(Dear President and Vice Presidents MEP Metsola, MEP Karas, MEP Picierno, MEP Pereira, MEP Kopacz, MEP Regner, MEP Wieland, MEP Barley, MEP Charanzová, MEP Šimečka, MEP Beer, MEP Zīle, MEP Papadimoulis, MEP Hautala, Dear Rapporteur, Opinion Rapporteurs and Shadow Rapporteurs MEP Jerković, MEP Terheş, MEP Arimont, MEP Ansip, MEP Terras, MEP Mituța, MEP Peksa, MEP Borchia, MEP Roos, MEP Kountoura, MEP Bielan, MEP Vandenkendelaere, MEP Pelletier, MEP Joron, MEP Maldonado López, MEP Maurel, MEP Benifei, MEP Breyer, MEP Melchior, MEP Kaljurand, MEP Toom, MEP Vilimsky, MEP Ernst)

1. Februar 2023

Sehr geehrter Vorsitzender, sehr geehrte stellvertretende Vorsitzende und Abgeordnete,

die unterzeichnenden Organisationen der Zivilgesellschaft (NGOs), Wissenschaftler und Experten sind wegen den bevorstehenden Abstimmungen zur eIDAS-Verordnung (EU) 2021/0136 (COD) im Europäischen Parlament besorgt. Digitale Identitätssysteme haben weltweit große Bedenken hinsichtlich der Grundrechte aufgeworfen.

Die Organisationen der Zivilgesellschaft, die dieses Schreiben unterzeichnet haben, wollen die Europäische Union in die Pflicht nehmen die Grundrechte zu schützen und ein System zu schaffen, das die sensibelsten Gesundheits-, Finanz- und Identitätsdaten nicht an Dritte weitergibt. Wenn Europa in dieser wichtigen Frage führend sein will, müssen Sie dies richtig machen.

Wir erkennen den gut entwickelten Datenschutzrahmen und die Rechtsgrundlage an, die Basis der aktuellen Reform der digitalen Identität in Europa sind. Diese sind notwendige, aber nicht hinreichende Voraussetzungen für ein System, das sich als zentrale, allgegenwärtige Plattform eignet und von dem künftig der Zugang zu E-Government, Handel, Bildung, sozialen Diensten und dem Arbeitsmarkt abhängen kann.

Es ist von entscheidender Bedeutung, dass potenziell Nutzende eine echte Wahl haben, ob sie dieses System verwenden oder nicht. Daher ist es notwendig gesetzlich einen starken Diskriminierungsschutz für diejenigen Teile der Bevölkerung zu verankern, die sich entscheiden das neue digitale Identitätssystem nicht zu nutzen, oder die dies nicht nutzen können. Senioren, digital weniger versierte Bevölkerungsschichten und Menschen ohne Smartphone dürfen nicht allein durch das Fehlen einer digitalen Identität an ihrer gesellschaftlichen Teilhabe gehindert werden. Entsprechende Schutzmaßnahmen müssen sowohl für den öffentlichen als auch für den privaten Sektor bestehen. So werden nicht nur Grundrechtsverletzungen und die Verstärkung sozialer Ungerechtigkeiten vermieden; dies trägt auch dazu bei das notwendige Vertrauen in der Bevölkerung für den Erfolg eines Systems zu schaffen, das für die meisten Nutzer ein Instrument einer echten Wahl darstellt.

Folglich erwarten wir, dass ein von der EU geschaffenes digitales Identitätssystem

den Prinzipien von Privacy by Design und by Default folgt. Es sollte technisch für die Betreiber des Systems, die verbundenen Unternehmen oder die Anbieter von Attributen unmöglich sein Kenntnis zu erlangen, wie Benutzer das System verwenden. Wenn das System große Verbreitung findet, könnte es einen panoptischen Überblick über alle Aspekte des täglichen Lebens liefern. Nur mit starken technischen Schutzmaßnahmen auf Architekturebene kann verhindert werden, dass Daten über das Benutzerverhalten kopiert und missbraucht werden können. Entsprechendes gelang bei dem digitalen EU-COVID-Zertifikat (EU) 2021/953 und ein solcher Standard muss auch hier eingehalten werden.

Privacy by Design verbietet auch die Erstellung einer eindeutigen und dauerhaften Kennung, die immer wieder dafür genutzt werden kann das Benutzerverhalten über Interaktionen mit einzelnen Unternehmen oder Regierungsbehörden hinweg zu verfolgen. Die Europäische Union wäre blauäugig zu glauben, dass eine eindeutige und dauerhafte Kennung nicht von Big-Tech-Unternehmen missbraucht würde, um deren Benutzer zu verfolgen und zu überwachen. Ein solches "Super-Cookie" würde nicht nur in mehreren Mitgliedstaaten ernsthafte verfassungsrechtliche Bedenken hervorrufen, sondern könnte auch den Zweck dieser Verordnung, datenschutzfreundliche Alternativen zu den dominierenden Big-Tech-Unternehmen zu bieten, zunichte machen. Letztendlich wird das System anhand der Robustheit und Wirksamkeit seiner technischen und rechtlichen Schutzmaßnahmen gegen die Überwachung und Profilerstellung von Benutzern beurteilt werden.

Deswegen muss die eIDAS-Verordnung regeln, welche Unternehmen oder staatlichen Stellen (Verwender) die Nutzer um welche Informationen bitten dürfen. Ein System, das den Zugriff auf Identitäts-, Finanz- und Gesundheitsinformationen von Hunderten von Millionen Menschen ermöglicht, wird immer eine lukrative Angriffsfläche für bösartige Akteure sein. Es muss in jedem Fall in jedem Mitgliedsstaat wirksame Rechtsschutzmöglichkeiten geben für Verbraucherschutz- und Betrugsbeschwerden im jeweiligen Hoheitsgebiet, unabhängig davon, wo der Verwender seinen Sitz hat. Eine wirklich vertrauenswürdige Umgebung kann nur entstehen, wenn Verwender von ihrem Niederlassungsmitgliedstaat für ihre Anwendung freigeschaltet werden müssen, bevor ihnen erlaubt wird persönliche Informationen von Benutzern über das neue System anzufordern. Dieser Aspekt wurde während der französischen Ratspräsidentschaft im Rat der Europäischen Union thematisiert. Zudem sollten staatlich zertifizierte Identifikationsdaten nur für Anwendungen verfügbar sein, wenn diese auf einer gesetzlichen Know-your-Customer-Verpflichtung beruhen.

Schließlich möchten wir das IT-Sicherheitsrisiko hervorheben, das durch die Verpflichtung zur Unterstützung qualifizierter Website-Authentifizierungszertifikate (QWACs) von Webbrowsern entsteht.[1] Obwohl dies kein direktes Problem der digitalen Identität ist, untergräbt es die Sicherheitsarchitektur des Internets auf Grund fragwürdiger kommerzieller Motive von Vertrauensdiensteanbietern. Dieser Ansatz hat in der Vergangenheit nicht nur dazu beigetragen die Sicherheit nicht zu erhöhen, da er den Nutzern verwirrende Informationen lieferte, sondern er ermöglicht auch die staatliche Überwachung des Internetverkehrs in großem Umfang[2]. Letztendlich sind solche Maßnahmen der Sicherheit aller Benutzer abträglich und gefährden die Akzeptanz der Bevölkerung für den Vorschlag insgesamt.

Die diesen Brief unterzeichnenden Organisationen glauben, dass ein europäisches System, das Grundrechte respektiert, ein globaler Gamechanger sein kann. Wir bitten Sie dringend diese Punkte bei den bevorstehenden Abstimmungen im Ausschuss für Industrie, Forschung und Energie und im Plenum sowie bei den bevorstehenden Trilog-Verhandlungen zu berücksichtigen. Bitte berücksichtigen Sie in dieser wichtigen Diskussion die Perspektive der Bürgerinnen und Bürger. Für weitere Konsultationen stehen wir zur Verfügung.

Zusammenfassend sind dies unsere wichtigsten Punkte[3]:
● Sicherung der freien Wahl über die Nutzung des digitalen Identitätssystems durch Schutzmaßnahmen vor Diskriminierung bei öffentlichen und privaten Dienstleistungen
● Verhinderung der Beobachtbarkeit des Benutzerverhaltens und aller persönlichen Transaktionen, die im System von Regierungen, Ausstellern und Attributanbietern vorgenommen werden
● Sicherstellung von Privacy-by-Design, indem keine eindeutigen und dauerhaften Kennungen festgelegt werden
● Effektive Regulierung von Anwendungsfällen, Verhinderung übermäßiger Informationsanfragen, Beschränkung von staatlich ausgestellten Identifizierungsinformationen auf solche, die auf einer gesetzlichen Know-your-Customer-Verpflichtung beruhen
● Verhinderung von Bestimmungen, welche die Unterstützung qualifizierter Website-Authentifizierungszertifikate von Webbrowsern vorschreiben.

Mit freundlichen Grüßen

Liste der Unterzeichnenden

---

[1] https://www.eff.org/de/deeplinks/2022/02/what-duck-why-eu-proposal-require-qwacs-will-hurt-internet-security

[2] https://blog.mozilla.org/netpolicy/2020/10/08/the-eus-current-approach-to-qwacs-qualified-website-authentication-certificates-will-undermine-security-on-the-open-web/

[3] Eine detailliertere Analyse der genannten Punkte in Bezug auf den Kommissionsvorschlag und die allgemeine Ausrichtung des Rates finden Sie unter: https://en.epicenter.works/document/3865 und https://en.epicenter.works/document/4384.