



MICHAEL B. BARNES

BÜRGERANLIEGEN • STELLUNGNAHMEN • KORRESPONDENZ



Hengelerstraße 1

49565 Bramsche



mbarnes61@outlook.com

2026-08-14

Das Fundament der Bürger-ID: Wie die digitale Identität den Alltag verändert



0. Einleitung: Die verschwindende analoge Welt

Es ist noch gar nicht lange her, da war unsere Alltagsidentität greifbar und verteilt. Der Personalausweis lag im Portemonnaie, die Plastikkarte der Krankenkasse in der Tasche. Wer etwas von der Verwaltung wollte, ging persönlich aufs Amt. Einkäufe wurden ganz



selbstverständlich mit Scheinen und Münzen bezahlt, und sensible Gesundheitsdaten ruhten wohlbehütet in den Hängeordnern von Arztpraxen und Krankenhäusern.

Diese analoge Vertrautheit löst sich nicht schlagartig auf – doch sie verändert ihr Gesicht grundlegend.

Schritt für Schritt halten digitale Strukturen Einzug in nahezu jeden Winkel unseres Zusammenlebens: Passwesen, Gesundheitsversorgung, öffentliche Verwaltung und der gesamte Zahlungsverkehr werden neu verdrahtet. Für jede einzelne dieser Maßnahmen gibt es nachvollziehbare Argumente wie Effizienz, Schnelligkeit und Komfort.

Doch was bedeutet diese Entwicklung, wenn man das Gesamtbild betrachtet?

Was früher auf völlig unterschiedliche Lebensbereiche, Institutionen, Aktenordner und dezentrale Systeme verteilt war, läuft nun in vernetzten, digitalen Architekturen zusammen. Dadurch entstehen technische Möglichkeiten zur Datenverknüpfung und Auswertung, die es in dieser Form noch nie gab. Eine demokratische Gesellschaft muss genau hinsehen: Welche Infrastruktur wird hier gerade im Hintergrund errichtet? Welche Daten fließen wohin, wer erhält Zugriff darauf – und welche Kontrollmöglichkeiten bleiben dem Einzelnen überhaupt noch erhalten?

Inhalt

Das Fundament der Bürger-ID: Wie die digitale Identität den Alltag verändert ..	1
0. Einleitung: Die verschwindende analoge Welt	1
1. Das Fundament der Bürger-ID: Wie die digitale Identität den Alltag verändert	4
2. Datenschutz als Abwehrrecht: Ihr Schutzwall gegen den digitalen Zugriff .	5
3. Die juristische Notbremse: Ihre praktische Anleitung zum Selbstschutz.....	6
Praktische Schritte zur Wahrnehmung der eigenen Rechte	6
4. Der strategische Ausblick: Warum Resilienz ein langfristiger Prozess bleibt	7
5. Politische Verantwortung: Wer den vernetzten Staat auf den Weg brachte	7
5.1 Der Ausgangspunkt auf EU-Ebene: Die Europäische Kommission legt 2021 den Grundstein	7
5.2 Vom Vorschlag zum europäischen Gesetz: Rat und Parlament übernehmen	8
5.3 Die entscheidende Abstimmung im Europäischen Parlament	9
5.4 Der endgültige europäische Rechtsrahmen.....	10
5.5 Deutschland 2026: Karsten Wildberger und die nationale Umsetzung	11
5.6 Wer trug die Entscheidung – und wer stellte sich dagegen?	11



5.7 Die deutsche Opposition wird aktiv: Der Streit um die nationale Umsetzung..	13
5.8 Grüne und Linke: Kontrolle der Regierung – aber unterschiedliche parlamentarische Aktivität	14
6. Die physische Säule: Technische Autarkie durch moderne Inselanlagen	15
7. Die materielle Basis: Wasserbehandlung und das rollierende Vorratssystem	16
8. Die finanzielle Resilienz: Bargeldschutz im vernetzten Zahlungsraum	17
8.1 Bargeld als analoge Rückfallebene	18
8.2 Die 10.000-Euro-Bargeldgrenze: Wer sie auf den Weg brachte und wer sie politisch mittrug	18
Was gilt tatsächlich?.....	20
8.3 Was unternahm die Opposition gegen die Bargeldbegrenzung?	20
8.4 Der digitale Euro: Wer ihn auf den Weg brachte und welche Rolle Christine Lagarde spielt	21
8.5 Regierung und Opposition: Wer unterstützte den digitalen Euro – und wer stellte sich dagegen?	23
8.6 Was bedeutet das für den Bürger? Bargeld und digitale Zahlung als bewusste Wahl.....	24
9. Die Zusammenführung: Wie Sie jetzt aktiv die Kontrolle behalten.....	25
10. Der persönliche Schutzfahrplan: Vom Wissen zum konsequenten Handeln	26
10.1 Sofortmaßnahmen – digitale Bestandsaufnahme	26
10.1.1 Kontrolle von Konten, Authentifizierung und Berechtigungen	26
10.1.2 Gezielte Wahrnehmung von Auskunftsrechten nach DSGVO	27
10.2 Gesundheit und ePA – Rechte konkret kennen.....	27
10.2.1 Gesetzliche Widerspruchsrechte zur elektronischen Patientenakte	27
10.3 Kurzfristige materielle Vorsorge	27
10.3.1 Lebensmittel- und Trinkwasserressourcen.....	28
10.4 Finanzielle Vorsorge	28
10.4.1 Erhalt der persönlichen Zahlungsfähigkeit	28
10.5 Mittelfristige technische Vorsorge	28
10.5.1 Notstrominfrastruktur und Kapazitätsplanung.....	29
10.6 Persönlicher Notfallordner	29
10.6.1 Analoge Absicherung kritischer Dokumente	29



10.7 Regelmäßige Kontrolle	30
10.7.1 Rhythmus zur Aktualisierung und Wartung	30
10.8 Weiterführender Schutz der digitalen Privatsphäre	30
11. Fazit: Selbstbestimmung beginnt mit Wissen – und endet nicht dort	30
Resümee – die wichtigsten Stationen auf einen Blick	31
Schlussgedanke: Infrastruktur bleibt – Regierungen wechseln	32
Impressum / Kontakt	33
Rechtlicher Hinweis	33

1. Das Fundament der Bürger-ID: Wie die digitale Identität den Alltag verändert

Was bisher als getrennte Modernisierungsprojekte deklariert wurde, fügt sich zunehmend zu einer vernetzten staatlichen Datenarchitektur zusammen. Am **20. Mai 2026** hat das Bundeskabinett den Entwurf für das **Digitale-Identitäten-Gesetz (DIdG)** beschlossen. Das Gesetz soll die nationale rechtliche Grundlage für die europäische EUDI-Wallet schaffen. Das Bundesministerium für Digitales und Staatsmodernisierung beschreibt die Wallet als Infrastruktur, mit der Bürger künftig unter anderem digitale Identitätsnachweise verwalten, sich online und offline ausweisen sowie perspektivisch elektronische Signaturen und weitere Nachweise über das Smartphone nutzen können. ([BMDs](#))

[BMDS – EUDI-Wallet und Digitale Identitäten](#)

Der europäische Rechtsrahmen dafür ist die **Verordnung (EU) 2024/1183 vom 11. April 2024**, mit der die bestehende eIDAS-Verordnung geändert und der europäische Rahmen für digitale Identitäten einschließlich der European Digital Identity Wallets geschaffen wurde. ([EUR-Lex](#))

[EUR-Lex – Verordnung \(EU\) 2024/1183 zum europäischen Rahmen für digitale Identitäten](#)

Parallel dazu hat das Bundeskabinett am **15. Juli 2026** Eckpunkte für ein **zentrales Pass- und Ausweisregister auf Bundesebene** beschlossen. Damit soll die bisherige Registerführung bei mehr als 6.000 Pass- und Ausweisbehörden sowie den Auslandsvertretungen durch ein Zentralregister des Bundes ersetzt werden. Nach Angaben der Bundesregierung sollen darin alle ausgegebenen und unter Beachtung der Löschfristen gültigen **Reisepässe, Personalausweise und eID-Karten** nachgewiesen werden. Der biometrische Fingerabdruck ist davon ausdrücklich ausgenommen; er soll weiterhin ausschließlich dezentral auf dem Chip des jeweiligen Ausweisdokuments gespeichert werden. ([Bundesregierung](#))

[Bundesregierung – Digitales Pass- und Ausweiszentralregister beschlossen](#)



Damit entstehen zwei unterschiedliche, aber für die künftige digitale Identitätsinfrastruktur zentrale Entwicklungen: **eine europaweit nutzbare digitale Identität auf dem Smartphone und eine Zentralisierung staatlicher Pass- und Ausweisdaten auf Bundesebene.** Welche Daten jeweils gespeichert werden, welche Stellen darauf zugreifen dürfen und welche technischen Verknüpfungen künftig möglich oder rechtlich zulässig sein werden, gehört deshalb zu den entscheidenden Fragen für Datenschutz und informationelle Selbstbestimmung. ([BMDs](#))

2. Datenschutz als Abwehrrecht: Ihr Schutzwall gegen den digitalen Zugriff

Beim rasanten Ausbau der neuen Bürger-ID wird von offizieller Seite stets betont, dass der Datenschutz nach wie vor die oberste Priorität habe. Nach Artikel 9 der Datenschutz-Grundverordnung (DSGVO) gehören Identitäts- und Biometriedaten zu den besonders geschützten Kategorien personenbezogener Daten. Ihre Verarbeitung ist im Grundsatz streng untersagt, es sei denn, der Gesetzgeber schafft ausdrückliche Ausnahmen.

Und genau hier liegt die entscheidende Weichenstellung für Ihre persönliche Resilienz: Der Datenschutz darf kein passiver Begriff sein – er ist Ihr aktives Abwehrrecht gegen die totale Vernetzung. Die DSGVO gibt Ihnen im Rahmen der Betroffenenrechte der Bundesdatenschutzbeauftragten (BfDI) das verbriefte Recht auf absolute Transparenz. Mittels eines Auskunftsbegehrens nach Artikel 15 DSGVO können Sie von jeder staatlichen Stelle und jedem Register schriftlich einfordern, welche Daten über Sie ausgetauscht wurden.

Gekoppelt mit konsequent genutzten Opt-out-Verfahren wird das Datenschutzrecht zum juristischen Schutzschild. Sie warten nicht darauf, dass der Staat Ihre Privatsphäre schützt – Sie setzen Ihre informationelle Selbstbestimmung mithilfe unserer rechtssicheren Musterbriefe selbst durch.

Ob gegenüber Pflegekassen, Krankenkassen, Behörden oder Finanzämtern: Nutzen Sie bestehende Einsichts- und Auskunftsrechte, um Entscheidungen und Berechnungen nachvollziehen zu können. Im allgemeinen Verwaltungsverfahren kann sich ein Recht auf Akteneinsicht aus § 29 VwVfG ergeben; bei Kranken- und Pflegekassen richtet sich die Akteneinsicht nach § 25 SGB X. Für das Besteuerungsverfahren enthält die Abgabenordnung dagegen kein vergleichbares allgemeines Akteneinsichtsrecht. Während eines laufenden Verwaltungsverfahrens kann beim Finanzamt Akteneinsicht beantragt werden; über einen solchen Antrag ist nach der Rechtsprechung des Bundesfinanzhofs grundsätzlich nach pflichtgemäßem Ermessen zu entscheiden. Daneben besteht nach Art. 15 DSGVO ein Auskunftsanspruch über verarbeitete personenbezogene Daten, der jedoch nicht mit einem Recht auf Einsicht in die vollständige Steuerakte gleichzusetzen ist.

Geprüft: § 29 VwVfG, § 25 SGB X und die BFH-Rechtsprechung tragen diese Fassung.

Rechtssichere Vorlagen & Widersprüche direkt nutzen:



Sämtliche Musterbriefe – vom universellen Akteneinsichts-Baustein bis hin zu konkreten Widerspruchsvorlagen – finden Sie direkt unter:

<https://www.klartext-info.online/widerspruch-einlegen/>

3. Die juristische Notbremse: Ihre praktische Anleitung zum Selbstschutz

Digitale Identität, elektronische Patientenakte und vernetzte Verwaltungsstrukturen verändern nicht nur technische Abläufe, sondern auch die Frage, wie Bürger ihre eigenen Rechte wirksam wahrnehmen können. Wo immer mehr persönliche Daten digital verarbeitet, gespeichert und zwischen verschiedenen Stellen ausgetauscht werden, gewinnt die Kenntnis der eigenen Schutzmöglichkeiten an Bedeutung.

Der wichtigste Ansatzpunkt liegt dabei nicht in einer grundsätzlichen Ablehnung digitaler Entwicklungen, sondern in der bewussten Nutzung der bestehenden rechtlichen Instrumente. Datenschutzrechtliche Ansprüche, Auskunftsrechte und gesetzliche Widerspruchsmöglichkeiten geben Bürgern konkrete Werkzeuge an die Hand, um nachvollziehen und beeinflussen zu können, was mit ihren Daten geschieht.

Ein zentraler Baustein ist das Recht auf Auskunft nach Artikel 15 der Datenschutz-Grundverordnung (DSGVO). Bürger können von verantwortlichen Stellen erfahren, ob personenbezogene Daten verarbeitet werden, welche Daten betroffen sind und zu welchen Zwecken diese Verarbeitung erfolgt. Dieses Recht schafft Transparenz und ermöglicht es, die eigenen digitalen Spuren besser zu kontrollieren.

Ebenso wichtig ist die bewusste Wahrnehmung von Widerspruchs- und Gestaltungsmöglichkeiten. Gerade bei digitalen Gesundheitsanwendungen oder automatisierten Verfahren entscheidet nicht allein die technische Entwicklung über den Umgang mit persönlichen Informationen, sondern auch die Frage, ob und wie Bürger ihre gesetzlichen Rechte kennen und nutzen.

Die digitale Selbstbestimmung beginnt deshalb mit Wissen: Wer seine Rechte kennt, kann Entscheidungen nachvollziehen, Auskünfte einfordern und dort widersprechen, wo der Gesetzgeber entsprechende Möglichkeiten vorgesehen hat.

Praktische Schritte zur Wahrnehmung der eigenen Rechte

Der erste Schritt besteht darin, einen Überblick über die eigenen digitalen Berührungspunkte zu gewinnen. Dazu gehören insbesondere genutzte Online-Konten, gespeicherte persönliche Daten, digitale Identitäten und bestehende Einwilligungen.

Anschließend können gezielt Auskunftsrechte genutzt werden, um Klarheit über gespeicherte Informationen und Datenverarbeitungen zu erhalten. Je nach Situation können weitere rechtliche Möglichkeiten hinzukommen, beispielsweise Widersprüche gegen bestimmte Datenverarbeitungen oder die Prüfung bestehender Berechtigungen.



Die folgenden Instrumente helfen dabei, die eigenen Rechte strukturiert wahrzunehmen und die Kontrolle über persönliche Daten im digitalen Raum zu behalten.

4. Der strategische Ausblick: Warum Resilienz ein langfristiger Prozess bleibt

Der Aufbau des digitalen Staates ist kein temporäres Phänomen, sondern ein über Jahre durchgetakteter Transformationsprozess. Ein Blick auf die offiziellen Fahrpläne der Europäischen Union zeigt unmissverständlich, dass die eigentlichen Weichenstellungen weit in die Zukunft reichen. So regelt die [EU-Verordnung 2025/327 zum Europäischen Gesundheitsdatenraum \(EHDS\)](#) eine schrittweise Umsetzung, deren entscheidende Phasen erst ab **März 2029** und **März 2031** vollständig greifen. Ab **26. März 2035** können Drittstaaten und internationale Organisationen unter den in der Verordnung festgelegten Voraussetzungen die Teilnahme an HealthData@EU beantragen. ([Ministerio de Sanidad](#))

Parallel dazu treiben die Institutionen das Gesetzgebungspaket für den digitalen Euro und den Schutz des Bargelds voran. Die [Europäische Zentralbank \(EZB\) – Digitaler Euro](#) nennt derzeit das Jahr **2029** als Ziel für die Bereitschaft zu einer möglichen ersten Ausgabe des digitalen Zentralbankgeldes, vorausgesetzt, die notwendige EU-Gesetzgebung wird verabschiedet. ([European Central Bank](#))

Diese langfristige Dimension der offiziellen Agenda macht eines unmissverständlich klar: Krisenvorsorge und der Schutz der eigenen Bürgerrechte sind keine einmaligen Aufgaben. Wahre Resilienz ist ein kontinuierlicher Prozess. Wer auch in zehn Jahren noch selbstbestimmt über seine Identität, seine Gesundheit und sein Geld verfügen will, muss die Strukturen von heute verstehen. Diese Plattform wird Sie auf diesem Weg dauerhaft begleiten – mit harten Fakten, unabhängigen Analysen und den nötigen juristischen Werkzeugen.

5. Politische Verantwortung: Wer den vernetzten Staat auf den Weg brachte

Die Digitalisierung staatlicher Identitäten ist weder ein plötzlich entstandenes Projekt noch das Ergebnis einer einzelnen deutschen Bundesregierung. Die heutige European Digital Identity Wallet (EUDI-Wallet) ist das Ergebnis eines mehrjährigen politischen und gesetzgeberischen Prozesses auf europäischer und nationaler Ebene. Wer verstehen will, wie diese Infrastruktur entstanden ist, muss deshalb nachvollziehen, **wer sie vorgeschlagen, politisch vorangetrieben, beschlossen und schließlich in nationales Recht überführt hat.**

Ebenso entscheidend ist die Frage nach der Opposition: Welche Parteien widersprachen den Vorhaben? Welche unterstützten sie? Welche Änderungs- oder Gegenanträge wurden gestellt? Und wie wurde tatsächlich abgestimmt?

5.1 Der Ausgangspunkt auf EU-Ebene: Die Europäische Kommission legt 2021 den Grundstein



Ein entscheidender Ausgangspunkt der heutigen EUDI-Wallet liegt im **3. Juni 2021**. An diesem Tag legte die Europäische Kommission ihren Vorschlag für einen neuen europäischen Rahmen für digitale Identitäten vor.

Die Kommission unter Präsidentin **Ursula von der Leyen (CDU/EVP)** trug damit die politische Verantwortung für die Vorlage des Gesetzgebungsvorschlags. Öffentlich vorgestellt und vertreten wurde das Vorhaben insbesondere durch die damalige Exekutiv-Vizepräsidentin der Europäischen Kommission **Margrethe Vestager** sowie den damaligen EU-Binnenmarktkommissar **Thierry Breton**.

Die Kommission wollte einen europaweit einheitlichen Rahmen schaffen, über den Bürger, Einwohner und Unternehmen eine digitale Identität verwenden können. Bereits der Vorschlag von 2021 sah eine digitale Brieftasche auf mobilen Geräten vor, über die Identitätsdaten und elektronische Dokumente genutzt werden können.

Die Kommission stellte dabei die Kontrolle des Nutzers über seine Daten und die Freiwilligkeit der Nutzung ausdrücklich als zentrale Prinzipien heraus.

Damit war die politische Richtung allerdings vorgegeben: Die digitale Identität sollte nicht mehr ausschließlich innerhalb nationaler Systeme betrachtet werden. Sie sollte zu einer **europaweit interoperablen Infrastruktur** ausgebaut werden.

Quellen:

Europäische Kommission, 3. Juni 2021 – Vorschlag für eine vertrauenswürdige und sichere digitale Identität für alle Europäer:

<https://digital-strategy.ec.europa.eu/en/news/commission-proposes-trusted-and-secure-digital-identity-all-europeans>

Vertretung der Europäischen Kommission in Deutschland, 3. Juni 2021 – Europäer sollen sich mit digitaler Identität sicher ausweisen können:

https://germany.representation.ec.europa.eu/news/europaer-sollen-sich-mit-digitaler-identitaet-sicher-ausweisen-können-2021-06-03_de

5.2 Vom Vorschlag zum europäischen Gesetz: Rat und Parlament übernehmen

Mit dem Vorschlag der Europäischen Kommission war die EUDI-Wallet noch kein geltendes Recht. Nun begann das europäische Gesetzgebungsverfahren.

Am **6. Dezember 2022** beschloss der Rat der Europäischen Union seine gemeinsame Position – die sogenannte allgemeine Ausrichtung – zum neuen Rechtsrahmen. Damit konnten die Verhandlungen mit dem Europäischen Parlament vorbereitet werden.

Der Rat bezeichnete die geplante Wallet bereits damals ausdrücklich als einen grundlegenden Wandel der digitalen Identität in Europa.



Am **29. Juni 2023** erreichten Rat und Europäisches Parlament eine erste vorläufige politische Einigung über wesentliche Bestandteile. Die abschließende vorläufige Einigung wurde am **8. November 2023** erzielt.

Berichterstatterin des Europäischen Parlaments für das Gesetzgebungsverfahren war **Romana Jerković (S&D, Kroatien)**.

Damit lässt sich die politische Verantwortung nicht auf eine einzelne Institution reduzieren: Die **Europäische Kommission** initiierte den Rechtsakt. **Europäisches Parlament und Rat der Europäischen Union verhandelten und beschlossen** als europäische Gesetzgeber den endgültigen Rechtsrahmen.

Quellen:

Rat der Europäischen Union, 6. Dezember 2022 – Allgemeine Ausrichtung zur europäischen digitalen Identität:

<https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/>

Rat der Europäischen Union, 8. November 2023 – Vorläufige Einigung zwischen Rat und Europäischem Parlament:

<https://www.consilium.europa.eu/en/press/press-releases/2023/11/08/european-digital-identity-council-and-parliament-reach-a-provisional-agreement-on-eid/>

5.3 Die entscheidende Abstimmung im Europäischen Parlament

Am **29. Februar 2024** stimmte das Europäische Parlament über die mit dem Rat ausgehandelte Fassung ab.

Das Ergebnis war eindeutig, aber keineswegs einstimmig:

335 Abgeordnete stimmten dafür.
190 Abgeordnete stimmten dagegen.
31 Abgeordnete enthielten sich.

Damit gab es im Europäischen Parlament eine erhebliche parlamentarische Opposition gegen die ausgehandelte Fassung.

Die Abstimmungsunterlagen zeigen außerdem, dass verschiedene Fraktionen Änderungsanträge beziehungsweise Anträge zum Abstimmungsverfahren eingebracht hatten. Dazu gehörten unter anderem **Grüne/EFA, ECR, The Left und die damalige ID-Fraktion**.

Gerade deshalb reicht es für eine politische Bewertung nicht aus, lediglich festzustellen, dass „das Europäische Parlament“ zugestimmt hat. Entscheidend ist die darunterliegende Ebene: **Welche deutschen Parteien und welche deutschen Abgeordneten stimmten tatsächlich dafür, dagegen oder enthielten sich?**



Diese Einzelanalyse ist für die Bewertung der politischen Verantwortung und der Oppositionsarbeit von besonderer Bedeutung und wird im folgenden Abschnitt gesondert dargestellt.

Quellen:

Europäisches Parlament – offizielles Abstimmungsergebnis vom 29. Februar 2024:

https://www.europarl.europa.eu/doceo/document/PV-9-2024-02-29-VOT_EN.html

Europäisches Parlament – angenommener Text und Gesetzgebungsverfahren 2021/0136(COD):

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_EN.html

5.4 Der endgültige europäische Rechtsrahmen

Am **26. März 2024** nahm auch der Rat der Europäischen Union den neuen Rechtsrahmen endgültig an.

Damit war der europäische Gesetzgebungsprozess im Wesentlichen abgeschlossen. Die Verordnung wurde anschließend als **Verordnung (EU) 2024/1183** veröffentlicht und änderte die bestehende eIDAS-Verordnung.

Die Mitgliedstaaten wurden damit verpflichtet, die europäische Infrastruktur für digitale Identitäten praktisch umzusetzen und entsprechende Wallet-Lösungen bereitzustellen.

Die politische Entstehungskette lässt sich damit klar nachvollziehen:

3. Juni 2021: Vorschlag der Europäischen Kommission.

6. Dezember 2022: Allgemeine Ausrichtung des Rates.

29. Juni und 8. November 2023: politische Einigungen zwischen Rat und Europäischem Parlament.

29. Februar 2024: Zustimmung des Europäischen Parlaments mit 335 zu 190 Stimmen bei 31 Enthaltungen.

26. März 2024: endgültige Annahme durch den Rat.

11. April 2024: Erlass der Verordnung (EU) 2024/1183.

Quellen:

Rat der Europäischen Union, 26. März 2024 – endgültige Annahme:

<https://www.consilium.europa.eu/de/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/>

EUR-Lex – Verordnung (EU) 2024/1183:



<https://eur-lex.europa.eu/eli/reg/2024/1183/oj>

5.5 Deutschland 2026: Karsten Wildberger und die nationale Umsetzung

Der europäische Rechtsrahmen verpflichtet Deutschland zur Umsetzung der EUDI-Wallet. Die konkrete nationale Ausgestaltung ist jedoch wiederum eine politische Entscheidung auf Bundesebene.

Federführend ist dabei das **Bundesministerium für Digitales und Staatsmodernisierung (BMDS)** unter Bundesdigitalminister **Dr. Karsten Wildberger (CDU)**.

Am **20. Mai 2026** beschloss das Bundeskabinett den Entwurf des **Digitale-Identitäten-Gesetzes (DIdG)**.

Wildberger begründete das Gesetz öffentlich damit, dass Bürger ihre Identität künftig europaweit digital nachweisen und entsprechende Nachweise über die EUDI-Wallet nutzen können sollen.

Damit trägt die seit 2025 amtierende Bundesregierung unter Bundeskanzler **Friedrich Merz (CDU)** die politische Verantwortung für diese Phase der nationalen gesetzlichen Umsetzung. Das bedeutet allerdings nicht, dass diese Bundesregierung die EUDI-Wallet ursprünglich erfunden oder auf europäischer Ebene initiiert hätte. Die entscheidenden europäischen Weichenstellungen reichen – wie gezeigt – bis mindestens 2021 zurück.

Diese Unterscheidung ist wesentlich: **Initiierung, europäische Gesetzgebung und nationale Umsetzung erfolgten zu unterschiedlichen Zeitpunkten und unter unterschiedlichen politischen Verantwortlichkeiten.**

Quelle:

Bundesministerium für Digitales und Staatsmodernisierung, 20. Mai 2026 – Kabinett beschließt Gesetz für digitale Identitäten:

<https://bmds.bund.de/aktuelles/pressemitteilungen/detail/kabinett-beschliesst-gesetz-fuer-digitale-identitaeten>

5.6 Wer trug die Entscheidung – und wer stellte sich dagegen?

Die Abstimmung über den europäischen Rechtsrahmen für die digitale Identität zeigt, dass sich die politischen Fronten nicht einfach entlang der klassischen Grenze zwischen Regierung und Opposition ziehen lassen.

Am **29. Februar 2024** nahm das Europäische Parlament die ausgehandelte Fassung mit **335 Ja-Stimmen gegen 190 Nein-Stimmen bei 31 Enthaltungen** an.

Bei den deutschen Abgeordneten zeigte sich jedoch ein anderes und politisch bemerkenswertes Bild: Die abstimmenden Abgeordneten von **CDU/CSU und SPD unterstützten die Verordnung**. Die abstimmenden deutschen Abgeordneten von **Bündnis**



90/Die Grünen, AfD und Die Linke lehnten sie ab. Die beteiligten FDP-Abgeordneten enthielten sich.

Damit verlief die Trennlinie quer durch die damaligen Regierungs- und Oppositionslager in Deutschland. Die SPD als Regierungspartei und CDU/CSU als damalige Opposition unterstützten die Regelung. Gleichzeitig lehnten mit Grünen, AfD und Linken politisch sehr unterschiedliche Parteien die Schlussfassung ab.

Allerdings bedeutete ein Nein nicht bei allen Parteien dasselbe.

Die europäischen **Grünen/EFA** versuchten, Änderungen an der bereits mit dem Rat ausgehandelten Fassung zu ermöglichen. Gemeinsam mit der **ECR-Fraktion** beantragten sie, Änderungsanträge anstelle der ausgehandelten Einigung zur Abstimmung zu stellen. Dieser Versuch scheiterte im Europäischen Parlament.

Auch die europäische Linksfraktion **The Left** brachte Änderungsanträge ein. Die deutsche Partei Die Linke begründete ihre Kritik an der europäischen digitalen Identität unter anderem mit Datenschutz-, Sicherheits- und Teilhabefragen. Sie warnte insbesondere vor einem faktischen Zwang zur Nutzung entsprechender digitaler Anwendungen und forderte zusätzliche Schutzmechanismen.

Die damalige europäische **ID-Fraktion**, der zu diesem Zeitpunkt auch die AfD angehörte, ging noch einen Schritt weiter: Sie beantragte im Europäischen Parlament die **Ablehnung des zugrunde liegenden Kommissionsvorschlags**. Dieser Antrag fand keine Mehrheit. Auch bei der anschließenden Schlussabstimmung stimmten die teilnehmenden deutschen AfD-Abgeordneten gegen die Verordnung.

Die **FDP** wiederum enthielt sich mit ihren abstimmenden deutschen Abgeordneten bei der Schlussabstimmung, obwohl sie das politische Grundprojekt einer europäischen digitalen Identität grundsätzlich unterstützt. Auch dies zeigt, warum das tatsächliche Abstimmungsverhalten und die programmatische Position einer Partei getrennt betrachtet werden müssen.

Für die Bewertung der politischen Verantwortung und der Oppositionsarbeit ergibt sich damit ein differenziertes Bild: **CDU/CSU und SPD trugen die Schlussfassung mit ihren abgegebenen Stimmen mit. Grüne, AfD und Linke lehnten sie ab, allerdings aus unterschiedlichen politischen Gründen und mit unterschiedlichen parlamentarischen Initiativen. Die FDP enthielt sich.**

Wer nachvollziehen möchte, wie die einzelnen Abgeordneten abgestimmt haben und welche Änderungs- beziehungsweise Ablehnungsanträge gestellt wurden, kann die vollständigen Originalunterlagen des Europäischen Parlaments unmittelbar einsehen.

Vollständige Abstimmungsunterlagen des Europäischen Parlaments vom 29. Februar 2024:

https://www.europarl.europa.eu/doceo/document/PV-9-2024-02-29-VOT_EN.html

Angenommener Text des Europäischen Parlaments – Verfahren 2021/0136(COD):

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0117_EN.html



Die Linke – Europawahlprogramm 2024:

<https://www.die-linke.de/europawahl/wahlprogramm-zur-europawahl/>

FDP – Europawahlprogramm 2024:

<https://www.fdp.de/das-wahlprogramm-der-freien-demokraten-zur-europawahl-2024>

5.7 Die deutsche Opposition wird aktiv: Der Streit um die nationale Umsetzung

Mit der deutschen Umsetzung der EUDI-Wallet verlagerte sich die politische Auseinandersetzung 2026 zunehmend nach Berlin.

Die Bundesregierung aus **CDU/CSU und SPD** brachte das Digitale-Identitäten-Gesetz (DIdG) auf den Weg. Federführend ist das Bundesministerium für Digitales und Staatsmodernisierung unter Bundesminister **Dr. Karsten Wildberger (CDU)**.

Doch auch die Opposition blieb nicht untätig.

Am **23. Juni 2026** brachte die **AfD-Bundestagsfraktion** einen eigenen Antrag mit dem Titel „**Keine digitale Identität und Geldbörse durch die EU – Mit nationaler Lösung echte Staatsmodernisierung vorantreiben**“ in den Deutschen Bundestag ein.

Darin fordert die AfD die Bundesregierung auf, sich auf europäischer Ebene für die Aufhebung der Vorschriften zur EUDI-Wallet einzusetzen und die Umsetzung des nationalen EUDI-Wallet-Projekts einzustellen. Stattdessen soll eine nationale digitale Lösung entwickelt werden, die freiwillig für Behördengänge genutzt werden kann.

Ein weiterer zentraler Punkt des Antrags betrifft die analoge Alternative: **Analoge Dokumente und Zugangswege sollen nach dem Willen der AfD vollständig erhalten und gleichberechtigt anerkannt bleiben.**

Am **25. Juni 2026** wurde der Antrag im Deutschen Bundestag erstmals beraten. Für die AfD sprach **Tobias Ebenberger**. An der Debatte beteiligten sich außerdem **Dr. Markus Reichel (CDU/CSU)**, **Rebecca Lenhard (Bündnis 90/Die Grünen)** und **Sonja Lemke (Die Linke)**; für die SPD wurde eine Rede von **Parsa Marvi** zu Protokoll gegeben.

Der Antrag wurde bei dieser ersten Beratung **nicht abschließend abgelehnt**, sondern zur weiteren Beratung an mehrere Ausschüsse überwiesen. Federführend ist der **Ausschuss für Digitales und Staatsmodernisierung**; beteiligt sind außerdem der Innenausschuss, der Ausschuss für Recht und Verbraucherschutz, der Finanzausschuss, der Ausschuss für Arbeit und Soziales sowie der Ausschuss für die Angelegenheiten der Europäischen Union.

Damit liegt ein konkreter parlamentarischer Gegenentwurf zur Linie der Bundesregierung vor. Für die Bewertung der Oppositionsarbeit ist dabei entscheidend, zwischen politischer Kritik und tatsächlichem parlamentarischem Handeln zu unterscheiden: **Die AfD hat sich in diesem Fall nicht auf öffentliche Ablehnung beschränkt, sondern einen eigenen Antrag in das parlamentarische Verfahren eingebracht.**



Ob und in welcher Form dieser Antrag in den Ausschüssen weiterbehandelt und schließlich zur Abstimmung gestellt wird, ist für die weitere Bewertung ebenso entscheidend wie die Frage, wie sich die übrigen Fraktionen dazu positionieren.

Originalquellen:

Deutscher Bundestag – Antrag gegen digitale EU-Identität debattiert; einschließlich parlamentarischem Verlauf und weiterführender Dokumente:

[Deutscher Bundestag – Debatte und Dokumente](#)

AfD-Antrag „Keine digitale Identität und Geldbörse durch die EU – Mit nationaler Lösung echte Staatsmodernisierung vorantreiben“, Bundestagsdrucksache 21/6650:
Der Antrag ist über die Dokumente der oben verlinkten Bundestagsseite abrufbar.

5.8 Grüne und Linke: Kontrolle der Regierung – aber unterschiedliche parlamentarische Aktivität

Auch die übrigen Oppositionsparteien beschäftigen sich mit der deutschen EUDI-Wallet – allerdings auf unterschiedliche Weise.

Bündnis 90/Die Grünen haben die Bundesregierung mit einer umfangreichen **Kleinen Anfrage vom 6. Juli 2026** unter Druck gesetzt. Federführend genannt werden die Abgeordneten **Rebecca Lenhard** und **Dr. Konstantin von Notz** sowie weitere Mitglieder der Grünen-Fraktion.

Die Fragen gehen deutlich über den bloßen Zeitplan hinaus. Die Grünen verlangen Auskunft über den geplanten Start der deutschen Wallet am **2. Januar 2027**, mögliche Verzögerungen, Projektsteuerung und Kosten sowie über die konkrete technische und datenschutzrechtliche Ausgestaltung.

Gefragt wird unter anderem nach **Pseudonymisierung, Zero-Knowledge-Proofs, biometrischen Daten, Sicherheitsprüfungen durch das BSI** und der Frage, welche **Funktionen zum Start tatsächlich verfügbar sein werden**.

Die Bundesregierung antwortete am **21. Juli 2026**. Sie hält weiterhin am 2. Januar 2027 als Zieltermin fest.

Damit verfolgen die Grünen derzeit einen anderen Oppositionsansatz als die AfD: Während die AfD mit ihrem Antrag die Umsetzung der europäischen EUDI-Wallet grundsätzlich stoppen und durch eine begrenzte nationale Lösung ersetzen will, konzentrieren sich die Grünen auf **parlamentarische Kontrolle der laufenden Umsetzung sowie auf technische, datenschutzrechtliche und sicherheitsrelevante Fragen**.

Bei **Die Linke** ist die Lage mit dem derzeit belegbaren Quellenstand anders. Die Fraktion beteiligte sich am **25. Juni 2026** durch die Abgeordnete **Sonja Lemke** an der Bundestagsdebatte über den AfD-Antrag zur EUDI-Wallet.



Einen eigenen Antrag oder eine vergleichbar umfassende parlamentarische Initiative der Linksfraktion speziell zur deutschen EUDI-Wallet in der laufenden 21. Wahlperiode konnte für diese Untersuchung bislang jedoch **nicht belastbar festgestellt werden**.

Damit zeigt sich auch innerhalb der Opposition ein unterschiedliches Vorgehen: **Die AfD hat einen eigenen Gegenantrag eingebracht. Die Grünen kontrollieren die konkrete Umsetzung mit einer umfangreichen parlamentarischen Anfrage. Bei der Linken ist bislang eine Beteiligung an der politischen Debatte belegt, aber keine vergleichbare eigene parlamentarische Initiative zur deutschen EUDI-Wallet gefunden worden.**

Das ist keine abschließende Bewertung der jeweiligen Oppositionsarbeit. Es zeigt aber, mit welchen parlamentarischen Mitteln die einzelnen Fraktionen bei diesem konkreten Projekt bisher tatsächlich in Erscheinung getreten sind.

Wer die Fragen der Grünen und die Antworten der Bundesregierung vollständig nachlesen möchte, findet hier die Originaldokumente:

Deutscher Bundestag – Kleine Anfrage der Grünen, Drucksache 21/6866:
<https://dserver.bundestag.de/btd/21/068/2106866.pdf>

Deutscher Bundestag – Antwort der Bundesregierung, Drucksache 21/7319:
<https://dserver.bundestag.de/btd/21/073/2107319.pdf>

Deutscher Bundestag – Debatte vom 25. Juni 2026 mit den Redebeiträgen von AfD, CDU/CSU, Grünen und Linken:
<https://www.bundestag.de/dokumente/textarchiv/2026/kw26-de-digitale-identitaet-1191872>

6. Die physische Säule: Technische Autarkie durch moderne Inselanlagen

Wahre Resilienz bleibt unvollständig, wenn sie sich ausschließlich auf den digitalen Raum beschränkt. Wenn das öffentliche Stromnetz wegbricht – sei es durch Überlastungen im Extremsommer, Unwetter oder technische Defekte –, steht die moderne Welt in Sekundenschnelle still. Wer in diesem Moment keine eigene Vorsorge getroffen hat, verliert einen erheblichen Teil seiner Handlungsfähigkeit. Das Handy kann nicht mehr geladen werden, Kühlgeräte fallen aus und wichtige Kommunikationsmittel stehen ohne alternative Stromversorgung nur noch begrenzt zur Verfügung.

Die Lösung für diese Abhängigkeit kann in einer zusätzlichen physischen Absicherung durch eine **private Solar-Inselanlage beziehungsweise eine leistungsfähige Powerstation mit Solarmodulen** liegen. Solche Systeme sind in erster Linie als **Notstrom- und Vorsorgelösung** zu verstehen. Sie verursachen Anschaffungskosten und ersetzen nicht automatisch die reguläre Stromversorgung eines gesamten Hauses. Wie viele Geräte versorgt werden können und wie lange der Betrieb möglich ist, hängt insbesondere von **Speicherkapazität, Ausgangsleistung, angeschlossenen Verbrauchern, Solarleistung und tatsächlichem Solarertrag** ab.



Moderne Systeme wie beispielsweise die [EcoFlow DELTA Pro Serie](#) zeigen, welche Größenordnungen inzwischen möglich sind. Bereits die DELTA Pro verfügt beispielsweise über **3,6 kWh Speicherkapazität und 3.600 Watt AC-Ausgangsleistung**; das System lässt sich zudem erweitern. ([EcoFlow](#))

Gekoppelt mit geeigneten Solarmodulen auf Terrasse, Balkon oder einer anderen geeigneten Fläche kann ein solches System während eines Stromausfalls zumindest **ausgewählte wichtige Verbraucher** weiter versorgen – beispielsweise Kommunikationsgeräte, Laptops oder, abhängig von Leistung und Kapazität der Anlage, Kühl- und Ventilationsgeräte. Bei ausreichendem Solarertrag lässt sich der Speicher zudem unabhängig vom öffentlichen Stromnetz nachladen. Wie lange eine solche Versorgung tatsächlich aufrechterhalten werden kann, hängt jedoch immer von der konkreten Dimensionierung der Anlage und dem jeweiligen Verbrauch ab. ([EcoFlow Germany](#))

Auch im normalen Alltag kann die Anlage genutzt werden, um ausgewählte Verbraucher zeitweise mit selbst erzeugtem Solarstrom zu betreiben. **Ihr eigentlicher Wert im Rahmen der Krisenvorsorge liegt jedoch in der Absicherung:** Fällt das öffentliche Netz aus, steht eine eigene, begrenzte Stromversorgung zur Verfügung, mit der zentrale Funktionen im Haushalt weiterbetrieben werden können. Technische Autarkie bedeutet dabei nicht zwangsläufig, ein ganzes Haus dauerhaft unabhängig versorgen zu können – sondern im Ernstfall **nicht vollständig ohne Strom und damit ohne wesentliche Handlungsmöglichkeiten dazustehen.**

7. Die materielle Basis: Wasserbehandlung und das rollierende Vorratssystem

Neben einer autarken Stromversorgung ruht die physische Resilienz auf einem zweiten, unumstößlichen Fundament: dem Schutz vor einem Ausfall der kritischen Infrastruktur im Lebensmittel- und Trinkwasserbereich. Die offiziellen Empfehlungen des [Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe \(BBK\)](#) sehen vor, dass sich Haushalte **möglichst zehn Tage selbst versorgen können**. Beim Trinkwasser empfiehlt das BBK **zwei Liter pro Person und Tag**.

Um diesen Schutz im Alltag ohne großen Aufwand und ohne abgelaufene Lebensmittel umzusetzen, hat sich das sogenannte „**rollierende System**“ bewährt. Dabei werden ausschließlich haltbare Vorräte gelagert, die Sie ohnehin regelmäßig im Alltag konsumieren. Was verbraucht wird, wird beim nächsten Einkauf einfach von hinten nachgekauft. So bleibt Ihr Notlager immer frisch und unbemerkt auf dem maximalen Stand.

Für den Fall, dass die öffentliche Wasserversorgung längerfristig kontaminiert wird oder komplett ausfällt, können **mobile Outdoor-Wasserfilter** eine zusätzliche Vorsorgemöglichkeit darstellen.

Der BBK-Link und die Angaben **10 Tage / 2 Liter** sind dagegen geprüft. Das BBK formuliert inzwischen ausdrücklich „**möglichst zehn Tage**“, nicht als zwingendes „mindestens zehn Tage“.



Die genannten Mengen sind als Orientierung für die grundlegende Notfallvorsorge zu verstehen. Wer über ausreichend Platz und finanzielle Möglichkeiten verfügt, sollte seine persönlichen Reserven großzügiger bemessen. Beim Wasser kann beispielsweise eine Reserve von bis zu sechs Litern pro Person und Tag eingeplant werden; der zusätzliche Bedarf von Haustieren ist gesondert zu berücksichtigen.

8. Die finanzielle Resilienz: Bargeldschutz im vernetzten Zahlungsraum

Ein oft übersehener, aber elementarer Baustein der Alltagsresilienz ist die finanzielle Unabhängigkeit. Unsere Gesellschaft verlässt sich zunehmend auf digitale Zahlungssysteme. Ein großflächiger Stromausfall, ein gezielter Cyberangriff auf das Bankensystem oder technische Störungen bei Kartenterminals können den elektronischen Zahlungsverkehr erheblich beeinträchtigen. Wer dann kein Bargeld besitzt, kann im Alltag schnell vor praktischen Problemen stehen.

Zudem verändern politische Weichenstellungen wie das neue EU-Anti-Geldwäschepaket den finanziellen Handlungsspielraum. Nach **Artikel 80 der Verordnung (EU) 2024/1624** dürfen Personen, die mit Gütern handeln oder Dienstleistungen erbringen, Barzahlungen grundsätzlich nur bis zu **10.000 Euro** annehmen oder vornehmen. Mitgliedstaaten dürfen niedrigere nationale Obergrenzen festlegen. **Private Zahlungen zwischen natürlichen Personen, die nicht in ihrer beruflichen Eigenschaft handeln, sind von dieser EU-weiten 10.000-Euro-Grenze ausdrücklich ausgenommen.** Wer beispielsweise ein Fahrzeug bei einem gewerblichen Händler kauft, fällt grundsätzlich unter die Begrenzung; ein rein privates Geschäft zwischen zwei Privatpersonen wird von dieser konkreten EU-Regel dagegen nicht erfasst. ([EUR-Lex](#))

[EU-Verordnung 2024/1624 – EUR-Lex](#)

Gleichzeitig arbeiten die europäischen Institutionen am **digitalen Euro**. Der Rat der Europäischen Union hat am **19. Dezember 2025** seine Verhandlungsposition beschlossen. Danach soll der digitale Euro das Bargeld **ergänzen und nicht ersetzen**. Parallel soll der Status des Euro-Bargelds als gesetzliches Zahlungsmittel gestärkt werden. Ziel ist ausdrücklich, die Annahme und Verfügbarkeit von Bargeld sowie die freie Wahl der Zahlungsmethode zu sichern. Die endgültige Entscheidung über eine tatsächliche Ausgabe des digitalen Euro liegt nach Verabschiedung des Rechtsrahmens bei der Europäischen Zentralbank. ([Rat der Europäischen Union](#))

[Rat der EU – Digitaler Euro und Stärkung des Bargelds](#)

Zur gelebten Resilienz gehört daher ein **angemessener Bargeldvorrat zu Hause, möglichst auch in kleineren Scheinen**. Er kann die eigene Handlungsfähigkeit sichern, wenn elektronische Zahlungsmittel vorübergehend nicht funktionieren. Bemessen werden sollte diese Reserve nach den persönlichen Verhältnissen und dem tatsächlichen Bedarf des



Haushalts. Bargeld liegt zudem außerhalb der bei digitalen Zahlungen entstehenden elektronischen Transaktionsketten und ermöglicht weiterhin eine unmittelbare Form des Bezahlens.

Solange Bargeld im Alltag praktisch verfügbar und akzeptiert bleibt, besteht damit eine eigenständige Alternative zu digitalen Zahlungsmitteln. Gerade für die Krisenvorsorge ist diese Wahlmöglichkeit von Bedeutung: **Strom, Internet oder Kartenterminal können ausfallen – Bargeld benötigt für den unmittelbaren Zahlungsvorgang keine funktionierende digitale Infrastruktur.**

8.1 Bargeld als analoge Rückfallebene

Bargeld ist im Alltag weit mehr als nur ein traditionelles Zahlungsmittel. Für die persönliche Resilienz erfüllt es eine besondere Funktion: Es ermöglicht Zahlungen unabhängig davon, ob Online-Banking, Kartenterminals, Mobilfunkverbindungen oder andere digitale Zahlungssysteme gerade verfügbar sind.

Ein großflächiger Stromausfall, ein gezielter Cyberangriff auf das Bankensystem oder technische Störungen bei Kartenterminals können den elektronischen Zahlungsverkehr erheblich beeinträchtigen. Wer dann kein Bargeld besitzt, kann im Alltag schnell vor praktischen Problemen stehen.

Zur persönlichen Vorsorge gehört deshalb ein **angemessener Bargeldvorrat zu Hause**, möglichst auch in kleineren Scheinen. Die Höhe sollte sich nach den persönlichen Verhältnissen und dem tatsächlichen Bedarf des Haushalts richten.

Bargeld besitzt dabei noch eine zweite Besonderheit: Eine unmittelbare Barzahlung erzeugt keine elektronische Transaktionskette wie eine Karten-, App- oder Online-Zahlung. Solange Bargeld praktisch verfügbar und akzeptiert bleibt, bildet es deshalb eine **eigenständige analoge Rückfallebene im zunehmend digitalisierten Zahlungsverkehr.**

Gerade für die Krisenvorsorge ist diese Wahlmöglichkeit entscheidend: **Strom, Internet, Bankserver oder Kartenterminals können ausfallen – Bargeld benötigt für den unmittelbaren Zahlungsvorgang keine funktionierende digitale Infrastruktur.**

8.2 Die 10.000-Euro-Bargeldgrenze: Wer sie auf den Weg brachte und wer sie politisch mittrug

Die ab 2027 geltende EU-weite Obergrenze für Barzahlungen von **10.000 Euro** ist keine Entscheidung der Europäischen Zentralbank und auch kein Projekt von EZB-Präsidentin Christine Lagarde. Sie ist Bestandteil des europäischen Gesetzespakets zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung.

Den Ausgangspunkt setzte die **Europäische Kommission**. Sie legte am **20. Juli 2021** ihr umfangreiches Geldwäschepaket vor. Bestandteil des Kommissionsvorschlags war bereits eine EU-weite Obergrenze von **10.000 Euro für Barzahlungen**. Damit sollte nach



Darstellung der Kommission verhindert werden, dass große Bargeldsummen zur Geldwäsche genutzt werden.

Im anschließenden europäischen Gesetzgebungsverfahren verschärfte sich die Auseinandersetzung. Im Europäischen Parlament gab es politische Kräfte, die eine deutlich niedrigere Grenze wollten. Die CDU-Europaabgeordneten **Ralf Seekatz und Karolin Braunsberger-Reinhold**, beide Berichterstatter der EVP-Fraktion für die Geldwäscheverordnung, erklärten nach Abschluss der Verhandlungen, **Sozialdemokraten, Grüne und Liberale hätten zunächst eine Bargeldobergrenze von 3.000 Euro angestrebt**. Die EVP habe dagegen zunächst 7.000 Euro durchgesetzt; in den abschließenden Verhandlungen mit dem Rat sei schließlich die Grenze von **10.000 Euro** vereinbart worden. ([CDU/CSU-Gruppe in der EVP-Fraktion](#))

Am **18. Januar 2024** erzielten Vertreter des Europäischen Parlaments und des Rates die politische Einigung über die Geldwäscheverordnung. Darin wurde die EU-weite Obergrenze von 10.000 Euro festgeschrieben. ([Rat der Europäischen Union](#))

Das Europäische Parlament verabschiedete die Geldwäscheverordnung am **24. April 2024**. Der Rat – und damit die Vertretung der Regierungen der EU-Mitgliedstaaten – nahm das Gesetzespaket am **30. Mai 2024** endgültig an. Damit war die Bargeldobergrenze europäisches Recht. ([EUR-Lex](#))

Für Deutschland ist deshalb wichtig: Die Begrenzung wurde **nicht allein „von Brüssel“ ohne Beteiligung deutscher Politik beschlossen**. Deutsche Abgeordnete waren am Gesetzgebungsverfahren im Europäischen Parlament beteiligt; die damalige Bundesregierung aus **SPD, Bündnis 90/Die Grünen und FDP** war über Deutschland zugleich auf der Ebene des Rates in das europäische Gesetzgebungsverfahren eingebunden.

Politisch verlief die Auseinandersetzung allerdings komplizierter als eine einfache Trennung zwischen Regierung und Opposition. Während Sozialdemokraten, Grüne und Liberale im Europäischen Parlament nach Darstellung der CDU/CSU-Europagruppe zeitweise sogar eine niedrigere Grenze von 3.000 Euro anstrebten, akzeptierte auch die **CDU/CSU-geprägte EVP-Seite** schließlich die 10.000-Euro-Regelung. Ralf Seekatz erklärte nach der Einigung ausdrücklich, mit der schließlich vereinbarten Grenze könne man leben. ([CDU/CSU-Gruppe in der EVP-Fraktion](#))

Damit gehörten maßgebliche Kräfte aus **SPD, Grünen, FDP und CDU/CSU** nicht zu den grundsätzlichen Gegnern einer europäischen Bargeldobergrenze – auch wenn sie über deren konkrete Höhe stritten.

Eine andere Position vertrat die **AfD**. Sie lehnte eine gesetzliche Bargeldobergrenze grundsätzlich ab. Die damalige AfD-Europaabgeordnete **Christine Anderson** richtete am **7. Februar 2024** eine parlamentarische Anfrage an die Europäische Kommission. Darin stellte sie ausdrücklich die Wirksamkeit der 10.000-Euro-Grenze gegen Geldwäsche infrage und fragte nach möglichen Auswirkungen auf Privatsphäre und Freiheitsrechte sowie nach weniger restriktiven Alternativen. ([Europäisches Parlament](#))

Auch die AfD-Bundestagsfraktion positionierte sich öffentlich gegen die Regelung. Ihr damaliger finanzpolitischer Sprecher **Kay Gottschalk** bezeichnete die Einigung im Januar



2024 als Angriff auf die individuelle Freiheit und kündigte weiteren Widerstand gegen Einschränkungen des Bargelds an. ([Kay Gottschalk](#))

Die Kritik kam allerdings nicht ausschließlich von der AfD. Auch der deutsche Piraten-Europaabgeordnete **Patrick Breyer** stimmte in den zuständigen Ausschüssen gegen die neuen Anti-Geldwäschebestimmungen und kritisierte insbesondere die Einschränkungen anonymer Barzahlungen. ([patrick-breyer.de](#))

Was gilt tatsächlich?

Artikel 80 der schließlich beschlossenen **Verordnung (EU) 2024/1624** erlaubt Barzahlungen für Waren und Dienstleistungen grundsätzlich nur noch bis **10.000 Euro**. Die Mitgliedstaaten dürfen sogar niedrigere nationale Grenzen festlegen.

Wichtig ist jedoch eine Einschränkung, die in der politischen Diskussion häufig untergeht: **Reine Zahlungen zwischen Privatpersonen, die dabei nicht beruflich handeln, fallen nicht unter diese EU-weite 10.000-Euro-Grenze.** ([EUR-Lex](#))

Damit handelt es sich nicht um ein allgemeines Verbot, privat mehr als 10.000 Euro Bargeld zu besitzen oder unter allen Umständen zu verwenden. Es handelt sich um eine gesetzliche Begrenzung großer Barzahlungen im geschäftlichen Verkehr.

KLARTEXT-Hinweis: Zu diesem Themenkomplex wird in Kürze ein eigenes Dossier erscheinen.

Quellen

[EUR-Lex – Verordnung \(EU\) 2024/1624, insbesondere Artikel 80](#)

[Rat der Europäischen Union – Einigung über die neuen Geldwäschevorschriften vom 18. Januar 2024](#)

[Europäisches Parlament/EUR-Lex – Gesetzgebungsverfahren und Beschluss vom 24. April 2024](#)

[CDU/CSU-Gruppe im Europäischen Parlament – Stellungnahme von Seekatz und Braunsberger-Reinhold vom 18. Januar 2024](#)

[Europäisches Parlament – parlamentarische Anfrage von Christine Anderson vom 7. Februar 2024](#)

8.3 Was unternahm die Opposition gegen die Bargeldbegrenzung?

Die politische Auseinandersetzung um die EU-weite Bargeldobergrenze zeigt, dass Kritik nicht nur außerhalb der Parlamente geäußert wurde. Teile der Opposition versuchten, das Thema auch parlamentarisch aufzugreifen.



Besonders deutlich positionierte sich die **AfD** gegen gesetzliche Bargeldobergrenzen. Die damalige AfD-Europaabgeordnete **Christine Anderson** stellte am **7. Februar 2024** eine schriftliche Anfrage an die Europäische Kommission. Darin verlangte sie unter anderem Auskunft darüber, auf welcher empirischen Grundlage die 10.000-Euro-Grenze Geldwäsche wirksam bekämpfen solle und welche Auswirkungen die Maßnahme auf **Privatsphäre und persönliche Freiheit** habe.

Damit wurde die Bargeldbegrenzung nicht lediglich öffentlich kritisiert, sondern zum Gegenstand eines formellen parlamentarischen Kontrollinstruments gemacht.

Auch im **Deutschen Bundestag** wurde die Entwicklung zum Thema. Die AfD-Fraktion brachte am **3. Juli 2024** den Antrag „**Bargeld als einziges gesetzliches Zahlungsmittel bewahren**“ zur Beratung. Darin wandte sie sich gegen eine Zurückdrängung des Bargelds und verband dies mit ihrer grundsätzlichen Ablehnung des digitalen Euro.

Der Antrag fand jedoch keine Mehrheit. **CDU/CSU, SPD, Bündnis 90/Die Grünen und FDP stimmten gegen den Antrag; die Gruppe Die Linke enthielt sich.** Damit zeigte sich auch auf nationaler Ebene eine klare parlamentarische Trennlinie: Die AfD verlangte einen wesentlich weitergehenden gesetzlichen Schutz des Bargelds, konnte dafür im Bundestag jedoch keine Mehrheit gewinnen.

Für die Bewertung der Oppositionsarbeit ist diese Unterscheidung wichtig: Man kann über Inhalt und Reichweite solcher Forderungen streiten. Die Behauptung, es habe zu diesem Themenkomplex überhaupt keine parlamentarischen Gegeninitiativen gegeben, wäre jedoch falsch. **Es gab konkrete Anfragen und Anträge – sie fanden nur keine ausreichende politische Mehrheit.**

Wer die einzelnen Redebeiträge, Anträge und Abstimmungsergebnisse nachvollziehen möchte, kann die vollständigen parlamentarischen Unterlagen über die nachfolgenden Originalquellen einsehen.

Quellen:

[Europäisches Parlament – Anfrage von Christine Anderson vom 7. Februar 2024](#)

[Deutscher Bundestag – Debatte über Bargeld und digitalen Euro vom 3. Juli 2024](#)

8.4 Der digitale Euro: Wer ihn auf den Weg brachte und welche Rolle Christine Lagarde spielt

Beim digitalen Euro muss zwischen **technischer Vorbereitung, politischem Rechtsrahmen und der späteren Entscheidung über eine tatsächliche Ausgabe** unterschieden werden. Die häufig verkürzte Darstellung, EZB-Präsidentin **Christine Lagarde** habe den digitalen Euro allein auf den Weg gebracht, trifft so nicht zu.

Den institutionellen Ausgangspunkt setzte das **Eurosystem unter Führung der Europäischen Zentralbank**. Im **Oktober 2020** veröffentlichte die EZB ihren ersten umfassenden Bericht über einen möglichen digitalen Euro. Im **Juli 2021** beschloss der EZB-



Rat anschließend, das Projekt offiziell zu starten. Von Oktober 2021 bis Oktober 2023 lief die sogenannte Untersuchungsphase, in der Gestaltung, technische Umsetzung und mögliche Verteilungsmodelle untersucht wurden.

Christine Lagarde, seit November 2019 Präsidentin der Europäischen Zentralbank, gehört damit zu den zentralen öffentlichen und institutionellen Akteuren dieses Projekts. Unter ihrer Präsidentschaft wurden sowohl die Untersuchungsphase als auch die anschließende technische Vorbereitung beschlossen und vorangetrieben.

Am **18. Oktober 2023** entschied der EZB-Rat, nach Abschluss der zweijährigen Untersuchungsphase in die nächste Stufe einzutreten. Die Vorbereitungsphase begann am **1. November 2023**. Dazu gehörten unter anderem die Entwicklung eines Regelwerks, die Auswahl möglicher Anbieter für Plattform und Infrastruktur sowie weitere technische Tests.

Parallel dazu wurde aus dem Zentralbankprojekt ein konkretes **EU-Gesetzgebungsverfahren**. Am **28. Juni 2023** legte die Europäische Kommission ihren Vorschlag für eine Verordnung zur Einführung des digitalen Euro vor. Damit kam eine zweite entscheidende Ebene hinzu: Die EZB kann die technische und geldpolitische Vorbereitung betreiben, für den gesetzlichen Rahmen sind jedoch die politischen EU-Institutionen zuständig.

Das bedeutet: **Europäische Kommission, Europäisches Parlament und Rat der Europäischen Union tragen Verantwortung für den gesetzlichen Rahmen. Der EZB-Rat entscheidet anschließend im Rahmen seiner Zuständigkeit darüber, ob und wann ein digitaler Euro tatsächlich ausgegeben wird.**

Auch nach Abschluss der Vorbereitungsphase wurde das Projekt weiter vorangetrieben. Am **30. Oktober 2025** gab die EZB bekannt, dass der EZB-Rat den Übergang in die nächste Projektphase beschlossen hat. Diese soll insbesondere die technische Bereitschaft für eine mögliche Ausgabe herstellen.

Nach dem derzeitigen Fahrplan könnte – **sofern die notwendigen europäischen Rechtsvorschriften 2026 verabschiedet werden** – ab Mitte **2027** ein Pilotprojekt mit ersten Transaktionen beginnen. Das Eurosystem will **2029** technisch für eine mögliche erste Ausgabe bereit sein. Eine endgültige Entscheidung über die Ausgabe ist damit jedoch noch nicht gefallen.

Die politische Bedeutung dieses Unterschieds ist erheblich: **Technische Vorbereitung ist nicht dasselbe wie demokratische Gesetzgebung – und Gesetzgebung wiederum noch nicht die endgültige Entscheidung über die Ausgabe.** Wer politische Verantwortung bewerten will, muss deshalb alle drei Ebenen betrachten.

Quellen:

[EZB – Geschichte und aktueller Stand des Projekts digitaler Euro](#)

[EZB – Beschluss über die Vorbereitungsphase vom 18. Oktober 2023](#)

[EZB – Übergang in die nächste Projektphase vom 30. Oktober 2025](#)



8.5 Regierung und Opposition: Wer unterstützte den digitalen Euro – und wer stellte sich dagegen?

Auch in Deutschland wurde der digitale Euro zum Gegenstand einer parlamentarischen Auseinandersetzung. Dabei zeigt sich allerdings kein einfaches Schema von Befürwortern und Gegnern. Die Parteien unterschieden sich sowohl bei der grundsätzlichen Bewertung des digitalen Euro als auch bei der Frage, **wer über seine Einführung entscheiden sollte und wie stark Bargeld geschützt werden muss.**

Am **7. November 2023** brachten sowohl die **CDU/CSU-Bundestagsfraktion** als auch die **AfD-Bundestagsfraktion** eigene Anträge zum digitalen Euro ein.

Die **CDU/CSU** lehnte den digitalen Euro nicht grundsätzlich ab. Sie verlangte jedoch, dass die Bundesregierung einer Einführung im Rat der Europäischen Union nur zustimmen sollte, wenn zuvor auch der **Deutsche Bundestag ausdrücklich zugestimmt** hat. Gleichzeitig forderte die Union, den Status des Bargelds als gesetzliches Zahlungsmittel unangetastet zu lassen und einer Schwächung des Bargelds entgegenzutreten.

Die **AfD** ging erheblich weiter. Sie forderte in ihrem Antrag „**Bargeld als einziges gesetzliches Zahlungsmittel bewahren und Überwachung der Bürger durch digitales Zentralbankgeld verhindern**“, dass die Bundesregierung sich auf europäischer Ebene **gegen die Einführung einer digitalen Zentralbankwährung** einsetzen sollte. Außerdem verlangte sie eine Ergänzung des Grundgesetzes um ein Recht auf uneingeschränkte Nutzung von Bargeld.

Beide Anträge wurden zunächst parlamentarisch behandelt und an den **Finanzausschuss** überwiesen. Am **19. Februar 2024** fand dort eine öffentliche Sachverständigenanhörung statt. Die oppositionellen Initiativen wurden damit nicht lediglich eingereicht, sondern tatsächlich Gegenstand des parlamentarischen Beratungsverfahrens.

Die entscheidende Abstimmung im Bundestag folgte am **4. Juli 2024**.

Der Antrag der **CDU/CSU**, eine vorherige Zustimmung des Bundestages zur Bedingung zu machen, wurde abgelehnt. **SPD, Bündnis 90/Die Grünen und FDP stimmten dagegen. CDU/CSU und AfD stimmten dafür.**

Auch der wesentlich weitergehende Antrag der **AfD gegen die Einführung eines digitalen Euro** wurde abgelehnt. Nach der offiziellen Dokumentation des Bundestages stimmten **alle übrigen Fraktionen gegen den AfD-Antrag.**

Damit lässt sich die damalige politische Lage klarer einordnen:

Die **Ampelkoalition aus SPD, Grünen und FDP** verhinderte gemeinsam mit ihrer Mehrheit den von der Union verlangten parlamentarischen Zustimmungsvorbehalt. Die FDP befürwortete den digitalen Euro ausdrücklich als **Ergänzung zum Bargeld**, verlangte allerdings zugleich den uneingeschränkten Erhalt von Bargeld und lehnte einheitliche Bargeldobergrenzen ab.



Die **CDU/CSU** stellte sich nicht grundsätzlich gegen den digitalen Euro, verlangte aber stärkere parlamentarische Kontrolle und Schutz des Bargelds.

Die **AfD** vertrat unter den damaligen Bundestagsfraktionen die grundsätzlichste Gegenposition: Sie wollte die Einführung einer digitalen Zentralbankwährung verhindern und den Bargeldgebrauch zusätzlich verfassungsrechtlich absichern.

Für die Bewertung der Oppositionsarbeit ist deshalb ein Unterschied entscheidend: **CDU/CSU und AfD wurden beide parlamentarisch aktiv, verfolgten aber unterschiedliche Ziele.** Die Union verlangte einen Zustimmungsvorbehalt des Bundestages; die AfD verlangte die Verhinderung des digitalen Euro selbst. Beide Initiativen scheiterten an den parlamentarischen Mehrheiten.

Wer die vollständigen Anträge, die Ausschussberatung und das Abstimmungsergebnis selbst überprüfen möchte, findet sie in der Dokumentation des Deutschen Bundestages:

[Deutscher Bundestag – Anträge und Abstimmung zum digitalen Euro vom 4. Juli 2024](#)

[Deutscher Bundestag – öffentliche Anhörung im Finanzausschuss vom 19. Februar 2024](#)

KLARTEXT-Hinweis: Zu diesem Themenkomplex wird in Kürze ein eigenes Dossier erscheinen.

8.6 Was bedeutet das für den Bürger? Bargeld und digitale Zahlung als bewusste Wahl

Die politische und technische Entwicklung des Zahlungsverkehrs ist noch nicht abgeschlossen. Der digitale Euro befindet sich weiterhin in Vorbereitung. Nach dem derzeitigen Konzept der Europäischen Zentralbank soll er **Bargeld ergänzen und nicht ersetzen**. Die EZB erklärt ausdrücklich, dass Bargeld gesetzliches Zahlungsmittel bleiben und weiterhin verfügbar sein soll.

Auch beim Datenschutz muss zwischen verschiedenen Zahlungsformen unterschieden werden. Nach dem derzeitigen Konzept sollen **Offline-Zahlungen mit dem digitalen Euro ein mit Bargeld vergleichbares Datenschutzniveau erreichen**: Die persönlichen Transaktionsdetails sollen dabei nur Zahler und Empfänger kennen. Bei Online-Zahlungen sollen EZB und nationale Zentralbanken Zahler und Empfänger nicht identifizieren können; Zahlungsdienstleister müssen jedoch weiterhin die gesetzlichen Vorgaben zur Geldwäschebekämpfung erfüllen.

Für den Bürger bedeutet das zunächst: **Es gibt keinen sachlichen Grund, Bargeld vorschnell aufzugeben.**

Gerade als Rückfallebene bleibt Bargeld wichtig. Ein angemessener Vorrat in kleineren Stückelungen kann die Zahlungsfähigkeit erhalten, wenn Kartenterminals, Online-Banking, Mobilfunk oder andere digitale Systeme vorübergehend ausfallen.



Gleichzeitig sollte der digitale Euro nicht mit einem bereits beschlossenen Bargeldersatz verwechselt werden. Nach dem derzeitigen Stand soll er eine zusätzliche Form von Zentralbankgeld darstellen und auch **offline** funktionieren. Die konkrete Ausgestaltung befindet sich jedoch weiterhin in Entwicklung; im Juli 2026 veröffentlichte die EZB beispielsweise eine neue Entwurfsfassung des Regelwerks.

Für einen selbstbestimmten Umgang mit Geld ergeben sich deshalb drei einfache Grundsätze:

- **Bargeld als funktionsfähige Rückfallebene erhalten.**
- **Neue digitale Zahlungsmittel nicht nach Versprechen, sondern nach den endgültigen gesetzlichen und technischen Regeln beurteilen.**
- **Politische Entscheidungen über Annahmepflichten, Datenschutz, Bargeldzugang und mögliche Nutzungsbeschränkungen weiter beobachten.**

Entscheidend ist nicht, digitale Zahlungsmittel grundsätzlich abzulehnen oder ihnen blind zu vertrauen. Entscheidend ist, **die Wahlmöglichkeit zwischen analogem und digitalem Bezahlen tatsächlich zu erhalten.**

KLARTEXT-Hinweis: Zu diesem Themenkomplex wird in Kürze ein eigenes Dossier erscheinen.

Quellen:

[Europäische Zentralbank – Häufig gestellte Fragen zum digitalen Euro, Stand März 2026](#)

[Europäische Zentralbank – Aktueller Projektstand zum digitalen Euro](#)

9. Die Zusammenführung: Wie Sie jetzt aktiv die Kontrolle behalten

Echte Resilienz im Alltag entsteht nicht durch einzelne Maßnahmen, sondern durch das bewusste Zusammenspiel verschiedener Schutzbereiche. Die physische Absicherung durch Notstromversorgung, Wasserreserven und einen durchdachten Vorrat schafft eine wichtige Grundlage für die eigene Handlungsfähigkeit.

Doch auch der digitale Raum gewinnt zunehmend an Bedeutung. Digitale Identität, elektronische Patientenakte, staatliche Register und moderne Zahlungssysteme verändern die Art und Weise, wie persönliche Daten verarbeitet, gespeichert und genutzt werden.

Entscheidend ist deshalb, die einzelnen Entwicklungen nicht isoliert zu betrachten. Erst der Blick auf die Zusammenhänge zeigt, welche technischen Möglichkeiten entstehen und welche Fragen sich daraus für Datenschutz, Transparenz und persönliche Selbstbestimmung ergeben.

Wer diese Entwicklungen versteht, kann seine eigenen Rechte bewusster wahrnehmen. Dazu gehören insbesondere der verantwortungsvolle Umgang mit persönlichen Daten, die Nutzung



gesetzlicher Auskunft- und Widerspruchsrechte sowie die regelmäßige Überprüfung eigener digitaler Sicherheitsmaßnahmen.

Selbstbestimmung im digitalen Zeitalter bedeutet nicht, jede technische Entwicklung abzulehnen. Sie bedeutet, informiert zu bleiben, die eigenen Rechte zu kennen und die vorhandenen Möglichkeiten zum Schutz der persönlichen Freiheit konsequent zu nutzen.

10. Der persönliche Schutzfahrplan: Vom Wissen zum konsequenten Handeln

Die Analyse der verabschiedeten Gesetzgebungen und technischen Infrastrukturen zeigt die Richtung der Transformation auf. Während die strukturelle Entwicklung auf staatlicher und europäischer Ebene verläuft, verbleibt die konkrete Umsetzung im eigenen Alltag im persönlichen Verantwortungsbereich. Die Vertiefung aus den vorangegangenen Kapiteln bildet das Fundament für eine systematische, schrittweise Anpassung der eigenen Vorsorge.

Ein strukturierter Handlungsfahrplan unterteilt diese Umsetzung in zeitlich und praktisch bewältigbare Schritte.

10.1 Sofortmaßnahmen – digitale Bestandsaufnahme

Der erste Schritt zur Wiederherstellung der eigenen digitalen Souveränität besteht in einer strukturierten Inventur der bestehenden digitalen Identitäten, Benutzerkonten und Datenverarbeitungen.

10.1.1 Kontrolle von Konten, Authentifizierung und Berechtigungen

Eine systematische Bestandsaufnahme erfasst sämtliche aktiven Online-Konten, genutzten Identitätszugänge und hinterlegten Notfalloptionen. Zur Absicherung dieser Zugänge dienen individuelle, komplexe Passwörter in Kombination mit einer Zwei-Faktor-Authentifizierung (2FA), bevorzugt über zeitbasierte Einmalpasswörter (TOTP) mittels Authentifikator-Apps oder Hardware-Sicherheits-Schlüsseln. Die technischen Vorgaben und Empfehlungen zur sicheren Passwortgestaltung und Authentifizierung werden von IT-Sicherheitsbehörden bereitgestellt.

Quellen:

[BSI – Basistipps zur IT-Sicherheit](#)

[BSI – Zwei-Faktor-Authentisierung](#)

[NIST – SP 800-63B-4: Digital Identity Guidelines – Authentication and Authenticator Management](#)



10.1.2 Gezielte Wahrnehmung von Auskunftsrechten nach DSGVO

Zur Feststellung, welche Datenstellen personenbezogene Informationen speichern oder verarbeiten, sieht das europäische Datenschutzrecht ein formelles Auskunftsrecht vor. Nach Art. 15 der Datenschutz-Grundverordnung (DSGVO) können Bürger von Verantwortlichen eine Bestätigung darüber verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Dieses Recht besteht gegenüber allen Stellen, die unter den Anwendungsbereich der Verordnung fallen, erfordert jedoch eine konkrete Adressierung der jeweiligen speichernden Stelle. Rechtliche Grundlagen und Anleitungen zur Ausübung stellen die Aufsichtsbehörden bereit.

Musterbriefe und praktische Vorlagen:

Für die konkrete Wahrnehmung Ihrer Rechte stellt KLARTEXT kostenlose Musterbriefe, Formulare und Schritt-für-Schritt-Anleitungen zur Verfügung. Die Vorlagen können individuell an den jeweiligen Fall angepasst werden.

[Zu den kostenlosen Musterbriefen und Widerspruchsvorlagen](#)

Quellen:

[EUR-Lex – Verordnung \(EU\) 2016/679 – DSGVO](#)

[BfDI – Auskunftsrecht nach Art. 15 DSGVO](#)

10.2 Gesundheit und ePA – Rechte konkret kennen

Im Gesundheitswesen wurden mit dem Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) und dem Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) grundlegende Weichenstellungen getroffen.

10.2.1 Gesetzliche Widerspruchsrechte zur elektronischen Patientenakte

Für die elektronische Patientenakte (ePA) gilt in Deutschland das Prinzip der automatischen Einrichtung mit Widerspruchsrecht („Opt-out“). Versicherte der gesetzlichen Krankenversicherung haben das gesetzlich verankerte Recht, der Einrichtung und Nutzung ihrer ePA zu widersprechen. Darüber hinaus bestehen weitere Widerspruchsmöglichkeiten, unter anderem gegen bestimmte Datenübermittlungen und -speicherungen sowie gegen Zugriffe auf Daten der ePA. Gesetzliche Grundlagen und Verbraucherinformationen stehen hierzu zur Verfügung.

Quellen:

Gesetze im Internet – §§ 342, 342a, 344 und 353 SGB V (Bereitstellung der ePA und Widerspruchsrechte)



10.3 Kurzfristige materielle Vorsorge

Die materielle Vorsorge sichert die grundlegende Versorgung des Haushalts bei unvorhergesehenen Störungen der Lieferketten oder Infrastrukturen.

10.3.1 Lebensmittel- und Trinkwasserressourcen

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) empfiehlt die Bevorratung von Lebensmitteln und Getränken für einen Zeitraum von möglichst zehn Tagen. Für Trinkwasser gilt ein Richtwert von zwei Litern pro Person und Tag. Zur Vermeidung von Lebensmittelverschwendung wird die Führung eines rotierenden Vorratssystems empfohlen, bei dem Vorräte fortlaufend in den täglichen Verbrauch integriert und nachgekauft werden.

Bei der Bemessung der Vorräte sind auch Haustiere sowie individuell benötigte Medikamente angemessen zu berücksichtigen. Mobile Wasserfilter können im Notfall zur Aufbereitung genutzt werden, entfernen jedoch je nach Filtertyp nicht sämtliche chemischen oder gelösten Schadstoffe.

Quellen:

[BBK – Essen und Trinken bevorraten](#)

[Ernährungsvorsorge – Vorrattabelle für den Notvorrat](#)

10.4 Finanzielle Vorsorge

Elektronische Zahlungssysteme hängen von einer unterbrechungsfreien Strom- und Dateninfrastruktur ab. Eine Bargeldreserve stellt sicher, dass alltägliche Transaktionen auch bei temporären Systemausfällen abgewickelt werden können.

10.4.1 Erhalt der persönlichen Zahlungsfähigkeit

Eine Notfallreserve in bar, aufgeteilt in kleinere Stückelungen, schützt vor unmittelbaren Engpässen bei Ausfällen von Kartenlesegeräten oder Online-Banking. Nach Artikel 80 der Verordnung (EU) 2024/1624 gelten für Personen, die mit Gütern handeln oder Dienstleistungen erbringen, Obergrenzen für Barzahlungen von 10.000 Euro. Die Mitgliedstaaten können niedrigere nationale Obergrenzen festlegen. Zahlungen zwischen natürlichen Personen, die nicht in ihrer beruflichen Eigenschaft handeln, sind von dieser EU-weiten 10.000-Euro-Grenze ausdrücklich ausgenommen.

Quelle:

[EUR-Lex – Verordnung \(EU\) 2024/1624, Artikel 80](#)

10.5 Mittelfristige technische Vorsorge



Bei einem Stromausfall verringert eine unabhängige Notstromversorgung die unmittelbaren Beeinträchtigungen im Haushalt.

10.5.1 Notstrominfrastruktur und Kapazitätsplanung

Mobile Powerstations und photovoltaische Inselanlagen ermöglichen das Nachladen von Kommunikationsgeräten, Beleuchtung und den kurzzeitigen Betrieb ausgewählter Verbraucher. Die Leistungsfähigkeit dieser Systeme wird durch die Akkukapazität in Wattstunden (Wh), die Dauerleistung des Wechselrichters in Watt (W) und den tatsächlichen Solarertrag begrenzt.

Eine vollständige energetische Autarkie eines gesamten Haushalts erfordert komplexere Installationen; kompakte Systeme dienen in erster Linie als begrenzte Notstrom- und Überbrückungslösung.

Quellen:

[BBK – Vorsorge und Handeln bei Stromausfall](#)

[Verbraucherzentrale – Photovoltaik-Inselanlagen: Solare Energie direkt nutzen](#)

[Verbraucherzentrale – Steckersolar: Solarstrom vom Balkon direkt in die Steckdose](#)

10.6 Persönlicher Notfallordner

Eine strukturierte Dokumentenmappe stellt sicher, dass kritische Informationen auch bei Ausfall digitaler Geräte verfügbar bleiben.

10.6.1 Analoge Absicherung kritischer Dokumente

Ein physischer Notfallordner bündelt wichtige Unterlagen in gedruckter Form oder als Kopie. Dazu gehören:

- Ausweisdokumente und Urkunden, beispielsweise Geburts- und Heiratsurkunden
- Notfallkontakte, medizinische Hinweise und Impfpässe
- Versicherungs- und Vertragsunterlagen
- Eigentumsnachweise und Finanzübersichten

Aus Gründen des Datenschutzes und des Diebstahlschutzes sollte dieser Ordner an einem gesicherten, vor unbefugtem Zugriff geschützten Ort aufbewahrt werden.

Quellen:

[BBK – Wichtige Dokumente sichern: Die Dokumentenmappe](#)

[BSI – Daten verschlüsseln, löschen und sichern](#)

[BSI – Back-up: Doppelt gesichert hält besser](#)



10.7 Regelmäßige Kontrolle

Resilienz ist ein fortlaufender Prozess, der regelmäßige Überprüfungen und Anpassungen erfordert.

10.7.1 Rhythmus zur Aktualisierung und Wartung

Ein strukturierter Kontrollrhythmus stellt die Funktionsfähigkeit der getroffenen Maßnahmen sicher:

- **Regelmäßig:** Überprüfung und Rotation der Lebensmittel- und Wasservorräte sowie Kontrolle der Verfalldaten bei Medikamenten.
- **Nach Herstellerangaben:** Kontrolle, Wartung und gegebenenfalls Testladung von Powerstations und Akkus; Aktualisierung des physischen Notfallordners bei Änderungen wichtiger persönlicher Dokumente oder Informationen.
- **Bei Rechtsänderungen:** Anpassung von Datenschutzeinstellungen, Prüfung aktualisierter Musterbriefe und Wahrnehmung bestehender gesetzlicher Widerspruchs- und Optionsrechte.

10.8 Weiterführender Schutz der digitalen Privatsphäre

Der Schutz der eigenen Daten endet nicht bei gesetzlichen Auskunfts- und Widerspruchsrechten. Auch die Absicherung der eigenen Geräte, Konten und Internetverbindungen ist ein wichtiger Bestandteil digitaler Selbstbestimmung.

Weiterführende KLARTEXT-Dossiers:

[Digitale Selbstverteidigung: So schützt du deine Daten im Internet vor Hackern](#)

[EU-Chatkontrolle: 450 Millionen Bürger unter Generalverdacht?](#)

11. Fazit: Selbstbestimmung beginnt mit Wissen – und endet nicht dort

Die Digitalisierung staatlicher, finanzieller und gesundheitlicher Strukturen ist kein abstraktes Zukunftsszenario. Viele der beschriebenen Systeme befinden sich bereits im Aufbau, sind gesetzlich verankert oder werden schrittweise eingeführt. Entscheidend ist deshalb nicht allein, diese Entwicklungen zu kennen, sondern die bestehenden eigenen Rechte und Handlungsmöglichkeiten auch tatsächlich zu nutzen.

Digitale Selbstbestimmung bedeutet dabei nicht, technische Entwicklungen grundsätzlich abzulehnen. Sie bedeutet, informiert entscheiden zu können, welche Daten preisgegeben



werden, welche gesetzlichen Widerspruchsmöglichkeiten bestehen und welche persönlichen Vorsorgemaßnahmen sinnvoll sind.

Der persönliche Schutzfahrplan aus Kapitel 10 zeigt, dass Vorsorge auf mehreren Ebenen gleichzeitig stattfinden kann: beim Schutz digitaler Konten und Identitäten, bei Gesundheitsdaten, bei der materiellen und finanziellen Absicherung, bei der technischen Notfallvorsorge und bei der Sicherung wichtiger Dokumente.

Entscheidend bleibt dabei ein Grundsatz: Resilienz entsteht nicht durch Angst vor möglichen Entwicklungen, sondern durch Wissen, Vorbereitung und die bewusste Wahrnehmung der eigenen Rechte.

Die in diesem Dossier dargestellten Entwicklungen zeigen zugleich, warum digitale und materielle Selbstbestimmung nicht getrennt voneinander betrachtet werden sollten. Wer seine Rechte kennt, seine Daten schützt und für Störungen grundlegender Versorgungsstrukturen vorsorgt, erweitert seinen eigenen Handlungsspielraum.

Der vernetzte Staat entwickelt sich weiter. Damit bleibt auch die Aufgabe bestehen, neue gesetzliche Regelungen, technische Infrastrukturen und tatsächliche Verknüpfungsmöglichkeiten kritisch zu beobachten. Informationelle Selbstbestimmung ist kein Zustand, der einmal erreicht und anschließend vergessen werden kann. Sie muss dort wahrgenommen und verteidigt werden, wo neue technische und rechtliche Strukturen in den persönlichen Lebensbereich eingreifen.

Wissen schafft die Voraussetzung. Konsequentes Handeln erhält die eigene Entscheidungsfreiheit.

Resümee – die wichtigsten Stationen auf einen Blick

Die Digitalisierung staatlicher Strukturen ist längst mehr als die Umstellung einzelner Behördengänge auf elektronische Verfahren. Digitale Identitäten, vernetzte Register, elektronische Gesundheitsdaten und neue digitale Zahlungssysteme entwickeln sich zunehmend zu einer Infrastruktur, die unterschiedliche Lebensbereiche miteinander verbindet.

Dieses Dossier hat gezeigt, dass diese Entwicklung **nicht auf eine einzelne Regierung, Partei oder Institution zurückgeführt werden kann**. Wesentliche Grundlagen entstehen auf europäischer Ebene, werden von Europäischer Kommission, Europäischem Parlament und Rat gestaltet und anschließend in Deutschland umgesetzt oder durch nationale Regelungen ergänzt. Gleichzeitig zeigen die untersuchten parlamentarischen Vorgänge, dass sich die Parteien in wichtigen Fragen unterschiedlich positionieren und Opposition nicht nur aus öffentlicher Kritik besteht, sondern auch durch Anträge, Änderungsanträge, parlamentarische Anfragen und Abstimmungen sichtbar wird.

Für den Bürger entstehen dadurch neue Möglichkeiten, aber auch neue Abhängigkeiten. Digitale Verfahren können Behördengänge vereinfachen, Nachweise beschleunigen und Dienstleistungen komfortabler machen. Gleichzeitig steigt die Bedeutung von Datenschutz, IT-Sicherheit, transparenten Zugriffsrechten und funktionierenden analogen Alternativen.



Deshalb gehören **digitale Selbstverteidigung und praktische Resilienz zusammen**. Sichere Konten und Geräte, die Wahrnehmung gesetzlicher Datenschutzrechte, Bargeld als Rückfallebene, Notstrom, Wasser- und Lebensmittelvorsorge sowie wichtige Dokumente in analoger Form verfolgen letztlich dasselbe Ziel: die eigene Handlungsfähigkeit auch dann zu erhalten, wenn technische Systeme ausfallen oder sich politische und rechtliche Rahmenbedingungen verändern.

Die entscheidende Erkenntnis dieses Dossiers liegt deshalb nicht in einer pauschalen Ablehnung der Digitalisierung. Sie liegt darin, **technischen Fortschritt, politische Verantwortung und persönliche Selbstbestimmung gemeinsam zu betrachten**.

Schlussgedanke: Infrastruktur bleibt – Regierungen wechseln

Digitalisierung wird häufig als Fortschritt und Innovation präsentiert. Und vieles daran kann tatsächlich nützlich sein. Doch staatliche digitale Infrastruktur ist mehr als eine komfortablere Form der Verwaltung.

Regierungen wechseln. Mehrheiten ändern sich. Gesetze können geändert werden. Eine einmal geschaffene technische Infrastruktur aber bleibt.

Mit jeder zusätzlichen Vernetzung entstehen deshalb nicht nur neue Dienstleistungen, sondern auch **neue technische Möglichkeiten**. Was heute unter bestimmten gesetzlichen Voraussetzungen aufgebaut wird, kann einer späteren Regierung Möglichkeiten eröffnen, die bei der Einführung weder vorgesehen noch politisch gewollt waren.

Das bedeutet nicht, dass diese Möglichkeiten zwangsläufig genutzt werden. Niemand kann seriös vorhersagen, welche politischen Mehrheiten Deutschland und Europa in zehn, zwanzig oder dreißig Jahren haben werden oder welche Gesetze dann gelten.

Gerade darin liegt die entscheidende Frage.

Nicht nur: Was soll diese Infrastruktur heute können?

Sondern auch: Was könnte sie morgen ermöglichen?

Freiheitsrechte müssen deshalb nicht erst dann verteidigt werden, wenn sie bereits eingeschränkt werden. Datenschutz, Zweckbindung, Transparenz, wirksame Kontrolle und analoge Alternativen müssen ebenso dauerhaft angelegt sein wie die technischen Systeme selbst.

Denn technischer Fortschritt bemisst sich nicht allein daran, **was möglich gemacht wird**.

Er bemisst sich auch daran, **welche Grenzen eine freie Gesellschaft der möglichen Nutzung staatlicher Macht setzt**.

Mit freundlichen Grüßen



Michael B. Barnes

Impressum / Kontakt

Michael B. Barnes
Hengeloer Str. 1
49565 Bramsche
E-Mail: info@klartext-info.online

Rechtlicher Hinweis

Dieses Dokument ist Teil des privaten Informations- und Aufklärungsprojekts KLARTEXT von Michael B. Barnes.

Der Bericht dient ausschließlich der Information sowie der öffentlichen Meinungs- und Diskussionsbildung. Er enthält eine Kombination aus dokumentierten Tatsachen, öffentlich zugänglichen Quellen, rechtlichen Einordnungen sowie persönlichen Bewertungen, Schlussfolgerungen, Vermutungen und Hypothesen des Autors. Diese sind entsprechend im Gesamtzusammenhang des jeweiligen Dossiers zu verstehen.

Alle Inhalte wurden nach bestem Wissen und Gewissen auf Grundlage der zum Zeitpunkt der Veröffentlichung verfügbaren Informationen erstellt. Trotz sorgfältiger Recherche kann keine Gewähr für Vollständigkeit, Aktualität oder die fortdauernde Richtigkeit sämtlicher Angaben übernommen werden. Neue Erkenntnisse oder spätere Entwicklungen können eine Überarbeitung oder Neubewertung einzelner Inhalte erforderlich machen.

Eine unveränderte Weitergabe des vollständigen Dokuments über den offiziellen Veröffentlichungsweg ist ausdrücklich erwünscht. Veränderungen, Kürzungen, aus dem Zusammenhang gerissene Zitate oder Bearbeitungen, die den Sinn oder die Aussage des Dokuments verfälschen, sind ohne ausdrückliche Zustimmung des Autors nicht gestattet.

Stand der Quellen und Rechtslage: Veröffentlichungsdatum des jeweiligen Dossiers.

Version: 1.0

© Michael B. Barnes – Alle Rechte vorbehalten.