Formelle Bemerkungen des EDSB zum 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

1. Einleitung und Hintergrund

- Am 3. Juni 2021 wurde der EDSB gemäß Artikel 42 Absatz 1 der Verordnung 2018/1725[1] zum 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[2] konsultiert.
- Der Begründung zufolge sollten mit dem Vorschlagsentwurf Mängel in der derzeit geltenden Verordnung[3] behoben werden, wie zum Beispiel:
  - begrenzte Abdeckung notifizierter elektronischer Identifizierungssysteme,
  - begrenzte Angebote von Authentifizierungen gemäß eIDAS für grenzübergreifend tätige Nutzer öffentlicher Dienste,
  - Begrenzung auf öffentliche Dienste, trotz der im privaten Sektor bestehenden Marktnachfrage,
  - keine Abdeckung von elektronischen Attributen wie ärztlichen Bescheinigungen oder Berufsqualifikationen, was die Gewährleistung der europaweiten rechtlichen Anerkennung solcher Berechtigungsnachweise in elektronischer Form erschwert.
- Dank des überarbeiteten Rahmens für die europäische digitale Identität sollten die Bürger und Einwohner darüber hinaus voll und ganz darauf vertrauen können, dass dieser Rahmen für die europäische digitale Identität jedem die Mittel an die Hand geben wird, um zu kontrollieren, wer Zugang zum eigenen digitalen Zwilling hat und auf welche Daten er im Einzelnen zugreifen kann.
- Dabei wird in Bezug auf alle Aspekte der Bereitstellung der digitalen Identität, einschließlich der Ausstellung einer Brieftasche für die europäische digitale Identität („EUid-Brieftasche“) und der Infrastruktur für die Erhebung, Speicherung und Offenlegung von Daten der digitalen Identität, ein hohes Maß an Sicherheit gewährleistet.

---

[1] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 vom 21.11.2018, S. 39 (Verordnung (EU) 2018/1725).

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281.

[3] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257 vom 28.8.2014, S. 73 .

- Mit dem Vorschlag wird die derzeitige Liste der Vertrauensdienste gemäß eIDAS-Verordnung um drei neue qualifizierte Vertrauensdienste erweitert, nämlich die Bereitstellung von Diensten für die elektronische Archivierung, elektronische Vorgangsregister und die Verwaltung von elektronischen Fernsignatur- und -siegelerstellungseinheiten.
- Die vorgeschlagene eIDAS-Verordnung besteht nach wie vor aus zwei sehr wichtigen Teilen, Kapitel II (bislang „Elektronische Identifizierung") und Kapitel III („Vertrauensdienste"). Allerdings ist Kapitel II jetzt in drei Abschnitte unterteilt, und auch Kapitel III wird um drei Abschnitte erweitert, was insgesamt elf Abschnitte ergibt. Die Kapitel IV bis VI sind aus datenschutzrechtlicher Sicht nicht relevant.
- Die geplante technische Umsetzung wird letztlich entscheidend dafür sein, ob zusätzliche Datenschutzgarantien in die Verordnung hätten aufgenommen werden sollen oder ob ihre Ausgestaltung überhaupt in Einklang mit der DSGVO[4] steht. Doch wie bereits bei der Verordnung (EU) Nr. 910/2014 kann die technische Architektur so lange nicht umfassend bewertet werden, bis die 28 Durchführungsrechtsakte der Kommission bekannt sind, die zur Festlegung technischer Spezifikationen und Referenzstandards geplant sind. Diese Rechtsakte dürften ebenfalls in den Geltungsbereich von Artikel 42 Absatz 1 der Verordnung 2018/1725 fallen und Gegenstand einer künftigen Konsultation des EDSB sein. Daher schließen diese formellen Bemerkungen künftige zusätzliche Bemerkungen des EDSB nicht aus, insbesondere, falls weitere Probleme festgestellt oder neue Informationen verfügbar werden sollten, beispielsweise infolge der Annahme einschlägiger Durchführungsrechtsakte oder delegierter Rechtsakte.
- Die vorliegenden formellen Bemerkungen des EDSB ergehen als Antwort auf die legislative Konsultation der Europäischen Kommission vom 3. Juni 2021 gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725. Diesbezüglich begrüßt es der EDSB, dass in Erwägungsgrund 37 des Vorschlags auf diese Konsultation verwiesen wird. Darüber hinaus lassen die Bemerkungen etwaige künftige Maßnahmen, die der EDSB in Ausübung seiner Befugnisse gemäß Artikel 58 der Verordnung (EU) 2018/1725 ergreift, unberührt.

2. Bemerkungen

- Der EDSB begrüßt das allgemeine Konzept des Vorschlags, wonach der Rahmen für eine europäische digitale Identität vollständig mit der Verordnung (EU) 2016/679 in Einklang stehen muss. Die Frage, ob die besonderen Schutzvorkehrungen ausreichen, hängt hauptsächlich von der Technologie ab, die zur Umsetzung des Vorschlags zum Einsatz kommt. Diesbezüglich begrüßt es der EDSB, dass in den Erwägungsgründen des Vorschlags erneut bekräftigt wird, dass die DSGVO voll anwendbar ist, und zwar auch

[4] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1.

für elektronische Vorgangsregister und qualifizierte elektronische Vorgangsregister.[5] Dieser Ansatz steht voll und ganz in Einklang mit Artikel 25 der DSGVO, wonach die Technologie entsprechend den Anforderungen an den Datenschutz gewählt werden sollte, und nicht umgekehrt.

- Von der Begründung, insbesondere auf den Seiten 10 und 11, lässt sich ableiten, dass elektronische Vorgangsregister als Vertrauensdienst kein unverzichtbarer Bestandteil der Brieftasche für die europäische digitale Identität sind, sondern auf bestimmte Anwendungsfälle begrenzt sein werden. Der EDSB begrüßt diese Klarstellung. Der EDSB würdigt die Tatsache, dass in der Begründung bestätigt wird, dass Diensteanbieter die DSGVO auch im Fall der Nutzung elektronischer Vorgangsregister einhalten müssen, und der Vorschlag keinerlei Bestimmungen enthält, die eine Abweichung von den DSGVO-Bestimmungen zulassen.

- Die Blockchain-Technologie gehört zu den Technologien, bei denen elektronische Vorgangsregister eingesetzt werden. Blockchain ruft in mehrfacher Hinsicht Bedenken hinsichtlich der Einhaltung der DSGVO hervor, etwa Datenübermittlungen außerhalb der EU, die Unmöglichkeit, Einträge in einer Blockchain zu löschen oder zu berichtigen, usw. Daher ist die Nutzung der Blockchain-Technologie möglicherweise nicht für alle Anwendungsfälle geeignet und könnte weitere Schutzvorkehrungen erforderlich machen. Dabei ist zu beachten, dass der Europäische Datenschutzausschuss die anstehenden „Leitlinien zu Blockchain“ in sein Arbeitsprogramm 2021/2022[6] aufgenommen hat. Der EDSB empfiehlt, diese Leitlinien, sobald sie vorliegen, bei der Prüfung von auf Blockchain basierten Vorgangsregistern im Zusammenhang mit diesem Vorschlag zu berücksichtigen.

- Der EDSB begrüßt es, dass die Brieftasche für die europäische digitale Identität dem Nutzer eine bessere und transparente Kontrolle darüber bietet, welche Daten er wem und zu welchem Zweck weitergibt. Mit der angestrebten Lösung könnten Probleme einer unverhältnismäßigen Datenverarbeitung gelöst werden, da die betroffene Person tatsächlich nur Daten offenzulegen bräuchte, die für einen bestimmten Zweck notwendig sind. Dies bedeutet, dass der Nutzer dann, wenn der Zweck eine Altersüberprüfung wäre, entscheiden könnte, sein Geburtsdatum zu übermitteln, alle anderen personenbezogenen Informationen, die für den Zweck nicht relevant sind, jedoch nicht weiterzugeben. Falls der Zweck eine Identifizierung beispielsweise im Bank- oder Telekommunikationsbereich ist, wie sie gesetzlich vorgeschrieben ist, könnte der Nutzer nur diejenigen Identitätsdaten offenlegen, deren Weitergabe gesetzlich vorgeschrieben ist (zum Beispiel ohne biometrische Identifikatoren, falls deren Verarbeitung nicht ausdrücklich verlangt wird).

- Der EDSB begrüßt ferner das ausdrückliche Verbot im neuen Artikel 6a Ziffer 7 für den Aussteller der EUid-Brieftasche, Informationen über die Verwendung der Brieftasche zu sammeln, die für die Erbringung der damit verbundenen Dienste nicht erforderlich sind. Dies und das Verbot, Personenidentifizierungsdaten für die Brieftasche mit anderen Daten aus anderen Diensten zu kombinieren, sowie die Verpflichtung, die

[5] Erwägungsgrund 35.
[6] https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf

personenbezogenen Daten für die Bereitstellung der Brieftaschendienste von allen anderen gespeicherten Daten physisch und logisch getrennt zu halten, werden das Vertrauen in die Sicherheit und Vertraulichkeit dieser technischen Lösung erhöhen.

- In diesem Zusammenhang begrüßt es der EDSB außerdem, dass mit Artikel 6c Ziffer 2 eine Zertifizierung gemäß der Verordnung (EU) 2016/679 für bestimmte Anforderungen an EUid-Brieftaschen eingeführt werden soll, einschließlich der Gewährleistung, dass Vertrauensdiensteanbieter, die qualifizierte Attributsbescheinigungen ausstellen, keinerlei Informationen über die Verwendung dieser Attribute erhalten. Der EDSB geht davon aus, dass auch diese Zertifizierung obligatorisch ist und keine entlastende Wirkung haben wird.

- Artikel 17 beinhaltet die Aufgaben der Aufsichtsstelle und sieht die Zusammenarbeit mit anderen Aufsichtsbehörden vor, etwa denjenigen im Sinne der Verordnung (EU) 2016/679. Demzufolge werden Datenschutzaufsichtsbehörden „unverzüglich [...] von den Ergebnissen der Überprüfungen qualifizierter Vertrauensdiensteanbieter [unterrichtet], falls gegen Datenschutzvorschriften verstoßen wurde, und von Sicherheitsverletzungen, die Verletzungen des Schutzes personenbezogener Daten darstellen". Der EDSB stellt fest, dass die Formulierung, wonach offenbar eine Untersuchung erforderlich ist, auf Artikel 17 der Verordnung (EU) Nr. 910/214 zurückgeht und insofern bereits eine Verbesserung gegenüber der derzeitigen Fassung darstellt, als eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 33 der DSGVO jetzt auch die Informationspflicht auslösen würde. Allerdings weist der EDSB den Mitgesetzgeber darauf hin, dass die frühere Formulierung einer anderen Rolle der Datenschutzbehörden entsprach, wohingegen Verantwortliche gemäß Artikel 33 der DSGVO qualifizierende Verletzungen des Schutzes personenbezogener Daten unverzüglich, binnen höchstens 72 Stunden, nachdem ihnen die Verletzung bekannt wurde, melden müssen, was es Aufsichtsbehörden ermöglicht, aktiv an Untersuchungen von Verletzungen und der Wahl der weiteren Maßnahmen mitzuwirken. Daher erscheint es angemessen, den Wortlaut von Artikel 17 Absatz 4 Buchstabe f an Nummer c des gleichen Absatzes anzupassen, wonach den zuständigen nationalen Behörden gemäß NIS-2-Richtlinie eine (mutmaßliche) Sicherheitsverletzung gemeldet werden müsste, ungeachtet dessen, ob bei der Überprüfung tatsächlich eine Verletzung festgestellt wurde. Die Datenschutzaufsichtsbehörden sollten immer dann unterrichtet werden, wenn die Aufsichtsstelle Informationen über eine mögliche Verletzung des Schutzes personenbezogener Daten erhält.

- Aus dem gleichen Grund sollte auch der letzte Satz von Artikel 20 Absatz 2 an die DSGVO angepasst und eine unverzügliche Meldung verfügt werden, unabhängig davon, ob die Überprüfung abgeschlossen oder noch im Gange ist.

- Mit dem Vorschlagsentwurf wird eine eindeutige und dauerhafte Kennung eingeführt, die von den Mitgliedstaaten verwendet werden muss, um den Identitätsabgleich zu erleichtern und die eindeutige Identifizierung für jeden Nutzer zu gewährleisten. Diese Kennung würde u. a. dann benutzt, wenn elektronische Attributsbescheinigungen zu einer Brieftasche hinzugefügt werden.

- Der EDSB erkennt durchaus die Bemühungen in Artikel 11a an, durch Verringerung des Missbrauchsrisikos oder von Mehrdeutigkeitsfehlern Vertrauen und Integrität zu

erhöhen. Gleichwohl gilt festzuhalten, dass diese eindeutige und dauerhafte Kennung eine weitere, zusätzliche Kategorie von Daten darstellt, die einzig und allein für den Zweck gespeichert werden, die Nutzung der Brieftasche zu erleichtern. Diese Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen ist keineswegs unerheblich; in manchen Mitgliedstaaten wurden eindeutige Kennungen in der Vergangenheit aufgrund einer Verletzung der Menschenwürde als verfassungswidrig eingestuft. Daher empfiehlt der EDSB die Prüfung alternativer Möglichkeiten zur Verbesserung der Sicherheit des Abgleichs.

- Der EDSB stellt fest, dass Artikel 45f weitere Regelungen für die Nutzung personenbezogener Daten durch Anbieter qualifizierter oder nichtqualifizierter Dienste für elektronische Attributsbescheinigungen vorsieht. Sie dürfen personenbezogene Daten in Bezug auf die Erbringung dieser Dienste nicht mit personenbezogenen Daten aus anderen von ihnen angebotenen Diensten kombinieren, und sie müssen die Daten von allen anderen gespeicherten Daten logisch und im Fall von personenbezogenen Daten in Bezug auf die Erbringung von Diensten für qualifizierte elektronische Attributsbescheinigungen auch physisch getrennt halten. Der EDSB vertritt die Auffassung, dass diese Verbote nicht durch Vertragsbestimmungen oder die Erteilung einer Einwilligung umgangen werden können. Der EDSB begrüßt diese Verbote als eine Maßnahme zur Verhinderung von Datenmissbrauch und zur Stärkung des Vertrauens in das System. Für Anbieter qualifizierter Dienste für elektronische Attributsbescheinigungen sieht Artikel 45f Ziffer 4 sogar vor, dass diese Dienste im Rahmen einer separaten juristischen Person erbracht werden, was zusammen mit den genannten Verboten einen wirksamen Mechanismus zur Verhinderung von Interessenkonflikten und einer unberechtigten Weitergabe personenbezogener Daten darstellen sollte.

Brüssel, 28. Juli 2021

Wojciech Rafał WIEWIÓROWSKI
(elektronisch unterzeichnet)