitale Kommunikation mit und zwischen Fachverfahren, die durch gemeinsam zu entwickelnde Standards gewährleistet wird. Das DIN-Whitepaper Normung und Standardisierung bei der Digitalisierung der öffentlichen Verwaltung vom 18.01.2023 bietet hier einen wichtigen Leitfaden.

§ 4 Elektronische Bezahlmöglichkeiten

Um Gebühren und Forderungen während des Verwaltungsaktes zu begleichen muss ein im Geschäftsverkehr übliches Zahlungsverfahren verfügbar sein.

Die Bezahlung muss einfach und sicher sein. Dafür sollten in der Wirtschaft und Finanzwelt etablierte Systeme anstatt einer Eigenentwicklung genutzt werden, um Nutzenden ihnen schon bekannte Zahlungswege barrierefrei zu ermöglichen (siehe hierzu ebenfalls § 9 und § 16). Wichtig ist dabei eine bundesweit einheitliche Bezahlplattform für alle Bundesländer.

§ 4a Elektronischer Rechnungsempfang; Verordnungsermächtigung

Papierrechnungen sollen zukünftig folgenlos zurückgewiesen werden können, wenn diese fälschlicherweise als solche anstatt einer verpflichtenden e-Rechnung versendet wurden.

Es ist konsequent auch die Papierrechnung weitestgehend abzulösen um medienbruchfreie Prozesse zu ermöglichen. Dies ist auch aus Umweltschutzgründen, mit der Reduktion des Papierverbrauchs, Einsparung von Transportemissionen und nicht zuletzt aus Gründen der finanziellen Einsparung zu begrüßen.

Jedoch erscheint es wenig praktikabel, dies von Bundesseite auch für Kommunalverwaltungen zu bestimmen, die überwiegend nicht in der Lage sind, elektronische Rechnungen zu empfangen und zu verarbeiten. Dies hätte für Lieferanten der Kommunalverwaltungen erhebliche negative Konsequenzen. Im Rahmen des Konnexitätsprinzips muss der Bund die Umstellungskosten auf digitale Rechnungen für die Kommunen tragen.

§ 5 Nachweisabrufe, Nachweiserbringung

Nachweiserbringung und -abruf soll zukünftig ebenfalls auf elektronischem Wege erfolgen. Dies kann in Sekundenschnelle und automatisch geschehen, wenn hierbei keine menschliche Interaktion notwendig ist. Neben der automatischen Bescheiderstellung durch die Behörde ist ebenfalls ein elektronischer Weg vom Antragsteller hin zur Behörde vorgesehen.

Eine regelbasierte automatische Bescheid- / Dokumente-Erstellung ist zu begrüßen. Die automatische Erstellung trägt dabei auch dem Once-Only-Gedanken Rechnung. Dies kann Verwaltungsakte beschleunigen (siehe hierzu ebenfalls die Begründung zu § 4). Weiterhin stellt hierbei auch die Registermodernisierung eine wichtige Grundlage dar, um durchgehend digitale medienbruchfreie Prozesse zu ermöglichen.

Bei der Registermodernisierung sollten daher schnellstmöglich Standards u.a. bei der IT-Architektur, bei den Schnittstellen und bei der Datenqualität gesetzt werden, um eine Interoperabilität zu ermöglichen. Weiterhin sind klare Vorgaben bei der Informationssicherheit und beim Datenschutz notwendig. Eine ausreichende dauerhafte Finanzierung auch für den Betrieb und Support muss sichergestellt werden. Dies ist notwendig um die Vorgaben der SDG-VO (EU) hinsichtlich dem Verfügbar machen von Daten im Sinne von Once-Only zu erfüllen.

Insgesamt erscheint allerdings die Regelung durch (1) 2 ausgehöhlt, da hier eine Möglichkeit zur Erfüllung durch digitale Einreichung des Nachweises durch Antragsteller eröffnet wird. Dies ist aber eben kein Once-Only und dient daher diesem Ziel nicht. Im Gegenteil können sich Behörden auf den Standpunkt stellen, ihre Pflicht mit der Bereitstellung eines Uploads erfüllt zu haben. Dies ist aber jetzt oft schon Status Quo und stellt daher keinen Fortschritt in Richtung Once-Only dar.

Die Regelungen in Absatz (4) sind zwar sinnvoll und vertrauensfördernd, jedoch erscheint der Ansatz, dass Antragsteller selbst die abgerufenen Daten kontrollieren, nicht sinnvoll. Oft werden Antragsteller dies nicht in Gänze beurteilen können. Wenn sie es können und die Informationen im Nachweis falsch sind, stellt sich die Frage wie dann verfahren werden soll? Hier muss es zwingend eine Meldefunktion geben, in der die Antragsteller eine Korrektur durchführen und an die nachweisliefernde Stelle senden können. Ansonsten würde die Situation dazu führen, dass Antragsteller ihren Antrag nicht stellen, oder ihn doch mit falschen Informationen stellen, nur um ihn absenden zu können.

§ 5a Grenzüberschreitende Nachweisabrufe

Um grenzüberschreitende Nachweisanrufe einer (1) zuständigen Behörde zu ermöglichen regelt § 5 die „Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten“. Dabei wird die (2) datenschutzrechtliche Rechtsgrundlage geschaffen auch automatisiert Nachweise abzurufen. Bei der Verarbeitung personenbezogener Daten können intermediäre Plattformen zum Einsatz kommen. Da die Registerstruktur in Deutschland vorwiegend dezentral aufgebaut ist eine Anbindung über intermediäre Plattformen angedacht.

Absatz (2) definiert, dass Behörden anderer Mitgliedsstaaten Nachweise bei deutschen Behörden abrufen können, sofern dieser Abruf notwendig und die abrufende Stelle zuständig ist. Wie soll eine Deutsche Behörde diese beiden Faktoren prüfen, bei Abruf von Daten aus dem EU-Ausland? Es müssen dazu zentrale EU-weite Register aufgebaut werden, welche genau diese Daten vorhalten, um eine Prüfung durch die nachweisgebende Stelle im Sinne dieses Gesetzes überhaupt möglich zu machen.

§ 9a Verwaltungsportal und Nutzerkonto des Bundes; Verordnungsermächtigung

Das Verwaltungsportal und das Nutzerkonto des Bundes werden „zur fachunabhängigen und fachübergreifenden Unterstützung der elektronischen Verwaltungstätigkeit der Behörden des Bundes zur Verfügung gestellt“. Mit den Ergänzungen sollen die Basisfunktionalitäten des Portals weiter präzisiert werden. Neben einer (1) Suchfunktion, sollen (2) ein elektronischer Identitätsnachweis über ein Nutzerkonto (inkl. Identifizierung), (3) Online-Formulare für die elektronische Beantragung und Abwicklung, (4) ein sicher elektronischer Übermittlungsweg und ein im (5) Geschäftsverkehr übliches Zahlungsverfahren verfügbar sein.

Diese Basisfunktionalitäten sind elementar und werden zur Nutzung der Verwaltungsleistung und Kommunikation mit den Bürger:innen benötigt. Die Funktionalitäten sollten benutzerfreundlich implementiert sein und sich beim Komfort an zeitgemäßen professionellen Nutzerportalen in der Geschäftswelt orientieren, um den Nutzenden eine professionelle und angenehme Abwicklung seiner Verwaltungsakte zu ermöglichen.

Die Erweiterung in Absatz (3) Satz 3 geht jedoch zu weit. Eine Abwicklung von Verwaltungsverfahren beinhaltet ein Verwaltungshandeln mit Übermittlung eines Ergebnisses, das jedoch nicht vollständig in ein Formular integriert werden kann. Die Beibringung von Nachweisen dagegen ist kein Verwaltungsverfahren selbst, sondern eine begleitende Pflicht des Antragstellers innerhalb eines Antragsverfahrens. Vollständige Antragsverfahren in einem einzigen Online-Formular sind daher weder sinnvoll noch möglich. Diese Erweiterung sollte daher gestrichen werden.

§ 9b Verarbeitung personenbezogener Daten im Verwaltungsportal des Bundes

Mit der Neufassung des § 9b soll die Datenverarbeitung im Bundesportal im Ganzen erfasst werden, um einen nutzerfreundlichen Gesamtprozess zu ermöglichen. Dies beinhaltet überhaupt die Möglichkeit im Verwaltungsportal (1) personenbezogene Daten (auch besondere Kategorien) zu verarbeiten und dies auch über einen (2) flexibel gestaltbaren Zeitraum auch (4) portalübergreifend zwischenzuspeichern. Eine (3) Löschung der zwischengespeicherten Verfahrensdaten ist erst nach 30 Tagen nach der letzten Bearbeitung des Nutzenden vorgesehen. Der Nutzer soll frühzeitig über eine Löschung informiert werden. Darüber hinaus ist eine längerfristige Speicherung von zwischengespeicherten Verfahrensdaten zur Erfüllung der vom „Verwaltungsportal des Bundes erfassten Zwecke“ möglich.

In den Absätzen (1) und (2) wird die längere Speichermöglichkeit von Verfahrensdaten eingeräumt. Dies erscheint vordergründig sinnvoll, um Anträge speichern und später weiter bearbeiten zu können. Jedoch entstehen im Rahmen des EfA-Prinzips an ganz vielen Stellen im Netz bei den EfA-Providern Datenbestände mit hochsensiblen Daten. Dies wird und kann den Nutzenden nicht bewusst sein, so dass zumindest transparent darauf hingewiesen werde muss, wo und bei wem diese Daten gespeichert werden. Durch diese Datenkopien entstehen daneben zusätzlichen Risiken durch Angriffe auf diese jeweils sehr unterschiedlich gesicherten Systeme.

In der Begründung auf Seite 27 / 1. Zeile / 3. Spalte / Satz 4 wird im Kommentar die Möglichkeit einer früheren Löschung erwähnt aber nicht präzisiert. Dies steht im Widerspruch mit der unter (3) erwähnten 30 Tagesfrist der Aufbewahrung, da technisch nicht erkennbar ist ob die Antragstellung nicht zu einem späteren Zeitpunkt fortgesetzt wird. Es sollte ergänzt werden, in welchen Fällen und wann eine frühere Löschung

getätigt wird. Eine Lösung wäre die Funktion „Speichern um zu einem späteren Zeitpunkt die Eintragung fortzusetzen“ die durch den Nutzenden ausgelöst werden könnte. Im anderen Fall könnten die Daten automatisch beim Beenden der Session gelöscht werden.

In Absatz (3) heißt es: „Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass die jeweils zuständige Behörde nicht auf die zwischengespeicherten Verfahrensdaten zugreifen kann.“

Wie soll eine Behörde einen Antrag bearbeiten, wenn kein Zugriff möglich ist? Diese Regelung muss dringend präzisiert und auf die Behörde oder den Dienstleister des jeweiligen Online-Dienstes bezogen werden.

§ 9c Datenschutzrechtliche Verantwortlichkeit

In § 9c wird unter (1) der „jeweils zuständigen Behörde des Bundes“ die datenschutzrechtliche Verantwortlichkeit für die Verarbeitung personenbezogener Daten im Verwaltungsportal des Bundes zugewiesen. Der für das „Verwaltungsportal des Bundes zuständige öffentliche Stelle“ ist lediglich die Rolle des Auftragsverarbeiter zugewiesen. Unter (2) führt die Verarbeitung personenbezogener Daten die „für das Verwaltungsportal des Bundes zuständige öffentliche Stelle“ (…) ausschließlich in „eigener datenschutzrechtlicher Verantwortlichkeit aus“.

Die jeweils datenschutzrechtliche Verantwortung muss transparent bei jeder Online-Dienstleistung für Nutzende angezeigt werden und nicht wie üblich an zentraler Stelle des Portals, da diese bei jeder Online-Dienstleistung im Rahmen des EfA-Prinzips unterschiedlich sei kann. Dabei müssen alle datenschutzrechtlich verantwortlichen Stellen des gesamten Prozesses offengelegt werden.

§ 16 Barrierefreiheit und Nutzerorientierung

Die Barrierefreiheit wird um die Fokussierung auf die Nutzerorientierung erweitert und ist an die UN-Behindertenrechtskonvention angelehnt. Der Bund hat bei der eGovernment-Gesetzgebung zudem verbindliche Standards einzuhalten.

Einfachheit und Verständlichkeit sind der Schlüssel, damit digitale Verwaltungsleistungen auch genutzt werden. Leistungen müssen allgemein verständlich sein. Barrierefreiheit und Nutzerorientierung sind elementare Eigenschaften und daher zu begrüßen. Allerdings erscheint die Einschränkung nur auf die Angebote des Bundes als nicht sinnvoll, da Angebote aller föderalen Ebenen in einem Portal zusammengefasst werden sollen. Damit entsteht ein bunter Mix aus mehr oder weniger barrierefreien Angeboten,

was für Außenstehende nicht nachvollziehbar ist. Außerdem erscheint die Fokussierung auf eine bestimmte Gesetzesversion (BITV2.0) nicht zielführend. Dies sollte allgemeiner formuliert werden „..es gelten die jeweils aktuellsten gesetzlichen Regelungen des Bundes und der EU…“.