Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss für Digitales

Ausschussdrucksache
20(23)55

Bonn, den 25.06.2022

29.06.2022

Antworten

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

auf die Fragen zur öffentlichen Sachverständigenanhörung des Ausschusses für Digitales

am 4. Juli 2022

zur Thematik Digitale Identitäten sowie zum Vorschlag der EU-KOM 2021/281 (eIDAS-VO)

Antworten: (begrenzt auf Fragen mit Datenschutzbezügen)

Fragen 1. und 2:
Wo steht Deutschland im Bereich der Digitalen Identitäten (eID, SmarteID und Wallet)? Wo sehen Sie die größten Hürden? Mit der eID gibt es seit mehr als 12 Jahren eine digitale Identitätslösung. Wie bewerten Sie diese und warum wurde die Lösung vergleichsweise wenig genutzt? Welche Rolle könnte die eID noch in der Zukunft spielen?

Mit der eID des elektronischen Personalausweises ist in Deutschland grundsätzlich eine sichere und datenschutzfreundliche eIDAS-notifizierte eID-Lösung verfügbar. Sie ist, auch im europäischen Vergleich, ein beachtliches Konzept und war bereits 2010 verfügbar. Sie wurde 2017 auf der Grundlage der aktuell geltenden eIDAS-Verordnung notifiziert und ist durch einen peer review-Prozess als mit dem Vertrauensniveau „hoch“ bestätigt, so dass sie prinzipiell für den Zugang zu Diensten des eGovernment in diesen Ländern anerkannt werden kann.

Die geringe Verbreitung des elektronischen Identitätsnachweises in der Bevölkerung war und ist nicht die Folge datenschutzrechtlicher Anforderungen. Vielmehr dürfte sie mit den geringen Anwendungsmöglichkeiten, den Kosten für die teilnehmenden Stellen und jahrelang fehlender PR für dieses ambitionierte Projekt zu tun haben.

Graurheindorfer Straße 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Die Bundesregierung will den elektronischen Personalausweis durch einen mobilen, ausschließlich App - gestützten Personalausweis (SmartID) weiterentwickeln. Diese Weiterentwicklung ist mit dem Datenschutz vereinbar, wenn bei der Schaffung des übergeordneten Rechtsrahmens ,insbesondere mit der eIDAS-Verordnung, und im Anschluss an die bestehende eID zentrale Datenschutzgrundsätze gewahrt bleiben (grundsätzliche Freiwilligkeit der Nutzung; Zweckbindung; pseudonyme Nutzungsmöglichkeiten; Schutz vor Profiling durch unbeobachtbare Nutzung; Nichtverkettbarkeit anfallender Metadaten). Auf der Ebene technischer Schutzvorkehrungen spielt etwa die Einbeziehung hardwaregestützter Secure Elements in den verwendeten Smartphones eine zentrale Rolle.

Wir begrüßen in diesem Zusammenhang das Bekenntnis der Bundesregierung zur Wahrung des Datenschutzes und das Versprechen des aktiven Einsatzes gegen Profiling in den weiteren Ausgestaltungsfragen, insbesondere im laufenden Gesetzgebungsverfahren zur eIDAS-Verordnung, aber auch bei den schon laufenden nationalen Projekten wie Smart eID und ID Wallet.

6. Welche Verfahren sind für die Revozierung einer Wallet vorgesehen? Was werden die Folgen für Bürger*innen sein, die den Zugang zu ihrem eID-Wallet nicht mehr haben, etwa weil ein Wallet revoziert (deaktiviert) wurde, weil sie ihre PIN vergessen oder ihr Smartphone verlieren oder es gestohlen wird?

Bürgerfreundliche und einfach zu handhabende Rückrufmöglichkeiten sind ein wichtiger Faktor für die Akzeptanz eines eID-Systems. Aus Sicht des Datenschutzes ist die Möglichkeit der Revozierung wegen des Personenbezugs der verarbeiteten Daten zudem zwingend erforderlich. Möglichkeiten, personenbezogene Daten zu korrigieren (Artikel 16 DSGVO), zu löschen (Artikel 17 DSGVO) und zu beauskunften (Artikel 15 DSGVO), sowohl in etwaigen Hintergrundsystemen als auch in der Wallet selbst, sind gesetzliche Rahmenvorgaben. Sinnvoll erscheint es, sowohl eine Möglichkeit für die Revozierung einer kompletten Wallet vorzusehen (etwa bei Kompromittierung oder Verlust des Smartphones), als auch für einzelne in der Wallet gespeicherte Attribute (wenn diese z.B. nicht mehr aktuell sind). Wichtig zu beachten bei der Ausgestaltung eines Rückrufmechanismus ist, dass der Rückrufstatus eines personenbezogenen Datums selbst wieder personenbezogen ist, d.h. entsprechend der Vorgaben der DSGVO verarbeitet werden muss, einschließlich der damit verbundenen Betroffenenrechte.

7. Wo sollten staatlich beglaubigte elektronische Personendaten eingesetzt werden dürfen? Wie kann gewährleistet werden, dass bei digitalen Identitäten Offenbarungsverbote (§ 5 Transsexuellengesetz) auch weiterhin eingehalten werden können? Wer

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

legt fest, welche Arten von Attributen die eID dokumentiert und mitteilt (bspw. Alter, Gender) und wer legt fest, welche „Werte“ diese Attribute haben können (im Fall von Gender: männlich, weiblich, noch weitere)?

Soweit mit der Formulierung „staatlich beglaubigte elektronische Personendaten“ die Anforderung eines elektronischen Identitätsnachweises im Sinne des Personalausweisgesetzes verstanden wird, gelten insoweit die nationalen gesetzlichen Vorgaben. Öffentliche Stellen bedürfen einer gesetzlichen Rechtsgrundlage, um eine entsprechende Identifizierung durchzuführen. Hier müssten ggf. zum Schutz vor einem Unterlaufen gesetzlicher Bestimmungen zum Personenstand auch ergänzende Regelungen geschaffen werden.

Die Identifizierung einer Person – insbesondere durch staatlich verbürgte Identitätsdaten – im nichtöffentlichen Bereich darf nicht in einen faktischen Zwang der Nutzung von ID Wallets, selbst für einfachste Vorgänge des täglichen Lebens, münden. im Einklang mit der DSGVO sollte sie vielmehr nur dort erfolgen, wo dies für einen Dienst nachweislich erforderlich erscheint oder wo der Nutzer dem freiwillig zustimmt. Voraussetzung für die Einwilligung wiederum ist, dass der Nutzer alle relevanten Informationen über Empfänger, Daten und Verwendungszweck erhält, sowie die Zustimmung auch ohne Nachteile verweigern kann. Hierfür sollte die Nutzung von ID-Wallets durch zusätzliche Transparenzvorgaben abgesichert werden.

Wenn eine Identifizierung oder der Nachweis einzelner Identitätsattribute notwendig sind, so sollte dies immer auf der Basis so weniger Attribute wie möglich erfolgen (Datenminimierung; Erforderlichkeitsprinzip) und - wenn möglich - auch pseudonym. Ein gutes Beispiel hierfür ist die Altersverifikation, bei der in der Umsetzung ausschließlich das Datum (etwa: „zulässiges Alter liegt vor“) übermittelt wird.

8. Wie definieren und bewerten Sie das Self-Sovereign Identity (SSI)-Konzept? Eine Kritik an SSI ist, dass beglaubigte Daten bei den Empfängern gespeichert würden. Wie bewerten Sie die Datensicherheit des SSI-Konzepts? Gibt es aus Ihrer Sicht technische Wege, wie diese Empfangsspeicherung durch SSI vermieden werden kann?

Von grundsätzlicher Bedeutung ist, zwischen der Grundidee einer „selbst-souveränen Identität“ und diversen Möglichkeiten der technischen Umsetzung dieser Idee zu unterscheiden. Eine allgemeingültige Definition des Konzeptes „selbst-souveräne Identität“ gibt es nicht. Unter dem Begriff werden vielmehr verschiedene Aspekte zusammengefasst, wobei die genaue Auswahl und Gewichtung der Aspekte von Fall zu Fall unterschiedlich ist. Meist genannt werden: (1) Kontrolle des Nutzers über seine Identität, (2) Volle Transparenz

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

für den Nutzer, sowohl über das System als auch über seine Daten, (3) Interoperabilität von Systemen, mit der Wahlmöglichkeit der Nutzer hinsichtlich der Nutzung dieser Systeme, (4) Datenübermittlung nur mit Zustimmung des Nutzers; Möglichkeit der Übermittlung nur eines Teils der vorhandenen Daten nach Wahl des Nutzers.

Aus Sicht des Datenschutzes sind einige Aspekte der SSI sehr begrüßenswert und entsprechen bekannten Grundprinzipien des Datenschutzes (Recht auf informationelle Selbstbestimmung; Pseudonymität; Erforderlichkeitsgrundsatz; Datenminimierungsgrundsatz) etwa die Möglichkeit selektiver Datenweitergabe und die individuelle Kontrolle des Nutzers über die Weitergabe. Andere Aspekte sind eher kritisch zu sehen oder fehlen. Nicht sinnvoll für ein Identitätssystem ist etwa der Aspekt, dass in jedem Fall auch die Identitätsdaten selbst vom Nutzer ausgestellt werden (können). Einige Ausprägungen der Idee der „selbst-souveränen Identität“ sehen vor, dass die Identitätsattribute nicht durch eine sichere Quelle (z.B. Meldeämter für die klassischen Attribute wie Name, Geburtsdatum usw.) ausgestellt werden, sondern diese Attribute durch den Nutzer selbst zugewiesen werden. Ein auf dieser Selbstzuweisung aufbauendes eID-System kann – Prinzip bedingt – keine für e-Government oder mit hohen Schutzanforderungen belegte e-Business-Anwendungen notwendige verlässliche Identitätsattribute bereitstellen. Sowohl die Richtigkeit der Daten (Artikel 5 (1) d DSGVO) als auch deren Integrität (Artikel 5 (1) f DSGVO) müssen sichergestellt werden können. Davon zu unterscheiden sind wiederum die typischerweise im nichtöffentlichen Bereich je nach Vertrauensniveau herangezogenen einfachen Formen der Bestätigung einer Identität. Im Geschäftsverkehr reicht die Palette von der Barzahlung als anonymer Möglichkeit einer Transaktion über Identifizierungen, die allein per Mailadresse erfolgen oder mit aufwändigeren Lösungen wie etwa der Zwei-Faktor-Authentifizierung bestätigt werden. Die Anforderungen und das Schutzniveau werden hier durch die Anbieter bestimmt.

Die Richtigkeit der Identitätsdaten wird meist nicht als Ziel einer selbst-souveränen Identität aufgezählt, ebenso werden individuelle Möglichkeiten der Korrektur / Löschen („Vergessen“) von Daten, anders als im Datenschutz (Beteiligtenrechte), oft nicht erwähnt. Die Qualität der Verifikation der Identitätsdaten ist ein wesentliches Element auch der Vorgaben der eIDAS-Verordnung für die Vertrauensniveaus von Identifizierungssystemen. Die Richtigkeit von Daten zählt zu den Grundprinzipien auch nach der Datenschutzgrundverordnung. Werden unrichtige Identitätsdaten für die Identifizierung gegenüber einem Dienst des öffentlichen Bereichs genutzt, besteht ggf. auch die Gefahr, dass auf Daten einer dritten Person unberechtigt zugegriffen wird. Allerdings gibt es auch hier Ausnahmen wie z.B. bei der Geltendmachung eines Auskunftsanspruches nach dem Informationsfreiheitsgesetz, dem auch ohne eine eindeutige Identifizierung nachgekommen werden kann.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Im nicht-öffentlichen Bereich gibt es wiederum, mit Blick auf das gewählte Schutzniveau der Anbieter (Akzeptanz etwa einer pseudonymen Nutzung) und in Ausübung der Privatautonomie, durchaus niedrigere Anforderungen.

Die genannten Aspekte der „selbst-souveränen Identität“ können durch verschiedenste technische Lösungen umgesetzt werden, wobei sich die Auswahl der Lösung auch nach der Gewichtung der Aspekte richten kann. Die Datensicherheit kann nicht pauschal, sondern nur in einer konkreten technischen Umsetzung bewertet werden. Ein Aspekt ist die Möglichkeit für den Empfänger, die Echtheit von Daten zu verifizieren. Dies kann etwa durch kryptographische Signaturen ermöglicht werden, die die Verifizierbarkeit der Echtheit der Daten dauerhaft sicherstellen („beglaubigte Daten“ in der Formulierung der Fragestellung). Dies ermöglicht die Überprüfung der Echtheit nicht nur durch den intendierten Empfänger, sondern auch durch jeden Dritten, an den die Daten weiterübermittelt werden. Ein Beispiel hierfür sind mittels qualifizierter Signatur unterschriebene Dokumente.

Andererseits können die Daten auch ohne Signatur über einen sicheren kryptographischen Kanal übermittelt werden. Dann ist die Echtheit nur für die Lebensdauer des Kanals, d.h. temporär und nur durch den intendierten Empfänger, nicht aber durch Dritte, überprüfbar. Für eine reine Identifizierung bzw. den Nachweis von Attributen gegenüber einem konkreten Empfänger ist dies ausreichend und daher aus Datenschutzsicht für eine Identifizierung zu bevorzugen. Dies ist z.B. in der eID des elektronischen Personalausweises so umgesetzt.

Eine Speicherung von einmal übermittelten Daten durch den Empfänger kann jenseits regulatorischer/rechtlicher Vorgaben (technisch) nicht verhindert werden. Dies unterstreicht die Wichtigkeit, von vornherein nur die für einen Anwendungszweck notwendigen Daten zu übermitteln (Datenminimierung) bzw. nach Möglichkeit technische Mittel zur Datenreduktion (Privacy-Enhancing-Technologies, Zero-Knowledge-Proofs, etc.) zu nutzen.

12. Wie schätzen Sie die Gefahr von Identitätsdiebstählen ein, wenn entsprechende Identifikationsdaten in einer Wallet auf Smartphones gespeichert werden und wie kann diese reduziert werden?

Identitätsdiebstahl beinhaltet die unbefugte Erlangung und zumeist auch Missbrauch personenbezogener Daten durch Dritte. Smartphones weisen, etwa in Abhängigkeit von Hersteller, Alter, Update-Fähigkeit und tatsächlichem Update-Verhalten der Nutzer, sehr unterschiedliche Schutzniveaus auf und können gehackt werden. Dabei handelt es sich um ein allgemeines Risiko, das bei der Nutzung dieser digitalen Technologie stets zu beachten

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

ist und der mit den bekannten Maßnahmen zu begegnen ist. Risiken einer mobilen eID können reduziert werden, wenn entsprechend dem elektronischen Personalausweis vergleichbare Schutzvorkehrungen getroffen werden. Es ist letztlich auch eine Frage von privacy by design, dass und auf welchem Niveau eine von Bürgerinnen und Bürgern verwendete mobile eID-Technologie ausreichende Schutzvorkehrungen gegen Identitätsdiebstahl aufweist.

Ein Smartphone mit einer eID-App oder Wallet muss eine Reihe von technischen Schutzvorkehrungen aufweisen, um den mit der Vorhaltung und Nutzung einer Vielzahl von identitätsrelevanten Attributen gesteigerten Schutzansprüchen zu genügen. Dabei kommt u.a. der Speicherung besonders schutzwürdiger Elemente des eID-Systems in einem hardwaregestützten Secure Element besondere Bedeutung zu. Eine rein softwaregestützte Lösung jedenfalls ist nicht ausreichend.

13. In Bezug auf die ID-Wallet-App weist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in seinem 30. Tätigkeitsbericht für das Jahr 2021 auf noch offene datenschutzrechtliche Fragestellungen beim Einsatz der Blockchain-Technologie hin. Wie bewerten Sie den Nutzen und die Erfordernis der Blockchain-Technologie in Konzepten digitaler Identitäten wie ID-Wallets?

Die rechtliche Ausgestaltung der Anforderungen eines eID-Systems sollte prinzipiell ohne Vorfestlegung und Bevorzugung einer bestimmten technischen Ausgestaltung erfolgen, um in der Anwendung die bestmögliche technische Umsetzung der Schutzanforderungen zu ermöglichen. Ich teile insoweit die mit Blick auf den Entwurf der eIDAS-Verordnung geltend gemachten Bedenken zu einzelnen Bestimmungen.

Ich bin nach wie vor nicht überzeugt, dass eine distributed ledger-Technologie die richtige Infrastruktur für eine Wallet bietet. Mir begegnet diese Debatte sowohl auf nationaler als auch europäischer Ebene. Die Gestaltungskonzepte von Self Sovereign Identity (SSI) sind in ihrer Betonung der Datenhoheit der Nutzerinnen und Nutzer durchaus zu begrüßen. Doch es erscheint mir kurzschlüssig, hieraus auf eine Implementierung von distributed ledger-Technologie zu setzen. Vielmehr erscheint eine datenschutzfreundliche und sicherheitstechnisch hochwertige Lösung auch mit den etablierten Ansätzen ohne weiteres realisierbar. Auch hier gilt wieder der Verweis auf das Konzept des existierenden eID-Systems, das bereits viele Prinzipien der Self Sovereign Identity – Nutzerkontrolle, Speicherung der Attribute beim Nutzer, Möglichkeiten der Weitergabe nur einzelner Attribute, pseudonyme Weitergabe usw. – umsetzt.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Rechtlich halte ich mit Blick auf die distributed ledger-Technologie an unseren im letzten Tätigkeitsbericht geäußerten Bedenken fest. Regelmäßig wird man bei den entsprechend erfassten Daten von einem Personenbezug auszugehen haben. Die Bewertung der auf einer „Blockchain“ gespeicherten oder abgesicherten Daten hängt grundsätzlich stark von der jeweiligen Ausgestaltung des Systems ab. Als Beispiel sei hier das bekannte ID-Wallet-Projekt der Bundesregierung genannt, bei dem die Sperrinformationen über eine Blockchain-Infrastruktur verwaltet werden. Aus meiner Sicht handelt es sich dabei um pseudonyme, also personenbezogene Daten im Sinne der DSGVO. Damit ist deren Anwendungsbereich eröffnet.

Sobald auf einem distributed ledger personenbezogene Daten gespeichert werden oder über diesen verwaltet werden, ergeben sich konkrete datenschutzrechtliche Fragen, die bisher nicht geklärt sind. Genannt seien die Frage der Umsetzung der Begrenzung der Speicherdauer, wenn Daten nicht mehr benötigt werden oder die Wahrung von Betroffenenrechten wie das Recht auf Korrektur und das Recht auf Löschung.

Ebenfalls nicht geklärt ist die Verteilung der datenschutzrechtlichen Verantwortung zwischen den verschiedenen beteiligten Stellen und damit verbunden die Frage nach dem Ansprechpartner für die Geltendmachung z.B. des verfassungsrechtlich verbürgten Auskunftsrechts der datenschutzrechtlich Betroffenen.

Der BfDI ist immer offen für neue Technologien, die den Datenschutz und die Datensicherheit fördern, Stichwort „privacy enhancing technologies“. Aber auch neue Technologien müssen den rechtlichen und technischen Anforderungen in Bezug auf die Gewährleistungsziele des Datenschutzes und der Datensicherheit entsprechen.

14. Die derzeitige Beschreibung des eID-Systems lässt noch technische Details offen. Weitere Verfeinerungen können einen Einfluss auf Datenschutz und Sicherheit haben. So könnte eine auf der Wallet basierende Architektur, bei der die Wallet immer dann mit einem zentralen Cloud-Anbieter interagiert, wenn sich die oder der Nutzer*in bei einem Dienst authentifiziert, zu unerwünschtem Informationsverlust führen (etwa, wann und bei welchem Dienst die Wallet verwendet wird). Wird dies berücksichtigt? Nach welchem Verfahren werden diese technischen Einzelheiten festgelegt, und welches Maß an demokratischer Kontrolle ist vorgesehen?

An der Erarbeitung der technischen Details ist der BfDI nicht beteiligt, daher können zu dem Verfahren und dem aktuellen Stand keine konkreten Aussagen gemacht werden.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Aus Datenschutzsicht ist eine Architektur, die auf einer direkten Kommunikation zwischen Wallet und Diensteanbieter beruht, einem cloud-basierten Verfahren immer vorzuziehen. Die Einbindung einer Cloud-Komponente, insbesondere wenn diese als Zentralkomponente ausgestaltet wird, bedeutet immer ein erhöhtes Potential der Nachverfolgbarkeit der Nutzeraktivitäten und damit der Profilbildung.

16. Wie bewerten Sie Berechtigungszertifikate, die verhindern sollen, dass bei einfachen Logins (bspw. Online-Shopping, Social Media) immer der Personalausweis vorgezeigt wird? Wer stellt diese Zertifikate aus? Wie schätzen Sie allgemein die Sicherheitsrisiken in diesem Kontext ein? Welche alternativen Möglichkeiten zur Verhinderung von Over-Identification gibt es? Bitte unterscheiden Sie diese nach technischen und regulatorischen Ansätzen.

Im Rahmen einer Diskussion unter dem Stichwort „selbst-souveräne Identität“ sind im Sinne dieser Frage zwei Aspekte hervorzuheben:

1. Voraussetzung für eine bewusste Entscheidung des Nutzers, seine Daten an einen Dritten zu übermitteln bzw. sich diesem gegenüber auszuweisen, ist die sichere Identifizierung dieses Dritten. Nur wenn der Nutzer sichergehen kann, dass die Daten auch genau an denjenigen übermittelt werden, an den er die Daten übermitteln möchte, kann der Nutzer seine Entscheidungsgewalt ausüben.

2. Die Freigabe durch den Nutzer muss tatsächlich freiwillig und informiert erfolgen. Sowohl im Umgang mit Behörden als auch im Umgang mit (großen) Wirtschaftsunternehmen ist – je nach Zweck der Verarbeitung – nicht immer von einer echten Wahlfreiheit des Nutzers auszugehen („Machtasymmetrie“). Insofern kann hier der Schutz der personenbezogenen Daten nicht ausschließlich auf den Nutzer abgewälzt werden, sondern das eID-System hat hier eine Schutzpflicht gegenüber dem Nutzer.

Beide Aspekte, die Identifizierung des Empfängers der Daten und die Verhinderung von unnötiger Datenweitergabe im Sinne einer Verhinderung von „Over-Identification“, können wirksam durch Berechtigungszertifikate, wie sie im bestehenden deutschen eID-System genutzt werden, erreicht werden. In diesem Sinne dienen die Berechtigungszertifikate der technischen Umsetzung („data protection by design“) der durch die DSGVO verankerten regulatorischen Ziele der Informiertheit des Nutzers und der Datenminimierung.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Alternative Systeme – z.B. die alleinige Nutzung von Transport Layer Security - TLS-Zertifikaten – können diese Ziele nicht in gleicher Weise erreichen. Weder kann über TLS-Zertifikate das Ziel der Datenminimierung technisch unterstützt werden, noch wird bei den üblichen TLS-Zertifikaten der Inhaber auf vergleichbarem Niveau identifiziert.

17. Wie kann aus Ihrer Sicht die Benutzerfreundlichkeit bei digitalen Identitäten noch besser berücksichtigt werden?

Benutzerfreundlichkeit wird allgemein als entscheidender Faktor für die Akzeptanz und tatsächliche Nutzung von eID-Verfahren durch die Bürgerinnen und Bürger angesehen. Dabei dürften in aller Regel zahlreiche weitere Fragen ebenfalls eine große Rolle spielen. Die vor allem in der Wirtschaft etablierten und oft als „de facto standardsetzend“ geltenden Verfahren stehen ebenfalls in einem Spannungsfeld zu Fragen des Datenschutzes und der IT-Sicherheit, wie z.B. die zunehmende Verbreitung der Zwei-Faktor-Authentifizierung zeigt. Der Datenschutz steht der Steigerung der Benutzerfreundlichkeit etwa des elektronischen Identitätsnachweises durch einen Wechsel auf eine rein App gestützte mobile eID nicht entgegen, wenn die bereits genannten, gesteigerten Schutzanforderungen eingehalten werden. Die Schutzanforderungen steigen bei Wallet- Lösungen, da diese eine Vielzahl an Attributen enthalten können.

18. Wie bewerten Sie die Beratungen und Diskussionen um die eIDAS Verordnung auf europäischer Ebene? An welcher Stelle der VO müsste nachgebessert werden?

Grundsätzlich werden in dem Entwurf der eIDAS 2.0-Verordnung bereits viele datenschutzrelevante Aspekte aufgegriffen, z.B. die Identifizierung von Diensteanbietern (vgl. Antwort auf Frage 16), der Grundsatz der Erforderlichkeit usw.

Weiter problematisch ist jedoch die Forderung nach einem eindeutigen und dauerhaften Identifizierungskennzeichen (Identifier) für Personen im Rahmen der Einführung der Wallet und als Teil des zu erfassenden Basisdatensatzes. Auch wenn noch kontrovers diskutiert wird, ob hier ein Identifier gemeint ist, der für alle Dienstanbieter gleich ist oder ob der Identifier spezifisch für jeden Dienstanbieter sein kann, so ist jedoch eine dauerhafte Gültigkeit des Identifiers (d.h. lebenslang) vorgesehen.

In jedem Fall führt ein solcher Identifier zu einer Möglichkeit der Nachverfolgbarkeit der Nutzer und einer entsprechenden Profilbildung. Daher ist dieser Vorschlag aus Datenschutzgesichtspunkten risikoreich und abzulehnen. Eine Notwendigkeit für einen solchen dauerhaften Identifier – gleich welcher Ausprägung – wird hier nicht gesehen.

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Darüber hinaus sollte eindeutig geregelt werden, dass bereits die technische Ausgestaltung der Wallet so erfolgt, dass weder die Herausgeber der Wallet noch die Anbieter elektronischer Identitätsbescheinigungen das weitere Verhalten der Nutzerinnen und Nutzer der Wallet tracken und hierüber womöglich Profile zur Verwendung für eigene Zwecke anlegen können. Auch die Möglichkeit pseudonymer Nutzung ohne Offenlegung der Identität für selektive Angaben (zum Beispiel der Fall der Altersverifikation) könnte eindeutiger gefasst werden. Ferner sollte im Hinblick auf die technische Umsetzung der Vorgaben der Grundsatz der Technikneutralität gewahrt bleiben und konkrete Regelungen der Verantwortlichkeit von Diensteanbietern bei Verstößen gegen die Bestimmungen der Verordnung erwogen werden. Klarstellende Hinweise auf die Geltung der DSGVO insgesamt als auch auf im Kontext besonders wichtige Datenschutzprinzipien (Zweckbindungsgrundsatz, Datenminimierung, Privacy by Design, Privacy bei Default) könnten ebenfalls zur Stärkung des Datenschutzes beitragen.

20. Wie schätzen Sie die Verhandlungen zur eIDAS-Verordnung im Kontext der deutschen eID-Strategie ein? Wie wird beides zeitlich aufeinander abgestimmt?

Das deutsche Vorgehen bei eID ist durch Planungen für die Weiterentwicklung des elektronischen Personalausweises hin zu einer rein mobilen Anwendung (SmartID) mit Möglichkeiten des Ausbaus zu einer ID-Wallet und entsprechenden Forschungsvorhaben - insbesondere mit Blick auf die Umsetzung des SSI-Konzeptes - gekennzeichnet.

Parallel läuft bereits das EU-Gesetzgebungsvorhaben zur eIDAS-Verordnung, das die bereits bestehende eIDAS-Verordnung von 2014 weiterentwickelt. Es ist von seinem Anwendungsbereich so weitgehend angelegt, dass es aufgrund seines die Mitgliedstaaten unmittelbar bindenden Verordnungscharakters maßgebliche rechtliche Vorgaben für die bekannten Vorhaben der bundesdeutschen eID-Strategie enthalten wird. Aus datenschutzrechtlicher Sicht kommt es darauf an, dass die Bundesregierung schon im Rahmen dieses Gesetzgebungsvorhabens der EU auf die Wahrung aller hier vorgehend genannten datenschutzrechtlichen Aspekte drängt. Dabei gilt es auch zu bedenken, dass wegen der unmittelbaren Anwendbarkeit der DSGVO und der nach dem Kommissionsentwurf der eIDAS-Verordnung auch nicht bestrittenen Anwendbarkeit kein Spielraum für grundlegende nationale Einzelgänge in Bezug auf Datenschutzfragen besteht. Ausnahmen davon kann es nur geben, wenn sie explizit in der Verordnung vorgesehen werden. Ein Abwarten des Ergebnisses des europäischen Gesetzgebungsprozesses erscheint vor diesem Hintergrund sachgerecht.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

21. Wie bewerten Sie den Plan der EU KOM, in sogenannten „Large Scale Pilots“ die „European Digital Identity Wallet“ zu testen? Wie schätzen Sie die Chancen ein, dass in jenen Pilots Standards – auch zum Datenschutz und der IT-Sicherheit gesetzt – werden?

Eine Erprobung neuer Konzepte und Standards im Rahmen von Piloten vor einem flächendeckenden Roll-Out ist grundsätzlich zu begrüßen. Wesentlich bei einer Pilotierung ist, dass die Themen Datenschutz und IT-Sicherheit von vornherein („Privacy by design“) mit berücksichtigt werden. Eine rein funktionale Pilotierung, in der dann nachträglich Datenschutz / IT-Sicherheit eingeführt werden, ist erfahrungsgemäß nicht zielführend. Ein Negativbeispiel in dieser Hinsicht bot die vorschnelle und deshalb aus Gründen nicht ausreichender IT-Sicherheit missglückte Einführung der ID-Wallet der letzten Bundesregierung. Insbesondere weist der BfDI darauf hin, dass auch in einem Pilotierungskontext die Anforderungen und Regelungen der DSGVO – sofern die Pilotierung mit echten Nutzerdaten erfolgt – einzuhalten sind.

22. Auf europäischer Ebene wird darüber diskutiert, die technische Ermöglichung von Zero-Knowledge-Proofs (ZKP), also sich rechtssicher auszuweisen ohne Daten preiszugeben, als verpflichtenden Standard in die eIDAS-VO aufzunehmen. Wie bewerten Sie das?

Aus Datenschutzsicht ist die Datenminimierung ein wichtiges Ziel. Die Nutzung von Zero-Knowledge-Proofs als technisches Mittel, die Notwendigkeit der Weitergabe von personenbezogenen Daten zu reduzieren (z.B. der Nachweis des Erreichens einer bestimmten Altersgrenze anstatt der Weitergabe des Geburtsdatums), ist im Sinne von „data protection by design“ zu fördern. Daher befürwortet der BfDI die Verankerung entsprechender Mechanismen – unter Wahrung der Technikneutralität – ausdrücklich. Im Rahmen der Umsetzung gilt aber auch für Zero-Knowledge-Proofs, dass die technische Sicherheit sichergestellt und geprüft werden muss.

24. Ein Kritikpunkt ist die Verpflichtung der Unternehmen oder relying Parties, die EUid-Wallets als Identifizierungsmittel zu akzeptieren. Dies sei eine größere Herausforderung, da sie bisher keine hoheitlichen Identifizierungsprozesse innerhalb ihrer Services vorsehen. Wie schätzen Sie diesen Punkt ein? Ist die Kritik berechtigt? Welche Folgen hat diese Regelung und wie könnte eine Alternative aussehen?

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

26. Der Artikel 12b des Kommissionsentwurfs zur eIDAS-Verordnung sieht vor, neben den großen Plattformbetreibern auch zahlreiche Branchen zur Akzeptanz der EU-Wallet zu verpflichten. Wie schätzen Sie diese Verpflichtung ein? Aktuell wird auf europäischer Ebene diskutiert, ob es nur eine staatliche Wallet geben soll oder verschiedene Wallets, die zertifiziert sind. Welchen Weg bevorzugen Sie und warum?

Die nach dem Kommissionsentwurf der eIDAS- Verordnung vorliegende Verpflichtung von Unternehmen und insoweit auch einzelnen Branchen, die EUid- Wallet als Identifizierungsmittel zu akzeptieren, zielt gerade auf die wirkungsvolle Schaffung einer hoheitlich abgesicherten Alternative zu den gängigen, zumeist privatwirtschaftlich angebotenen, eID-Systemen. Damit sieht es der Staat analog zu seiner Kompetenz im Ausweiswesen als seine Aufgabe an, auch im digitalen Raum eine staatlich verbürgte Identität anzubieten. Kennzeichen zahlreicher privatwirtschaftlich vermittelter Systeme, insbesondere bei größeren Anbietern oder Zusammenschlüssen von Anbietern als LogIn-Portale, ist hingegen gerade das möglichst umfassende Tracking und Profiling der Nutzerinnen und Nutzer, zum Nachteil ihrer Datenschutzrechte.

Aus datenschutzrechtlicher Sicht stellt die vorgesehene gesetzliche Verpflichtung der Unternehmen im Grundsatz eine die Selbstbestimmung der Bürgerinnen und Bürger erweiternde Alternative dar, wenn und soweit bei den gesetzlichen und technischen Rahmenbedingungen der EUiD- Wallet eine tatsächlich datenschutzfreundliche Anwendung geschaffen wird. Die Möglichkeit des Angebots von EUiD- Wallets auch durch nichtstaatliche Anbieter würde das Erfordernis umfänglicher konkretisierender datenschutzrechtlicher Regelungen eher steigern. Im Hinblick auf die Möglichkeit, dass dann auch die sog. Gatekeeper im Sinne des Digital Markets Act (DMA) oder vergleichbar große Unternehmen Anbieter werden könnten, bedarf es auch aus Perspektive der durch das Gesetzgebungsvorhaben besonders berührten Datenschutzaufsicht der Schaffung hinreichend präziser Regelungen zur Sicherstellung eines effektiven Vollzugs der Bestimmungen der eIDAS-Verordnung.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de