eIDAS-Postionspapier

25. Januar 2022

Einleitung

Im Juni 2021 begann die EU-Kommission mit der Reform der eIDAS-Verordnung aus dem Jahr 2014 und damit mit der Neugestaltung des europäischen Rechtsrahmens für elektronische Identitätssysteme (eID).[3] Ziel dieses ambitionierten Reformprojektes ist die Schaffung eines Gegengewichts zu den bekannten Loginsystemen von Google, Facebook und Apple und die Bereitstellung eines eID-Systems, das große Teile der Bevölkerung für eGovernment-Dienste und Onlinehandel verwenden. Der neue Verordnungsentwurf sieht eine Software namens „Brieftasche für die europäische digitale Identität" (Wallet App) vor, mit der sich Bürger*innen und Einwohner*innen online und offline ausweisen können, und die ihnen die Möglichkeit gibt, Attribute wie Alter, Führerschein oder Studierenden-Status nachzuweisen. Die breite Akzeptanz dieses neuen europäischen elektronischen Identifizierungssystems soll laut Verordnungsentwurf erreicht werden, indem sogenannte „sehr große Online-Plattformen"[4] wie Facebook und Google verpflichtet werden, die europäische Wallet als Login-Möglichkeit zu ihren Diensten zu unterstützen. In ähnlicher Weise werden auch Mitgliedstaaten verpflichtet, dieses System als Ausweis für Bürger*innen einzusetzen, wenn sie eGovernment-Dienste nach der alten Verordnung von 2014 nutzen. Kleineren Internetunternehmen wiederum kann die Kommission mittels delegiertem Rechtsakt vorschreiben, die neue Wallet App ebenfalls zu unterstützen.

Mit diesem Papier sollen die größten Probleme des Kommissionsvorschlags in Bezug auf Datenschutz und digitale Rechte erörtert werden. Ein europäisches elektronisches Identitätssystem muss die Grundrechte von Bürger*innen und Einwohner*innen achten, denn die positiven Potenziale des Systems hängen von seiner weiten Verbreitung und dem Vertrauen aller Beteiligten ab. Erreicht werden kann das nur durch eine Abschätzung der Folgen, die dieses System auf das derzeitige digitale Ökosystem in Europa haben wird. Doch der vorliegende Vorschlag verschiebt die Regelung von vielen zentralen Fragen zur Architektur in delegierte Rechtsakte, wodurch eine umfassende Bewertung so gut wie unmöglich wird. Die Verordnung selbst muss diese Themen klar regeln und angemessene Schutzbestimmungen enthalten, um Privacy by Design (Datenschutz durch Technikgestaltung), Wahlmöglichkeiten der Nutzer*innen und Datenminimierung zu gewährleisten. Wir akzeptieren durchaus die Ausgangsbasis der Verordnung und die Notwendigkeit von vertrauenswürdigen digitalen Identitäten und Bescheinigungsinfrastruktur, doch sollte die Nichtverwendung des Systems keine negativen Konsequenzen für Bürger*innen, die sich gegen die Verwendung der Wallet App entscheiden oder die kein Smartphone besitzen, haben. Im vorliegenden Papier möchten wir diese Themen erläutern und hoffen, dass unsere Vorschläge für Schutzbestimmungen zur Verbesserung der Verordnung im Gesetzgebungsprozess angenommen werden.

Eindeutige, lebenslange Identifikatoren für jede/n Bürger*in und Einwohner*in

Eine der Kernfunktionalitäten der Wallet App, Nutzer*innen mittels Bekanntgabe ihres bürgerlichen Namens Dritten gegenüber auszuweisen, wird von einer Bestimmung in Artikel 11a begleitet, die den Mitgliedstaaten auferlegt, jede Person mit einer alphanumerischen Zeichenfolge, die für den Rest ihres Lebens gilt, eindeutig zu identifizieren. Dieser dauerhafte („persistente") und eindeutige

3 Siehe https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0281

4 Dieser Ausdruck bezieht sich auf Artikel 25 Absatz 1 des Vorschlags für eine Verordnung über digitale Dienste.

Identifikator aller europäischen Bürger*innen und Einwohner*innen wird von der Wallet App mit privaten und staatlichen Akteuren geteilt. Zwar muss der/die Nutzer*in seiner/ihrer Identifizierung immer noch mittels Interaktion in der App zustimmen, aber da der/die Nutzer*in in Ausweissituationen sehr oft einem Machtgefälle unterliegt und diese Funktionalität ja gerade auf Fälle beschränkt ist, in denen eine Identifikation aufgrund von nationalem oder europäischem Recht verpflichtend ist, kann bezweifelt werden, ob diese Zustimmung freiwillig erteilt wird. Dazu kommt, dass nicht nachvollziehbar ist, wie die Wallet App unterscheiden soll, in welchen Fällen eine Identifikation gesetzlich vorgeschrieben ist und in welchen nicht. Die Regelungen können von Mitgliedsstaat zu Mitgliedsstaat unterschiedlich sein; zum Beispiel könnte ein ungarisches Gesetz eine Ausweispflicht auf Demonstrationen vorschreiben, oder ein österreichisches Social-Media-Gesetz von Facebook verlangen, die Identität seiner Nutzer*innen zu kennen. Alles in allem können Facebook und andere Unternehmen es kaum erwarten, einen behördlichen, eindeutigen, lebenslangen Identifikator zu ihren Nutzer*innen-Identitäten hinzuzufügen, und sie werden Wege finden, um Nutzer*innen dazu zu überlisten. Um zu verhindern, dass diese eindeutigen, lebenslangen Identifikatoren die datenbasierte Macht von Facebook und Co. noch weiter stärken, sollten sie erst gar nicht geschaffen werden.

Lösungsvorschlag

Streichung von Artikel 11a.

Breite Verfügbarkeit von behördlichen Identitätsdaten und Informationen zum Onlineverhalten

Nach Artikel 6b Absatz 1 des Verordnungsentwurfs können sogenannte Relying Parties („vertrauende Beteiligte“, d.h. Unternehmen, die möchten, dass ihre Kund*innen die Wallet App als Ausweis oder zum Nachweis gewisser Attribute verwenden) in dem Mitgliedstaat, in dem sie niedergelassen sind, Zugang zum EU-System beantragen und einen Blanko-Zugang für die gesamte EU erhalten. Das ermöglicht Forum Shopping, denn jeder Unternehmer kann sich die Rechtsordnung aussuchen, die für ihn am vorteilhaftesten ist. Jedes Unternehmen, das Zugang zu den Identitätsdaten oder Attributen in der Wallet erlangen möchte, kommt als Relying Party in Frage. In der Verordnung finden sich keine genauen Angaben darüber, wie das Bestätigungsverfahren einer Relying Party in einem Mitgliedsstaat ablaufen soll. In Artikel 6b Absatz 4 ist vorgesehen, dass die Kommission sechs Monate nach Inkrafttreten der Verordnung mittels delegiertem Rechtsakt festlegt, wie diese wichtige Überprüfung ablaufen wird. In der Verordnung ist weiters kein Mechanismus vorgesehen, wie der Zugang einer Relying Party zum eIDAS-System widerrufen werden kann. Der letzte Satz von Absatz 1 lässt sogar offen, ob der angegebene Zweck der Verarbeitung von Identitätsdaten ausreichend für die Ablehnung eines Antrages ist.

Die eIDAS-Regulierer in den jeweiligen Mitgliedsstaaten sind verantwortlich, die Einhaltung der Verordnung durch die Relying Parties zu prüfen. Im Fall von Irland ist das das Ministerium für Umwelt, Klima und Kommunikation, welches keine unabhängige Regulierungsbehörde ist. Die irische Datenschutzbehörde ist berüchtigt dafür, das europäische Datenschutzrecht zu unterminieren, und dieses Risiko könnte auch für das vorgeschlagene eIDAS-System bestehen, wenn die zuständige Behörde nicht unabhängig und rechenschaftspflichtig ist. In den neuen eIDAS-Regelungen fehlen nicht nur die notwendigen Schutzbestimmungen für die Schaffung einer Umgebung, der wir unsere Identitätsinformation anvertrauen können, sondern es werden auch aktiv Fehler aus früheren EU-

Gesetzesprojekten bei der Durchsetzung wiederholt, was einen Missbrauch des neuen Systems durch bekannte Akteure geradezu herausfordert.

Schon jetzt verfolgen Google und andere Big-Tech-Unternehmen, deren Geschäftsmodell auf gezielter Werbung basiert, beinahe jede unserer Online-Handlungen und erstellen Profile zu jedem Aspekt unseres Lebens. Eines der letzten Dinge, das sie nicht mit Sicherheit wissen, ist in vielen Fällen unser bürgerlicher Name. Mit der Bereitstellung eines kostengünstigen und großteils unregulierten Zugangs zu behördlich zertifizierten Identitätsdaten und sogar einer Verpflichtung für sehr große Online-Plattformen, die Wallet App als Loginmethode anzubieten, präsentiert die EU auf dem Silbertablett, was sie eigentlich schützen sollte.

In der breiten Verfügbarkeit von behördlich zertifizierten Identitätsdaten sehen wir ein hohes Risiko in Bereichen wie gezielte Werbung, Bankdienstleistungen und Bonitätsbewertung, sowie Onlinehandel und Medien. Die bestehenden Mängel bei der Durchsetzung der DSGVO, wie beim Kopplungsverbot und „Pay or Okay"-Verbot, werden das Problem noch verstärken. Die eIDAS-Verordnung muss angemessene Schutzbestimmungen gegen den Missbrauch von Identitätsdaten in dem bestehenden Ökosystem, das verändert werden soll, verankern.

Lösungsvorschläge

Unserer Ansicht nach muss die Verordnung mit Schutzbestimmungen gegen den Missbrauch der Wallet App durch Relying Parties verbessert werden.

Unter diesem Gesichtspunkt ist Artikel 6b wie folgt anzupassen:

Relying Parties müssen verpflichtet werden, den konkreten Anwendungsfall, für den sie auf die Wallet App zurückgreifen wollen, bei der eIDAS-Regulierungsbehörde ihres Landes zu registrieren, die ihn im Voraus mit schwarzen und weißen Listen von Anwendungsfällen abgleicht und auch eine Datenschutzfolgenabschätzung verlangen kann. Eine Genehmigung durch eine eIDAS-Regulierungsbehörde muss bei der eIDAS-Regulierungsbehörde eines beliebigen anderen Mitgliedsstaates von Konsumenten- und Datenschutzorganisationen anfechtbar sein, mit dem möglichen Ergebnis, dass dieser Anwendungsfall in diesem Mitgliedsstaat untersagt wird. Beispiele für Anwendungsfälle auf der schwarzen Liste sind Werbung, Bonitätsbewertung und Klarnamenpflicht auf Social-Media-Plattformen. In Fällen, wo die Datenschutzfolgenabschätzung ein hohes Risiko für die Betroffenen zeigt, muss die eIDAS-Regulierungsbehörde in der Lage sein, den Anwendungsfall auf die schwarze Liste zu setzen.

Zentrale Überwachung aller Identitäts- und Attributsbescheinigungen

Die Wallet App soll bestehende Methoden zur Feststellung von Identität, Alter und anderen Attributen ersetzen. Das neue System darf sich dabei nicht schlechter auf die Privatsphäre und den Datenschutz auswirken als die bestehenden Methoden, die ersetzt werden sollen. Wir anerkennen, dass ein konkretes Problem gelöst wird, wenn ein/e Nutzer*in im Fall einer Altersfeststellung keinen Ausweis mehr herzeigen muss, der mehr Informationen als notwendig enthält (Name, Geburtsdatum, Ausstellungsland). Jedoch birgt der Vorschlag das ernsthafte Risiko einer zentralen Überwachung aller Online- und Offline-Vorgänge zur Identifizierung und Attributsbescheinigung mit der Wallet App. Vergleichbar mit dem Digitalen COVID-Zertifikat der EU hätte die Kommission in der vorgeschlagenen Verordnung die Befugnis, wichtige Fragen zur Architektur zu einem späteren Zeitpunkt einseitig mittels delegiertem Rechtsakt zu entscheiden, anstatt das Privacy-by-Design-Prinzip im Gesetz festzuschreiben. Wir fordern die Mitgesetzgeber daher auf, Datenschutz-, Privatsphäre- und

Cybersicherheits-Schutzbestimmungen direkt bei der Gesetzgebung zu regeln, anstatt die Befugnis dazu der EU-Kommission zu überlassen. Die Unbeobachtbarkeit aller über die Wallet App abgewickelten Vorgänge zur Identifikations- und Attributsbescheinigung muss in der Verordnung gewährleistet werden. Nachdem wir im Zuge der Diskussionen[5] um das Digitale EU-COVID-Zertifikat auf dieses Thema aufmerksam gemacht hatten, wurde eine entsprechende Schutzbestimmung hinzugefügt.[6]

Es gibt durchaus selbstbestimmte („self-sovereign") eID-Systeme, die auf einem Zero-Knowledge- und Unverknüpfbarkeitsparadigma basieren, wodurch es systembedingt unmöglich ist, dass ein zentrale Stelle Identifikations- oder Authorisierungsvorgänge mitverfolgen kann. Technologien wie did:peer, DIDComm, OpenID Connect SIOP und BBS+ Signatures[7] können genutzt werden, um eine die Privatsphäre respektierende digitale Infrastruktur aufzubauen, mit der Identitäten und Attribute erzeugt und mitgeteilt werden können, ohne dass es dazu zentraler Akteure oder einer Blockchain bedarf. Derartige Garantien fehlen aber im Vorschlag der Kommission. Diese Unschärfen hinsichtlich vieler Fragen zur Architektur der Wallet App vergrößern die Lücken im Rechtstext von Artikel 6a Absatz 7, der die Rechtsgrundlage für die Verarbeitung von Nutzungsdaten und für das Verknüpfen mit Daten von Dritten bildet.

In seiner derzeitigen Form ermöglicht der Rechtsrahmen einer zentralen Stelle, jeden Identifikationsvorgang und jede Attributsbescheinigung in der Bevölkerung auf der Makro-Ebene zu beobachten. Beispielsweise erlaubt die Verordnung den Providern der Wallet App (Staaten) die Gewinnung von Informationen zu allen Loginvorgängen bei sehr großen Online-Plattformen (wie Facebook oder Google), zu Altersüberprüfungen beim Online- und Offline-Kauf gewisser Waren (Alkohol, Tabak, etc.), und zu Diensten, die Nutzer*innen nur offenstehen, weil sie über gewisse Attribute verfügen, die verifiziert werden müssen (Behinderung, Alter, etc.). Und da es das erklärte Ziel ist, dass die Wallet App flächendeckend und in allen Gruppen der Bevölkerung weit verbreitet sein soll, werden die negativen Auswirkungen des eIDAS-Vorschlags auf Privatsphäre und Datenschutz nur noch verstärkt.

Lösungsvorschläge

Ähnlich dem Digitalen COVID-Zertifikat der EU muss die Verordnung sicherstellen, dass für die Wallet App Privacy by Design gilt. Deshalb schlagen wir vor, Artikel 6a Absatz 7 wie folgt anzupassen:

> *„Der Nutzer hat die uneingeschränkte Kontrolle über die EUid-Brieftasche. Der Aussteller der EUid-Brieftasche sammelt weder Informationen über die Verwendung der Brieftasche~~, die für die Erbringung der damit verbundenen Dienste nicht erforderlich sind~~, noch kombiniert er Personenidentifizierungsdaten und andere gespeicherte oder im Zusammenhang mit der Verwendung der EUid-Brieftasche stehende personenbezogene Daten mit personenbezogenen Daten aus anderen vom Aussteller angebotenen Diensten oder aus Diensten Dritter~~, die für die Bereitstellung der Brieftaschendienste nicht erforderlich sind, es sei denn, der Nutzer hat dies ausdrücklich verlangt~~. Personenbezogene Daten in Bezug auf die Bereitstellung von EUid-Brieftaschen werden von allen anderen gespeicherten Daten physisch und logisch getrennt gehalten."*

5 Siehe https://en.epicenter.works/document/3425 und https://epicenter.works/content/eu-parliament-adopts-the-covid-pass-risks-for-data-protection-and-new-forms-of

6 Siehe Artikel 4 Absatz 2 der Verordnung (EU) 2021/953 und https://epicenter.works/content/fuenf-gruende-den-sieg-beim-digitalen-covid-zertifikat-der-eu-zu-feiern

7 Siehe https://identity.foundation/peer-did-method-spec/, https://identity.foundation/didcomm-messaging/spec/, https://openid.net/specs/openid-connect-self-issued-v2-1_0.html und https://w3c-ccg.github.io/ldp-bbs2020/

Zusätzlich müssen die technischen Spezifikationen der Wallet App im Rechtstext sicherstellen, dass Privacy-by-Design-Prinzipien eingehalten werden. Die Verordnung muss gewährleisten, dass Nutzer*inneninteraktionen mit der Wallet App unbeobachtbar sind, um Nutzer*innen vor Überwachung, wie sie ihre Wallet verwenden, zu schützen. Diese Änderungen sind notwendig, weil die in Artikel 6a Absatz 11 vorgesehenen delegierten Rechtsakte der Kommission die Befugnis verleihen, festzulegen, wie die Wallet in der Praxis funktionieren soll. Die Verwendung von delegierten Rechtsakten muss darauf beschränkt werden, Spezifikationen angesichts neuer technologischer Entwicklungen zu aktualisieren, aber die Gestaltungsprinzipen, welche die Auswirkungen der Technologie auf die Privatsphäre grundlegend bestimmen, müssen bereits in der Verordnung verankert sein. Es ist notwendig, den Hinweis auf „für die Erbringung der damit verbundenen Dienste [erforderlichen]“ Informationen überhaupt zu streichen, um sicherzugehen, dass die Digitale-Identitäts-Wallet auf eine Art implementiert wird, wo solche Informationen für das Funktionieren überhaupt nicht benötigt werden. Bestehende (selbstbestimmte) eID-Systeme zeigen, dass eine derartige Implementierung möglich ist.

Biometrie und Smartphone-Sicherheit

Die Sicherheit der Wallet-Software wird von Prüfdienstleistern zertifiziert, die gemäß Artikel 6c von den Mitgliedsstaaten benannt und nur den anderen Mitgliedstaaten, nicht aber der Öffentlichkeit, mitgeteilt werden. Welche Kriterien die Wallet-Software konkret erfüllen muss wird wieder innerhalb von sechs Monaten nach Inkrafttreten der Verordnung von der Kommission mittels delegiertem Rechtsakt festgelegt.

Gemäß Erwägungsgrund 11 kann die Wallet App auch biometrische Methoden zur Authentifizierung der Nutzer*innen verwenden und derselbe Erwägungsgrund gestattet auch die Speicherung von Authentifizierungsinformationen in der Cloud. Erwägungsgrund 21 bezieht sich auf Bestimmungen im Gesetz über digitale Märkte, welche Betreiber zentraler Plattformdienste wie Google oder Apple verpflichten, Interoperabilität mit Nebendienstleistungen wie Identifizierung zu ermöglichen, und hält fest, dass diese Bestimmung den Wallet Apps Zugriff auf Hardwareelemente der sicheren Enklave, auf denen moderne Smartphones biometrische Informationen wie Fingerabdrücke und Gesichtserkennungsmuster speichern, ermöglichen würde. Je nach technischer Ausgestaltung könnte das äußerst problematisch sein, denn es könnte die Sicherheit der Smartphones schwächen und möglicherweise zur Exponierung von biometrischer Information in Cloudspeichern oder auf staatlich kontrollierten Apps führen. Da alle technischen Einzelheiten erst in delegierten Rechtsakten nach Annahme des Gesetzes festgelegt werden, ist es sehr schwierig, die Privatsphäre- und Sicherheitsauswirkungen dieser weitgefassten Befugnisse der Wallet-App-Provider zu bewerten, weshalb der Verordnungsentwurf in dieser Hinsicht hohe Risiken birgt.

Ähnlich wie die ungewissen technischen Spezifikationen der Wallet App ignoriert die Verordnung auch vollkommen die enormen Unterschiede bei der Sicherheit von Smartphones. Die Wallet App wird selbstverständlich von der Sicherheit des Smartphones, auf dem sie läuft, abhängig sein. Niedrigverdiener*innen werden seltener Geräte auf dem Stand der Technik besitzen, und in vielen Fällen erhalten sie nicht einmal mehr Sicherheitsupdates von ihrem Anbieter. Technisch weniger versierte Nutzer*innen werden nicht so gut in der Lage sein, das Betriebssystem ihrer Geräte auf dem neuesten Stand zu halten und korrekt zu konfigurieren. Wir sehen bereits eine Zunahme an Cyberattacken auf Smartphones, und mit der Wallet App werden diese Geräte noch interessantere Ziele für Identitätsdiebstahl. Die digitale Kluft, wie wir sie heute kennen, wird sich mit dem derzeitigen eIDAS-Vorschlag noch verschärfen, denn es bilden sich schon jetzt unterschiedliche Preise, d.h.

analoge / persönliche Behördendienste werden teurer als eGovernment-Dienste, die auf eIDAS-zertifizierten Ausweismethoden basieren.[7]

Lösungsvorschläge

Die einzige Lösung der Sicherheitsprobleme des derzeitigen Entwurfs ist eine genauere Festschreibung der technischen Anforderungen und der Datenschutz- und Sicherheitsarchitektur in der Verordnung, sowie eine breit angelegte Diskussion darüber bereits jetzt, anstatt blind darauf zu vertrauen, dass die Kommission diese Arbeit fünf Monate nach Abschluss des legislativen Mitentscheidungsverfahrens leistet.

Eine Lösung zur Verhinderung von Ausgrenzung aufgrund unterschiedlicher Sicherheitsniveaus bei Smartphones wäre das Hinzufügen einer Anti-Diskriminierungsverpflichtung gegenüber Bürger*innen und Einwohner*innen, die sich gegen die Nutzung der Wallet App entscheiden, möglicherweise weil sie kein Smartphone (mit ausreichendem Sicherheitsniveau) besitzen.

Aushebelung der Websicherheit durch erzwungene Root-Zertifikate in jedem Browser

Gemäß Artikel 45 im Kommissionsvorschlag wären Hersteller von Webbrowsern verpflichtet, Root-Zertifizierungsstellen („certificate authorities" oder CAs) von Mitgliedstaaten in ihre Produkte aufzunehmen. Zertifizierungsstellen sind unentbehrlich für die Sicherheit von verschlüsseltem https-Webtraffic und die Authentizität von Webseiten. Browserhersteller haben strenge Regeln, welche Zertifizierungsstellen sie in diese Vertrauensliste aufnehmen, und sind oft Druck von Staaten ausgesetzt, staatliche Zertifizierungsstellen zum Ausspionieren des Webtraffics seiner Bürger*innen zu inkludieren. Hier einen Präzedenzfall für die Aufnahme von staatlichen Zertifizierungsstellen zu schaffen, könnte die Sicherheitsinfrastruktur des Webs schwer beschädigen, eine Zunahme der Überwachung von verschlüsseltem Webtraffic ermöglichen und in weiterer Folge antidemokratische Tendenzen stärken.[8]

Lösungsvorschlag

Beibehaltung der Originalversion von Artikel 45 der Verordnung 910/2014 und Streichung des neuen Wortlauts in der neuen Verordnung.

Verpflichtende Identifizierung vor jeder Attributsbescheinigung

Der derzeitige Wortlaut von Artikel 6a Absatz 4 Buchstabe d suggeriert, dass die elektronische Bescheinigung von Attributen eine vorhergehende Authentifizierung des/der Nutzers/in durch die Relying Party erfordert. Das läuft dem grundlegenden Zweck von selektiven Offenlegungen als Datenschutzmaßnahme zuwider, die beispielsweise eine Altersbestätigung ohne Bekanntgabe des Namens oder des Geburtsdatums einer Person ermöglichen sollen. In Erwägungsgrund 29 werden solche selektiven Offenlegungen als klares Ziel der Verordnung genannt, und sie haben den Vorteil, keine weiteren Informationen über die Person preiszugeben. Artikel 3 Absatz 5 in der derzeit geltenden 2014 Version des Gesetzes vermengt die Begriffe Authentifizierung und Identifizierung – und gestattet damit im Endeffekt in jedem Online- oder Offline-Anwendungsfall die Nachverfolgung einer jeden Person, die ein Attribut von sich mittels der Wallet App bescheinigt.[9]

7 https://www.wien.gv.at/amtshelfer/verkehr/parken/kurzparkzone/parkpickerl.html

8 Siehe https://www.eff.org/deeplinks/2021/12/eus-digital-identity-framework-endangers-browser-security und https://blog.mozilla.org/netpolicy/files/2021/11/eIDAS-Position-paper-Mozilla-.pdf

9 Siehe Kapitel 2.3 https://brusselsprivacyhub.eu/publications/the-european-commission-proposal-amending-the-eidas-regulation

Lösungsvorschlag

Die Bescheinigung von Attributen soll keine vorherige Authentifizierung oder Identifizierung des/der Nutzers/in gegenüber einer Relying Party erfordern, auch nicht mit einem pseudonymen Identifikator.

Folgewirkungen von kostengünstiger elektronischer Identifizierung

In den vergangenen Jahren kam es zu mehreren Versuchen auf einzelstaatlicher und EU-Ebene, eine Klarnamenpflicht oder verpflichtende Identifikation für Nutzer*innen von Sozialen Medien oder Video-Sharing-Plattformen einzuführen.[10] Oft sind diese Versuche daran gescheitert, dass sie aufgrund der Kosten einer behördlichen Online-Idenzifizierung von Nutzer*innen in großem Umfang schlicht unrentabel sind. Das ändert sich, wenn die Wallet App die Kosten der Identifizierung von Nutzer*innen im Internet in Europa auf praktisch null senkt.

Weil das Hinzufügen von verifizierten Identitätsdaten von Nutzer*innen bereits gesammelte persönliche Daten bereichert, werden viele Akteure einen Anreiz haben, diese Information von den Nutzer*innen zu erlangen. Die derzeitige Praxis zeigt, dass Nutzer*innen leicht überlistet werden können, der Weitergabe ihrer Daten zuzustimmen, und dass viele nicht über das notwendige Interesse oder Verständnis verfügen. Eine mögliche Konsequenz wäre die Kombination von gezielter Werbung mit verifizierten Identitäten.

Die treibenden Kräfte hinter dem Vorschlag

Die COVID-19-Pandemie hat die eIDAS-Reform beschleunigt. Im Lockdown wurde einer Mehrheit die praktische Notwendigkeit von eGovernment-Diensten und Onlinehandel bewusst. Darüber hinaus bestehen gewisse gegenseitige Abhängigkeiten mit der NIS2-Richtlinie, weshalb eine Reform der eIDAS-Verordnung von 2014 für die Kommission unerlässlich wurde. Insgesamt wirkt der Vorschlag der Kommission überhastet. Die wirtschaftlichen Interessen hinter dem Vorschlag sind beispielsweise Anbieter vertrauenswürdiger Dienste (TSP), die mit dieser Verordnung ihr Geschäftsmodell erweitern und an Bedeutung gewinnen wollen. Die Wallet App muss natürlichen Personen kostenlos angeboten werden, aber bei juristischen Personen kann ein Entgelt für die Software verlangt werden.

Ein weit verbreitetes eID-System ruft viele weitere Branchen auf den Plan, die daran teilhaben möchten. Der Bankensektor ist ein prominentes Beispiel, wo es um die Senkung der Compliance-Kosten für Know-Your-Customer-Vorschriften (KYC) geht. Andere Akteure in der Finanzbranche möchten die Zielgenauigkeit ihrer Finanzbewertung (Liquiditäts-Scores, Betrugserkennung, etc.) verbessern. In einigen EU-Ländern unterliegen Mobilanbieter ebenfalls KYC-Vorschriften und könnten von derartigen Technologien profitieren. In manchen Ländern würden Medienhäuser gerne Werbung ausspielen, die auf qualitativ äußerst hochwertiger Zielgruppenfokussierung beruht, und dazu eID-Daten nutzen. Schließlich würde auch der Onlinehandel diese Technologie gerne implementieren, um langfristig Kosten zu sparen und Compliance-Verbesserungen zu erzielen.

10 Siehe https://www.politico.eu/article/austrian-conservatives-want-to-end-online-anonymity-and-journalists-are-worried/ , https://netzpolitik.org/2021/tkg-novelle-seehofer-will-personalausweis-pflicht-fuer-e-mail-und-messenger-einfuehren/ und https://netzpolitik.org/2021/digitale-dienste-gesetz-eu-koennte-anonyme-uploads-auf-pornoseiten-verbieten/