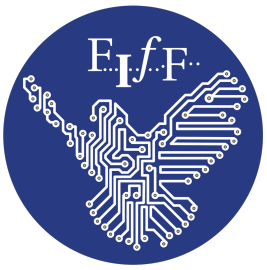
Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)614 C



Forum InformatikerInnen
für Frieden
und gesellschaftliche
Verantwortung e. V.

Über die Digitalisierung von Verwaltungsverfahren und Pfadabhängigkeiten

Sachverständigenauskunft zum Gesetzentwurf der Bundesregierung zur **Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen** – Drucksache 19/21987 – inklusive dem Änderungsantrag der Fraktionen der CDU/CSU und der SPD im Innenausschuss des Deutschen Bundestages.

Dipl. Inf. Rainer Rehak (CC BY) für das FIfF
rainer.rehak@fiff.de
0D66 63E5 70A3 964A EE60D927 4427 CFE5 8C19 AE19

Donnerstag, 29.10.2020
Version 1.3

Inhaltsverzeichnis

0 Zusammenfassung

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung nimmt gern zum vorliegenden Gesetzesentwurf (DS 19/21987) inklusive Änderungsantrag (19(4)587) Stellung. Die Bestrebungen, jegliche Verwaltungsleistungen neben anderen Wegen auch digital und online anzubieten, sind auch aus unserer Ansicht grundsätzlich zu befürworten. Jedoch kritisieren wir die folgenden Punkte, die sich auf die angelegten Funktionen, geplante technische Umsetzung und spezielle Datenschutzfragen beziehen. Im Dokument selbst finden sich jeweils Vorschläge, wie der Kritik von der Gesetzgeberïn konstruktiv begegnet werden kann.

Folgende Kernkritikpunkte werden in dieser Stellungnahme behandelt:

- Die Schaffung einer isolierten Behördeninsel, die nach außen hin – auch den Bürgerïnnen gegenüber – abgeschottet ist und innerhalb der Verwaltung zwischen den Behörden keinerlei Beschränkungen unterliegt, ist mindestens aus Datenschutz-, IT-Sicherheits- und Interoperabilitätsgesichtspunkten hochproblematisch.
- Sichere Kommunikation zwischen Bürgerïnnen und Behörden ist auch mit den neuen Postfächern nicht möglich, sie sind Einbahnstraßen behördlicher Kommunikation und nicht abgesichert, wegen der auch schon bei De-Mail fatalen „Zustellfiktion“ wenig attraktiv und nur umständlich nutzbar.
- Interoperabilität wurde an vielen Stellen ignoriert. Weder beim Abruf der Postfächer noch bei der Spezifikation der Postfächerfunktionen wurde auf bewährte Standards gesetzt (IMAP, eDelivery etc.), die eine Ver-

bindung mit anderen Systemen, etwa mit EU-Behörden, der Verwaltung anderer Länder oder den Systemen der Bürgerïnnen grundsätzlich ermöglicht hätte.

- Die Nutzung eines eindeutigen Personenkennzeichens beispielsweise der Steuer-Identifikationsnummer (StID) wird unserer Ansicht nach implizit vorausgesetzt, mindestens aber nicht explizit abgelehnt. Da bereichsspezifische Kennzeichen die gleiche Funktionalität erlauben, sind diese grundsätzlich zu verwenden und eindeutige Personenkennzeichen abzulehnen. Dies ist auch aus Akzeptanzgründen der zu wählende Weg.
- Im Entwurf fehlt ein zentrales Element von E-Government: eine qualifizierte elektronische Signatur (QES) etwa zur Signierung von Dokumenten sowohl durch Behörden und Bürgerïnnen, mit welcher signierte Nachrichten oder Urkunden etc. digital ausgestellt werden könnten.

Auch wenn die Gewährung von Familienleistungen nur ein erster Schritt bei der Digitalisierung von Verwaltungsverfahren ist, so werden hier dennoch Grundlagen auch für weitere Leistungen gelegt. Nötig ist hier – im Gegensatz zum aktuellen Entwurf – eine langfristige Planung und Perspektive, sonst stellen sich die oben angerissenen Fragen und Probleme in ein paar Jahren wieder, dann aber mit bereits geschaffenen Tatsachen, die im Wege stehen. Noch kann der Kurs korrigiert werden und sollte dies auch.

1 Einleitung

Die Bestrebungen, jegliche Verwaltungsleistungen neben anderen Wegen auch digital und online anzubieten, sind auch unserer Ansicht nach grundsätzlich zu befürworten. Dabei ist besonders die konkrete Zielstellung, dass „die Papierformulare aber nicht einfach nur in eine digitale Form gebracht und auf elektronischem Wege an die Behörde gesendet werden, sondern die Potenziale der Digitalisierung für die Abwicklung der Verwaltungsprozesse gehoben werden“ sollen, hervorzuheben und sehr zu begrüßen. Allein das Once-Only-Prinzip, nachdem bestimmte Grundinformationen nicht mehr jedes Mal erneut an Behörden und Verwaltungen mitgeteilt werden müssen, verspricht eine enorme Erleichterung bei allen Behördeninteraktionen.

Demnach ist der Gegenstand dieses Gutachtens nicht die defensive Frage nach dem *Ob*, sondern die gestalterische Frage nach dem *Wie* einer solchen digitalen Transformation. Ein derartiges Vorhaben kann dabei viele Vorteile für die Verwaltung selbst und vor allem für die Bürgerïnnen und Organisationen bedeuten.

Besonderer Dank gilt Kirsten Bock, Markus Drenger, Constanze Kurz und Heidi Rehak für den wertvollen Austausch und hilfreiche Hinweise.

2 Kritische Analyse

Leider fällt die konkrete Ausgestaltung des digitalen Angebots von Familienleistungen, so wie sie im Gesetz inklusive Änderungsantrag angelegt sind, nicht nur weit hinter die zuvor ausgegebene Losung zurück, sondern erzeugt zusätzlich gravierende Probleme hinsichtlich Datenschutzfragen beim E-Government sowie bezüglich der perspektivischen Weiterentwicklung und Interoperabilität digitaler Verwaltungssysteme.

Entgegen den Beteuerungen von Bürgerïnnenfreundlichkeit und Hebung digitaler Potenziale ist das vorgesehene System Ergebnis einer speziellen Verwaltungsdenkweise, in der die Antragstellerïnnen zwar von außen ein monolithisches System in Gang setzen können, jedoch ab diesem Moment keinerlei Einsichts-, Interaktions- oder gar Interventionsmöglichkeiten mehr besitzen, während sich die inneren Elemente des Systems wiederum gegenseitig blind vertrauen.

Ebenfalls stark kritikwürdig erscheint uns der Ansatz, die ursprünglich nur für die Steuerübermittlung gedachten ELSTER-Zertifikate für die Authentifizierung von Organisationen am Portalverbund (PV) zweckzuentfremden. Ein System mit derartig schwachen Sicherheitseigenschaften wie etwa einem Zwei-Faktor-Mechanismus basierend auf der Zertifikatsdatei und einer PIN taugt nicht (auch nicht provisorisch) als organisationale Authentifizierung für jegliche staatliche Leistungen.

Zuletzt sei an dieser Stelle auch eine parlamentarische Prozesskritik erlaubt. Einerseits ist das zentrale Funktionselement der Postfächer erst im Änderungsantrag zu finden, andererseits umfasst der vorgelegte Entwurf auch diverse tiefgreifende Änderungen am Online-Zugangs-Gesetz (OZG). Dadurch wird offensichtlich, dass hier weder thematisch umsichtig noch gesetzgeberisch systematisch vorgegangen worden ist, was gerade bei der Planung von (digitalen) Infrastrukturen – also der Erzeugung enormer Pfadabhängigkeiten – dringend geboten wäre.

2.1 Eine deutsche Verwaltungsinsel

Mit dem vorliegenden Entwurf wird eine riesige deutsche Verwaltungsinsel geschaffen, die weder aus Datenschutz- noch aus IT-Sicherheitssicht nötig oder sinnvoll ist. Alle Behörden im Verbund vertrauen einander blind und der PV etwa kann technisch gesehen beliebig auf alle anderen Behörden zugreifen. Diese sogenannte Perimeter-Denkweise – ähnlich einer Burg – geht also von einer riesigen, inneren Verwaltungs-Vertrauens-Community aus, die nur nach „außen“ hin geschützt werden muss. Nichts innerhalb dieser Burg wird kryptographisch abgesichert. Es ist daher beispielsweise zu keiner Zeit zuverlässig belegbar, ob eine Nutzerïn einen bestimmten Abfrage- oder Verwal-

tungsprozess angestoßen hat oder nicht.[1] Es existieren weder Transparenz- noch Kontrollfähigkeit der Verfahren auf Daten-, System- und Prozess-Ebene. Externe Audits sind daher ebenfalls nicht möglich.

Zusätzlich ist der aktuelle Entwurf nur dann sinnvoll umsetzbar, wenn ein zentrales einheitliches Identifikationsmerkmal über alle Behörden hinweg zum Einsatz kommt. Im Kontext der aktuellen politischen Bestrebungen des Bundesministeriums des Innern, für Bau und Heimat, anhand des Registermodernisierungsgesetzes deutschlandweit die Steuer-Identifikationsnummer (StID) als zentrales Personenkennzeichen zu etablieren, ist es einfach, Eins und Eins zusammenzuzählen. Dies umso mehr, als die eindeutigen Personenkennzeichen durch den Entwurf nicht ausgeschlossen werden.

Jedoch ist diese zentralisierte Herangehensweise einerseits technisch nicht nötig und daher aus Datenschutzgründen dringend zu verhindern, auch wenn ein partitioniertes System minimal anspruchsvoller ist. Andererseits ist diese StID-basierte Herangehensweise aufgrund handfester[2] und breiter[3] grundsätzlicher verfassungsrechtlicher Zweifel bezüglich zentraler Personenkennzeichen auch strategisch und systemplanerisch eine schlechte Idee.

Zusätzlich wurde auch die Interoperabilität außer Acht gelassen. Weder europäische Vertrauensdienste noch die europäische eDelivery-Architektur sind hier berücksichtigt worden. Statt die bereits geschaffenen Rechtsgrundlagen (z.B. eIDAS-Verordnung) und die bereits bestehenden IT-Systeme und Dienste im Sinne einer nachhaltigen IT-Governance-Strategie wiederzuverwenden, werden künstlicher Mehraufwand für die Verwaltung und zusätzliche Belastungen für die Zivilgesellschaft und die Wirtschaft geschaffen.

Das Ziel, einer Vereinfachung von deutschen Behördenabläufen für die deutsche Behörden, wird unnötig umständlich verfolgt. Die Verwaltungsprozesse wurden ausschließlich mit Blick auf die deutsche Verwaltung digitalisiert.

2.2 Postfächer

Die Funktionalität sogenannter Postfächer zur sicheren digitalen Kommunikation zwischen Bürgerïnnen, Organisationen und Behörden sind eine großartige Idee. Dabei liegt die Betonung auf *Sicherheit* im Sinne von authentifiziert, vertraulich und integer, denn unzulängliche Kommunikationskanäle sind mit gewöhnlicher E-Mail oder Fax schon länger verfügbar. Der vorliegende Ent-

1 Es sei an die diversen politisch motivierten Abfragen aus polizeilichen Datenbanken erinnert.
2 https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/21_Registermodernisierung.html
3 https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/DSK-Entschlie%C3%9Fung-Registermodernisierung-2020.pdf, https://gi.de/fileadmin/GI/Allgemein/PDF/2020-09-04_GI-Stellungnahme_zum_Registermodernisierungsgesetz.pdf oder http://www.humanistische-union.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/stellungnahme-registermodernisierungsgesetz/

wurf der Postfächer leistet jedoch genau diese Verbesserung nicht und ist daher eine Fehlkonstruktion. Dass die Idee erst im Änderungsantrag aufgegriffen wird, kann als Indiz dafür gelten, mit welch heißer Nadel hier gestrickt worden ist.

Die Idee ist ja auch nicht neu und ist mit der europäischen eDelivery-Architektur sowohl rechtlich durch die eIDAS-Verordnung[4] als auch technisch bereits realisiert. Es würde daher völlig ausreichen, eine zustellfähige elektronische Anschrift bei einem Verwaltungsvorgang zu hinterlegen. Und etwas weitergedacht wäre auch die Nutzung von Zustelldiensten nicht in jedem Fall notwendig, etwa, wenn für die Nutzerinnen und Nutzer ein Anreiz besteht, den Empfang einer Nachricht rechtswirksam und einfach zu bestätigen.

Dabei ist die genaue Funktion der Postfächer gar nicht spezifiziert. Wichtige Vorgaben für den Funktionsumfang oder etwa die notwendige Verfügbarkeit der Dienste wurden in dem Antrag nicht formuliert. Somit ist auch nicht verlässlich ersichtlich, welche Eigenschaften beabsichtigt sind. Ohne verlässlichen Kommunikationsweg ist aber keine Antwort- und damit Steuerungs- oder Widerspruchsmöglichkeit für die Nutzerïnnen gegeben. Insoweit bringt das Postfach keinen Gewinn über „gescannte PDFs“ hinaus gegenüber einem analogen Briefkasten.

Zusätzlich sind auch die Abrufmöglichkeiten nicht geregelt. Es werden keine Standards verlangt und keine Eigenschaften ausgeschlossen. Kann das Postfach nur per Web abgerufen werden oder auch per Mail-Client (IMAP), können kryptographische Schlüssel einer eigenen Public-Key-Infrastructure (PKI) verwendet werden oder wird es dazu staatliche Angebote geben? Nichts davon wird expliziert und es ist zu befürchten, dass inkompatibler Wildwuchs die vorprogrammierte Folge ist. Aktuell schon vorhandene Implementationen etwa in Baden-Württemberg bestehen aus einer einfachen Webseite, wo beispielsweise PDFs heruntergeladen werden können. Weder gibt es eine Absicherung der Dokumentenechtheit noch einen kommunikativen Rückkanal. Das „Postfach“ befindet sich demnach in der Hoheit der Verwaltung, und Änderungen an liegenden Dokumenten – bei fehlerhaften Bescheiden bzw. „Korrekturen“ – sind seitens der Verwaltung technisch gesehen ohne weiteres möglich und für die Nutzerïnnen nicht belegbar. Dadurch entsteht ein Graubereich bei der Bekanntgabe von Verwaltungsakten.

Ein weiteres wesentliches Konstruktionsproblem ist die sogenannte „Zustellfiktion“, nach der ins Postfach gestellte Dokumente automatisch als rechtlich „zugestellt“ gelten, also verwaltungslogische Mechanismen in Gang setzen, Fristen beginnen und Rechtsfolgen greifen lassen. Diese Eigenschaft ver-

4 EU-Verordnung 910/2014 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02014R0910-20140917&from=EN

pflichtet die Nutzerïnnen praktisch, regelmäßig nach neuen Dokumenteneingängen zu schauen. Dies war schon eine der Ursachen für die fehlende Akzeptanz und letztendlich des Scheiterns des eigentlich von der Idee her sinnvollen De-Mail-Systems.

Im vorliegenden Vorschlag werden nicht einmal Anforderungen an die Verschlüsselung definiert. Denn ob jede Behörde einen digitalen Brief direkt zustellen kann oder ob es eine zentrale Stelle gibt, die jeden ein- und ausgehenden Brief lesen und überwachen kann, ist von wesentlicher Bedeutung. An dieser Stelle holen den Gesetzgeber die Fehler der Vergangenheit wieder ein: Es wurde keine Infrastruktur für einen flächendeckenden Schlüsselaustausch mit der Zivilgesellschaft oder der Wirtschaft etabliert. Weder über die neuen Personalausweise noch über die oft im Kontext der eGovG-Reform geforderten sekundären Identitäten, etwa GPG-Schlüssel oder Anwendungen auf Basis von SIM-Karten in Mobiltelefonen.

Da nicht einmal im Gesetz geregelt ist, wie viele Postfächer eine Nutzerïn haben kann oder muss – denn denkbar sind ja verschiedene Postfächer in verschiedenen Bundesländern – ergibt sich folglich eine Pflicht, alle Postfächer regelmäßig abzurufen, im schlimmsten Falle via umständlichem Web-Login.

Zusätzlich sei noch angemerkt, dass die Ergebnisse von Verwaltungsprozessen dieses digitalen Systems – also etwa Bescheide oder Dokumente, die dann als PDF im Postfach vorliegen – nach bisheriger Planung nicht kryptographisch signiert vorliegen, also auch keinerlei tragbare Basis für eine digitale Verwaltungslandschaft darstellen. Wirklich belegt werden kann mit solchen ungesicherten Dateien nichts. Ein digitaler Urkundenversand etwa ist nicht möglich und Verantwortlichkeiten sind ebenfalls nicht nachvollziehbar.

Zuletzt zeigt sich auch an den Postfächern, dass das System ohne einen Gedanken an Interoperabilität konzipiert worden ist. Weder sind die Postfächer für die Behörden anderer Länder noch für EU-Stellen nutzbar.

2.3 Datenschutz und Einwilligung

Aktuell ist für die Datenverarbeitung die datenschutzrechtliche Rechtsgrundlage der Einwilligung vorgesehen, wobei eine Einwilligung Freiwilligkeit voraussetzt. Freiwilligkeit bei Verwaltungsdienstleistungen jedoch setzt voraus, dass diese im Bereich der Leistungsverwaltung erfolgt und durch die Ablehnung der Bürgerïn keine Nachteile entstehen oder sie von den Angeboten der Verwaltung ausgeschlossen wird.[5]

Da einer der wesentlichen Gründe für Digitalisierung von Verwaltungsverfahren die für die Nutzerïnnen enorme Zeitersparnis ist, grenzt es schon an Zy-

5 Bock, Kirsten: in Specht/Manz (Hg.) Handbuch europäisches und deutsches Datenschutzrecht, S. 570f.

nismus von Freiwilligkeit zu sprechen. Um diesen Aspekt deutlich zu machen, bedarf es nicht einmal des alleinerziehenden Elternteils in ständiger Zeitnot, auch Familien mit vielen Schultern werden dankbar jede Vereinfachung annehmen. Von echter Freiwilligkeit sollte hier nicht gesprochen werden.

Zusätzlich ist die Einwilligung üblicherweise gegenüber der Verantwortlichen der Datenverarbeitung zu erteilen, also der jeweiligen Behörde, die jedoch im Zweifelsfall und verständlicherweise ihre eigenen organisationalen Interessen verfolgt. Sehr viel besser für alle Betroffenen wäre es also, der Gesetzgeberïn die Gestaltung der Datenverarbeitung zu überlassen und als Rechtsgrundlage ein Gesetz zu verwenden, das auch die Zweckbindung der Datenverarbeitung klar definiert.

Weiterhin ist es nicht geplant, Nutzerïnnen differenzierte Freigabemöglichkeiten konkreter Informationen, Dokumente oder Anträge an die Hand zu geben oder auch Verarbeitungsprozesse transparent zu verfolgen. Nutzerïnnen haben also weder Einsicht noch Kontrolle im Sinne echter Interventionsmöglichkeiten. Statt der Hebung der digitalen Potenziale echter Handlungsoptionen und Verwaltungstransparenz wird aus der analogen einfach eine vielfach komplexere digitale Verwaltungs-Black-Box.

So etwas wie „digitale Souveränität“ wird nicht realisiert, weil die Kontrollfähigkeit weder auf Daten-, noch System- und Prozess-Ebene gewährleistet wird. Eine Umsetzung der Datenschutz-Schutzziele – u. a. Transparenz, Nichtverkettbarkeit und Intervenierbarkeit – sähe radikal anders aus.

2.4 IT-Sicherheit

Laut Gesetzesentwurf sollte das Bundesministeriums des Innern, für Bau und Heimat spezielle Anforderungen an die IT-Sicherheit des PV und verbundener Systeme formulieren, was bislang nicht erfolgte. Da einige der beschriebenen Systeme bereits in Betrieb sind – als Nutzerïnnenkonto gelten etwa die schon existierenden Service-Konten bestimmter Bundesländer wie Berlin oder Baden-Württemberg – ist der sinnvolle Zeitpunkt für umzusetzende Anforderungen längst verstrichen. In der Konsequenz sind die öffentlichen Stellen ohne spezielle und vor allem ohne koordinierte Sicherheitseigenschaften direkt ans Internet angebunden. Angesichts der mehr oder weniger Deutschland-einheitlichen Nutzung einer bestimmten Software-Suite ist das entstehende Verwaltungskonglomerat entweder zur Gänze sicher oder gänzlich verwundbar. Aufgrund der schon etwas betagten java-basierten Softwaregrundlage ist wahrscheinlich leider letzeres der Fall, weshalb das Bundesministeriums des Innern, für Bau und Heimat mindestens hinsichtlich IT-Sicherheits-Maßgaben dringend nachziehen muss.

3 Verbesserungsvorschläge

Da auch wir der Ansicht sind, das die Digitalisierung von Verwaltungsleistungen sinnvoll sein kann, folgen einige kurze Ausführungen, um auf Basis der oben geäußerten Kritik zu einem konstruktiven Dialog beizutragen und somit den Digitalisierungsprozess langfristig sinnvoll mitzugestalten.

3.1 Verteiltes System

Das sogenannte Once-Only-Prinzip der EU ist für Bürgerïnnen praktisch im Sinne der einfachen Nutzbarkeit von Verwaltungsdiensten, eine datenschutzfreundliche Ausgestaltung[6] der Dienste ist gut und sogar notwendig für Bürgerïnnen, Organisationen und die Gesellschaft als Ganzes. Im Sinne einer informationellen Gewaltenteilung[7] etwa darf ein solches digitales Verwaltungssystem die jeweils nötigen Daten nicht anhand von national eindeutigen Personenkennzeichen zusammenführen, ist schon die Existenz eindeutiger Personenkennzeichen aus Datenschutzsicht ein fundamentales Problem. Denn im Datenschutz (im Gegensatz zur IT-Sicherheit) geht die primäre Gefahr immer von der Verarbeiterïn selbst aus – in diesem Falle von der Verwaltung –, und diese Gefahr vergrößert sich immens mit der Existenz eines eindeutigen Personenkennzeichens, welches die Verkettung unterschiedlichster Datensätze ermöglicht. Die gleiche Funktionalität kann jedoch (und muss daher auch) dezentralisiert mit bereichsspezifischen Kennzeichen umgesetzt werden. Nur so kann die datenschutzrechtliche Anforderung der Zweckbindung zweifelsfrei umgesetzt werden. Dann sind das Once-Only-Prinzip und Datenschutzfreundlichkeit keine Gegensätze.

Gemäß eines datenschutzfreundlichen Ablaufs würden sich die Nutzerïnnen im PV mithilfe eines eIDAS-Vertrauensdienstes anmelden und könnten anhand ihrer bereichsspezifischen Kennzeichen verschiedener Behörden diese diversen „Behördenkonten“ virtuell zusammenzuführen. Separate „Servicekonten“ wären dafür nicht notwendig. Sogleich könnte der PV rein vorgangsbezogen die nötigen Daten zusammenziehen, Verwaltungsabläufe in Gang setzen und die (Zwischen-)Ergebnisse ins Postfach leiten. Die Zusammenführung der bereichsspezifischen Kennzeichen über das PV-Konto kann jederzeit wieder aufgelöst werden. Die verschiedenen Behörden wären in dieser Ausgestaltung ganz absichtlich nicht in der Lage, von sich aus diverse Datensätze zusammenzuführen. Dies entspricht einer Beschränkung des technisch Möglichen zur Einhegung der Macht der Verwaltung auf das nötige Maß zum Schutze der

6 Pohle, J. (2018): *Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung*. Berlin, Germany: Humboldt-Universität zu Berlin. DOI: 10.18452/19136

7 Podlech, Adalbert (1976): »Die Trennung von politischer, technischer und fachlicher Verantwortung in EDV-unterstützten Informationssystemen«. In: Informationsrecht und Informationspolitik. Hrsg. von Wilhelm Steinmüller. Rechtstheorie und Informationsrecht. München: Oldenbourg Verlag, S. 207–216.

Betroffenen und der Aufrechterhaltung der (informationellen) Gewaltenteilung.

Die Etablierung einer dauerhaften „Clearingstelle“ etwa nach österreichischem Vorbild, die in ganz bestimmten Fällen die bereichsspezifischen Kennzeichen miteinander in Beziehung setzen kann, wäre zumindest für die soeben skizzierte Herangehensweise gar nicht nötig.

3.2 Sichere Kommunikation zwischen Bürgerïnnen und Behörden

Eines der Kernelemente einer digitalen Verwaltung ist die sichere Kommunikation zwischen Bürgerïnnen, Organisationen und Behörden. Es geht also um einen vertrauenswürdigen, authentifizierten, abgesicherten und zuverlässigen Kommunikationskanal zwischen den Beteiligten. Dafür wären die Postfächer der Nutzerïnnenkontos beim PV eine ideale Möglichkeit. Dazu könnte der EU-Standard „eDelivery“[8] herangezogen werden, der nach dem 4-Säulen-Modell funktioniert, also verschiedene Provider vorsieht, die miteinander Daten austauschen können. Der eDelivery-Standard ermöglicht dabei ganz bestimmte Dienstmerkmale durch technische Spezifikationen und Standards, installierbare Software und zusätzliche Services, um auf diese Weise interoperabel zu sein. Dies betrifft die Kommunikation zwischen Bürgerïnnen, Organisationen und Behörden, aber auch zwischen Behörden untereinander oder gar mit Behörden oder Organisationen anderer EU-Länder oder mit den EU-Institutionen.

Doch damit Nutzerïnnen den Postfach-Service auch annehmen, ist es nötig, Anreize zu schaffen und Hindernisse abzubauen. Die „Zustellfiktion“, nach der Dokumente im Postfach automatisch als „zugestellt“ gelten, also verwaltungslogische Mechanismen in Gang setzen, Fristen beginnen und Rechtsfolgen greifen lassen, hat schon beim De-Mail-Projekt die Akzeptanz enorm sinken lassen, wenn nicht sogar sein Scheitern (mit-)verursacht. Dieser Fehler sollte hier nicht wiederholt werden. Denkbar wäre beispielsweise eine Regelung, nach der nach einer gewissen Zeit des Nichtabrufs ein (traditioneller) postalischer Versand ausgelöst wird.

Wichtig ist zusätzlich, dass es nicht mehrere Postfächer im PV geben kann, obwohl Nutzerïnnen sich mit verschiedenen Servicekonten anmelden können. Mindestens aber müssten Postfächer nutzerïnnenfreundlich verbunden bzw. automatisiert abrufbar sein, bestenfalls über etablierte Standards.

Abschließend sei unterstrichen, dass Postfächer eine beidseitige Kommunikation erlauben müssen. Ein reiner Dokumentenabruf ist weder interoperabel noch zukunftsfähig.

8 https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery

3.3 Gesetzliche Regelung statt Einwilligung

Die datenschutzrechtliche Einwilligung ist von einer freiwilligen Nutzung (Zustimmung) zu unterscheiden. Die datenschutzrechtliche Einwilligung bezieht sich auf eine Datenverarbeitung zu bestimmten Zwecken, über die vorab ausreichend zu informieren ist. Bei einer freiwilligen Nutzung hingegen werden die Datenverarbeitung und die Zwecke der Verarbeitung gesetzlich geregelt, nicht wie im Falle der Einwilligung von der Verwaltung.

Da es im vorliegenden Falle verwaltungsseitig weder technisch noch inhaltlich Spielräume geben sollte, sind die Bedingungen der Datenverarbeitung hier gesetzlich zu regeln. Ausgehend vom Rechtsstaatsgebot ist es nicht akzeptabel, dass sich Datenverarbeitung der Verwaltung auf die unsichere Rechtsgrundlage einer datenschutzrechtlichen Einwilligung stützen muss, die jederzeit widerrufen werden kann oder gar mangels ausreichender oder versäumter Information unwirksam erfolgt.

3.4 Qualifizierte Elektronische Signatur (QES)

Es muss dringend eine staatliche anerkannte digitale Signatur-Infrastruktur (wieder) erschaffen werden, mit der kryptographisch abgesichert die Urheberschaft und Integrität von digitalen Dokumenten oder Nachrichten bewiesen werden kann. Ist diese funktionsbereit, so können Nutzerïnnen Aufträge und Anfragen signieren, Behörden ihre Dokumente und Antworten, sogar Urkunden und Belege könnten digital ausgestellt werden.

Der neue Personalausweis (nPA) erlaubte diese Funktionalität der qualifizierten elektronische Signatur (QES), doch sie müsste wiederbelebt und nach nunmehr 13 Jahren vielleicht aktualisiert und angepasst werden. Ebenfalls müsste eine Lösung für Organisationen wie Firmen, Verbände und Behörden erdacht werden. Das ELSTER-System wäre auch hier ein Provisorium und übers Knie gebrochen.

Diese Ausgestaltung bräuchte gegebenenfalls etwas Vorlauf, aber brächte dann wirklich einen Mehrwert in der Digitalisierung der Verwaltung – konkret und perspektivisch.

4 Fazit und Abschluss

Am konkreten Fall der Familienleistungen soll der mit dem Online-Zugangs-Gesetz (OZG) im Jahre 2017 gesteckte Rahmen für digitale Verwaltungsabläufe nun mit Leben gefüllt werden. Anstatt jedoch mit den Kernfunktionen modernen E-Governments die Grundlage für alle Services zu legen, wird auf Dokumentenebene analoges Verwalten verbessert. Die zwei Kernfunktionen – also die sichere Kommunikation zwischen Bürgerïnnen und Behörden einer-

seits und die qualifizierte elektronische Signatur von Dokumenten (QES) andererseits – sind mit den im Gesetzesentwurf vorgeschlagenen Ansätzen weder geplant noch möglich.

Mit der im Entwurf praktizierten überpragmatischen Herangehensweise werden jedoch technische Pfadabhängigkeiten betoniert, die mittel- und langfristig wirklich gute digitale Lösungen enorm erschweren und zudem datenschutzfreundliche Wege versperren. Wie heißt es so treffend: „Nichts hält länger als ein Provisorium“. Dieser Fehler sollte vermieden werden, besonders beim Fundament.

5 Über das FIfF

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. ist ein deutschlandweiter Zusammenschluss von Menschen, die sich kritisch mit Auswirkungen des Einsatzes der Informatik und Informationstechnik auf die Gesellschaft auseinandersetzen. Unsere Mitglieder arbeiten überwiegend in informatiknahen Berufen, vom IT-Systemelektroniker bis hin zur Professorin für Theoretische Informatik. Das FIfF wirkt in vielen technischen und nichttechnischen Bereichen der Gesellschaft auf einen gesellschaftlich reflektierten Einsatz von informationstechnischen Systemen zum Wohle der Gesellschaft hin. Zu unseren Aufgaben zählen wir Öffentlichkeitsarbeit sowie Beratung und das Erarbeiten fachlicher Studien. Zudem gibt das FIfF vierteljährlich die „FifF-Kommunikation – Zeitschrift für Informatik und Gesellschaft“ heraus und arbeitet mit anderen Friedens- sowie Bürgerrechtsorganisationen zusammen.

https://www.fiff.de/about