eIdentity im neuen Datenrecht: Das Zusammenspiel dezentraler rechtssicherer elektronischer Identifizierung und dem Recht auf Anonymität

Maxi Nebel und Paul C. Johannes

Zusammenfassung

Zentraler Bestandteil von eGovernment-Überlegungen ist die sichere Authentifizierung natürlicher Personen. Dies ergibt sich nicht nur aus einem Bedürfnis der Rechtssicherheit, sondern auch aus Praktikabilitätserwägungen. Die Europäische Kommission hat einen Vorschlag zur neuen Europäischen digitalen Identität (EUid) vorgelegt: Dabei handelt es sich um eine Art digitaler Brieftasche, in der die nationale elektronische Identität (eID) hinterlegt ist, aber auch Nachweise anderer persönlicher Attribute gespeichert werden können. Ziel soll es sein, dass Nutzende online auf Dienste zugreifen können, ohne private Identifizierungsmethoden verwenden oder unnötig personenbezogene Daten weitergeben zu müssen. Der Beitrag nimmt die Reform der eIDAS-VO zum Anlass, um diese vorzustellen, einen Überblick über den neuen Vertrauensdienst EUid zu geben und zu untersuchen, ob die Notwendigkeit der Identifizierung einer Person bei der Nutzung digitaler Dienste mit den Bedürfnissen nach Anonymität im Internet ausreichend ausgeglichen werden kann. Dabei wird auch auf das neue europäische Datenrecht eingegangen.

1. Einleitung: Identifizierung und Authentifizierung als zentrale Bausteine der Sicherheit digitaler Dienste

Digitale Geschäftsmodelle boomen und auch die öffentliche Verwaltung erweitert ihr Angebot für Online-Dienste stetig.[1] Grundlegende Vorausset-

1 Siehe z.B. Onlinezugangsgesetz (OZG), entsprechendes Änderungsgesetz „OZG 2.0", das Anfang 2023 auf den Weg gebracht wurde. Die Verwaltungsportale von Bund, Ländern und Kommunen sollen demzufolge interoperabel werden und Bürger und Unternehmen sollen eine digitale Identität bekommen, um Verwaltungsdienstleistungen online zu nutzen.

zung hierfür ist die sichere Authentifizierung der Nutzenden. Es geht dabei um Datensicherheit durch die Autorisierung der Nutzenden und die Authentizität der übermittelten Daten, aber auch um Vertrauen in rechtssichere digitale Dienste und Geschäfte. Dem steht das Recht auf Datenschutz und insbesondere das Bedürfnis nach Anonymität in einem schwer auflösbaren Widerspruch gegenüber. So müssen Anbieter von Social Networks beispielsweise Nutzenden nach § 19 Abs. 2 Telemedien-Teledienste-Datenschutzgesetz (TTDSG) die Möglichkeit bieten, die Plattform – wenn zumutbar – anonym zu nutzen, unterliegen andererseits nach § 3a Abs. 4 Nr. 2 NetzDG aber der Pflicht, strafbare Inhalte nebst Nutzername, IP-Adresse und ähnliches des erstellenden Nutzenden dem Bundeskriminalamt zu melden.[2]

Zentraler Bestandteil von eGovernment-Anwendungen muss dennoch die sichere Authentifizierung natürlicher Personen sein. Dies ergibt sich nicht nur aus einem Bedürfnis der Rechtssicherheit, um Rechtsgeschäfte und Verwaltungsvorgänge digital abzuwickeln, sondern auch aus Praktikabilitätserwägungen, um etwa Berechtigungen für System- und Dienstezugriffe nachzuweisen. Letzteres zeigt sich insbesondere durch die Nachfrage nach Single-Sign-On (SSO) und die Entwicklung von Modellen der Self-Sovereign Identity (SSI).[3] Insbesondere zentral gesteuerte Systeme bergen jedoch datenschutzrechtliche Risiken, etwa hinsichtlich der Nachverfolgbarkeit oder Profilbildung.[4]

2. eIDAS-VO: Europäisches Dateninfrastrukturrecht

Elektronische Transaktionen in Wirtschaft und Verwaltung benötigen Sicherungsmittel wie Signaturen und Zeitstempel, um Manipulationen

2 Möglicherweise schafft das das „Gesetz gegen digitale Gewalt" einen Ausweg aus diesem Widerspruch zu Gunsten des Betroffenen, zu dessen Vorbereitung das BMJ im April 2023 ein Eckpunktepapier vorgestellt hat. In diesem ist eine Accountsperre für den Fall wiederholter Rechteverletzung vorgesehen, die es ermöglichen würde, die Persönlichkeitsrechtsverletzung durch einen bestimmten Account eines Social Networks oder sonstigen Diensteanbieters zu verhindern. Eine Identifizierung des Accounterstellers, mögliche strafrechtliche Konsequenzen sowie die (dauerhafte) Sperrung der hinter dem Account stehenden Person werden dadurch jedoch nicht verbessert.

3 Dazu *Kudra/Seegebart/Schwalm*, DuD 2022, 9.

4 Hinweis zum Stand: Die Ausführungen beziehen sich auf die Rechtslage zum März 2023. Da das Verfahren noch nicht abgeschlossen ist, sind weitere Änderungen möglich.

zu verhindern, Formerfordernisse einzuhalten und Beweissicherheit zu gewährleisten. Um diese zusammenhängend zu regeln, hat die Union die eIDAS-VO erlassen.[5] Diese „Verordnung 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt" koordiniert zum einen die nationalen Systeme zur elektronischen Identifizierung und zum anderen die unionseinheitliche Regelung von Vertrauensdiensten. Ihr Ziel ist es unter anderem, einen einheitlichen europäischen Markt für elektronische Sicherungsmittel zu schaffen und hierdurch das Vertrauen in den elektronischen Rechtsverkehr in der EU zu stärken. Die eIDAS-VO sieht zu diesem Zweck Vorgaben zur Vereinfachung und Harmonisierung der Nutzung von elektronischen Signaturen und vergleichbaren Identifikationssystemen vor, die für alle EU-Mitgliedstaaten unmittelbar und verbindlich gelten. Neben allgemeinen Bestimmungen enthält die eIDAS-VO vor allem zwei voneinander getrennte inhaltliche Regelungskomplexe: Einen zur Koordination nationaler Systeme zur elektronischen Identifizierung[6] und einen zur unionseinheitlichen Regelung von Vertrauensdiensten.[7] Ein „Vertrauensdienst" ist nach Art. 3 Nr. 16 eIDAS-VO „ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und entweder der Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln und Diensten für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten oder der Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder der Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten dient". Vertrauensdienste können einfach,[8] fortgeschritten oder qualifiziert sein. Die jeweiligen Anforderungen ergeben sich aus der eIDAS-VO, wobei die Einstufung aufeinander aufbaut.[9]

Die eIDAS-VO gilt seit 1. Juli 2016 unmittelbar in allen Mitgliedstaaten, bedarf also keiner zusätzlichen Umsetzungs- oder Anpassungsakte durch die Mitgliedstaaten. Verordnungen sind Teil der Rechtsordnungen der

5 Zu Entstehungsgeschichte und Entwurf *Roßnagel/Johannes*, ZD 2013, 65.

6 Dazu *Spindler/Rockenbauch*, MMR 2013, 139.

7 *Johannes*, in: Hentschel/Hornung/Jandt (Hrsg.), Mensch – Technik – Umwelt: Verantwortung für eine sozialverträgliche Zukunft, 2020, 587 (588).

8 „Einfach" ist ein allgemein anerkannter Sammelbegriff für die Arten von Vertrauensdiensten, die die Anforderungen „fortgeschritten" nicht erreichen.

9 Qualifizierte Vertrauensdienste sind fortgeschrittene Vertrauensdienste, die zusätzlich die einschlägigen Anforderungen der eIDAS-VO erfüllen.

Mitgliedstaaten und genießen Anwendungsvorrang vor mitgliedstaatlichen Gesetzen. Ergänzt und präzisiert wird die eIDAS-VO in Deutschland unter anderem durch das Vertrauensdienstegesetz, das Personalausweisgesetz und diverse Vorschriften in Verfahrensordnungen. Nationale Vorschriften behalten gegenüber der eIDAS-VO grundsätzlich ihre Gültigkeit und können sogar die Regelungen der eIDAS-VO ergänzen und konkretisieren, soweit sie inhaltlich nicht im Widerspruch zu diesen stehen.[10] Der nationale Gesetzgeber darf kein gegen Unionsrecht verstoßendes Recht setzen.[11]

3. Reformvorschlag zur eIDAS-VO: Regulierung digitaler Identitäten

Um die Wirksamkeit der eIDAS-VO zu verbessern, ihre Vorteile auf den privaten Sektor auszuweiten und vertrauenswürdige digitale Identitäten für alle Europäer zu fördern, hat die EU-Kommission einen Vorschlag zur Reform der eIDAS-VO vorgelegt.[12] Der Gesetzgebungsprozess ist noch nicht abgeschlossen. Der Rat der EU hat am 6. Dezember 2022 einen gemeinsamen Standpunkt[13] veröffentlicht. Anfang 2023 hat das Europäische Parlament erste Änderungsvorschläge vorgelegt[14] und eine entsprechende Position für die Trilog-Verhandlungen beschlossen (A9-0038/2023).[15] Der Europäische Rat und das Parlament erzielten am 29. Juni 2023 eine vorläufige politische Einigung über die Kernelemente der eIDAS-Reform.[16] Bis Anfang August 2023 war noch keine finale Version des Reformgesetzes veröffentlicht. Es wird erwartet, dass das Gesetzgebungsverfahren noch im Jahr 2023 abgeschlossen wird.

---

10 *Roßnagel*, MMR 2015, 359, 360.

11 EuGH, Rs. C-74/86, ECLI:EU:C:1988:198, Rn. 10 – Kommission/Deutschland; EuGH, Rs. C-106/77, ECLI:EU:C:1978:49, Rn. 17, 18 – Simmenthal II.

12 Vorgang 2021/0136/COD.

13 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, Gemeinsamer Standpunkt vom 6 Dezember 2022, Dokument ST 15706 2022 INIT.

14 Konsolidierter Vorschlag des Europäischen Parlaments: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2023/02-09/05_CA_eIDAS_EN.pdf;

15 https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_DE.pdf.

16 PM Rat der EU vom 29. Juni 2023, https://www.consilium.europa.eu/de/press/press-releases/2023/06/29/council-and-parliament-strike-a-deal-on-a-european-digital-identity-eid/.

Anstoß der Reform ist, dass sich auf dem Markt ein neues Umfeld abzeichnet, in dem sich der Schwerpunkt von der Bereitstellung und Verwendung starrer digitaler Identitäten auf die Bereitstellung und Verwendung einzelner Attribute dieser Identitäten verlagert hat. Die Nachfrage nach Lösungen für die elektronische Identität, mit denen diese Anforderungen erfüllt werden und nicht nur Effizienzgewinne, sondern auch ein hohes Maß an Vertrauen sowohl im privaten als auch im öffentlichen Sektor in der gesamten EU erzielt werden, ist gestiegen.[17] Die derzeitige Verordnung würde diesen neuen Marktanforderungen nicht gerecht, weil sie ausschließlich auf den öffentlichen Sektor beschränkt ist, die Verknüpfung privater Online-Anbieter mit eID-Lösungen kompliziert und nur begrenzt möglich ist, notifizierte eID-Lösungen nicht in allen Mitgliedstaaten ausreichend verfügbar sind und die Verordnung keine ausreichende Flexibilität böte, um eine Vielzahl von Anwendungsfällen abzudecken. Alternative Identitätslösungen, die nicht in den Anwendungsbereich der eIDAS-Verordnung fallen, etwa solche, die von Betreibern sozialer Medien und von Finanzinstituten angeboten werden, geben zudem Anlass zu Bedenken hinsichtlich des Schutzes der Privatsphäre und des Datenschutzes.[18] Außerdem ist es bisher den meisten Menschen nicht möglich, Informationen über ihre Identität, Alter, berufliche Qualifikation, Führerschein oder andere Berechtigungen sowie Zahlungsdaten sicher und unter Einhaltung eines hohen Datenschutzniveaus grenzüberschreitend auszutauschen.[19]

3.1 EUid-Brieftasche

Um diese Lücke zu schließen, schlägt die EU-Kommission die sogenannte EUid-Brieftasche vor.[20] Diese soll es den Nutzenden gemäß Art. 6a Abs. 1

17 Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS), COM(2021) 290 final, S. 7 f.

18 Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS), COM(2021) 290 final, S. 8.

19 Erwägungsgrund 35 eIDAS-VO-E.

20 Der Architecture and Reference Framework (Architektur und Referenzrahmen für die EUid-Brieftasche) Januar 2023, Version 1.0, Repository: https://code.europa.eu/eudi/architecture-and-reference-framework soll als gemeinsamer Standard zur Entwicklung der EUid-Brieftasche dienen.

und Erwägungsgrund 9 eIDAS-VO-E ermöglichen, sich online und offline grenzübergreifend für öffentliche und private Dienste elektronisch zu identifizieren und zu authentifizieren. Neben dem Ziel, bürger- und unternehmensfreundliche digitale Dienste anzubieten, soll vor allem eine Alternative zu Wallets großer US-Konzerne wie Apple Wallet geboten werden, um zu verhindern, dass EU-Bürger wichtige Daten und Dokumente dort hinterlegen.[21] Das ist wirtschaftlich für die EU unvorteilhaft. Für die EU-Bürger ist es riskant, da für personenbezogene Daten von EU-Bürgern, die in den USA gespeichert werden, kein ausreichender Schutz gewährleistet werden kann und dem Zugriff der jeweiligen Nachrichtendienste ausgesetzt sind.[22] Die Regelungen zum „EU-US Data Privacy Framework" bieten hier zwar neue Rechtschutzmöglichkeiten, lösen das in der Speicherung wichtiger elektronischer Dokumente in Drittländern liegende immanente Probleme jedoch nicht auf.

Um eine möglichst breite Verfügbarkeit und Nutzbarkeit der EUid-Brieftasche zu erreichen, sollen neben der öffentlichen Verwaltung auch private Anbieter etwa in den Bereichen Verkehr, Energie, Bank- und Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Wasserversorgung, Postdienste, digitale Infrastruktur, Bildung oder Telekommunikation als sogenannte private vertrauende Beteiligte die Nutzung der Brieftasche akzeptieren, wenn aufgrund rechtlicher oder vertraglicher Verpflichtungen eine starke Nutzerauthentifizierung notwendig ist.[23] Dies würde das Online-Ausweiswesen erheblich voranbringen. Zudem sollen auch große Online-Plattformen im Sinne des Art. 33 DSA die EUid-Brieftasche akzeptieren müssen, sofern sie von den Nutzenden eine Authentifizierung für Online-Dienste, etwa zur Überprüfung des Alters, verlangen.[24] Der Verordnungsentwurf statuiert damit einen zumindest teilweisen Anbindungszwang privater Diensteanbieter.[25]

Jeder Mitgliedstaat hat gemäß Art. 6a Abs. 1 eIDAS-VO-E 12 Monate nach Inkrafttreten der Verordnung eine EUid-Brieftasche herauszugeben.

21 So können in einzelnen Bundesstaaten der USA bereits Führerscheindaten in der Apple Wallet hinterlegt werden, *Wölbert*, c't 09/2022, S. 144.

22 Zu letzterem Punkt *Roßnagel u.a.,* DuD 2022, 156.

23 Erwägungsgrund 28 und Art. 12b Abs. 2 eIDAS-VO-E.

24 Art. 12 Abs. 3 eIDAS-VO-E und Erwägungsgrund 28 eIDAS-VO-E. Der für diese Ausarbeitung zugrunde liegende eIDAS-VO-E spricht noch von Art. 25 DSA. In der rechtsgültigen Fassung des DSA (Verordnung (EU) 2022/2065) handelt es sich dabei aber um Art. 33 DSA.

25 *Liptak*, DuD 2022, 18 (19).

Gemäß Abs. 2 kann diese alternativ von einem anderen Aussteller herausgegeben werden, entweder im Auftrag des Mitgliedstaates (lit. b) oder auch unabhängig, aber von einem Mitgliedstaat anerkannt (lit. c). Der Ausbau der nationalen eID-Systeme wird so beschleunigt und der Prozess der Notifizierung verändert, denn eID-Systeme sollen nach Art. 12a eIDAS-VO-E zertifiziert werden und die Übergangsfrist zur Pflicht einer gegenseitigen Anerkennung wird von zwölf auf sechs Monate verkürzt.[26]

Mindestanforderungen an die EUid-Brieftasche sind nach Art. 6a Abs. 3 eIDAS-VO-E die Online- und Offline-Authentifizierung für öffentliche und private Online-Dienste durch sicheres, transparentes und nachvollziehbares Anfordern und Erhalten, Speichern, Auswählen, Kombinieren und Weitergeben der erforderlichen gesetzlichen Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen (lit. a) sowie das Unterzeichnen mit qualifizierten elektronischen Signaturen (lit. b).[27]

Für eine größtmögliche Praktikabilität und weitreichende Anwendbarkeit der EUid-Brieftasche definiert Art. 6a Abs. 4 lit. a eIDAS-VO-E, für wen und für welche Zwecke gemeinsame Schnittstellen vorhanden sein müssen. Zur Gewährleistung der Vertrauenswürdigkeit der EUid-Brieftasche formuliert der Verordnungsentwurf verschiedene Anforderungen. So muss die EUid-Brieftasche gemäß Art. 6a Abs. 4 lit. c eIDAS-VO-E das Sicherheitsniveau „hoch" im Sinne des Art. 8 eIDAS-VO erfüllen, insbesondere bezüglich der Anforderungen an Identitätsnachweis und Identitätsüberprüfung und an die Verwaltung und Authentifizierung elektronischer Identifizierungsmittel. Außerdem dürfen gemäß Art. 6a Abs. 4 lit. b eIDAS-VO-E die Vertrauensdiensteanbieter, die Attributsbescheinigungen ausstellen, keinerlei Informationen darüber erhalten, wie das entsprechende Attribut verwendet wurde.

Weiterhin verspricht der Verordnungsentwurf in Art. 6a Abs. 7 Satz 1 eIDAS-VO-E, dass die uneingeschränkte Kontrolle über die EUid-Brieftasche beim Nutzenden liegt. Das bedeutet gemäß Satz 2 insbesondere, dass Aussteller der Brieftasche Informationen über die Verwendung der Brieftasche, die für die Erbringung der damit verbundenen Dienste nicht erforderlich sind, nicht sammeln dürfen. Außerdem darf der Aussteller auch andere Personenidentifizierungsdaten oder andere Daten nicht mit personenbezogenen Daten aus anderen vom Aussteller angebotenen Diensten oder aus

26 *Seegebart*, DuD 2022, 5 (6).
27 *Seegebart*, DuD 2022, 5 (6).

Diensten Dritter kombinieren. Etwas anderes gilt nur, wenn der Nutzende dies ausdrücklich verlangt.

Die zur Bereitstellung der Brieftasche erforderlichen Daten (der Verordnungsentwurf spricht von „Daten in Bezug auf die Bereitstellung") müssen gemäß Art. 6a Abs. 7 Satz 3 eIDAS-VO-E von allen anderen gespeicherten Daten physisch und logisch getrennt gehalten werden. Genauere technische Vorgaben gibt es keine. Zwar darf die Kommission gemäß Art. 6a Abs. 11 eIDAS-VO-E innerhalb von 6 Monaten nach Inkrafttreten der Verordnung per Durchführungsrechtsakt technische und betriebliche Spezifikationen erlassen, dies gilt jedoch nur für die Anforderungen der Absätze 3, 4 und 5, nicht jedoch für das Versprechen der uneingeschränkten Kontrolle des Nutzenden und die physische und logische Trennung der Daten nach Absatz 7.

Nach Art. 11a eIDAS-VO-E müssen Mitgliedstaaten für ihre notifizierten Identifizierungsmittel und EUid-Brieftaschen eine eindeutige Identifizierung gewährleisten. Dies soll durch eine eindeutige und dauerhafte Kennung geschehen, die mit einem von den Mitgliedstaaten nach Art. 12 Abs. 4 lit. d eIDAS-VO-E zu definierenden Mindestsatz an Personenidentifizierungsdaten verknüpft werden, um den Nutzenden zu identifizieren, wenn diese gesetzlich vorgeschrieben ist.

3.2 Neue Vertrauensdienste

Vertrauensdienste dienen dazu sicherzustellen, dass elektronische Daten nicht unbemerkt verändert wurden und schaffen so einen Vertrauensraum im elektronischen Rechtsverkehr. Neben den in der eIDAS-VO bisher schon geregelten Vertrauensdiensten zur Erstellung, Überprüfung, Validierung von Signaturen, Siegeln Zeitstempeln und Zertifikaten zur Webseitenauthentifizierung kommen in Art. 3 Nr. 16 eIDAS-VO-E neue hinzu. Diese dienen in erster Linie der Durchführung und Umsetzung der EUid-Brieftasche.

Die Vertrauensdienste zur Beweiswerterhaltung von Signaturen und Siegeln werden ergänzt um einen Vertrauensdienst zur langfristigen Aufbewahrung elektronischer Dokumente. Der Vertrauensdienst zur elektronischen Archivierung elektronischer Dokumente gemäß Art. 3 Nr. 16 lit. d, Nr. 47 eIDAS-VO-E ist ein Dienst für die Entgegennahme, Speicherung Löschung und Übermittlung elektronischer Daten und Dokumente, der ihre Unversehrtheit, die Richtigkeit ihrer Herkunftsangaben und ihre recht-

lichen Merkmale während des gesamten Aufbewahrungszeitraums gewährleistet.[28] Denkbarer Anwendungsbereich könnte die revisionssichere elektronische Finanzbuchhaltung sein,[29] mit dem erklärten Ziel bestehende nationale Anforderungen zur Archivierung zu vereinheitlichen und grenzüberschreitende Anerkennung qualifizierter Dienste zu erleichtern.[30] In jedem Fall sind aber weitere technische Vorgaben notwendig, die gemäß Art. 45g eIDAS-VO-E per delegiertem Rechtsakt durch die Kommission zu erlassen wären.

Der Vertrauensdienst zur Verwaltung von elektronischen Fernsignatur- und Siegelerstellungseinheiten gemäß Art. 3 Nr. 16 lit. e eIDAS-VO-E gehört ebenfalls zu den im Reformvorschlag neu aufgenommenen Vertrauensdiensten. Gemäß Art. 3 Nr. 23 a und b eIDAS-VO-E sind qualifizierte elektronische Fernsignatur- und Siegelerstellungseinheiten solche, bei denen ein qualifizierter Vertrauensdiensteanbieter die elektronischen Signatur- bzw. Siegelerstellungsdaten im Namen eines Unterzeichners bzw. Siegelerstellers erzeugt, verwaltet oder vervielfältigt. Konkrete Anforderungen an die qualifizierten Dienste finden sich in Art. 29a und 39a eIDAS-VO-E. Soweit die Authentifizierung eines Fernsignaturnutzers durch eine eID abgesichert würde, könnten solche Fernsignaturen schnell im Bedarfsfalle genutzt werden, da ein längeres und medienbrechendes Authentifizierungsverfahren vermieden werden könnte.[31]

Das elektronische Vorgangsregister aus Art. 3 Nr. 16 lit. f eIDAS-VO-E ist gemäß Art. 3 Nr. 53 eIDAS-VO eine fälschungssichere Aufzeichnung elektronischer Daten, die die Echtheit und Unversehrtheit der enthaltenen Daten, die Richtigkeit ihres Datums und ihrer Uhrzeit sowie die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet. Es dient damit der fälschungssicheren Gewährleistung der Eindeutigkeit, Echtheit und richtigen Abfolge von Dateneinträgen.[32] So können zuverlässige Audit-Trails für die Herkunft von Waren im grenzüberschreitenden Handel geschaffen, der Schutz der Rechte des geistigen Eigentums unterstützt, Flexibilitätsmärkte für Strom ermöglicht, die Grundlage für fortgeschrittene Lösungen für eine

28 *Granc/Fiedler*, DuD 2022, 27 (28 f.).
29 *Liptak*, DuD 2022, 18 (21).
30 Erwägungsgrund 33 eIDAS-VO-E.
31 Einsatzszenario: Eine Bank bietet Kreditabschlüsse online an. Verbraucherkreditverträge bedürfen der Schriftform. Die Unterschrift des Kunden kann durch Fernsignatur erfolgen, wobei die Authentifizierung durch den Vertrauensdiensteanbieter mittels eID erfolgt. Der Vorgang geschieht aus Sicht des Verbrauchers medienbruchfrei.
32 Erwägungsgrund 34 eIDAS-VO-E.

selbst-souveräne Identität geschaffen und effizientere und transformative öffentliche Dienstleistungen unterstützt werden. Abschnitt 11 des Reformvorschlags schafft einen Rahmen für Vertrauensdienste in Bezug auf die Erstellung, Pflege und Rechtswirkungen elektronischer Vorgangsregister und Anforderungen an qualifizierte elektronische Vorgangsregister.

Kein Vertrauensdienst im engeren Sinne, weil nicht in Art. 3 Nr. 16 eIDAS-VO-E genannt, aber von größter Bedeutung für die Praktikabilität und Akzeptanz der EUid-Brieftasche, sind elektronische Attributsbescheinigungen im Sinne des Art. 3 Nr. 44 eIDAS-VO-E. Dabei handelt es sich um elektronische Bescheinigung zur Authentifizierung von Attributen. Attribute sind gemäß Art. 3 Nr. 43 eIDAS-VO-E elektronische Elemente, Eigenschaften oder Merkmale einer natürlichen oder juristischen Person. Mögliche Anwendungsbereiche sind vielfältig, etwa Sozialversicherungsdaten, Geburtsurkunden, Führerschein, Abschlusszeugnisse oder Reisedokumente.[33] Denkbar sind darüber hinaus auch Angaben über die Vertretungsmacht des EUid-Nutzenden für eine andere natürliche oder juristische Person, amts- und berufsbezogene oder sonstige Angaben zur Person des EUid-Nutzenden oder weitere personenbezogene Angaben.[34] Abschnitt 9 des Reformentwurfs beinhaltet Bestimmungen über die Rechtswirkung elektronischer Attributsbescheinigungen in Art. 45a eIDAS-VO-E, ihre Verwendung in öffentlichen Diensten in Art. 45b eIDAS-VO-E und die Anforderungen an qualifizierte Attributsbescheinigungen in Art. 45c eIDAS-VO-E. Um ein hohes Maß an Vertrauen zu gewährleisten, beinhaltet Art. 45d eIDAS-VO-E eine Bestimmung über die Überprüfung von Attributen anhand authentischer Quellen. Damit die Verfügbarkeit elektronischer Attributsbescheinigungen den Nutzenden der EUid-Brieftasche zugutekommt und damit die Nutzenden sich solche Bescheinigungen für EUid-Brieftaschen ausstellen lassen können, müssen Anbieter elektronischer Attributsbescheinigungen nach Art. 45e eIDAS-VO-E eine Schnittstelle zur EUid-Brieftasche bereitstellen. Art. 45f eIDAS-VO-E enthält zusätzliche Vorschriften für die Erbringung von Diensten für elektronische Attributsbescheinigungen, unter anderem zum Schutz personenbezogener Daten.

33 Erwägungsgrund 26 und 27 des Verordnungsentwurfs.
34 So bereits § 12 Abs. 1 Nr. 1-3 VDG.

4. Digitale Identitäten im Kontext des neuen europäischen Datenrechts

Als neues Rechtsgebiet hat das Datenrecht mittlerweile schon sehr konkrete Konturen angenommen. Data Governance Act (DGA), Digital Services Act (DSA), Digital Markets Act (DMA), Artificial Intelligence Act (AIA) und Data Act (DA) bestimmen zukünftig neben der Datenschutz-Grundverordnung (DSGVO) über Austausch, Nutzung und Dienste um Daten. Diese Rechtsakte hängen auf verschiedene Art und Weise zusammen und greifen ausdrücklich und indirekt ineinander.[35] Diese (geplanten) Rechtsakte der Europäischen Union zum Datenrecht sind direkt und indirekt mit der eIDAS-VO verzahnt und verlangen zum Beispiel eine rechtssichere Identifizierung. Diese darf die Nutzenden jedoch nicht in ihren grundrechtlich gewährleisteten Rechten einschränken. Aus den verfassungsrechtlich garantierten Rechten auf Schutz personenbezogener Daten aus Art. 8 Grundrechtecharta (GrCh) sowie dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 Grundgesetz (GG), aber auch dem Recht auf freie Meinungsäußerung aus Art. 11 GrCh sowie Art. 5 GG, erwächst das Recht von Nutzenden, das Internet anonym oder unter Pseudonym zu nutzen.[36] Daraus erwächst zwar kein absolutes Recht auf Anonymität, ein Eingriff in diese Grundrechte ist aber nur möglich, wenn dieser verhältnismäßig ist.

Im Rechts- und Geschäftsverkehr gibt es Vorgaben, die ein Anonymbleiben verhindern. Bei Bankgeschäften und im Versicherungswesen gibt es Vorschriften, die eine Identitätsprüfung zwingend voraussetzen, etwa im Geldwäschegesetz. Auch die Durchführung von Verwaltungsangelegenheiten setzt eine Identitätsprüfung voraus. Und schließlich bedarf es für eine effektive Strafverfolgung der Möglichkeit, die Personalien einer Person festzustellen. Für Online-Plattformen gibt es keine gesetzlich vorgeschriebene Prüfung zur Feststellung der Identität bei Erstellung eines Accounts. Gerade auf Social-Media-Plattformen besteht jedoch eine erhebliche Gefahr für die Verbreitung von Desinformationen[37] und sogar die Begehung von Straf-

35 Ausführlich *Geminn/Johannes* (Hrsg.), Europäisches Datenrecht, 2023, passim.

36 Z.B. *Jarass*, in: Jarass/Pieroth (Hrsg.), Grundgesetz, 2022, Art. 5 GG, Rn. 13, 110; *Polenz*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 2022, Teil 13, Kap. 130 Rn. 59. S. auch das Urteil des EuGH zum Verstoß der deutschen Vorratsdatenspeicherung gegen Unionsrecht, EuGH (Große Kammer), Urt. v. 20.9.2022 – C-793/19, C-794/19 (Bundesrepublik Deutschland/SpaceNet AG ua), Rn. 54.

37 Dazu *Steinebach u.a.* (Hrsg.): Desinformation aufdecken und bekämpfen, 2020, passim.

taten, Urheberrechtsverletzungen und Hasskriminalität, die dadurch nur schwer verfolgbar ist.[38] Häufig wird daher darüber diskutiert, ob eine Identifizierung der Nutzenden notwendig ist, um Straftaten besser verfolgen zu können. Die sogenannte Klarnamenpflicht sollte zur Konsequenz haben, dass alle Nutzenden einer Online-Plattform sich immer dem Plattformbetreiber gegenüber eindeutig identifizieren müssten und eine anonyme oder pseudonyme Nutzung faktisch ausgeschlossen wäre. Für die informationelle Selbstbestimmung und die Meinungsfreiheit stellt eine Verpflichtung aller Nutzenden zur Identifizierung gegenüber dem Plattformbetreiber in Abwägung mit Strafverfolgungsinteressen der Allgemeinheit und anderer schwerwiegender Risiken[39] aber einen unverhältnismäßigen Eingriff dar.[40]

Möglicherweise ließe sich die EUid-Brieftasche hier interessenausgleichend und grundrechtschonend nutzbar machen. Grundsätzlich wäre es möglich, dass eine Online-Plattform, z.B. ein Kurznachrichtendienst, eine Authentifizierung eines Nutzenden anstößt, die darauf beschränkt ist festzustellen, dass diese eine eineindeutige eID verwendet.[41] Auf diese Weise könnte die Plattform versuchen sicherzustellen, dass hinter jedem Nutzenden auch tatsächliche eine natürliche Person steht. So könnte sie sog. Trollfabriken und -netzwerken sowie Fake-Accounts entgegenwirken. Denkbar wäre aber auch, ein Pseudonym zu generieren, das in Form eines Attributs im Sinne des Art. 3 Nr. 43 eIDAS-VO-E in der EUid-Brieftasche hinterlegt ist. Dieses Pseudonym müsste von einem Treuhänder, etwa einem Vermittlungsdienst nach Art. 10 lit. a DGA, vergeben und verwaltet werden. Im Falle einer möglichen Strafverfolgung wegen krimineller Handlungen auf Online-Plattformen kann der Treuhänder die Identifizierung der Person gegenüber den Strafverfolgungsbehörden ermöglichen. Wirkungsvoll wäre diese Lösung nur, wenn Nutzende verpflichtet wären, sich mit der EUid-Brieftasche zu identifizieren – wenn auch nur mit Pseudonym. Dies widerspricht aber dem Ansatz des Art. 12b Abs. 3 eIDAS-VO-E, dass der Einsatz der EUid-Brieftasche alleinig auf Verlangen der Nutzenden geschehen soll.

38 Dies ist außerdem ein immer wieder bemühtes Argument für die Vorratsdatenspeicherung, die der EuGH zum Schutz der Anonymität im Netz nur für sehr eingeschränkt unionsrechtsmäßig hält, EuGH (Große Kammer), Urt. v. 20.9.2022 – C-793/19, C-794/19 (Bundesrepublik Deutschland/SpaceNet AG ua). Siehe dazu ausführlich *Roßnagel*, ZD 2022, 650.

39 ZB *Schmierer*, Klarnamenpflicht als Risiko für marginalisierte Gruppen, 2023.

40 Ausführlich zur Klarnamenpflicht *Nebel*, K&R 2019, 148 sowie *dies*., ZD-Aktuell 2022, 01077.

41 Zero Knowledge Proof, s.a. Art. 6a Abs. 4 (a) (vi) eIDAS-VO-E-Parl.

Hier obliegt es dem Gesetzgeber, die Voraussetzungen dafür zu schaffen, dass der Einsatz der EUid-Brieftasche größere Bedeutung erlangt.

Auch jenseits der Diskussion um die mögliche Identifikation von Personen für Zwecke der Strafverfolgung stellt sich die Frage, ob die EUid-Funktion im restlichen europäischen Datenrecht nutzbar zu machen ist bzw. welchen Beitrag die EUid-Brieftasche zur effektiven Umsetzung der Vorgaben in den jeweiligen Gesetz(-entwürf)en leisten kann.

4.1 eIDAS-VO-E

Der eIDAS-VO-E selbst verweist nur an einer Stelle explizit auf den DSA. Gemäß Art. 12b Abs. 3 eIDAS-VO-E sowie Erwägungsgrund 28 werden sehr große Online-Plattformen im Sinne des Art. 33 DSA[42] verpflichtet, die EUid-Brieftasche zu akzeptieren, wenn diese von ihren Nutzenden für den Zugang zu Online-Diensten eine Authentifizierung verlangen. Die Online-Plattformen dürfen die Nutzung der EUid-Brieftasche jedoch nicht einfordern, da es allein dem Nutzenden obliegt, ob er sich mit der EUid-Brieftasche authentifizieren möchte oder den Nachweis anders erbringt.

4.2 Digital Services Act (DSA)

Die Verordnung über einen Binnenmarkt für digitale Dienste trat am 16. November 2022 in Kraft und gilt ab dem 17. Februar 2024 unmittelbar in allen Mitgliedstaaten.[43] Der DSA richtet sich an Anbieter von Vermittlungsdiensten, zum Beispiel Internetdienstleister, Cloud-Anbieter, Suchmaschinen, Social Networks und andere Online-Plattformen sowie Online-Marktplätze. Er deckt eine Reihe von Fragen ab, unter anderem ein Verbot von gezielter Werbung, die sich an Minderjährige richtet oder auf besonderen Datenkategorien beruht; ein Verbot irreführender Praktiken und Schnittstellen; die Sorge für mehr Transparenz bei den Parametern für die Empfehlung, Kuratierung oder Priorisierung von Inhalten für Nut-

42 Der für diese Ausarbeitung zugrunde liegende eIDAS-VO-E spricht noch von Art. 25 DSA. In der rechtsgültigen Fassung des DSA (Verordnung (EU) 2022/2065) handelt es sich dabei aber um Art. 33 DSA.

43 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. EU vom 27.10.2022, L 277, 1.

zende; die Pflicht zu „Notice and Action"-Verfahren, um die Meldung und Entfernung illegaler Online-Inhalte zu ermöglichen, und die Pflicht zu „Know your business customer"-Anforderungen für Online-Marktplätze, um die Zuverlässigkeit von Händlern zu gewährleisten.[44]

Der DSA beinhaltet zwei Vorschriften, die für die EUid-Brieftasche von Bedeutung sein könnten. Gemäß Art. 23 Abs. 1 DSA setzen Anbieter von Online-Plattformen die Erbringung ihrer Dienste für Nutzende aus, die häufig und offensichtlich rechtswidrige Inhalte bereitstellen. Um diese Vorgabe effektiv umzusetzen und um zu verhindern, dass sich der betreffende Nutzende nicht unter falschem Namen als anderer Nutzender ausgibt, müsste jeder Nutzende eindeutig identifizierbar sein. Dies ließe sich grundsätzlich mit der EUid-Brieftasche bewerkstelligen. Um zu verhindern, dass jeder Vermittlungsdienst Kenntnis über die Identifikation seiner Nutzenden erlangt, könnte auch hier – wie im Zusammenhang mit der Klarnamenpflicht diskutiert – ein Rückgriff auf durch Treuhänder verwaltete Pseudonyme hilfreich sein.

Art. 30 DSA belegt Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, mit der Pflicht, die Nachverfolgbarkeit dieser Unternehmer sicherzustellen. Hierzu müssen die Unternehmer dem Anbieter der Online-Plattform bestimmte Informationen zur Verfügung stellen, die in Abs. 1 lit. a bis e näher aufgezählt sind. Hierzu zählen neben dem Namen und Kontaktdaten des Unternehmers (lit. a) die Kopie des Identitätsdokuments oder eine elektronische Identifizierung im Sinne des Art. 3 eIDAS-VO (lit. b), Angaben zum Zahlungskonto des Unternehmers (lit. c), sofern zutreffend Handelsregisternummer oder eine gleichwertige Kennung aus einem öffentlichen Register (lit. d) sowie eine Selbstbescheinigung des Unternehmers, in der sich dieser verpflichtet, nur Produkte oder Dienstleistungen anzubieten, die den geltenden Vorschriften des Unionsrechts entsprechen (lit. e). Hier kann die EUid-Brieftasche erhebliche Vereinfachungen bringen, da bis auf lit. e alle geforderten Angaben grundsätzlich als elektronische Attribute in der EUid-Brieftasche des Unternehmers hinterlegt und so rechtssicher und einfach nachgewiesen werden könnten. Voraussetzung ist lediglich, dass Informationen wie Kennungen aus öffentlichen Registern als elektronisches Attribut verfügbar gemacht werden. Gemäß Abs. 2 obliegt dem Anbieter der Online-Plattform die Pflicht zur Überprüfung dieser Informationen.

44 *Johannes*, ZD-Aktuell 2022, 01166.

Der Einsatz der EUid-Brieftasche würde dieses Verfahren erheblich vereinfachen.

4.3 Data Governance Act (DGA)

Der DGA[45] zielt darauf ab, das Vertrauen in die gemeinsame Nutzung von Daten zu stärken. Er soll neue EU-Regeln für die Neutralität von Datenmarktplätzen schaffen und die Wiederverwendung bestimmter Daten im Besitz des öffentlichen Sektors erleichtern.[46] Der DGA ist am 23. Juni 2022 in Kraft getreten und ist ab dem 24. September 2023 anwendbar.

Einer der zentralen Regelungsbereiche des DGA ist die Etablierung so genannter Datenvermittlungsdienste. Dabei handelt es sich gemäß Art. 2 Nr. 11 DGA um „einen Dienst, mit dem durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen". Anbieter von Datenvermittlungsdiensten müssen diese Tätigkeit gemäß Art. 11 DGA bei der zuständigen Behörde anmelden. Die Anmeldung muss gemäß Abs. 6 lit. a bis g bestimmte Informationen zum Anbieter enthalten, wie Name, Kontaktangaben, Rechtsform, Vertreter und einiges mehr. Hier könnte die EUid-Brieftaschen-Infrastruktur gut nutzbar gemacht werden, da viele der verlangten Angaben typische Attribute sind, die in einer EUid-Brieftasche hinterlegt werden könnten. Die Übermittlung der Anmeldedaten per EUid-Brieftasche könnte das Verfahren deutlich beschleunigen.

Ein weiterer zentraler Regelungsbereich im DGA ist der Datenaltruismus. Dabei handelt es sich um eine freiwillige Zurverfügungstellung von personenbezogenen und nicht-personenbezogenen Daten, um diese für Ziele von allgemeinem Interesse zu nutzen, wie die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die

45 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. EU vom 3.6.2022, L 152, 1.

46 *Johannes*, ZD-Aktuell 2022, 01166.

staatliche Entscheidungsfindung oder die wissenschaftliche Forschung.[47] Die Datenspende basiert auf der Einwilligung der spendenden Personen, so dass die nach Art. 17 ff. DGA zuständigen anerkannten datenaltruistischen Organisationen zum Einwilligungsmanagement verpflichtet sind. Art. 25 DGA sieht hierfür die Entwicklung eines Europäischen Einwilligungsformulars vor, um Datenspenden europaweit zu vereinfachen. Die Einbindung der EUid-Brieftasche könnte das Einwilligungsmanagement in jedem Fall vereinfachen, insbesondere hinsichtlich der Authentizität des Einwilligenden.

4.4 Data Act-Entwurf (DA-E)

Der Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz) – im öffentlichen Diskurs vorrangig als Data Act bekannt – wurde am 24. Februar 2022 durch die Europäische Kommission in das offizielle Gesetzgebungsverfahren der EU eingebracht.[48] Der DA-E enthält u. a. Regelungen für ein Recht auf Zugang von bei der Nutzung von Produkten oder verbundenen Diensten erzeugten Daten; ein Verbot unfairer Vertragsklauseln in standardisierten Datenlizenzverträgen; ein Recht auf Datenzugang und -nutzung durch öffentliche Stellen; eine Erleichterung des Wechsels von Datenverarbeitungsdiensten (insbesondere Cloud- und Edge-Anbieter) sowie Anforderungen an die Interoperabilität von Datenverarbeitungsdiensten sowie an die internationale Datenübertragung.[49] Am 20. Juni 2023 erzielten das Europäische Parlament und der Rat im Trilogverfahren eine politische Einigung über den Data Act. Diese Version war bis Anfang August 2023 noch nicht veröffentlicht. Allseits erwartet eird, dass der Data Act noch in 2023 offiziel verabschiedet wird.

Da der DA-E bisher nur als Vorschlag vorlag, können sich im Laufe des Gesetzgebungsprozesses noch Änderungen ergeben. Anknüpfungspunkte für die eIDAS-VO bieten insbesondere zwei Aspekte. Gemäß Erwägungsgrund 20 DA-E sollen „Nutzer von Produkten, die Daten erzeugen, […] in der Regel ein Nutzerkonto einrichten. Dies ermöglicht die Identifizierung des Nutzers durch den Hersteller sowie die Kommunikation zur Ausfüh-

47 *Geminn/Johannes/Müller/Nebel*, Is that even legal? A guide for builders experimenting with data governance in Germany, 2023.
48 Vorgang 2022/0047/COD.
49 *Johannes*, ZD-Aktuell 2022, 01166.

rung und Bearbeitung von Datenzugangsverlangen" im Sinne des Art. 4 DA-E. Erwägungsgrund 27 DA-E stellt zugunsten des Dateninhabers klar, dass dieser eine geeignete Nutzeridentifizierung verlangen kann, um die Berechtigung des Nutzenden auf Zugang zu den Daten zu überprüfen. Hier könnte die EUid-Brieftasche zum Einsatz kommen, und zwar sowohl zur Identifizierung mittels des Namens als auch möglicherweise mittels Pseudonyms, wenn dieses als elektronisches Attribut hinterlegt ist.

Zweiter Anknüpfungspunkt sind „intelligente Verträge". Dabei handelt es sich gemäß Art. 2 Nr. 16 DA-E um ein in einem elektronischen Vorgangsregistersystem gespeichertes Computerprogramm, bei dem das Ergebnis der Programmausführung in dem elektronischen Vorgangsregister aufgezeichnet wird. Elektronische Vorgangsregister sind gemäß Art. 2 Nr. 17 DA-E solche im Sinne des Art. 3 Nr. 53 eIDAS-VO. Diese Computerprogramme in elektronischen Vorgangsregistern sorgen dafür, Transaktionen zu vorab festgelegten Bedingungen auszuführen und abzuwickeln. Sie haben das Potenzial, Dateninhabern und Datenempfängern Garantien dafür zu bieten, dass die Bedingungen für die gemeinsame Nutzung von Daten eingehalten werden.[50] Art. 30 DA-E nennt des Weiteren wesentliche Anforderungen an intelligente Verträge für die gemeinsame Datennutzung.

5. Kritik und Vorschläge zur Rechtsfortbildung

Die EUid-Brieftasche ist konzipiert als Lösung für elektronische Identitäten, die sowohl im öffentlichen als auch im privaten Sektor nutzbar gemacht werden kann, die flexibel genug für viele verschiedene Anwendungsszenarien ist und einen sicheren grenzüberschreitenden Austausch von Informationen zur Identität einer Person zulässt. Eine flächendeckende Einführung einer EUid-Lösung ist begrüßenswert, um mehr Verfahren und Dienste, insbesondere in der öffentlichen Verwaltung, zukünftig rein digital rechtssicher durchführen zu können und sollte zum Anlass genommen werden, noch mehr Angebote hierfür zu schaffen.[51] Dennoch gibt es eine Reihe von Punkten, die aus Sicht des Schutzes der informationellen Selbstbestimmung und des Rechts auf Datenschutz bedenklich sind. Im Laufe des

50 Begründung zum Kommissionsvorschlag 2022/0047/COD, S. 4.

51 Allgemein zu Akzeptanzproblemen der derzeitigen deutschen eID-Lösung durch den neuen Personalausweis (nPA) *Seegebart*, DuD 2022, 5; *Skierka/Parycek*, HMD Praxis der Wirtschaftsinformatik, 1.

Gesetzgebungsverfahrens wurden einige dieser Punkte durch den für das Europäische Parlament federführenden Ausschuss für Industrie, Forschung und Energie (ITRE-Ausschuss) adressiert.[52] Ob und wie diese Eingang in die finale Fassung finden, bleibt jedoch abzuwarten. Im Folgenden werden die kritischen Punkte daher noch einmal zusammengefasst und Vorschläge zur Rechtsfortbildung gemacht.

5.1 Identifizierungskennziffer

Zunächst muss die Erforderlichkeit einer eindeutigen Identifizierungskennziffer bezweifelt werden. Zwar soll dies nach Art. 11a Abs. 2 eIDAS-VO-E „im Einklang mit dem Unionsrecht", also auch unter Zugrundelegung der Grundsätze der DSGVO erfolgen. Allerdings widerspricht es dem Zweck der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO, dem „Mindestsatz von Personenidentifizierungsdaten", die für sich genommen die Identifizierung der Person ermöglichen müssen, eine zusätzliche Kennziffer hinzuzufügen, die dauerhaft mit der Person des Nutzenden verknüpft ist. Die eindeutige dauerhafte Kennung zur Identifizierung des Nutzenden der EUid-Brieftasche birgt gleich eines „Super-Cookies"[53] erhebliche Risiken für die betroffene Person. Wird eine solche Kennung bereichsübergreifend von Behörden bis Onlineplattformen für digitale Services verwendet, könnten über alle Dienste hinweg umfassende Persönlichkeitsprofile erstellt werden.[54] Diese Gefahr wird noch dadurch verstärkt, dass jeder Mitgliedstaat selbst eine gesetzliche Identifizierung vorschreiben kann. So wäre es ein Leichtes, zum Beispiel eine Klarnamenpflicht in Social Media vorzuschreiben, die nur durch eine persönliche Identifizierung mit der EUid-Brieftasche durchgesetzt werden kann.[55] Privaten Online-Diensten würde die eigene umfassende Profilbildung durch eine staatlich verifizierte Kennziffer einfach gemacht werden. Auch die Entwurfsfassung des Rates vom

52 Konsolidierter Vorschlag des Europäischen Parlaments: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2023/02-09/05_CA_eIDAS_EN.pdf; *Greis*, Elektronische Identität: Europaparlament will lebenslange Personenkennziffer stoppen.

53 Offener Brief von Epicenter.works, weiteren NGOs und Datenschützern vom 1. Februar 2023, https://epicenter.works/sites/default/files/open_letter_eidas_2023-01_0.pdf.

54 So auch *Wölbert*, c't 09/2022, 144.

55 Zur Kritik an Art. 11a eIDAS-VO-E *Wölbert*, c't 9/2022, 144; s.a. *Nebel*, K&R 2019, 148; *dies.*, ZD-Aktuell 2022, 01077.

6. Dezember 2022 nimmt von der Kennziffer keinen Abstand.[56] Das Europäische Parlament möchte die Nutzung einer solchen Kennziffer zumindest erheblich einschränken und nur für grenzüberschreitende Transaktionen vorsehen, schließt eine solche aber nicht grundsätzlich aus (vgl. Art. 11a Abs. 2 eIDAS-VO-E-Parl). Aus datenschutzrechtlicher Sicht ist die Vergabe einer solcher Kennziffern grundsätzlich äußerst risikobehaftet. Eine dauerhafte, also lebenslang bestehende, eindeutige Kennung ist zur Identifizierung einer Person ist in der Regel nicht zwingend erforderlich, da der Abgleich des Namens und Geburtsdatums ggf. mit weiteren Attributen zur eindeutigen Identifizierung einer Person zumeist ausreichen wird. Daher liegt ein Verstoß gegen das Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO nahe und sollte zum Anlass genommen werden, Art. 11a eIDAS-VO-E insgesamt zu streichen.

Problematisch ist zudem, dass keine einheitlichen Vorgaben gemacht werden, für welche Zwecke eine Identifizierung samt eindeutiger dauerhafter Kennung notwendig sein soll. Vielmehr kann jeder einzelne Mitgliedstaat über die Zwecke der Identifizierung bestimmen. Dies lässt nicht nur einen Flickenteppich befürchten, sondern könnte darüber hinaus dazu führen, dass die Ausweispflicht online wie offline deutlich ausgeweitet wird. Wenn Mitgliedstaaten beispielsweise festlegen, dass jede Registrierung auf einer Online-Plattform mit Namen und eindeutiger Kennung zu erfolgen hat,[57] käme dies der Einführung einer Klarnamenpflicht durch die Hintertür gleich. Daher sollte klar geregelt werden, für welche Zwecke eine Identifizierung notwendig ist und wer welche Daten abfragen darf. Technische Vorkehrungen sollten unterstützen, dass nicht mehr Informationen abgefragt werden als rechtlich zulässig.

Zwar legt der Reformvorschlag der Kommission fest, dass die alleinige Kontrolle über die Daten beim Nutzenden verbleibt. Es steht jedoch zu befürchten, dass sich am Machtgefälle zwischen Nutzenden einerseits und großen Online-Plattformen andererseits nicht grundsätzlich etwas ändern wird. Der Datenschatz der EUid-Brieftasche könnte Begehrlichkeiten wecken und insbesondere private Anbieter dazu bringen, Nutzende durch Dark Patterns oder Versprechungen dazu zu verleiten, mehr Daten preiszugeben als nötig. An dieser Stelle müsste etwa durch gesetzlich vorgeschriebene restriktive Voreinstellungen sichergestellt werden, dass Nutzende

56 Vgl. Erwägungsgründe 17a und 17aa des Ratsentwurfs.
57 *Wölbert*, c't 9/2022, 144.

nicht etwa aus Unwissenheit oder Bequemlichkeit mehr Daten übermitteln als erforderlich.[58] Der Parlamentsentwurf sieht entsprechend eindeutig in Art. 6a Abs. 7a vor, dass die Nutzung der Europäischen digitalen Brieftasche freiwillig sei. Der Zugang zu öffentlichen und privaten Dienstleistungen und die Berufsfreiheit dürften in keiner Weise eingeschränkt werden für Personen, die keine EUid-Brieftasche verwenden. Kritisch hervorzuheben sind auch die fehlenden ausdrücklichen Möglichkeiten pseudonymer Nutzung.[59] Zwar sieht Art. 5 eIDAS-VO-E vor, dass die pseudonyme Nutzung bei elektronischen Transaktionen nicht untersagt werden darf. Wünschenswert, weil datenschutzfreundlich, wäre darüber hinaus aber die explizite Verpflichtung auf Ermöglichung der pseudonymen Identifizierung, auch und gerade gegenüber großen Online-Plattformen. Hierin würde ein großer Gewinn für die alltägliche Nutzung der Wallet liegen, um Straftaten im Internet leichter verfolgbar zu machen, ohne die wahre Identität aller Nutzenden in die Hände von einzelnen Online-Plattformen zu legen.

5.2 Verlust oder Missbrauch der EUid-Brieftasche

Bisher nur unzureichend geregelt ist zudem das Vorgehen bei Verlust oder Missbrauch der EUid-Brieftasche. Der Kommissionsentwurf sieht keine Regelungen für die Sperrung vor. Hier hat der Ratsentwurf zwar nachgebessert, weil Art. 6 Abs. 4a des Ratsentwurfs die Mitgliedstaaten verpflichten, entsprechende Regelungen für die Meldung des Verlusts oder Missbrauchs der EUid-Brieftasche oder Beantragung des Widerrufs vorzusehen. Auch der Parlamentsentwurf sieht in Art. 6a Abs. 5a vor, dass es möglich sein muss die Gültigkeit der EUid-Brieftasche zu widerrufen, und zwar entweder auf ausdrücklichen Antrag des Nutzenden, wenn die Sicherheit der Brieftasche beeinträchtigt wurde, beim Tod des Nutzenden oder bei Einstellung der Tätigkeit der juristischen Person. Dennoch bleibt weiter unklar, wie sichergestellt werden soll, dass eine Person nur die eigene EUid-Brieftasche sperrt oder widerruft und nicht die einer beliebigen anderen Person.

58 Die Regelung geht über Art. 25 DSGVO hinaus, da sie sich an die Entwickler der EUid-Brieftasche richtet und die Pflicht zu Privacy by Design und Default für die EUid-Brieftasche konkretisiert.

59 Der Parlamentsentwurf bessert hier nach, siehe insbesondere Art. 5.

5.3 Dezentrale Speicherung

Grundsätzlich begrüßenswert ist der Ansatz, dass die EUid-Brieftasche dezentral auf den Endgeräten der Nutzenden gespeichert wird und nicht zentral in einer einzigen Datenbank. Dennoch bleiben Bedenken hinsichtlich einer ausreichenden Datensicherheit. Die Speicherung auf den persönlichen Endgeräten der Nutzenden hat zur Folge, dass ihnen auch die große Verantwortung obliegt, für ausreichende Datensicherheit ihrer Endgeräte zu sorgen. Hier sind neben der grundsätzlich vorauszusetzenden Sicherheit und Verlässlichkeit der Software weitere Maßnahmen notwendig, die Nutzende niedrigschwellig dazu bringen, ein möglichst hohes Maß an Datensicherheit zu gewährleisten. Dies beginnt mit einer ausreichenden Zugangssperre zur EUid-Brieftasche (Passwort), Vermeiden von Spähsoftware auf dem Endgerät und hört bei konkreten automatisierten Hinweisen auf mögliche Gefahren auf dem Endgerät nicht auf.

Wichtige Aspekte der technischen Umsetzung der EUid-Brieftasche obliegen Durchführungsrechtsakten der Kommission, beispielsweise Art. 6a Abs. 11 und Art. 6b Abs. 4 eIDAS-VO-E. Dass konkrete technische Vorgaben nicht im Gesetz selbst spezifiziert sind, ist nicht ungewöhnlich und hat den Vorteil, dass sie sich bei schnellem technischem Wandel leichter anpassen lassen. Es wäre jedoch wünschenswert, konkrete Anforderungen an die Technik wie Interoperabilität, dezentrale Speicherung und die Verwendung offener Standards explizit im Gesetz zu normieren, um einen umfassenden Grundrechtsschutz zu gewährleisten und einen hohen technischen Standard zu gewährleisten. Insbesondere der Vorschlag des Parlaments ist hinsichtlich der Nennung technischer Zielvorgaben konkreter.

5.4 Bedeutung im Datenrecht erhöhen

Neben den konkreten Kritikpunkten zur EUid-Brieftasche, die sich aus dem eIDAS-VO-E ergeben, bleibt zu überlegen, wie deren Bedeutung im restlichen Datenrecht der Union intensiviert werden kann. Möglicherweise wäre eine explizite Bezugnahme auf die EUid-Brieftasche in anderen Rechtsakten oder eine Privilegierung ihres Einsatzes sinnvoll, um deren Verbreitung voranzutreiben. Denkbar wäre dies beispielsweise bei Art. 11 Abs. 6 DGA[60] im Rahmen der Anmeldung der Anbieter von Datenvermitt-

60 S. Kapitel 4.3.

lungsdiensten, bei Art. 25 DGA[61] im Rahmen des Europäischen Einwilligungsformulars oder bei der Durchsetzung der Sperrung solcher Nutzenden nach Art. 23 DSA[62], die rechtswidrige Inhalte auf Online-Plattformen bereitstellen.

6. Fazit

Die EUid-Brieftasche verspricht eine deutliche Vereinfachung bei der Nutzung elektronischer Dienste – unabhängig davon, ob diese grenzüberschreitend sind oder nicht. Auch das neue europäische Datenrecht bietet genügend Anknüpfungspunkte, um der EUid-Brieftasche zu noch mehr Bedeutung zu verhelfen. Einige der Vorschläge zur Umsetzung sind jedoch durchaus bedenklich und sollten der Legislative Anlass geben, auf eine datenschutzfreundliche Umsetzung hinzuarbeiten. Die Verhandlungen über die Kernelemte sind wohl abgeschlossen.[63] Die fachlichen Arbeiten zur Vervollständigung des Rechtstextes dauerten Anfang August 2023 noch an. Es bleibt abzuwarten, ob die Trilogverhandlungen die Interessen der Nutzenden der EUid-Brieftasche besser in den Blick genommen haben und insbesondere Aspekte wie die eindeutige lebenslange Kennziffer überdenken sowie Möglichkeiten pseudonymen Handelns, dezentrale Speicherung und ausreichende Datensicherheit im Gesetz verankern werden. Wenigstens Letzteres deutet das vorläufige Trilogergebnis an.

Literaturverzeichnis

Geminn, Christian L. und Johannes, Paul C. (Hrsg.): (2023): *Europäisches Datenrecht*. Baden-Baden: Nomos (in Vorbereitung).

Geminn, Christian L.; Johannes, Paul C.; Müller, Johannes und Nebel, Maxi (2023): *Is that even legal? A guide for builders experimenting with data governance in Germany*. Berlin: Mozilla Foundation. URL: https://foundation.mozilla.org/en/research/library/is-that-even-legal/germany/.

Granc, Franziska und Fiedler, Arno (2022): Nationale und europäische Sicht auf eIDAS 2.0 – Aufwand und Nutzen. *Datenschutz und Datensicherheit (DuD),* S. 27-31.

Greis, Friedhelm (9. Feb. 2023): Elektronische Identität: Europaparlament will lebenslange Personenkennziffer stoppen. URL: https://glm.io/171792.

61 S. Kapitel 4.3.
62 Kapitel 4.2.
63 PM Rat der EU vom 29. Juni 2023 (siehe oben Fn. 16).

Jarass, Hans D. und Kment, Martin (Hrsg.) (2022): *Grundgesetz für die Bundesrepublik Deutschland, Kommentar,* 17. Aufl. München: Beck. Zitiert als Jarass/Pieroth (Begr.).

Johannes, Paul C. (2020): Vertrauensdienste oder Bärendienste? Rechtssicherheit von Kundenportalen Blockchain & Co durch oder neben der eIDAS-VO. In: Hentschel, Anja; Hornung, Gerrit und Jandt, Silke (Hrsg.): *Mensch – Technik – Umwelt: Verantwortung für eine sozialverträgliche Zukunft*. Baden-Baden: Nomos, S. 587-602.

Johannes, Paul C. (2022): Europäisches Datenrecht – ein Spickzettel. *ZD-Aktuell*, 01166.

Kudra, Andre; Seegebart, Christian und Schwalm, Steffen (2022): Ein digitaler Vertrauensraum für Identitäten und Dienste – Europa ist auf dem richtigen Weg. *Datenschutz und Datensicherheit (DuD)*, Heft 1, S. 9-11.

Liptak, Patrick (2022): Ein neuer Rahmen für eine europäische digitale Identität. *Datenschutz und Datensicherheit (DuD)*, Heft 1, S. 18-21.

Nebel, Maxi (2019): Die Zulässigkeit der Erhebung des Klarnamens nach den Vorgaben der Datenschutz-Grundverordnung. *Kommunikation und Recht (K&R)*, Heft 3, S. 148-152.

Nebel, Maxi (2022): Klarnamenpflicht nach DS-GVO und TTDSG. *ZD-Aktuell*, 01077.

Roßnagel, Alexander (2015): Der Anwendungsvorrang der eIDAS-Verordnung – Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar? *Multimedia und Recht (MMR)*, Heft 6, S. 359-364.

Roßnagel, Alexander (2022): Vorratsdatenspeicherung – was geht noch und was nicht mehr? *Zeitschrift für Datenschutz (ZD)*, Heft 12, 650-655.

Roßnagel, Alexander; Geminn, Christian L.; Johannes, Paul C.; Müller, Johannes (2022): Auswirkungen ausländischer Gesetzgebung auf die deutsche Cybersicherheit. *Datenschutz und Datensicherheit (DuD)*, Heft 3, S. 156-163.

Roßnagel, Alexander und Johannes, Paul C. (2013): Entwurf einer EU-Verordnung über elektronische Identifizierung und Vertrauensdienste – Neue Regeln für elektronische Sicherheitsdienste. *Zeitschrift für Datenschutz (ZD)*, Heft 2, S. 65-72.

Schmierer, Anna-Lena (14. April 2023): Klarnamenpflicht als Risiko für marginalisierte Gruppen. URL: https://netzpolitik.org/2023/meta-verified-klarnamenpflicht-als-risiko-fuer-marginalisierte-gruppen/.

Seegebart, Christian (2022): eIDAS-Novellierung 2021 – erste Analyse des Proposals. *Datenschutz und Datensicherheit (DuD)*, Heft 1, S. 5-8.

Skierka, Isabel und Parycek, Peter (2023): Einwurf – Kann Deutschland seine eID noch retten? HMD Praxis der Wirtschaftsinformatik (8. März 2023), S. 1-6, https://doi.org/10.1365/s40702-023-00958-0.

Spindler, Gerald und Rockenbauch, Matti (2013): Die elektronische Identifizierung – Kritische Analyse des EU-Verordnungsentwurfs über elektronische Identifizierung und Vertrauensdienste. *Multimedia und Recht (MMR)*, Heft 3, S. 139-148.

Steinebach, Martin; Bader, Katarina; Rinsdorf, Lars; Krämer, Nicole und Roßnagel, Alexander (Hrsg.): (2020): *Desinformation aufdecken und bekämpfen. Interdisziplinäre Ansätze gegen Desinformationskampagnen und für Meinungspluralität.* Baden-Baden: Nomos.

Taeger, Jürgen und Pohle Jan (Hrsg.) (2022): *Computerrechts-Handbuch*, 37. Ed. München: Beck.

Wölbert, Christian (2022): Orwells Brieftasche. Die umstrittenen Pläne für eine europäische digitale Identität. *c't Magazin*, Heft 9, S. 144.