„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

6 / 2025
Juni 2025

Digitale Zeugnisse, elektronische Signaturen und elektronische Siegel

Die Ausstellung von digitalen Zeugnissen im Hochschulkontext wirft eine Reihe rechtlicher und praktischer Fragen auf

Brieftaschen-Update: Loading…

Die digitale Identität soll in Deutschland ab 2027 nutzbar sein

Für die IT-Sicherheit haben wir jetzt jemanden

Die Beauftragung externer Dienstleister für die IT-Sicherheit stößt paradoxerweise immer wieder auf datenschutzrechtliche Bedenken

Kurzbeitrag: Europäischer KI-Masterplan

EU-Kommission veröffentlicht KI-Kontinent-Aktionsplan

Digitale Zeugnisse, elektronische Signaturen und elektronische Siegel

Die Ausstellung von digitalen Zeugnissen im Hochschulkontext wirft eine Reihe rechtlicher und praktischer Fragen auf

Von Philipp Schöbel, Berlin

Hochschulen stellen Studierenden und Mitarbeitenden regelmäßig Zeugnisse aus. Gerade die Aushändigung von Zeugnissen als Beweis für den Erwerb eines Hochschulgrades ist für Studierende elementar für den weiteren Lebensweg. Seit einigen Jahren gibt es vermehrt Projekte in einzelnen Bundesländern und auf europäischer Ebene, um diese Prozesse zu digitalisieren.

I. Die Bedeutung digitaler Zeugnisse für Hochschulen

Hochschulen stellen regelmäßig Zeugnisse aus. So werden zum Beispiel regelmäßig Abschlusszeugnisse über den Erwerb eines Hochschulgrades oder Arbeitszeugnisse nach Beendigung eines Arbeitsverhältnisses ausgestellt. Dabei kann die Digitalisierung dieses Vorgangs einige Vorteile bringen. Eigenhändig eingescannte Zeugnisse verlieren durch den Scanvorgang Sicherheitsmerkmale, sodass nachträgliche Änderungen schwer nachvollziehbar sind.[1] Digitale Zeugnisse mit einer qualifizierten elektronischen Signatur weisen ein erhöhtes Maß an Fälschungssicherheit auf. Digitale Zeugnisse sind leicht zu speichern und zu teilen – was Bewerbungsprozesse vereinfacht. Maschinenlesbare digitale Dokumente können zudem automatisiert ausgelesen werden.[2]

1. Abschlusszeugnis

Aufgrund der Hochschulprüfung, mit der ein berufsqualifizierender Abschluss erworben wird, kann die Hochschule einen Hochschulgrad mit Angabe der Fachrichtung verleihen (§ 18 Abs. 1 S. 1 Hochschulrahmengesetz (HRG)).[3] Ein Hochschulgrad oder akademischer Grad ist die Dokumentation des ordnungsgemäßen Abschlusses einer Hochschulprüfung und stellt einen Verwaltungsakt dar.[4] Digitale Bildungsnachweise können schneller ausgestellt, ausgehändigt und überprüft werden.[5] Darüber hinaus können maschinenlesbare Informationen zu einzelnen Lerninhalten den automatischen Abgleich von Kenntnissen ermöglichen.[6]

---

1 Bundesamt für Sicherheit in der Informationstechnik, Handreichung „Digitale Zeugnisse“ - Version 1.0, 2024, S. 5, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Oeffentliche_Verwaltung/Moderner-Staat/Handreichung-Digitale-Zeugnisse.pdf?__blob=publicationFile&v=4 (Alle Links zuletzt abgerufen am 08.05.2025).

2 Vgl. zu digitalen Schulzeugnissen: Bundesdruckerei, Digitales Zeugnis, einfach und sicher, abrufbar unter: https://www.bundesdruckerei.de/de/newsroom/pressemitteilungen/digitales-zeugnis-einfach-und-sicher.

3 Zu den entsprechenden landesgesetzlichen Regelungen siehe weiter unten.

4 Becker in: HK-NHG, 2. Aufl. 2023, NHG § 8 Rn. 14.

5 Rentzsch, Digitale Bildungsnachweise – Der Stand 2020 in Deutschland und Europa, 2021, S. 5, abrufbar unter: https://www.iit-berlin.de/wp-content/uploads/2021/03/Digitale-Bildungsnachweise-2021.pdf.

6 Ebd.

2. Arbeitszeugnisse

Hochschulen sind als Arbeitgeberinnen zur Ausstellung von Arbeitszeugnissen verpflichtet (§ 109 Abs. 1 S. 1 Gewerbeordnung (GewO)). Das Zeugnis kann mit Einwilligung des/der Arbeitnehmer:in seit dem 1. Januar 2025 in elektronischer Form erteilt werden (§ 109 Abs. 3 GewO).[7] Der/die Arbeitgeber:in muss dem Arbeitszeugnis seinen/ihren Namen hinzufügen und das elektronische Dokument mit seiner/ihrer qualifizierten elektronischen Signatur versehen (§ 109 Abs. 3 GewO iVm § 126a Abs. 1 Bürgerliches Gesetzbuch (BGB)). Die Möglichkeit der qualifizierten elektronischen Signatur ist deshalb auch für Hochschulen im Arbeitskontext relevant. Dieser Beitrag geht im Weiteren aber auf die Ausstellung von Zeugnissen im Sinne von Bildungsnachweisen ein.

II. Der Lebenszyklus eines digitalen Zeugnisses

Der Lebenszyklus eines digitalen Zeugnisses kann in verschiedene Stadien unterteilt werden. In der folgenden Darstellung wird der durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) getroffenen Unterteilung in Beantragung, Erstellung, Übergabe, Verwendung und Löschung gefolgt.[8]

1. Beantragung

Die Beantragung des Zeugnisses kann optional sein. Ansonsten muss der/die Zeugnisempfänger:in das digitale Zeugnis zum Beispiel über ein Online-Verfahren beantragen. Zur Bestätigung der Identität ist dann regelmäßig ein Authentifizierungsmittel erforderlich. Das BSI empfiehlt hier eine Zwei-Faktor-Authentifizierung. Studierende könnten dazu beispielsweise die Online-Ausweisfunktion mit PIN und Personalausweis nutzen.[9]

2. Erstellung

Ein digitales Zeugnis kann grundsätzlich eine menschen- und/oder eine maschinenlesbare Form haben. Das BSI empfiehlt für die menschenlesbare Form die Verwendung des PDF (für eine Langzeitspeicherung das Format PDF/A). Als maschinenlesbare Formate empfiehlt das BSI für strukturierte Zeugnisdaten Extensible Markup Language (XML) oder JavaScript Object Notation (JSON). Relevanter Standard für den internationalen Transfer von Studierendendaten ist EMREX. Die Überprüfung der Echtheit und Unversehrtheit eines digitalen Zeugnisses funktioniert über digitale Signaturverfahren mit asymmetrischer Kryptografie. Wird diese digitale Signatur im Namen einer juristischen Person (z. B. Bildungseinrichtung) erstellt, handelt es sich um ein elektronisches Siegel. Für alle gängigen Dateiformate existieren europäisch standardisierte Signaturformate.[10]

3. Übergabe

Digitale Zeugnisse können auf verschiedene Arten zugestellt/übergeben werden. Sie können etwa nach Authentifizierung auf einem Webportal heruntergeladen werden. Alternative Verfahren sind die Übermittlung an das Nutzerkonto-Postfach oder durch Bereitstellung in eine Smartphone-Wallet.[11] Vor Erhalt sollte sich der Empfänger stets authentifizieren.[12]

4. Verwendung/Validierung

Ein signiertes digitales PDF-Zeugnis kann mit Standardsoftware angezeigt und auf Integrität geprüft werden. Für die Überprüfung der Echtheit der Signatur ist ein zusätzlicher Schritt nötig. Maschinenlesbare Formate ermöglichen eine Automatisierung dieses Vorgangs. Die vollständige Validierung umfasst in der Regel vier Schritte: Syntaxprüfung der inhaltlichen Elemente, Überprüfung der mathematischen Gültigkeit der digitalen Signatur, Kontrolle

---

7 Früher war die elektronische Form für die Ausstellung des Arbeitszeugnisses ausgeschlossen: Novak in: BeckOGK, 1.4.2025, GewO § 109 Rn. 41.

8 Vgl. Bundesamt für Sicherheit in der Informationstechnik, Handreichung „Digitale Zeugnisse“ - Version 1.0, 2024, S. 7.

9 Siehe dazu insgesamt: Bundesamt für Sicherheit in der Informationstechnik, Handreichung „Digitale Zeugnisse“ - Version 1.0, 2024, S. 8.

10 Siehe dazu insgesamt: Bundesamt für Sicherheit in der Informationstechnik, Handreichung „Digitale Zeugnisse“ - Version 1.0, 2024, S. 8.

11 Zur europäischen EUDI-Wallet: Yang-Jacobi, Brieftaschen-Update: Loading…, DFN-Infobrief Recht 6/2025.

12 Siehe dazu insgesamt: Bundesamt für Sicherheit in der Informationstechnik, Handreichung „Digitale Zeugnisse“ - Version 1.0, 2024, S. 9.

der Zertifikatsgültigkeit und Prüfung der Zertifikatskette zur Bestätigung der berechtigten Bildungseinrichtung.[13]

5. Löschung

Bei der langfristigen Aufbewahrung digitaler Zeugnisse, die oft mehrere Jahrzehnte gespeichert werden müssen, sind folgende Aspekte zu beachten: die Zukunftsfähigkeit des Datenformats, die Sicherung gegen technische Defekte und physische Schäden, der langfristige Datenschutz sowie der Beweiswerterhalt trotz fortschreitender kryptografischer Entwicklungen. Nach Ablauf der Aufbewahrungsfrist sollten digitale Zeugnisse dem zuständigen Archiv angeboten werden, bevor sie gelöscht werden. Hierfür existieren bereits zertifizierte Softwarelösungen für digitale Langzeitarchive, die auch langfristig die Beweiswerterhaltung sicherstellen.[14]

III. Die Qualifizierte elektronische Signatur

Damit Rechtssicherheit hinsichtlich der Anforderungen an die elektronische Signatur besteht, sind diese gesetzlich festgelegt. Diese rechtlichen Anforderungen gelten auch für die Ausstellung von digitalen Zeugnissen.

1. Rechtliche Anforderungen

Was eine qualifizierte elektronische Signatur ist, wird in der eIDAS-VO[15] geregelt. Die eIDAS-VO unterscheidet zwischen drei unterschiedlichen Arten der Signatur: elektronische Signatur, fortgeschrittene elektronische Signatur und qualifizierte elektronische Signatur.[16] Eine „elektronische Signatur“ sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet (Art. 3 Nr. 10 eIDAS-VO).
Eine fortgeschrittene elektronische Signatur muss vier Kriterien erfüllen: Sie ist eindeutig dem Unterzeichner zugeordnet; sie ermöglicht die Identifizierung des Unterzeichners; sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann; sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann (Art. 3 Nr. 11 iVm Art 26 Abs. 1 eIDAS-VO).

Eine qualifizierte elektronische Signatur ist eine fortgeschrittene elektronische Signatur, die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht (Art. 3 Nr. 12 eIDAS-VO). Eine qualifizierte elektronische Signatur muss vor allem fälschungssicher sein, das heißt „dass die Signatur eines Dokuments durch die Person erfolgt ist, der die Signatur tatsächlich zugeordnet ist und dass das Dokument nicht unbemerkt verändert worden ist.“[17] Darüber hinaus muss die Signatur langfristig prüfbar und sollte bei vielen, idealerweise sogar bei allen eGovernment-Anwendungen, im privaten Rechtsverkehr und im Ausland, anwendbar sein.[18]

Nach Art. 25 Abs. 2 eIDAS-VO hat eine qualifizierte elektronische Signatur die gleiche Rechtswirkung wie eine handschriftliche Unterschrift. Ein qualifiziert elektronisch signiertes Dokument erfüllt die gesetzliche Schriftform nach § 126 iVm § 126a BGB.[19] Auch im Bereich des Verwaltungshandelns ersetzt ein elektronisches Dokument mit qualifizierter elektronischer Signatur die

13 Siehe dazu insgesamt: Bundesamt für Sicherheit in der Informationstechnik, Handreichung „Digitale Zeugnisse“ - Version 1.0, 2024, S. 9.

14 Siehe dazu insgesamt: Bundesamt für Sicherheit in der Informationstechnik, Handreichung „Digitale Zeugnisse“ - Version 1.0, 2024, S. 10.

15 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 S. 73.

16 Vgl. BMUV, eANV - qualifizierte elektronische Signatur und deren Einsatz, abrufbar unter: https://www.bmuv.de/faqs/eanv-qualifizierte-elektronische-signatur-und-deren-einsatz.

17 Müller in: BeckOK VwVfG, 66. Ed. 1.10.2023, VwVfG § 3a Rn. 13.

18 Müller in: BeckOK VwVfG, 66. Ed. 1.10.2023, VwVfG § 3a Rn. 14.

19 Vgl. Bundesnetzagentur, Übersicht aller elektronischen Vertrauensdienste, abrufbar unter: https://www.elektronische-vertrauensdienste.de/EVD/DE/Uebersicht_eVD/Dienste/1_Signatur.html?nn=691386.;Zu möglichen Anpassungen nach den Neuerungen der eIDAS-VO 2024, Yang-Jacobi, Brieftaschen-Update: Loading…, DFN-Infobrief-Recht 6/2025..

Schriftform, wenn nicht ausnahmsweise etwas anderes bestimmt ist (§ 3 a Abs. 2 S. 1,2 Verwaltungsverfahrensgesetz (VwVfG[20])).[21] Das heißt, dass elektronische Dokumente durch die qualifizierte elektronische Signatur in praktisch allen Lebensbereichen das handschriftlich unterschriebene Papierdokument ersetzen können, wenn in dem eingesetzten Bereich keine Sonderregelungen existieren.[22]

In Deutschland fungiert das Vertrauensdienstegesetz (VDG) als das eIDAS-Durchführungsgesetz.[23]

2. Digitale Signatur

Eine elektronische Signatur ist nicht zwangsläufig gleichbedeutend mit einer digitalen Signatur. Im Gegensatz zur rechtlichen Definition einer qualifizierten elektronischen Signatur beschreibt eine digitale Signatur ein mathematisch-kryptografisches Konzept, das häufig als praktisches Beispiel für elektronische Signaturen dient. Die ETSI 119 100 Definition[24] beschreibt sie als Daten, die einer Dateneinheit beigefügt werden, oder als kryptografische Transformation, die dem Empfänger ermöglicht, sowohl die Herkunft als auch die Unversehrtheit der Daten zu verifizieren und sich gleichzeitig gegen eventuelle Fälschungen, beispielsweise durch den Empfänger selbst, abzusichern.[25]

3. Funktionsweise der elektronischen Signatur

Elektronische Signaturen verwenden zwei mathematische Verfahren: asymmetrische Verschlüsselung und Hash-Algorithmen. Bei der asymmetrischen Verschlüsselung erhält jede/r Benutzer:in zwei Schlüssel: einen privaten (geheimen) Schlüssel, den nur er/sie kennt und einen öffentlichen Schlüssel, den jeder kennen darf. Der private Schlüssel dient der Verschlüsselung (Signatur). Der öffentliche Schlüssel dient der Verifizierung der Signatur. Was mit dem privaten Schlüssel verschlüsselt wurde, kann nur mit dem zugehörigen öffentlichen Schlüssel entschlüsselt werden. Aus dem öffentlichen Schlüssel kann nicht auf den privaten Schlüssel geschlossen werden.[26]

Die Erstellung einer elektronischen Signatur funktioniert wie folgt: Aus dem Dokument wird ein Hashwert berechnet („digitaler Fingerabdruck“), den der Unterzeichnende mit seinem privaten Schlüssel verschlüsselt. Diese verschlüsselte Information ist die elektronische Signatur und wird an das Dokument angehängt. Bei der Prüfung der Signatur berechnet der Empfänger selbst den Hashwert des Dokuments und entschlüsselt danach die Signatur mit dem öffentlichen Schlüssel des Absenders. Stimmen beide Hashwerte überein, wurde das Dokument nicht verändert. Weichen sie voneinander ab, könnte das Dokument manipuliert worden sein. Alternativ könnte auch ein technisches Problem die Ursache für die Nichtübereinstimmung sein. Selbst kleinste Veränderungen an der Datei führen zu einem völlig anderen Hashwert, und es ist praktisch unmöglich, zu einem bestimmten Hashwert passende Dateien zu finden.[27]

Bei qualifizierten Signaturen wird der öffentliche Schlüssel (Signaturprüfschlüssel) als Zertifikat im Internet hinterlegt. Dieses Zertifikat enthält zusätzlich Informationen über die Identität des Anwenders, die Gültigkeitsdauer und den Zertifizierungsdiensteanbieter.[28]

---

20 In allen Verwaltungsverfahrensgesetzen der Länder existiert eine inhaltsgleiche Regelung – zur Übersicht siehe weiter unten.

21 Vgl. Brisch/Brisch in: Hoeren/Sieber/Holznagel MMR-HdB, 62. EL Juni 2024, Teil 13.3 Rn. 92.

22 Brisch/Brisch in: Hoeren/Sieber/Holznagel MMR-HdB, 62. EL Juni 2024, Teil 13.3 Rn. 86.

23 Roßnagel, Das Vertrauensdienstegesetz, MMR 2018, 31.

24 ETSI TR 119 100 V1.1.1 (2016-03), Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation, abrufbar unter: https://www.etsi.org/deliver/etsi_tr/119100_119199/119100/01.01.01_60/tr_119100v010101p.pdf.

25 Dazu insgesamt: Bundesnetzagentur, Fragen zu elektronischen Vertrauensdiensten, abrufbar unter: https://www.elektronische-vertrauensdienste.de/EVD/DE/Nutzer/Infothek/Fragen/start.html#faqt_2.

26 Dazu insgesamt: Müller in: BeckOK VwVfG, 66. Ed. 1.10.2023, VwVfG § 3a Rn. 16.

27 Ebd.

28 Ebd.

IV. Elektronische Signaturen und elektronische Siegel

Neben der elektronischen Signatur gibt es noch das elektronische Siegel. Das elektronische Siegel wird nicht an eine natürliche, sondern an eine juristische Person gebunden.[29] Das elektronische Siegel fungiert als elektronische Signatur für juristische Personen.[30] „Das elektronische Siegel ist das digitale Gegenstück des Behördenstempels und verringert den administrativen Aufwand."[31] Elektronisches Siegel und elektronische Signatur haben unterschiedliche Rechtsfolgen. Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift (Art. 25 Abs. 2 eIDAS-VO). Für ein qualifiziertes elektronisches Siegel gilt die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist (Art. 35 Abs. 2 eIDAS-VO).[32]

Genauso wie bei der elektronischen Signatur wird beim elektronischen Siegel auch zwischen dem elektronischen Siegel, dem fortgeschrittenen elektronischen Siegel und dem qualifizierten elektronischen Siegel unterschieden. Das qualifizierte elektronische Siegel ersetzt die Schriftform genauso wie die qualifizierte elektronische Signatur (§ 3a Abs. 3 Nr. 3 lit. a VwVfG).

Fordert eine Rechtsvorschrift eine Unterschrift und einen Behördenstempel, können für digitale Zeugnisse elektronische Signaturen und elektronisches Siegel kombiniert werden. Daneben ist auch die Verwendung mehrerer elektronischer Signaturen rechtlich möglich.

V. Verwaltungsverfahrensgesetze und elektronische Signatur

Die elektronische Kommunikation mit der Verwaltung ist im Verwaltungsverfahrensgesetz des Bundes geregelt. Danach kann eine durch Rechtsvorschrift angeordnete Schriftform, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden (§ 3a Abs. 2 S. 1 VwVfG).

Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur versehen ist (§ 3a Abs. 2 S. 2 VwVfG). Die Verwaltungsverfahrensgesetze der Länder enthalten inhaltsgleiche Regelungen oder verweisen auf die Regelung des Verwaltungsverfahrensgesetzes des Bundes.

Tabelle 1: Verwaltungsverfahrensgesetze der Länder

Bundesland	Norm
Baden-Württemberg	§ 3a Abs. 2 S. 1, 2 VwG BW
Bayern	§ 3a Abs. 2 S. 1, 2 BayVwVfG
Berlin	§ 3a Abs. 2 S. 1, 2 VwVfG iVm § 1 Abs. 1 VwVfG BE
Brandenburg	§ 3a Abs. 2 S. 1, 2 VwVfG iVm § 1 Abs. 1 S. 1 VwVfGBbg
Bremen	§ 3a Abs. 2 S. 1, 2 VwVfG iVm § 1 Abs. 1 S. 1 BremVwVfG
Hamburg	§ 3a Abs. 2 S. 1, 2 HmbVwVfG
Hessen	§ 3a Abs. 2 S. 1, 2 HVwVfG
Mecklenburg-Vorpommern	§ 3a Abs. 2 S. 1, 2 VwVfG M-V
Niedersachsen	§ 3a Abs. 2 S. 1, 2 VwVfG iVm § 1 Abs. 1 NVwVfG
Nordrhein-Westfalen	§ 3a Abs. 2 S. 1, 2 VwVfG NRW
Rheinland-Pfalz	§ 3a Abs. 2 S. 1, 2 VwVfG iVm § 1 Abs. 1 LVwVfG RP
Saarland	§ 3a Abs. 2 S. 1, 2 SVwVfG
Sachsen	§ 3a Abs. 2 S. 1, 2 VwVfG iVm § 1 Abs. 1 S. 1 SächsVwVfG
Sachsen-Anhalt	§ 3a Abs. 2 S. 1, 2 VwVfG iVm § 1 Abs. 1 S. 1 VwVfG LSA
Schleswig-Holstein	§ 52a Abs. 2 S.1, 2 LVwG
Thüringen	§ 3a Abs. 2 S. 1, 2 VwVfG iVm § 1 Abs. 1 S. 1 ThürVwVfG

29 Hornung in: Schoch/Schneider, 5. EL Juli 2024, VwVfG vor § 3a, Rn. 58.

30 Roßnagel in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2. Auflage 2024, § 14, Rn. 57.

31 Yang-Jacobi, Von Papierbergen zur e-Verwaltung?, DFN-Infobrief Recht 4 / 2025 | Seite 6.

32 Vgl. Hornung in: Schoch/Schneider, 5. EL Juli 2024, VwVfG vor § 3a, Rn. 58.

1. Ausschluss der elektronischen Form

Der Ausschluss der elektronischen Form muss durch eine Rechtsvorschrift speziell angeordnet werden (§ 3a II S. 1 VwVfG).[33] Beispiele für den Ausschluss der elektronischen Form finden sich etwa in § 38a Staatsangehörigkeitsgesetz (StAG) oder in § 17 Abs. 1 S. 1 Atomgesetz (AtG).[34] In § 38a StAG heißt es: „Eine Ausstellung von Urkunden in Staatsangehörigkeitssachen in elektronischer Form ist ausgeschlossen." Neben einem solchen expliziten Ausschluss kann auch ein implizierter Ausschluss der elektronischen Form durch eine vorgeschriebene Medienwahl erfolgen: etwa durch einen bestimmten Papiervordruck oder eine bestimmte Papierqualität.[35] Umstritten ist, ob eine Vorschrift, die die Aushändigung einer Urkunde verlangt, die elektronische Form ausschließt.[36] Teilweise wird vertreten, dass z. B. im Beamtenrecht in § 10 Abs. 2 S. 1 Bundesbeamtengesetz (BBG) die Ernennung von Beamt:innen durch eine Urkunde „die willentliche Verschaffung des körperlichen Besitzes der Originalurkunde" verlange. [37]Diese Auffassung wird abgelehnt, weil der Gesetzgeber im Jahr 2009, die Vorschrift im BBG mit der ausdrücklichen Begründung geändert hat, dass die qualifizierte elektronische Signatur in umfassender Weise die Sicherheit und Dauerhaftigkeit des elektronischen Verwaltungshandelns gewährleiste.[38]

Eine ähnliche Diskussion gibt es auch im Zivilrecht. Dort wird argumentiert, dass die bloße Verwendung der Wörter „Urkunde" oder „Aushändigung" in einer Norm nicht automatisch einen Ausschluss der elektronischen Form bedeutet. Vielmehr müssten diese Begriffe technologieoffen ausgelegt werden. Der Gesetzgeber habe durch § 126 Abs. 3 BGB gerade eine Gleichstellung von elektronischer Form und Schriftform sicherstellen wollen.[39] Bei der Ausstellung von Zeugnissen bedeutet dies, dass Zeugnisse grundsätzlich mittels qualifizierter elektronischer Signatur als elektronisches Dokument ausgestellt werden können, wenn keine spezialgesetzliche Regelung etwas anderes vorschreibt. Der bloße Verweis auf eine Aushändigung einer Urkunde durch eine Regelung eines Landeshochschulgesetzes sollte nicht automatisch als implizierter Ausschluss der elektronischen Form verstanden werden.

2. Recht auf analoge Verwaltung

In der Rechtswissenschaft ist bisher nicht abschließend geklärt, ob die Adressat:innen einen elektronischen Zugang ausdrücklich eröffnen müssen, damit die Behörde mit ihnen auf elektronischem Weg kommunizieren kann. Einerseits wird argumentiert, dass Bürger:innen durch die Einführung des § 3a VwVfG nicht zur Entgegennahme elektronischer Dokumente verpflichtet worden sind.[40] Eine elektronische Kommunikation dürfe den Adressat:innen grundsätzlich nicht ohne ausdrückliche Einwilligung aufgedrängt werden.[41] Andererseits wird vertreten, dass es kein allgemeines IT-Abwehrrecht gebe.[42]

Durch spezielle gesetzliche Grundlage kann verlangt werden, dass ausschließlich der behördliche elektronische Zugang benutzt wird.[43] Durch Hochschulsatzung kann zum Beispiel ein reines Online-Zulassungsverfahren von Universitäten festgelegt werden.[44] Daher dürfte bei der Ausstellung eines digitalen Zeugnisses in der Regel auch eine analoge Ausstellung angezeigt sein, wenn durch Satzung oder andere Rechtsvorschrift keine

33 Kastner in: HK-VerwR/, 5. Aufl. 2021, VwVfG § 3a Rn. 27.

34 Kastner in: HK-VerwR/, 5. Aufl. 2021, VwVfG § 3a Rn. 27.

35 Hornung in: Schoch/Schneider, 5. EL Juli 2024, VwVfG § 3a, Rn. 69.

36 Hornung in: Schoch/Schneider, 5. EL Juli 2024, VwVfG § 3a, Rn. 70.

37 Kastner in: HK-VerwR/, 5. Aufl. 2021, VwVfG § 3a Rn. 28.

38 Hornung in: Schoch/Schneider, 5. EL Juli 2024, VwVfG § 3a, Rn. 70; der sich auf BT-Drs. 16/7076 S. 101 bezieht.

39 Dazu insgesamt: Funke/Quarch, Ersetzung der Schriftform durch die elektronische Form, NJW 2022, 569 f.

40 Müller in: BeckOK VwVfG, 66. Ed. 1.10.2023, VwVfG § 3a Rn. 5a.

41 Müller in: BeckOK VwVfG, 66. Ed. 1.10.2023, VwVfG § 3a Rn. 6.

42 Schulz in: NK-VwVfG, 2. Aufl. 2019, VwVfG § 3a Rn. 64.

43 Schmitz/Prell in: Stelkens/Bonk/Sachs, 10. Aufl. 2022, VwVfG § 3a Rn. 10.

44 OVG Hamburg, 05.02.2010, 3 Bs 179/09, 3 So 158/09.

Pflicht der Studierenden zur Entgegennahme von digitalen Zeugnissen besteht.

VI. Hochschulrahmengesetz

Die Verleihung von Hochschulgraden wird im Hochschulrahmengesetz (HRG) und in den Hochschulgesetzen der Länder geregelt. Das HRG kennt kein spezielles Formerfordernis für die Verleihung eines Hochschulgrades.[45] Ebenfalls existiert kein spezielles Formerfordernis für Zwischenzeugnisse. Einen expliziten Ausschluss der elektronischen Form für die Verleihung von Hochschulgraden kennt das HRG nicht.

VII. Hochschulgesetze der Länder

Einige Landesgesetze sehen für die Ausstellung von Hochschulzeugnissen eine Verleihungsurkunde vor. Andere Landesgesetze machen keine Aussage über die Form der Verleihung des Hochschulgrades (siehe Tabelle 2).

Treffen die Landesgesetze keine ausdrückliche Regelung zur Form des Zeugnisses, ist die Ausstellung eines digitalen Zeugnisses möglich. Sieht das einschlägige Landesrecht eine Verleihungsurkunde vor, so ist fraglich, ob diese auch in digitaler Form „ausgehändigt" werden kann. Der Bundesgesetzgeber geht für das Beamtenrecht davon aus, dass die Aushändigung einer Urkunde nicht implizit die elektronische Form ausschließt. Auch bei der Auslegung landesrechtlicher Regelungen liegt es nahe, sich daran zu orientieren. Die bloße Verwendung der Wörter „Urkunde" und „aushändigen" sollte deshalb auch hier nicht als implizierter Ausschluss der elektronischen Form verstanden werden.

45 Vgl. § 18 HRG.

VIII. Amtliche Beglaubigung von Zeugnissen

Rein tatsächlich besteht die Möglichkeit, sowohl ein digitales als auch ein physisches Zeugnis auszustellen. Zudem kann von einem physischen Zeugnis eine digitale Abschrift ausgestellt werden. Alternativ kann ein digitales Zeugnis ausgestellt und eine physische beglaubigte Abschrift ausgehändigt werden. Der rechtliche Weg von einem digitalen Zeugnis zu einem Papierzeugnis

Tabelle 2: Landesgesetze

Bundesland	Norm	Formerfordernis
Baden-Württemberg	§ 36 Abs. 5 S. 1 LHG	Sieht Verleihungsurkunde vor
Bayern	§ 90 Abs. 5 BayHIG	Sieht Verleihungsurkunde vor
Berlin	§ 34 Abs. 2 S. 1 BerlHG	Sieht Verleihungsurkunde vor
Brandenburg	§ 30 Abs. 3 S. 2 BbgHG	Sieht Verleihungsurkunde vor
Bremen	Vgl. § 64 BremHG	**Keine** ausdrückliche Regelung
Hamburg	§ 67 Abs. 1 S. 2 HmbHG	Sieht Verleihungsurkunde vor
Hessen	Vgl. § 26 HessHG	**Keine** ausdrückliche Regelung
Mecklenburg-Vorpommern	Vgl. 41 LHG M-V	**Keine** ausdrückliche Regelung
Niedersachsen	Vgl. § 8 NHG	**Keine** ausdrückliche Regelung
Nordrhein-Westfalen	§ 66 Abs. 3 S. 1 NRW HG	Sieht Verleihungsurkunde vor
Rheinland-Pfalz	§ 30 Abs. 1 S. 2 HochSchG	Sieht Verleihungsurkunde vor
Saarland	§ 66 Abs. 7 SHS	Sieht Verleihungsurkunde vor
Sachsen	§ 40 Abs. 2 S. 2 SächsHG	Sieht Verleihungsurkunde vor
Sachsen-Anhalt	§ 17 Abs. 2 HSG LSA	Sieht Verleihungsurkunde vor
Schleswig-Holstein	§ 53 Abs. 4 HSG	Sieht Verleihungsurkunde vor
Thüringen	§ 58 Abs. 9 S. 2 ThürHG	Sieht Verleihungsurkunde vor

funktioniert über den beglaubigten Ausdruck eines elektronischen Dokuments (§ 33 Abs. 4 Nr. 3 VwVfG). Andersherum kann eine elektronische Version einer Papierurkunde ausgefertigt und beglaubigt werden (§ 33 Abs. 7 VwVfG). Der letzte Weg kann nach einer Literaturansicht allerdings nur dann bestritten werden, wenn für den Empfang des digitalen Zeugnisses auf der Studierendenseite ein Zugang eröffnet worden ist.

Die Beglaubigung von Dokumenten ist in § 33 VwVfG geregelt. In allen Bundesländern existieren im Wesentlichen inhaltsgleiche Regelungen in den entsprechenden Verwaltungsverfahrensgesetzen.

Tabelle 3: Verwaltungsverfahrensgesetze der Länder zu Beglaubigungen

Bundesland	Norm
Baden-Württemberg	§ 33 VwG BW
Bayern	§ 33 BayVwVfG
Berlin	§ 33 VwVfG iVm § 1 Abs. 1 VwVfG BE
Brandenburg	§ 33 VwVfG iVm § 1 Abs. 1 S. 1 VwVfGBbg
Bremen	§ 33 VwVfG iVm § 1 Abs. 1 S. 1 BremVwVfG
Hamburg	§ 33 HmbVwVfG
Hessen	§ 33 HVwVfG
Mecklenburg-Vorpommern	§ 33 VwVfG M-V
Niedersachsen	§ 33 VwVfG iVm § 1 Abs. 1 NVwVfG
Nordrhein-Westfalen	§ 33 VwVfG NRW
Rheinland-Pfalz	§ 33 VwVfG iVm § 1 Abs. 1 LVwVfG RP
Saarland	§ 33 SVwVfG
Sachsen	§ 33 VwVfG iVm § 1 Abs. 1 S. 1 SächsVwVfG
Sachsen-Anhalt	§ 33 VwVfG iVm § 1 Abs. 1 S. 1 VwVfG LSA
Schleswig-Holstein	§ 91 LVwG
Thüringen	§ 33 VwVfG iVm § 1 Abs. 1 S. 1 ThürVwVfG

1. Beglaubigte Ausdrucke elektronischer Dokumente

Elektronische Dokumente können ausgedruckt und der Ausdruck dann durch die ausstellende Behörde beglaubigt werden (§ 33 Abs. 4 Nr. 3 VwVfG). Der Beglaubigungsvermerk muss eine Reihe von Angaben enthalten. Das Schriftstück, dessen Abschrift beglaubigt wird, muss dann genau bezeichnet sein. Es muss festgestellt sein, dass die beglaubigte Abschrift mit dem vorgelegten Schriftstück übereinstimmt. Darüber hinaus muss ein Hinweis enthalten sein, dass die beglaubigte Abschrift nur zur Vorlage bei der angegebenen Behörde erteilt wird (wenn die Urschrift nicht von einer Behörde ausgestellt worden ist). Zudem müssen Ort und Tag der Beglaubigung, die Unterschrift des für die Beglaubigung zuständigen Bediensteten und das Dienstsiegel enthalten sein (§ 33 Abs. 3 S. 2 VwVfG).

Der Ausdruck eines elektronischen Dokuments, das mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel einer Behörde verbunden ist, muss zudem drei zusätzliche Feststellungen enthalten. Es muss angegeben sein, wen die Signaturprüfung als Inhaber der Signatur ausweist oder welche Behörde die Signaturprüfung als Inhaber des Siegels ausweist. Darüber hinaus muss der Zeitpunkt der Signaturprüfung für die Anbringung der Signatur oder des Siegels enthalten sein. Schließlich muss festgestellt sein, welche Zertifikate mit welchen Daten dieser Signatur oder diesem Siegel zugrunde lagen (§ 33 Abs. 5 S. 1 Nr. 1 VwVfG).

2. Elektronische Version einer Papierurkunde

§ 33 Abs. 7 VwVfG regelt die Umwandlung eines Papierdokuments in ein elektronisches Dokument und die Aushändigung einer beglaubigten Abschrift eines elektronischen Dokuments. Die Ausstellung nach § 33 Abs. 7 VwVfG ist an einen Antrag gebunden. Die Behörde kann zur Ausstellung elektronischer Dokumente nicht verpflichtet werden, wenn sie nicht über die dafür nötigen technischen Mittel verfügt.

3. Fazit

Hochschulen können ein digitales Zeugnis ausdrucken und beglaubigen. Alternativ können sie aber auch den gegenteiligen Weg gehen und von einem physischen Zeugnis auf Antrag eine

digitale Version ausstellen. Rechtlich gesehen haben Hochschulen bei der Umsetzung der Zeugnisdigitalisierung also eine Wahlmöglichkeit: Sie können immer ein digitales und ein physisches Zeugnis ausstellen oder sie stellen ein physisches Zeugnis aus und ein digitales nur auf Antrag. Es ist nach jetziger Rechtslage mindestens fraglich, ob Hochschulen auch ein digitales Zeugnis ausstellen und nur auf Antrag eine physische beglaubigte Abschrift aushändigen können.

Brieftaschen-Update: Loading…

Die digitale Identität soll in Deutschland ab 2027 nutzbar sein

Von Anna Maria Yang-Jacobi, Berlin

Bereits 2014 trat die europäische eIDAS-Verordnung[1] (eIDAS-VO) in Kraft. Zehn Jahre später, im April 2024, folgte eine umfassende Ergänzung der Verordnung. Eine neue digitale Brieftasche, die sogenannte European Digital Identity (EUDI)-Wallet, soll elektronische Transaktionen und damit auch den Alltag erleichtern. Ende 2024 folgten erste europäische Durchführungsverordnungen, die die Kernfunktionen und Zertifizierung der EUDI-Wallet festlegen. Hochschulen und Forschungseinrichtungen können sich bereits frühzeitig mit den Möglichkeiten beschäftigen.

I. Der Anfang der eIDAS-VO

Wie viele andere Gegenstände und Verfahren soll die Brieftasche als zwar tragbares, aber bisher körperliches Behältnis für Ausweise, Papiergeldscheine und andere Dokumente digitalisiert werden. Den Anfang der elektronischen Identifizierungsmöglichkeiten machte 2014 die Einführung der eIDAS-VO. Die eIDAS-VO löste die Signatur-Richtlinie[2] von 1999 ab. Als Verordnung gilt sie unmittelbar in jedem EU-Mitgliedstaat (Art. 288 Abs. 2 AEUV (Vertrag über die Arbeitsweise der Union)). Übergreifendes Ziel war es, elektronische Transaktionen im Alltag für den Handel und die Verwaltung attraktiver zu gestalten. Die Gesetzgeber hatten festgestellt, dass Wirtschaft und Verwaltung mit der Nutzung elektronischer Mittel zögerten. Immerhin waren die rechtliche Geltung und Sicherheit einer elektronischen Umstellung noch weitestgehend ungeklärt. Mit der eIDAS-VO schuf der europäische Gesetzgeber daraufhin erstmals europaweit verbindliche und einheitliche Rahmenbedingungen zu elektronischen Identifizierungs- und Vertrauensdiensten. Der elektronische Rechtsverkehr sollte über die ausgewählten Vertrauensdienste (Art. 3 Nr. 16 eIDAS-VO) wie elektronische Signaturen und Siegel, aber auch durch die Erstellung entsprechender Zertifikate gestärkt werden. So greifen bereits seit der vollständigen Anwendbarkeit der eIDAS-VO ab 2016 (und verstärkt durch die Corona-Pandemie 2020) Unternehmen und Verwaltung auch mit Hinblick auf die steigende Nachfrage zunehmend auf Vertrauensdienste, insbesondere die elektronische Signatur, zurück.[3]

In den letzten zwei Jahren hat sich im Bereich elektronische Identifizierung und digitale Identitäten zudem einiges getan.[4] Verwaltungsleistungen können mittlerweile vermehrt elektronisch beantragt werden.[5] Digitale Identitätsnachweise wie elektronische Identitäten (eIDs) existieren bereits und ersetzen einige früher notwendige Behördengänge wie die Anmeldung eines

1 Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG zuletzt geändert durch Verordnung (EU) Nr. 2024/1183, „electronic Identification, Authentication and Trust Services“ (eIDAS), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02014R0910-20241018 (alle Links dieses Beitrags zuletzt abgerufen am 30.4.2025).

2 Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (bis 30.6.2016 durch unmittelbare Geltung der eIDAS-VO seit dem 1.7.2016 außer Kraft getreten).

3 e-Commerce Magazin, Elektronische Signaturen: Jeder zweite Deutsche will auf digital umsteigen, 6.11.2023, https://www.e-commerce-magazin.de/elektronische-signaturen-jeder-zweite-deutsche-will-auf-digital-umsteigen-a-74db2fc6bc04fbab35d8c154cb293e07/.

4 Für einen Überblick zum Entwurf zur Anpassung der eIDAS-VO von 2023, siehe Sonak, ID(een) muss man haben, DFN-Infobrief Recht 6/2023.

5 Zur Digitalisierung der Verwaltung siehe Yang-Jacobi, Von Papierbergen zur e-Verwaltung?, DFN-Infobrief Recht 4/2025.

Wohnsitzes.[6] Zu den eIDs zählt die Onlineausweisfunktion des Personalausweises, des elektronischen Aufenthaltstitels oder der eID-Karte für Bürger:innen aus EU-Mitgliedstaaten.

2024 verabschiedete der europäische Gesetzgeber eine Anpassung der eIDAS-VO[7], die am 20.5.2024 in Kraft trat. Die Hauptneuerung ist die EUDI-Wallet. Mithilfe der EUDI-Wallet soll eine unionsweite digitale Identifikation möglich sein, die noch mehr Funktionen anbietet als die eIDs. Die Art. 5a bis Art. 5f eIDAS-VO enthalten Vorgaben für die Mitgliedstaaten, aber auch für die Anbieter von EUDI-Wallets. Die Mitgliedstaaten sind nach Art. 5a eIDAS-VO dazu verpflichtet, mindestens eine EUDI-Wallet bis Ende 2026 bereitzustellen. Die EUDI-Wallets sollen Bürger:innen und Unternehmen eine sichere Identifizierung sowie die Nutzung von Authentifizierungsdiensten in der gesamten EU online und offline ermöglichen.

II. Die EUDI-Wallet als vielfältiges Instrument

Für die EUDI-Wallet sind unterschiedliche Nutzungsfunktionen vorgesehen, die über die eID-Infrastruktur hinausgehen. So sollen sich Nutzende zum einen mithilfe der EUDI-Wallet elektronisch identifizieren und authentifizieren können. Darüber hinaus sollen sie aber auch eine Reihe von elektronischen Dokumenten speichern und verwalten können (Art. 3 Nr. 42 eIDAS-VO). Dabei geht es nicht nur um reine Identitätsdokumente, sondern auch um Attributsbescheinigungen, welche Kenntnisse, Fähigkeiten oder Mitgliedschaften nachweisen. Dazu gehören der Führerschein, Hochschulabschlusszeugnisse, eine Gesundheitskarte oder auch Tickets.[8] Diese Dokumente können durch die EUDI-Wallet sicher gespeichert und bei Bedarf abgerufen werden. Gerade die Identitätsnachweise sollen bereits beim Abspeichern in der Wallet von einer unabhängigen Stelle auf ihre Gültigkeit geprüft werden. Die EUDI-Wallet knüpft dabei an bekannte elektronische Technologien an. So können Nutzende die EUDI-Wallet auch einsetzen, um mittels qualifizierter elektronischer Signaturen Dokumente zu unterzeichnen bzw. mittels qualifizierten elektronischen Siegels zu besiegeln.[9] Die EUDI-Wallet erleichtert somit den Zugang zu privaten und öffentlichen elektronischen Diensten.

In der Praxis wird die digitale Brieftasche als Smartphone-App verfügbar sein.[10] Auf dem Markt existieren bereits einzelne Technologien wie die elektronische Altersverifikation oder Zahlungsmöglichkeiten per App. Die in der App gespeicherten Dokumente und Nachweise sollen durch spezielle Zugriffsschranken gesichert werden und in der Wallet verschlüsselt sein. Jede Weitergabe der Daten bedarf einer Zustimmung der Dateninhaber:innen. Die EUDI-Wallet ist interoperabel zu gestalten und mit den Daten ist möglichst sparsam umzugehen. Um die Datensouveränität zu wahren, sollen die personenbezogenen Daten unter der alleinigen Kontrolle der Nutzenden stehen (Art. 5a Abs. 4 lit. a eIDAS-VO) und nur die tatsächlich erforderlichen Informationen an Dritte weitergegeben werden. Zudem haben Nutzende das Recht, ein Pseudonym in der EUDI-Wallet zu generieren, sofern keine eindeutige Identifizierung über eine rechtliche Pflicht vorgesehen ist (Art. 5, Art. 5a Abs. 4 lit. b, Art. 5b Abs. 9 S. 2 eIDAS-VO). Öffentliche oder private Stellen, die Daten aus der EUDI-Wallet nutzen wollen, müssen sich registrieren (dann sind es sogenannte vertrauenswürdige Stellen).

Eine Nutzung der EUDI-Wallet erfolgt auf freiwilliger Basis (Art. 5a Abs. 15 S. 1 eIDAS-VO). Des Weiteren soll die EUDI-Wallet für die Bürger:innen kostenfrei ausgestellt und kostenfrei verwendet werden sowie widerrufbar sein (Art. 5a Abs. 13 eIDAS-VO).

---

6 Bundesministerium des Inneren und für Heimat (BMI), Pressemitteilung vom 20.9.2022, https://www.personalausweisportal.de/SharedDocs/kurzmeldungen/Webs/PA/DE/2022/09_wohnsitzanmeldung.html. Eine Übersicht, in welchen Städten und Kommunen die elektronische Wohnsitzanmeldung möglich ist, ist hier zu finden: https://wohnsitzanmeldung.gov.de/aktuelles-643078.

7 Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität.

8 Art. 3 Nr. 43, 44 eIDAS-VO.

9 Siehe zu qualifizierten elektronischen Signaturen und Siegeln ebenfalls, Schöbel, Digitale Zeugnisse und elektronische Signatur, DFN-Infobrief Recht 6/2025. Zur Nutzung in der Verwaltung bereits Yang-Jacobi, Von Papierbergen zur e-Verwaltung?, DFN-Infobrief Recht 4/2025.

10 Die bisherigen Prototypen von deutschen EUDI-Wallets sind hier zu finden, Bundesagentur für Springinnovationen (SPRIN-D), Funke „EUDI-Wallet Prototypes“, https://www.sprind.org/taten/challenges/eudi-wallet-prototypes#anchor-teams.

III. Umsetzung der EUDI-Wallet

Die EU-Mitgliedstaaten müssen innerhalb von 24 Monaten nach Inkrafttreten der Durchführungsrechtsakte mindestens eine standardisierte EUDI-Wallet zur Verfügung stellen. Die ersten Durchführungsrechtsakte wurden Anfang Dezember 2024 beschlossen, sodass die Frist nun auf Ende Dezember 2026 gesetzt ist. Die genauen Anforderungen an die EUDI-Wallet sind teilweise in den Art. 5a bis Art. 5f eIDAS-VO enthalten oder werden von der EU-Kommission über Durchführungsrechtsakte festgelegt. Insgesamt sollen der eIDAS-VO über 40 Durchführungsrechtsakte folgen. Zusätzlich müssen auch nationale Bestimmungen angepasst werden.

1. Europäische Durchführungsrechtsakte

Die technischen Standards der EUDI-Wallet legt die EU-Kommission mit laufenden Veränderungen in einem sogenannten Architecture and Reference Framework (ARF)[11] fest. Über die Open-Source-Softwareplattform Github ist eine Liste an „repositories" zu finden, die ständig bearbeitet und aktualisiert wird.[12] Divergierende Ansätze sollen vermieden und die Umsetzung der Anforderungen an die EUDI-Wallet harmonisiert werden, sodass auf eine Open-Source-Zusammenarbeit gesetzt wird. Zur technischen Umsetzung bestehen in Europa bereits seit April 2023 Pilotprojekte, um die technischen Grundlagen einer EUDI-Wallet zu testen.[13]

Zusätzlich hat die EU-Kommission Ende 2024 die ersten Durchführungsrechtsakte verabschiedet, die in einigen Regelungen der eIDAS-VO vorgesehen sind. Die bisher verabschiedeten Durchführungsverordnungen beziehen sich auf Referenzstandards und legen Spezifikationen und Verfahren für die EUDI-Wallet fest. Das sind erstens Anforderungen zur Integrität und den Kernfunktionen von eID-Brieftaschen[14], die sich an die Anbieter der Wallets richten. Zweitens sind es Regeln für Protokolle und Schnittstellen von EUDI-Wallets[15] bezüglich der Identitätsdaten und Attribute, die ebenso die Brieftaschenanbieter betreffen. Darin finden sich auch Vorgaben zur Möglichkeit der Löschung von Daten durch die Nutzenden nach Art. 17 Datenschutzgrundverordnung (DSGVO). Drittens werden Vorschriften über Personenidentifizierungsdaten und elektronische Attributsbescheinigungen für Brieftaschen[16] konkretisiert. Dabei werden neben den Regelungen für die Anbieter von Personenidentifizierungsdaten auch (im Vergleich aber wenige) Anforderungen an Anbieter elektronischer Attributsbescheinigungen gestellt (Art. 4 DurchführungsVO 2024/2977). Eine vierte Durchführungsverordnung enthält Vorgaben und Verpflichtungen zur Notifizierung der EU-Kommission.[17] Die letzte Durchführungsverordnung[18] betrifft verschiedene Bereiche der Zertifizierung wie den Rahmen von Funktionalität, Cybersicherheit und Datenschutz aber auch die Zertifizierungsstellen als solche. Weitere Durchführungsrechtsakte sollen noch folgen.[19]

Die Durchführungsrechtsakte haben einige Kritik erfahren. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wies im 33. Tätigkeitsbericht für den Datenschutz und Informationsfreiheit 2024 beispielsweise darauf hin, dass das „Recht auf pseudonyme Nutzung" in den Durchführungsrechtsakten und technischen Vorgaben bisher noch nicht ausreichend Beachtung findet.[20] Andere nationale und europäische Organisationen haben außerdem Bedenken zu den weiteren geplanten

11 ARF, Version 1.6.1, https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.6.1/.

12 https://github.com/eu-digital-identity-wallet.

13 EU-Kommission, EU Digital Identity Wallet Pilot implementation, 18.2.2025, https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation.

14 Durchführungsverordnung (EU) 2024/2979, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32024R2979.

15 Durchführungsverordnung (EU) 2024/2982, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402982.

16 Durchführungsverordnung (EU) 2024/2977, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402977.

17 Durchführungsverordnung (EU) 2024/2980, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402980.

18 Durchführungsverordnung (EU) 2024/2981, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402981.

19 Die geplanten Rechtsakte sind hier zu finden: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives_en?text=European%20Digital%20Identity%20Wallets&feedbackOpenDateFrom=28-11-2024&feedbackOpenDateClosedBy=03-01-2025.

20 BfDI, Tätigkeitsbericht 2024, S. 80, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/33TB_24.pdf?__blob=publicationFile&v=3.

Durchführungsrechtsakten geäußert.[21] Dabei geht es darum, dass die vertrauenswürdigen Stellen sich laut der Konkretisierung des Durchführungsrechtsakts bisher nicht zwingend als solche registrieren müssen. Vertrauenswürdige Stellen können Unternehmen oder öffentliche Einrichtungen sein. Diese sollten sich nach der eIDAS-VO eigentlich vorab in ihrem EU-Mitgliedstaat registrieren und darlegen, welche Daten sie zu welchem Zweck von den Nutzenden abfragen werden. Erst danach können sie die Daten tatsächlich abfragen. In den noch nicht erlassenen Durchführungsrechtsakten ist es den Mitgliedstaaten allerdings selbst überlassen, ob sie eine Zertifizierungsstelle für die Zulassung von Registrierungszertifikaten ermächtigen oder nicht. Falls ein Mitgliedstaat jedoch keine Zertifizierungsstelle festlegt, könnten die vertrauenswürdigen Stellen die Daten der Nutzenden ohne vorherige Kontrolle abfragen.[22] Dies gilt es, im Sinne der Datensparsamkeit und Datensouveränität zu vermeiden.

2. Nationale Umsetzung der Veränderungen in Deutschland

Als europäische Verordnung ist die eIDAS-VO zwar verbindlich und gilt unmittelbar in allen Mitgliedstaaten der EU. Für die nationale Durchführung und zur Festlegung von Zuständigkeiten sind jedoch ergänzende Regelungen im deutschen Recht zu treffen. 2017 verabschiedete der deutsche Gesetzgeber bereits das Vertrauensdienstegesetz (VDG). Das VDG regelt die Mitwirkungspflichten von Vertrauensdiensteanbietern und legt die Bundesnetzagentur als zuständige Aufsichtsbehörde fest. Nach den Neuerungen der eIDAS-VO muss das VDG angepasst werden. Weitere Anpassungen betreffen die Vertrauensdiensteverordnung (VDV), das Telekommunikationsgesetz (TKG) und das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG). Die Ampelregierung hatte noch im Oktober 2024 ein eIDAS-Durchführungsgesetz II[23] entworfen. Im TDDDG soll beispielsweise die Identifizierung über die EUDI-Wallet hinzugefügt werden, um einem Verlangen nach der Vorlage eines amtlichen Ausweises zu entsprechen (§ 7 Abs. 2 TDDDG-E). Das eIDAS-Durchführungsgesetz II wurde nicht mehr in der alten Legislaturperiode verabschiedet. Momentan befindet sich der Entwurf in der Ressortabstimmung zwischen Bundesministerien und dem Nationalen Normenkontrollrat.[24] Womöglich müssen mit der Zeit weitere nationale Gesetze wie das Verwaltungsverfahrensgesetz (VwVfG) oder die Sozialgesetzbücher (SGB) an die neueren Regeln der eIDAS-VO angepasst werden.[25]

Für die technische Umsetzung der EUDI-Wallet in Deutschland ist die Bundesagentur für Sprunginnovationen (SPRIND) zuständig. Diese startete im April 2024 im Auftrag des Bundesministeriums für Innern und für Heimat (BMI) einen Innovationswettbewerb. In den darauffolgenden 13 Monaten werden in mehreren Stufen Prototypen für die Infrastruktur von EUDI-Wallets entwickelt. Im September 2025 soll die dritte und letzte Stufe des Wettbewerbs mit dem erfolgreichen Abschluss eines umfassenden Architekturkonzepts und des Prototyps einer EUDI-Wallet enden. Das Ergebnis des Innovationswettbewerbs liefert Impulse für die genaue Ausgestaltung einer deutschen staatlichen EUDI-Wallet.[26] Staatliche Angebote müssen einfach und anwenderfreundlich gestaltet sein und dennoch ein hohes Sicherheits- und Datenschutzniveau gewährleisten, um für die Nutzenden attraktiv zu sein. Zusätzlich sollen allerdings auch private Anbieter EUDI-Wallets anbieten können, sobald der nationale Zertifizierungsprozess festgelegt wurde. Die Zertifizierungsstelle für die EUDI-Wallet in Deutschland wird voraussichtlich das Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen mit der Deutschen Akkreditierungsstelle (DAkkS). Die privaten Anbieter werden

21 Open Letter of Digital Rights and Consumer Organisations Concering eIDAS Implementing Acts, 20.1.2025, https://epicenter.works/fileadmin/medienspiegel/user_upload/eIDAS_iAs_OpenLetter_2025.pdf; Bereits vorher bestehende Kritik zu den ersten Durchführungsrechtsakten mit Bezug zu Pseudonymen, „Unverknüpfbarkeit“ und „Unbeobachtbarkeit“, Leisegang, Bürgerrechtsorganisation warnt vor „alarmierenden Mängeln“, 17.9.2024, https://netzpolitik.org/2024/digitale-brieftasche-buergerrechtsorganisation-warnt-vor-alarmierenden-maengeln/.

22 Leisegang, EU-Kommission öffnet Schlupflöcher für Überidentifikation, 2.4.2025, https://netzpolitik.org/2025/digitale-brieftasche-eu-kommission-oeffnet-schlupfloecher-fuer-ueberidentifikation/.

23 Bundesministerium für Digitales und Verkehr, 15.10.2024, Referentenentwurf zu eIDAS-Durchführungsgesetz II, https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-20/eIDAS-durchfuehrungsgesetz.pdf?__blob=publicationFile.

24 BMDV, eIDAS-Verordnung und Vertrauensdienste, 13.3.2025, https://bmdv.bund.de/DE/Themen/Digitales/Digitale-Dienste-Plattformen-Sicherheit/eIDAS-Verordnung-und-Vertrauensdienste/eidas-verordnung-und-vertrauensdienste.html.

25 Seegebarth, DuD 2022, 5, 8.

26 BMI, Pressemitteilung vom 30.9.2024, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/09/eudi-wallet-sep.html.

höchstwahrscheinlich etablierte Digitalunternehmen sein, die ihr bisheriges Wallet-Angebot um die Funktionen der EUDI-Wallet erweitern. Aber auch private Forschungseinrichtungen oder Stiftungen sind denkbar. Positiv ist, dass durch viele Angebote eine schnelle Verbreitung und hohe Nutzerfreundlichkeit folgen könnten.

Außerdem ist geplant, die im Rahmen der Neuerung des Onlinezugangsgesetzes (OZG) eingeführte BundID (bald DeutschlandID[27]) und die EUDI-Wallet zu verknüpfen. Sofern die DeutschlandID deutschlandweit an die technische Infrastruktur der Behörden angebunden wird, könnte eine Schnittstelle dafür sorgen, dass sich Nutzende über die EUDI-Wallet identifizieren können und den Behörden (aber auch umgekehrt die Behörden den Nutzenden) Informationen und Nachweise schneller und rechtssicherer zukommen lassen können.[28]

IV. Bedeutung für Hochschulen und Forschungseinrichtungen

Die Identifizierung durch Ausweise oder die Vorlage von Nachweisen sind bei Hochschulen und Forschungseinrichtungen von alltäglicher Bedeutung. In vielen Situationen müssen sich Studierende, Lehrende, Forschende und andere Universitätsangestellte ausweisen oder Fähigkeiten und Mitgliedschaften nachweisen. Eine digitale Identifizierung könnte die erforderlichen Verfahren vereinfachen und zu Entlastungen führen.[29] Die Möglichkeit, in der EUDI-Wallet Attributsbescheinigungen, also elektronische Nachweise bestimmter Fähigkeiten, Qualitäten oder Mitgliedschaften zu hinterlegen, können auch im Hochschulkontext bei der Immatrikulation, bei Bewerbungen oder in einem Einstellungsverfahren eine Erleichterung der Prozesse darstellen. Zusätzlich vereinfacht die gegenseitige Anerkennung dieser Nachweise innerhalb Europas Auslandsaufenthalte oder Auslandsstudien-/forschungen. Den Hochschulen und Forschungseinrichtungen ist zu raten, sich frühzeitig mit den digitalen Alternativen zu beschäftigen und die notwendige Infrastruktur für das digitale Auslesen von Attributen zu schaffen.

Die ausstellenden Einrichtungen müssten sich selbst gegenüber den Brieftaschen identifizieren und sicherstellen, dass die Attributsbescheinigungen die erforderlichen Informationen enthalten (Art. 4 DurchführungsVO 2024/2977).

Die weitere Möglichkeit, über die EUDI-Wallet Dokumente mittels qualifizierter elektronischer Signatur zu unterzeichnen oder qualifiziertem elektronischem Siegel zu besiegeln, erleichtert die Arbeit der Hochschulverwaltung außerdem bei der eigenen Erstellung von Dokumenten wie Zeugnissen oder Bescheinigungen.[30] So können die Verfahren nicht nur beschleunigt, sondern auch eine höhere Rechtssicherheit gewährleistet werden. Immerhin sind nachträgliche Änderungen an den Dokumenten nach dem Hinzufügen eines qualifizierten elektronischen Siegels leichter erkennbar. Dies schützt vor Manipulationen. Die europaweite Anerkennung der Technik erleichtert zudem die Nutzung des Zeugnisses im europäischen Ausland. Die EUDI-Wallet hat also großes Potenzial, die Digitalisierung, gerade in Deutschland und gerade auch im Hochschulbereich, voranzutreiben.

---

27 Siehe zur DeutschlandID und Bürgerkonten in der Verwaltung, Yang-Jacobi, Von Papierbergen zur e-Verwaltung, DFN-Infobrief Recht 4/2025.

28 Link/Drengwitz, Die BundID als Brückentechnologie, 8.4.2024, https://www.egovernment.de/die-bundid-als-brueckentechnologie-a-065b0426e8d24ffec59d276e17c2b671/?p=1.

29 Siehe dafür bereits Sonak, ID(een) muss man haben, DFN-Infobrief Recht 6/2023.

30 Zur Verwendung in digitalen Zeugnissen, Schöbel, Digitale Zeugnisse und elektronische Signatur, DFN-Infobrief Recht 6/2025.

Für die IT-Sicherheit haben wir jetzt jemanden

Die Beauftragung externer Dienstleister für die IT-Sicherheit stößt paradoxerweise immer wieder auf datenschutzrechtliche Bedenken

Von Marc-Philipp Geiselmann, Münster

Klassischerweise verwalten Hochschulen selbst ihre IT-Infrastruktur in Form von Hochschulrechenzentren. Diese werden immer öfter Ziel koordinierter Hacker-Angriffe.[1] Die Hacker-Angriffe bringen die IT-Systeme der Hochschulen zunehmend an ihre Kapazitätsgrenzen. Vermehrt greifen sie deshalb auf externe IT-Sicherheits-Dienstleister zurück. Diese müssen zumeist aufgrund der technischen Gegebenheiten die in den IT-Systemen der Hochschulen übermittelten Daten entschlüsseln und als sogenannte Klardaten lesen. Dabei tauchen auch datenschutzrechtliche Bedenken auf, die den Einsatz externer Dienstleister zur Erhöhung der IT-Sicherheit zu hemmen drohen. Dieser Beitrag soll einen Überblick über den datenschutzrechtlichen Rahmen geben.

I. Rechtsnatur der Beauftragung externer Dienstleister

Zunächst ist zu klären, ob es sich bei der Beauftragung um eine gemeinsame Verantwortung nach Art. 26 Datenschutz-Grundverordnung (DSGVO) oder um eine Auftragsverarbeitung nach Art. 28 DSGVO handelt.[2] Abgrenzungskriterium hierfür ist die Weisungsgebundenheit des Auftragsverarbeiters. Der Auftragsverarbeiter verarbeitet die Daten nach dem Willen des Auftraggebers, dem die Art und der Zweck der Datenverarbeitung obliegt.[3] Die Entscheidung über die technischen und organisatorischen Mittel, also die Auswahl der Hard- und Software, kann dabei an den Auftragsverarbeiter delegiert werden.[4] Auch standardisierte IT-Dienstleistungen und Cloud-Services sind als Auftragsverarbeitung zu bewerten.[5]

Zudem spielt die Bewertung der verfolgten Interessen für die Beurteilung eine Rolle. Verfolgt der Auftragsverarbeiter bei der Verarbeitung eigene Interessen unmittelbar an den personenbezogenen Daten, so scheidet eine Auftragsverarbeitung aus. Ein finanzielles Eigeninteresse bei der Durchführung des Auftrags ist dagegen unschädlich.[6]

---

1 S. DER SPIEGEL vom 01.11.2023: Hackerangriff beeinträchtigt Teile der Hochschule Hannover, abrufbar unter https://www.spiegel.de/netzwelt/web/ransomware-hackerangriff-beeintraechtigt-teile-der-hochschule-hannover-a-e6247f8b-7adb-4bdd-986c-7a85068b38a3, Hessenschau vom 08.07.2024: Hacker-Attacke auf Frankfurter Hochschule, abrufbar unter: https://www.hessenschau.de/panorama/hacker-attacke-auf-frankfurter-university-of-applied-sciences-v1,uas-frankfurt-hacker-100.html (alle Links dieses Beitrags zuletzt abgerufen am 30.04.2025).

2 Zur gemeinsamen Verantwortung siehe Geiselmann, Gemeinsam sind wir verantwortlich!, DFN-Infobrief Recht 01/2024.

3 Spoerr, in: BeckOK DatenschutzR, 51. Edition, Art. 28 DSGVO Rn. 18.

4 Spoerr, in: BeckOK DatenschutzR, 51. Edition, Art. 28 DSGVO Rn. 18a.

5 Spoerr, in: BeckOK DatenschutzR, 51. Edition, Art. 28 DSGVO Rn. 18a und 24c.

6 Spoerr, in: BeckOK DatenschutzR, 51. Edition, Art. 28 DSGVO Rn. 19.

II. Rechtsgrundlage für die Auftragsverarbeitung

Die Auftragsverarbeitung ist eine privilegierte Arbeitsteilung. Der Umfang der Privilegierung und die Erforderlichkeit einer Rechtsgrundlage sind in der juristischen Literatur jedoch umstritten.

Es wird einerseits vertreten, dass die Datenverarbeitung im Rahmen der Auftragsverarbeitung nicht voraussetzungslos ist, sondern einer datenschutzrechtlichen Rechtfertigung bedarf. Die Weitergabe der Daten an den Auftragsverarbeiter stellt einen Verarbeitungsvorgang dar, der rechtfertigungsbedürftig ist, auch wenn die Intensität der Verarbeitung geringer ist, als bei einer Übermittlung personenbezogener Daten an einen Dritten.[7] Daraus folgt für die Weitergabe der Daten, dass eine Rechtsgrundlage nach Art. 6 oder 9 DSGVO erforderlich ist. Regelmäßig ist Art. 6 Abs. 1 lit.f DSGVO einschlägig. Dies hat zur Konsequenz, dass die Erforderlichkeit für jede Weitergabe an den Dienstleister mittels einer Interessenabwägung bejaht werden muss, wie bei der Verarbeitung durch den Verantwortlichen selbst.[8]
Andererseits wird weit überwiegend vertreten, dass die Privilegierung so weit geht, dass die Verarbeitung voraussetzungslos möglich ist.[9] Zur Begründung wird ausgeführt, dass die Privilegierung des Art. 28 DSGVO dem Verantwortlichen Effizienzvorteile erschließen soll.[10] Da der Auftragsverarbeiter kein Dritter nach Art. 4 Nr. 10 DSGVO ist, liegt auch keine Übermittlung der Daten und damit keine Verarbeitung nach Art. 4 Nr. 2 DSGVO vor. Deshalb ist auch keine Rechtsgrundlage nach Art. 6 DSGVO erforderlich.[11] Zudem kennt die Definition der Verarbeitung nicht nur einzelne kleinteilige Vorgänge als Verarbeitung, sondern auch Vorgangsreihen, sodass die Auftragsverarbeitung als Teil einer Verarbeitung verstanden werden kann.[12]

Die Erforderlichkeit einer Rechtsgrundlage für die Datenübertragung zwischen Auftraggeber und Auftragsverarbeiter würde bedeuten, dass der Auftragsverarbeiter selbst zum Verantwortlichen aufsteigt und ein weitergehendes Pflichtenprogramm zu erfüllen hätte, als es die Trennung zwischen Verantwortlichem und Auftragsverarbeiter vorsieht. Das Erfordernis einer Rechtsgrundlage nach Art. 6 oder 9 DSGVO höhlt die Privilegierung des Art. 28 DSGVO aus. Im Falle besonderer Kategorien personenbezogener Daten wäre eine Auftragsverarbeitung praktisch nur sehr eingeschränkt möglich.[13]

Nur durch eine Befreiung von dem Rechtfertigungsregime der Art. 6 und 9 DSGVO kann die Auftragsverarbeitung in der Wirtschaftspraxis Synergien entfalten.[14]

Ein Absinken des Schutzniveaus in Bezug auf sensible Daten im Sinne des Art. 9 DSGVO ist zudem durch die Privilegierung des Art. 28 DSGVO nicht zu befürchten, da die Art. 25 und 32 DSGVO durch die zu ergreifenden technisch-organisatorischen Maßnahmen ein ausreichendes Schutzniveau sicherstellen.[15]

Als Ergebnis kann somit festgehalten werden, dass die Datenverarbeitung im Rahmen der Auftragsverarbeitung keiner zusätzlichen Rechtsgrundlage bedarf, sondern voraussetzungslos möglich ist. Grundsätzliche datenschutzrechtliche Bedenken bestehen bei der Einschaltung eines IT-Dienstleisters daher nicht.

III. Auswahl des Auftragsverarbeiters

Als Auftragsverarbeiter kommt nur in Betracht, wer nach Art. 28 Abs. 1 DSGVO hinreichende Garantien dafür bietet, dass geeignete

---

7 Spoerr, in: BeckOK DatenschutzR, 51. Edition, Art. 28 DSGVO Rn. 29b.

8 Spoerr, in: BeckOK DatenschutzR, 51. Edition, Art. 28 DSGVO Rn. 31 f., Bertermann, in: Ehmann/Selmayr, Art. 28 DSGVO Rn. 6.

9 Bertermann, in: Ehmann/Selmayr, Art. 28 DSGVO Rn. 7; Martini, in: Paal/Pauly, Art. 28 DSGVO, Rn. 8a-10a; Gabel/Lutz, in: Taeger/Gabel, Art. 28 DSGVO Rn. 11; Hartung, in: Kühling/Buchner, Art. 28 DSGVO Rn. 15 ff.; Ingold, in: Sydow/Marsch, Art. 28 DSGVO Rn. 28; Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 28 DSGVO Rn. 33; Plath, in: Plath, Art. 28 DSGVO Rn. 9.

10 Martini, in: Paal/Pauly, Art. 28 DSGVO Rn. 8 und 9.

11 Martini, in: Paal/Pauly, Art. 28 DSGVO Rn. 8a. Hartung, in: Kühling/Buchner, Art. 28 DSGVO Rn. 17.

12 Bertermann, in: Ehmann/Selmayr, Art. 28 DSGVO Rn. 7; Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 28 DSGVO Rn. 33.

13 Gabel/Lutz, in: Taeger/Gabel, Art. 28 DSGVO Rn. 11; Martini, in: Paal/Pauly, Art. 28 DSGVO Rn. 10, Hartung, in: Kühling/Buchner, Art. 28 DSGVO Rn. 10 und 21; Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 28 DSGVO Rn. 33.

14 Martini, in: Paal/Pauly, Art. 28 DSGVO Rn. 10a.

15 Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 28 DSGVO Rn. 33.

technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DSGVO erfolgt und die Rechte der betroffenen Personen wahrt. Erwägungsgrund (ErwG.) 81 S. 1 DSGVO führt dazu aus, dass als Kriterien dafür insbesondere Fachwissen, Zuverlässigkeit und Ressourcen in Betracht zu ziehen sind, um zu beurteilen, ob technische und organisatorische Maßnahmen auch für die Sicherheit der Verarbeitung getroffen werden.[16] Den Verantwortlichen, also die Hochschule, trifft die Verantwortung bezüglich der Auswahl des Auftragsverarbeiters, die Überwachung der Art und Weise der Datenverarbeitung durch den Auftragsverarbeiter und die Prüfung des Auftragsverarbeitungsvertrags.[17] Die Pflicht der fortlaufenden Überprüfung des Auftragsverarbeiters ergibt sich nicht ausdrücklich aus der DSGVO. Sie wird jedoch aus der Formulierung „arbeitet" des Art. 28 Abs. 1 DSGVO hergeleitet, die sich auf den gesamten Zeitraum der Auftragsverarbeitung bezieht.[18] Zertifizierungen des Auftragsverarbeiters bieten nach ErwG. 81 S. 2 DSGVO lediglich einen Anhaltspunkt, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.[19]

Die Maßnahmen des Auftragsverarbeiters sind zu dokumentieren.[20]

IV. Inhalt eines Auftragsverarbeitungsvertrags (AVV)

Ist der Auftragsverarbeiter ausgewählt, so sieht Art. 28 Abs. 3 DSGVO den Abschluss eines Vertrags vor. Für den Inhalt eines Auftragsverarbeitungsvertrags ist nach Art. 28 Abs. 3 lit. a bis h DSGVO ein Mindestinhalt vorgegeben.

Demnach verarbeitet der Auftragsverarbeiter die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dies gilt auch für die Übermittlung an Drittländer oder internationale Organisationen, es sei denn, dass andere gesetzliche Verpflichtungen innerhalb der EU oder den Mitgliedstaaten bestehen. In solchen Fällen informiert der Auftragsverarbeiter den Verantwortlichen im Voraus, es sei denn, das betreffende Recht untersagt eine solche Mitteilung aus wichtigem öffentlichen Interesse (lit. a). Zudem stellt der Auftragsverarbeiter sicher, dass alle Personen, die Zugriff auf personenbezogene Daten haben, zur Vertraulichkeit verpflichtet sind oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen (lit. b).

Darüber hinaus ergreift der Auftragsverarbeiter alle gemäß Art. 32 DSGVO erforderlichen Sicherheitsmaßnahmen (lit. c) und hält die Bedingungen für den Einsatz weiterer Auftragsverarbeiter gemäß den relevanten Absätzen ein (lit. d). Zusätzlich unterstützt er den Verantwortlichen, soweit möglich, durch technische und organisatorische Maßnahmen, um dessen Verpflichtungen zur Beantwortung von Anträgen auf die Ausübung der in Kapitel III genannten Rechte der betroffenen Personen zu erfüllen (lit. e).[21]

Unter Berücksichtigung der Verarbeitungsart und der verfügbaren Informationen leistet der Auftragsverarbeiter auch Unterstützung bei der Einhaltung der in den Artikeln 32 bis 36 festgelegten Pflichten (lit. f). Nach Beendigung der Verarbeitungsleistungen werden auf Wunsch des Verantwortlichen alle personenbezogenen Daten entweder gelöscht oder zurückgegeben, es sei denn, es besteht eine gesetzliche Verpflichtung zur Speicherung (lit. g). Schließlich stellt der Auftragsverarbeiter dem Verantwortlichen alle notwendigen Informationen bereit, um die Einhaltung der festgelegten Pflichten zu belegen und ermöglicht sowie unterstützt erforderliche Überprüfungen und Inspektionen durch den Verantwortlichen oder dessen beauftragte Prüfer (lit. f).

Für einen Auftragsverarbeitungsvertrag stellen sowohl die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

16 Hartung, in: Kühling/Buchner, Art. 28 DSGVO Rn. 56; Spoerr, in: BeckOK DatenschutzR, 51. Edition, Art. 28 DSGVO Rn. 33.

17 Hartung, in: Kühling/Buchner, Art. 28 DSGVO Rn. 55; Spoerr, in: BeckOK DatenschutzR, 51. Edition, Art. 28 DSGVO Rn. 33.

18 Hartung, in: Kühling/Buchner, Art. 28 DSGVO Rn. 60; Spoerr, in: BeckOK DatenschutzR, 51. Edition, Art. 28 DSGVO Rn. 35.

19 Hartung, in: Kühling/Buchner, Art. 28 DSGVO Rn. 59.

20 Hartung, in: Kühling/Buchner, Art. 28 DSGVO Rn. 58.

21 Zu den technischen und organisatorischen Maßnahmen siehe Müller, Ich glaub, es hackt, DFN-Infobrief Recht 4/2024.

(BfDI) als auch mehrere Landesdatenschutzbeauftragte Formulierungshilfen bereit.[22]

V. Weitere Pflichten des Verantwortlichen

Der Verantwortliche sollte betroffenen Personen die Identität sämtlicher Auftragsverarbeiter und Unterauftragsverarbeiter mitteilen. Dies kann in der Datenschutzerklärung geschehen.[23]

Bei Beendigung der Auftragsverarbeitung hat der Verantwortliche darauf zu achten, dass der Auftragsverarbeiter alle personenbezogenen Daten an den Verantwortlichen herausgibt oder tatsächlich löscht und eine Bescheinigung über die Löschung erstellt. Genügt der Verantwortliche dieser Kontrollpflicht nicht, so kann er sich nicht auf einen Exzess des Auftragsverarbeiters berufen.[24]

VI. Fazit

Auftragsverarbeitungen unterliegen einer datenschutzrechtlichen Privilegierung. Diese führt dazu, dass der Auftraggeber keine zusätzliche Rechtsgrundlage für deren Einschaltung benötigt. Ganz aus dem Pflichtenprogramm der DSGVO ist der Auftraggeber jedoch nicht entlassen. Er hat den Auftragsverarbeiter auszuwählen und zu überwachen.

---

22 Vereinbarung zu Auftragsverarbeitung des BfDI: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Muster_zur_Auftragsverarbeitung.pdf?__blob=publicationFile&v=2; Formulierungshilfe des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/01/muster_adv.pdf; Formulierungshilfe des Bayerischen Landesamt für Datenschutzaufsicht: https://www.lda.bayern.de/media/muster/formulierungshilfe_av.pdf.

23 EDPB, Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s), Adopted on 7 October 2024, Rn. 21, abrufbar unter https://www.edpb.europa.eu/system/files/2024-10/edpb_opinion_202422_relianceonprocessors-sub-processors_en.pdf, (zuletzt abgerufen am 30.04.2025); Heynike/Ringel/Taraz, CCZ 2025, 75 (77).

24 OLG Dresden, Urteil vom 5. November 2024, Az.: 4 U 729/24; OLG Dresden, Urteil vom 15. Oktober 2024, Az.: 4 U 940/24; Heynike/Ringel/Taraz, CCZ 2025, 75 (76 f.).

DFN Infobrief-Recht-Aktuell

- ## Plattformrecht: Vorläufige Feststellung der EU-Kommission zu Verstößen von TikTok gegen den Digital Services Act (DSA) im Bereich der Werbetransparenz

  Die EU-Kommission hat am 15. Mai 2025 eine vorläufige Einschätzung zu Verstößen von TikTok gegen den DSA wegen intransparenter Werbung veröffentlicht. Sie hat dabei vor allem festgestellt, dass TikTok nicht die erforderlichen Informationen über den Inhalt der Werbung und darüber, wer diese finanziert, bereitstellt. Es könnte eine Geldbuße von bis zu 6 % des gesamten weltweiten Jahresumsatzes verhängt werden.

  Hier erhalten Sie den Link zur Pressemitteilung der EU-Kommission:
  https://ec.europa.eu/commission/presscorner/api/files/document/print/de/ip_25_1223/IP_25_1223_EN.pdf

- ## Arbeitsrecht: Landesarbeitsgericht (LAG) Köln zur Überwachung während der Arbeitszeit nach § 26 Abs. 1 S. 2 Bundesdatenschutzgesetz (BDSG)

  Das LAG Köln, Urteil vom 11. Februar 2025 – 7 Sa 635/23, hält die Überwachung während der Arbeitszeit durch eine Detektei sowie das Anbringen eines GPS-Senders an einem während der Schichtzeit genutzten Dienstfahrzeug für zulässig. Das Gericht hatte eine außerordentliche Kündigung zu überprüfen, der die Frage zugrunde lag, ob aufgrund der Überwachung ein Beweisverwertungsverbot anzunehmen ist. Es kam zu dem Ergebnis, dass zwar ein Eingriff in die Persönlichkeitsrechte und die Rechte auf informationelle Selbstbestimmung vorliegt, dieser aber von geringer Intensität ist.

  Hier erhalten Sie den Link zur Entscheidung:
  https://nrwe.justiz.nrw.de/arbgs/koeln/lag_koeln/j2025/7_Sa_635_23_Urteil_20250211.html

- ## Prozessrecht: Entscheidung des Landgerichts (LG) Berlin zur Zulässigkeit von Klagen von Forschenden gegen die Plattform X in deren Mitgliedstaat

  Die Nichtregierungsorganisation Democracy Reporting International (DRI) hatte zusammen mit der Gesellschaft für Freiheitsrechte (GFF) gegen X auf Herausgabe öffentlich verfügbarer Daten geklagt. Der Anspruch wurde nach Art. 40 Abs. 12 DSA geltend gemacht. Das Gericht stellte in seiner Entscheidung fest, dass Forschende ihren Anspruch auf Zugang zu Forschungsdaten in dem Land geltend machen können, in dem sie forschen.

  Hier erhalten Sie den Link zur Pressemitteilung der GFF:
  https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-x-teilerfolg

Kurzbeitrag: Europäischer KI-Masterplan

EU-Kommission veröffentlicht KI-Kontinent-Aktionsplan

von Johannes Müller, Münster

Die Europäische Kommission hat einen KI-Kontinent-Aktionsplan[1] veröffentlicht. Dieser legt Maßnahmen fest, die dazu beitragen sollen, dass die Europäische Union eine führende Rolle in der weiteren KI-Entwicklung einnimmt.

I. KI als Schlüsseltechnologie

Der Aktionsplan der Europäischen Kommission baut auf der Erkenntnis auf, dass vertrauenswürdige KI, die den Menschen in den Mittelpunkt stellt, sowohl entscheidend für das wirtschaftliche Wachstum sei als auch für die Wahrung der Grundrechte und Grundwerte, auf denen unsere Gesellschaft basiert. Nach Auffassung der EU-Kommission ist das globale Wettrennen um die Vorreiterrolle in der KI-Entwicklung noch nicht entschieden.[2] Die EU müsste ihren eigenen Ansatz beibehalten und sich auf ihre Stärken konzentrieren. Diese bestünden unter anderem in einem großen Binnenmarkt mit einheitlichen Sicherheitsregeln, hochwertiger Forschung und Wissenschaft, einer wachsenden Startup-Szene, industrieller Expertise und hohen Rechenkapazitäten. Als Maßnahmen für die weitere Entwicklung beschäftigt sich der Aktionsplan mit dem Ausbau von Recheninfrastrukturen, einer Verbesserung des Zugangs zu qualitativ hochwertigen Daten, Maßnahmen zur Förderung neuer industrieller und wissenschaftlicher Anwendungen und der Förderung der Talentbasis in Europa. Darüber hinaus beschäftigt sich der KI-Aktionsplan aber auch mit möglichen Verbesserungen in der KI-Regulierung.

II. Praktikabilität der KI-Regulierung

Den Schwerpunkt der europäischen KI-Regulierung bildet die KI-Verordnung (KI-VO).[3] Nach den Aussagen des Aktionsplans soll sie einen gut funktionierenden Binnenmarkt für KI schaffen, der den freien Verkehr zu harmonisierten Bedingungen in der EU gewährleistet. Gleichzeitig gewährleiste die Verordnung die Sicherheit von KI-Anwendungen und respektiere die Grundrechte. Hiermit erzeuge sie Kaufargumente für europäische KI-Anwendungen.

Ebenso ist sich die EU-Kommission bewusst, dass der Erfolg der KI-VO entscheidend von ihrer Praktikabilität abhängt. Hierzu werden die Mitgliedstaaten und die Kommission einen „Service Desk“ für die KI-VO einrichten. Dieser soll eine zentrale Informationsdrehscheibe zum KI-Gesetz sein. Hier können Interessenvertreter Hilfe anfordern und maßgeschneiderte Antworten erhalten. Die Initiative soll unkomplizierten und kostenlosen Zugang zu Informationen und Anleitungen zur Verordnung bieten. Die Antworten sollen praktische Ratschläge umfassen, um das Verständnis und die Einhaltung der KI-VO zu erleichtern. Der Service Desk wird vom KI-Büro der Kommission betrieben. Darüber hinaus wird die Kommission weitere Veröffentlichungen zur Anwendung der KI-VO bereitstellen, um die Einhaltung zu unterstützen. Dazu gehören Durchführungs- und delegierte Rechtsakte sowie Leitlinien, die beispielsweise die kohärente Anwendung des KI-Gesetzes mit sektorspezifischen Produktvorschriften (z. B. der Medizinprodukteverordnung) und das Zusammenspiel mit anderer verwandter Gesetzgebung erleichtern sollen.

Zudem möchte die Kommission auf den Erkenntnissen der aktuellen Umsetzungsphase aufbauen und weitere Maßnahmen

1 Aufrufbar in englischer Sprache unter https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan (zuletzt abgerufen am 05.05.2025).

2 Zum Aufbau europäischer Sprachmodelle Schöbel, Ki-Modelle made in Europe?, DFN-Infobrief Recht 04/2025.

3 Zu den Regelungen der KI-VO Schöbel, AI Act – Licht der Europäischen Union?, DFN-Infobrief Recht 12/2024.

identifizieren, die notwendig sind, um eine einfache Anwendung der KI-VO zu ermöglichen, insbesondere für kleinere Unternehmen. Hierzu wurde gleichzeitig mit dem Aktionsplan eine öffentliche Konsultation zu den Herausforderungen bei der Umsetzung der KI-VO gestartet. Ziel ist es, herauszufinden, wo regulatorische Unsicherheit die Entwicklung und Einführung von KI behindert und wie die Kommission und die Mitgliedstaaten die Akteure besser unterstützen können. Die Ergebnisse fließen in die Bereitstellung von Vorlagen, Leitlinien, Webinaren und Schulungen ein. Sie werden auch in die umfassendere Bewertung, ob die Verordnung den Praxisbedürfnissen angemessen Rechnung trägt, einfließen.

III. Bedeutung für wissenschaftliche Einrichtungen

Die geplante Unterstützung bei der Anwendung der KI-Verordnung kann auch für wissenschaftliche Einrichtungen bedeutsam sein. Trotz des Wissenschaftsprivilegs sind auch diese – etwa bei Einsatz von KI-Systemen in der Verwaltung – verpflichtet, die Vorschriften der KI-VO zu beachten.[4] Damit kann etwa auch der „Service Desk" zur KI-VO wissenschaftliche Einrichtungen bei praktischen Anwendungsfragen unterstützen. Für etwaige Nachbesserungsvorschläge sollte die öffentliche Konsultation beachtet werden.

4 Ausführlich, Schöbel, Der AI Act und die Wissenschaft, DFN-Infobrief Recht 2/2025.

Impressum

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: dfn-verein@dfn.de

Texte:

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Universität Münster und der Freien Universität Berlin.

Universität Münster
Institut für Informations-,
Telekommunikations- und Medienrecht
-Zivilrechtliche Abteilung-
Prof. Dr. Thomas Hoeren
Leonardo Campus 9, 48149 Münster

Tel. (0251) 83-3863, Fax -38601

E-Mail: recht@dfn.de

Freie Universität Berlin
Professur für Bürgerliches Recht,
Wirtschafts-, Wettbewerbs- und
Immaterialgüterrecht
Prof. Dr. Katharina de la Durantaye, LL. M. (Yale)
Van't-Hoff-Str. 8, 14195 Berlin

Tel. (030) 838-66754

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht", der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn