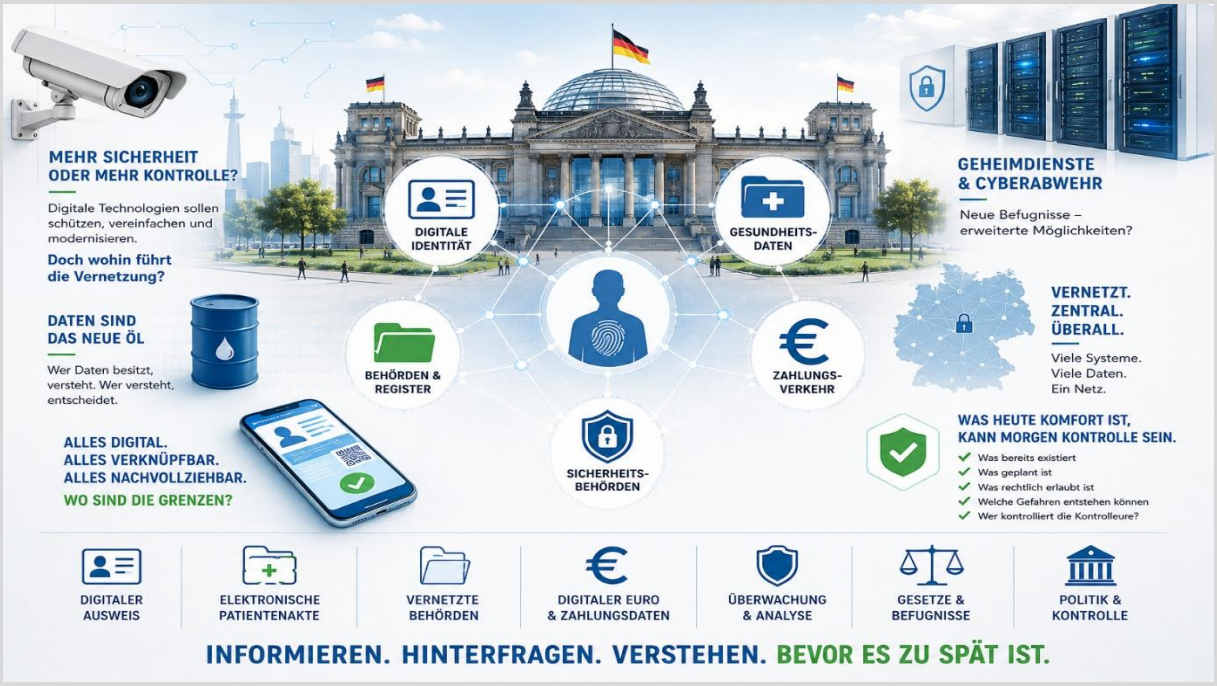
MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

2026-08-13

Der vernetzte Staat



Geheimdienste, Cyberabwehr, digitale Identität – und die Frage, wer künftig über unsere Daten verfügt

Inhalt

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Einleitung:

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Es ist noch gar nicht lange her, da bestand eine Identität im Alltag aus wenigen Dokumenten. Der Personalausweis steckte im Portemonnaie. Die Krankenversicherungskarte diente dem Arztbesuch. Behördengänge fanden auf dem Amt statt. Bezahlt wurde selbstverständlich mit Bargeld. Gesundheitsdaten lagen dort, wo sie entstanden: in Arztpraxen, Krankenhäusern und bei den jeweils zuständigen Stellen.

Diese Welt verschwindet nicht von heute auf morgen. Aber sie verändert sich grundlegend.

Immer mehr Bereiche unseres Lebens werden digitalisiert. Identität, Gesundheit, Verwaltung und Zahlungsverkehr erhalten digitale Strukturen. Behördenregister werden modernisiert und stärker vernetzt. Gleichzeitig entwickeln Deutschland und die Europäische Union neue digitale Identitätslösungen. Im Gesundheitswesen wird die elektronische Patientenakte zur zentralen digitalen Infrastruktur. Parallel wird über den digitalen Euro gearbeitet. Und auch die staatliche Sicherheitsarchitektur verändert sich: Nachrichtendienste, Cyberabwehr und neue Befugnisse stehen auf der politischen Tagesordnung.

Das sind keine Science-Fiction-Szenarien. **Die einzelnen Bausteine sind Realität, befinden sich im Aufbau oder sind Gegenstand konkreter politischer und gesetzgeberischer Vorhaben.**

Genau deshalb sind Aufklärungsdossiers zu diesem Thema wichtig.

Denn die entscheidende Entwicklung erkennt man möglicherweise nicht, wenn man jeden Baustein ausschließlich für sich betrachtet. Die digitale Identität wird mit Komfort und sicheren Nachweisen begründet. Die elektronische Patientenakte soll die medizinische Versorgung verbessern. Vernetzte Register sollen Bürokratie reduzieren. Digitale Zahlungssysteme versprechen moderne und schnelle Transaktionen. Erweiterte Sicherheitsbefugnisse sollen den Staat gegen Cyberangriffe, Spionage und Sabotage schützen.

Für jeden einzelnen Schritt gibt es Argumente.

Doch was ergibt sich aus der Summe?

Was früher auf unterschiedliche Lebensbereiche, Institutionen, Akten und Systeme verteilt war, wird zunehmend digital erfasst und verarbeitet. Damit entstehen Möglichkeiten, die es in dieser Form früher nicht gab.

Das bedeutet nicht automatisch, dass daraus ein umfassender Überwachungsstaat entsteht. Es bedeutet aber sehr wohl, dass eine demokratische Gesellschaft wissen sollte, **welche Infrastruktur gerade geschaffen wird, welche Daten sie verarbeitet, wer darauf zugreifen darf, welche Systeme miteinander kommunizieren können und welche Kontrollmöglichkeiten technisch überhaupt entstehen.**

Die Geschichte der Digitalisierung lässt sich bereits an ganz alltäglichen Beispielen erkennen: Der klassische Ausweis bekommt ein digitales Gegenstück. Gesundheitsinformationen wandern in elektronische Akten. Behördendaten werden digital verknüpft. Zahlungen hinterlassen bei elektronischer Abwicklung Datenspuren. Sicherheitsbehörden arbeiten längst mit digitalen Datenbeständen und sollen auf neue digitale Bedrohungen reagieren können.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Keines dieser Beispiele beweist für sich eine missbräuchliche staatliche Überwachung.

Aber zusammen begründen sie eine Frage, die man stellen muss, bevor die technische Infrastruktur vollständig geschaffen ist – nicht erst danach.

Wie viel Wissen über einen Menschen kann in einer zunehmend vernetzten digitalen Gesellschaft grundsätzlich zusammengeführt werden? Wer setzt die Grenzen? Wer kontrolliert diejenigen, die Zugriff erhalten? Welche Schutzmechanismen bestehen heute? Und was geschieht, wenn eine spätere Regierung diese Grenzen verschiebt?

Denn Gesetze können geändert werden. Politische Mehrheiten wechseln. Technische Infrastruktur dagegen verschwindet nicht automatisch mit einer Wahl.

Genau hier beginnt dieses Dossier.

Es untersucht, was bereits Realität ist, was beschlossen oder geplant wurde, welche Befugnisse der Staat besitzt und welche zusätzlichen Befugnisse diskutiert werden. Es dokumentiert die Positionen von Regierung und Opposition, prüft Schutzmechanismen und Gegenargumente und trennt konsequent zwischen belegten Tatsachen und möglichen zukünftigen Risiken.

Es geht nicht darum, dem Leser vorzuschreiben, was er denken soll. Es geht darum, ihm zu zeigen, was vorhanden ist, was daraus entstehen könnte und welche Fragen gestellt werden müssen, solange noch Zeit ist, sie zu stellen.

1. Die digitale Identität – Das Fundament des vernetzten Bürgers

1.1 Von eIDAS zur EUDI-Wallet: Wie Europas digitale Identität entstand

Die europäische digitale Identität ist kein plötzlich entstandenes Projekt. Ihre heutige Form hat eine politische Vorgeschichte.

Bereits am **19. Februar 2020** kündigte die Europäische Kommission im Rahmen ihrer Strategie „Gestaltung der digitalen Zukunft Europas“ eine Überarbeitung der bestehenden eIDAS-Verordnung an. Ziel war unter anderem, digitale Identitäten stärker auf den privaten Bereich auszuweiten. Diese Entwicklung mündete schließlich in die **Verordnung (EU) 2024/1183**, die das Europäische Parlament und der Rat am **11. April 2024** verabschiedeten und die seit **20. Mai 2024** gilt. (EUR-Lex)

EU-Verordnung 2024/1183 – vollständiger Originaltext bei EUR-Lex

Damit wurde die rechtliche Grundlage für die **European Digital Identity Wallet (EUDI-Wallet)** geschaffen.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die Mitgliedstaaten müssen mindestens eine solche digitale Brieftasche bereitstellen. Die EU-Verordnung legt dabei keinen simplen festen Termin „Anfang 2027“ fest, sondern eine Frist von **24 Monaten nach Inkrafttreten der einschlägigen Durchführungsrechtsakte**. (EUR-Lex)

Die Wallet soll es ermöglichen, Identitätsdaten und elektronische Nachweise digital anzufordern, zu speichern, miteinander zu kombinieren und gegenüber öffentlichen oder privaten Stellen vorzuzeigen. Dazu gehört ausdrücklich die Möglichkeit, nur bestimmte erforderliche Informationen freizugeben. (EUR-Lex)

Das ist wichtig für die weitere Untersuchung: **Die EUDI-Wallet ist rechtlich nicht als zentrale Datenbank konzipiert, in der sämtliche Lebensdaten eines Bürgers zusammengeführt werden.** Die EU-Regelung enthält ausdrücklich Vorgaben zur Nutzerkontrolle, selektiven Datenfreigabe und zum Datenschutz. Sie verlangt zudem, dass Menschen, die die Wallet nicht verwenden wollen, nicht allein deswegen vom Zugang zu öffentlichen oder privaten Dienstleistungen ausgeschlossen werden; alternative Lösungen sollen bestehen bleiben. (EUR-Lex)

Damit ist zunächst die Rechtslage beschrieben.

Die weitergehende Frage dieses Dossiers lautet jedoch: **Welche Bedeutung bekommt eine solche Infrastruktur, wenn dieselbe digitale Identität künftig in immer mehr Bereichen des täglichen Lebens eingesetzt werden kann?**

1.2 Deutschland schafft die nationale Grundlage

Deutschland setzt den europäischen Rahmen inzwischen national um.

Am **20. Mai 2026** beschloss das Bundeskabinett den Entwurf für das **Digitale-Identitäten-Gesetz (DIdG)**. Nach Angaben des Bundesministeriums für Digitales und Staatsmodernisierung soll damit die Voraussetzung für die EUDI-Wallet in Deutschland geschaffen werden. (BMDs)

Bundesministerium für Digitales und Staatsmodernisierung – Kabinettsbeschluss vom 20. Mai 2026

Die Bundesregierung nennt bereits konkrete Anwendungsbeispiele: digitale Behördengänge, die Eröffnung eines Bankkontos oder die sichere Anmeldung bei Online-Diensten. (BMDs)

Die europäische Verordnung geht noch erheblich weiter. Sie sieht die Verwendung der Wallet grundsätzlich auch in Bereichen wie **Banken und Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Bildung, Telekommunikation, Verkehr und digitale Infrastruktur** vor, sofern dort die entsprechenden Voraussetzungen für eine elektronische Identifizierung bestehen. (EUR-Lex)

Das verändert die Bedeutung digitaler Identität grundlegend.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Früher war der Personalausweis in erster Linie ein staatliches Identitätsdokument. Die EUDI-Wallet ist dagegen als **digital verwendbare Identitätsinfrastruktur für öffentliche und private Dienstleistungen** angelegt.

Dabei gelten ausdrücklich Datenschutzvorgaben. Die EU verlangt unter anderem Datenminimierung und ermöglicht sogenannte selektive Offenlegung: Ein Nutzer soll beispielsweise eine erforderliche Eigenschaft nachweisen können, ohne zwangsläufig sämtliche dahinterliegenden persönlichen Daten preiszugeben. (EUR-Lex)

Die entscheidende Entwicklung liegt deshalb nicht allein darin, dass der Personalausweis digital wird.

Sie liegt darin, dass digitale Identität zu einem wiederverwendbaren Zugangsschlüssel für immer mehr Lebensbereiche werden kann.

1.3 Das zentrale Pass- und Ausweisregister: Deutschland zentralisiert einen weiteren Baustein

Parallel zur EUDI-Wallet hat die Bundesregierung im Sommer 2026 ein weiteres großes Digitalisierungsvorhaben auf den Weg gebracht.

Am **15. Juli 2026** beschloss das Bundeskabinett Eckpunkte für ein **zentrales Pass- und Ausweisregister auf Bundesebene**. (Bundesregierung)

Bundesregierung – Digitales Pass- und Ausweiszentralregister, Beschluss vom 15. Juli 2026

Bislang werden Pass- und Ausweisdaten dezentral bei den zuständigen Behörden geführt. Nach den Eckpunkten der Bundesregierung sollen künftig alle ausgegebenen Reisepässe, Personalausweise und eID-Karten in einem zentralen Register nachgewiesen werden. (Bundesregierung)

Hier muss sprachlich genau unterschieden werden:

Das Zentralregister existiert im August 2026 noch nicht als vollständig umgesetztes neues System. Beschlossen wurden zunächst die politischen Eckpunkte. Deshalb wäre die Aussage, die bisherige dezentrale Struktur *sei bereits beendet*, falsch.

Aber die politische Richtung ist eindeutig: **Die Bundesregierung will diese bislang dezentrale Registerstruktur zentralisieren.**

Das ist für die Gesamtbetrachtung dieses Dossiers von Bedeutung. Denn neben der europäischen digitalen Identitätsinfrastruktur entsteht damit ein weiteres staatliches Vorhaben, das Identitätsverwaltung stärker digital und zentral organisiert.

Die Frage nach möglichen Risiken darf deshalb gestellt werden – aber sie muss von der heutigen Rechtslage getrennt bleiben.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

2. Zwischen Komfort und Kontrolle – Was die neue Infrastruktur tatsächlich ermöglicht

2.1 Eine digitale Identität für immer mehr Lebensbereiche

Die politische Begründung für digitale Identitäten ist nachvollziehbar: weniger Papier, schnellere Behördengänge, sichere digitale Nachweise und eine europaweit verwendbare Identität.

Doch gerade der breite Anwendungsbereich macht die Entwicklung gesellschaftlich relevant.

Die EUDI-Wallet soll nicht nur gegenüber Behörden funktionieren. Die EU-Verordnung sieht ihre Akzeptanz unter bestimmten Voraussetzungen auch bei privaten Anbietern vor – darunter Banken, Finanzdienstleister, Gesundheitsdienste, Telekommunikationsunternehmen und weitere Bereiche. (EUR-Lex)

Damit entsteht keine zentrale „Bürgerakte“, in der automatisch sämtliche Informationen zusammenlaufen.

Aber es entsteht eine gemeinsame digitale Identitätsinfrastruktur, über die ein Bürger gegenüber sehr unterschiedlichen Stellen Identitäts- und Attributsnachweise verwenden kann.

Das ist ein wesentlicher Unterschied.

Denn die gesellschaftliche Bedeutung eines solchen Systems hängt nicht nur davon ab, **welche Daten gespeichert werden**, sondern auch davon, **wie unverzichtbar die Infrastruktur für das tägliche Leben eines Menschen irgendwann wird.**

2.2 Freiwilligkeit – was die EU tatsächlich vorschreibt

An dieser Stelle muss das Dossier sauber bleiben.

Die Behauptung, die EU-Wallet werde bereits als verpflichtende digitale Identität eingeführt, wäre nach der geltenden Rechtslage nicht haltbar.

Die EU-Verordnung enthält vielmehr ausdrücklich Schutzbestimmungen für Menschen, die sich **gegen die Verwendung der EUDI-Wallet entscheiden**. Ihnen darf der Zugang zu öffentlichen oder privaten Dienstleistungen nicht allein deswegen unmittelbar oder mittelbar verwehrt werden; alternative Lösungen sollen angeboten werden. (EUR-Lex)

Das ist Tatsache.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Eine andere Frage ist, wie sich die praktische Freiwilligkeit entwickelt, wenn immer mehr Behörden und Unternehmen digitale Identitätsnachweise in ihre Prozesse integrieren.

Das ist derzeit eine Risikofrage, keine feststehende Tatsache.

Ein rechtlich freiwilliges System könnte gesellschaftlich erheblich an Bedeutung gewinnen, wenn seine Nutzung wesentlich schneller, einfacher oder verbreiteter wird als analoge Alternativen.

Ob daraus irgendwann ein **faktischer Nutzungsdruck** entsteht, lässt sich heute nicht als Tatsache feststellen.

Aber genau diese Entwicklung sollte beobachtet werden.

2.3 Datenschutz: Die Schutzmechanismen gehören zur Wahrheit dazu

Wer die möglichen Gefahren einer digitalen Identitätsinfrastruktur untersucht, muss ebenso deutlich darstellen, welche Schutzmechanismen eingebaut wurden.

Die EUDI-Verordnung schreibt unter anderem Datenschutz, Datenminimierung, Nutzerkontrolle und selektive Offenlegung vor. Sie sieht außerdem technische Verfahren zum Schutz der Privatsphäre vor. (EUR-Lex)

EUR-Lex – Datenschutz- und Sicherheitsvorgaben der EUDI-Verordnung

Diese Schutzmechanismen sind kein nebensächliches Detail. Sie gehören zur Tatsachenlage.

Deshalb wäre es ebenfalls falsch, die EUDI-Wallet schon heute als fertiges staatliches Überwachungssystem darzustellen.

Das ist sie nach den geprüften Rechtsgrundlagen nicht.

Damit endet die Untersuchung aber nicht.

Denn Datenschutzrecht beschreibt, **was heute erlaubt und verboten ist**. Eine politische Risikoanalyse muss zusätzlich fragen, welche technischen Strukturen dauerhaft geschaffen werden und wie widerstandsfähig die gesetzlichen Grenzen gegenüber späteren Veränderungen sind.

Gesetze können geändert werden. Politische Mehrheiten können wechseln.

Technische Infrastruktur dagegen kann Jahrzehnte bestehen.

3. Der politische Streit – Wer treibt die digitale Identität voran, wer widerspricht?

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

3.1 Die politische Verantwortung: EU und Bundesregierung

Die heutige EUDI-Wallet geht auf eine Initiative der **Europäischen Kommission** zurück. Die rechtliche Grundlage wurde anschließend im ordentlichen europäischen Gesetzgebungsverfahren durch **Europäisches Parlament und Rat** geschaffen. Die Verordnung (EU) 2024/1183 wurde am 11. April 2024 verabschiedet. (EUR-Lex)

Deutschland setzt diesen europäischen Rechtsrahmen unter der seit 2025 amtierenden Bundesregierung national weiter um. Der Kabinettsbeschluss zum Digitale-Identitäten-Gesetz erfolgte am **20. Mai 2026**. (BMDs)

Damit lässt sich die politische Entwicklung zeitlich nachvollziehen:

2020: Die EU-Kommission kündigt die Weiterentwicklung des europäischen Systems digitaler Identitäten an. (EUR-Lex)

2024: Europäisches Parlament und Rat schaffen mit der Verordnung (EU) 2024/1183 den Rechtsrahmen für die EUDI-Wallet. (EUR-Lex)

2026: Die Bundesregierung beschließt den Entwurf des deutschen Digitale-Identitäten-Gesetzes. (BMDs)

15. Juli 2026: Das Bundeskabinett beschließt zusätzlich Eckpunkte für ein zentrales Pass- und Ausweisregister. (Bundesregierung)

Damit ist die Entwicklung **nicht das Projekt einer einzigen deutschen Partei oder einer einzigen Bundesregierung**. Sie erstreckt sich über mehrere Jahre und über die europäische wie die nationale politische Ebene.

3.2 Die Opposition: Die AfD fordert den Stopp der EUDI-Wallet

Im Deutschen Bundestag gibt es inzwischen ausdrücklichen politischen Widerstand gegen die europäische Wallet.

Am **25. Juni 2026** beriet der Bundestag erstmals einen Antrag der AfD-Fraktion mit dem Titel **„Keine digitale Identität und Geldbörse durch die EU – Mit nationaler Lösung echte Staatsmodernisierung vorantreiben“**. (Deutscher Bundestag)

Deutscher Bundestag – Debatte über den AfD-Antrag vom 25. Juni 2026

Die AfD fordert darin nicht die vollständige Abschaffung digitaler Identitäten.

Sie verlangt vielmehr, dass sich die Bundesregierung auf EU-Ebene für die Aufhebung der einschlägigen EUDI-Wallet-Regelungen einsetzt und das nationale EUDI-Wallet-Projekt beendet. Stattdessen soll nach ihrem Antrag eine **nationale Wallet ausschließlich für den**

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

freiwilligen Gebrauch bei behördlichen Vorgängen entwickelt werden. Außerdem fordert die Fraktion, analoge Alternativen zu digitalen Dokumenten dauerhaft und gleichberechtigt zu erhalten. (Deutscher Bundestag)

Der Antrag wurde nach der ersten Beratung an die Ausschüsse überwiesen. Federführend ist der Ausschuss für Digitales und Staatsmodernisierung. (Deutscher Bundestag)

Damit liegt eine klar dokumentierte Oppositionsposition vor.

3.3 Noch kein vollständiges Parteienbild

Für ein vollständiges politisches Bild reicht es nicht, Bundesregierung und AfD gegenüberzustellen. Entscheidend ist, wie sich auch CDU/CSU, SPD, Bündnis 90/Die Grünen, Die Linke und weitere parlamentarisch relevante Akteure zur konkreten Ausgestaltung der EUDI-Wallet, zur Freiwilligkeit, zu analogen Alternativen, zum Digitale-Identitäten-Gesetz und zum zentralen Pass- und Ausweisregister positionieren.

Dabei genügt es nicht, ausschließlich öffentliche Erklärungen der Parteien heranzuziehen. Wo parlamentarische Vorgänge vorliegen, sind Anträge, Ausschussberatungen und insbesondere das tatsächliche Abstimmungsverhalten aussagekräftiger.

Die bisher dokumentierte Auseinandersetzung zeigt bereits, dass die politischen Konfliktlinien differenzierter verlaufen als eine einfache Gegenüberstellung von Regierung und Opposition. Die AfD hat mit ihrem am **25. Juni 2026 erstmals im Bundestag beratenen Antrag** eine klar dokumentierte Position gegen die europäische EUDI-Wallet in ihrer vorgesehenen Form bezogen und stattdessen eine nationale, freiwillige Lösung für behördliche Vorgänge sowie dauerhaft gleichberechtigte analoge Alternativen gefordert. Der Antrag wurde nach der ersten Beratung an die Ausschüsse überwiesen.

Für die politische Bewertung muss deshalb bei jedem weiteren Schritt nachvollziehbar bleiben:

Wer hat welche Strukturen geschaffen oder unterstützt? Wer fordert Änderungen oder lehnt bestimmte Elemente ab? Und wie stimmen die Parteien tatsächlich ab, wenn aus politischen Erklärungen konkrete parlamentarische Entscheidungen werden?

Erst diese Gegenüberstellung ermöglicht ein belastbares Parteienbild und verhindert, dass politische Verantwortung pauschal einer „Regierung“ oder einer „Opposition“ zugeschrieben wird.

4. Vom digitalen Ausweis zum digitalen Zugangsschlüssel

4.1 Entscheidend ist nicht nur, was gespeichert wird

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die Diskussion über digitale Identität wird häufig auf eine einfache Frage reduziert: Welche persönlichen Daten befinden sich in der Wallet?

Das greift zu kurz.

Mindestens ebenso wichtig ist die Frage, **wofür die digitale Identität verwendet werden kann**.

Mit zunehmender Verbreitung kann eine digitale Identität zum Zugangsschlüssel für immer mehr Dienstleistungen werden. Gerade darin liegt einer der wesentlichen Unterschiede zum klassischen Personalausweis: Dieser bestätigt die Identität seines Inhabers. Eine digitale Wallet kann dagegen in digitale Prozesse eingebunden werden und dabei jeweils die für einen bestimmten Vorgang erforderlichen Nachweise bereitstellen.

Das kann erhebliche Vorteile bringen: weniger Papier, schnellere Verwaltungsverfahren, sichere digitale Nachweise und weniger wiederholte Dateneingaben.

Aber dieselbe Entwicklung erzeugt eine neue Abhängigkeit:

Je mehr gesellschaftliche Funktionen über digitale Identitätsnachweise erreichbar werden, desto wichtiger wird die Infrastruktur, über die diese Nachweise erbracht werden.

4.2 Vom Behördengang bis zum Bankkonto

Schon die derzeit diskutierten und vorgesehenen Anwendungen zeigen, dass es längst nicht mehr nur um einen digitalen Ersatz für den Personalausweis geht.

Die Wallet soll Identitäts- und andere Nachweise gegenüber öffentlichen wie privaten Stellen ermöglichen. Genau deshalb nennt auch die Bundesregierung als praktische Anwendungsfälle neben Behördengängen beispielsweise die **Eröffnung eines Bankkontos und die Anmeldung bei Online-Diensten**.

Damit berührt digitale Identität zunehmend unterschiedliche Lebensbereiche.

Und genau an diesem Punkt muss zwischen zwei Aussagen unterschieden werden:

Belegt ist: Digitale Identitätsnachweise sollen in zahlreichen staatlichen und privaten Anwendungsbereichen eingesetzt werden können.

Nicht belegt ist: Dass dadurch automatisch eine zentrale staatliche Stelle sämtliche Aktivitäten eines Bürgers verfolgen kann.

Dieser Unterschied ist entscheidend.

Denn eine breite Verwendung digitaler Identität schafft nicht automatisch Überwachung. Sie schafft jedoch eine Infrastruktur, deren **technische Architektur, Zugriffsrechte und**

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

gesetzliche Grenzen darüber entscheiden, welche Kontrollmöglichkeiten tatsächlich bestehen.

4.3 Die Freiwilligkeit wird zum Prüfstein

Auf dem Papier ist die Frage zunächst klar: Die europäische Regelung enthält Schutzvorgaben für Menschen, die die Wallet nicht nutzen wollen.

Die gesellschaftlich entscheidende Frage beginnt jedoch dort, wo rechtliche Freiwilligkeit und praktische Lebenswirklichkeit auseinanderfallen könnten.

Solange ein Bürger ohne wesentliche Nachteile zwischen digitalem und analogem Weg wählen kann, bleibt die Entscheidung tatsächlich bei ihm.

Anders könnte es aussehen, wenn digitale Verfahren irgendwann erheblich schneller, günstiger oder einfacher werden oder bestimmte Dienstleistungen überwiegend auf digitale Identitätsnachweise ausgerichtet werden.

Das ist **heute kein nachgewiesener Zwang**.

Es ist ein mögliches zukünftiges Risiko.

Gerade deshalb wird der Erhalt gleichwertiger analoger Zugänge zu einer entscheidenden Frage. Dass diese Problematik nicht nur theoretisch diskutiert wird, zeigt der politische Streit: Die AfD verlangt ausdrücklich die dauerhafte gleichberechtigte Anerkennung analoger Alternativen. Auch außerhalb der Parteienpolitik gibt es Forderungen, einen faktischen oder formalen Nutzungszwang auszuschließen; der Paritätische Gesamtverband etwa begrüßt die EUDI-Wallet grundsätzlich, fordert aber unter anderem Schutz vor Exklusion, Profilbildung und faktischer Nutzungspflicht.

Deutscher Bundestag – dokumentierte Forderungen zum Erhalt analoger Alternativen

Bundestags-Lobbyregister – Stellungnahme des Paritätischen zur EUDI-Wallet

Damit verläuft die Debatte nicht einfach zwischen „Digitalisierung“ und „Digitalisierungsgegnern“. Selbst Befürworter der digitalen Infrastruktur diskutieren darüber, **welche Grenzen notwendig sind, damit aus einem freiwilligen Angebot keine praktische Voraussetzung gesellschaftlicher Teilhabe wird.**

5. Die entscheidende Schnittstelle – Wenn digitale Systeme auf Sicherheitsinteressen treffen

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

5.1 Eine digitale Infrastruktur verändert die Ausgangslage

Bis hierher ergibt sich noch kein Beweis für einen Überwachungsstaat. Aber es entsteht eine neue Ausgangslage.

Identitätsverwaltung wird digitalisiert. Staatliche Register werden modernisiert und technisch stärker miteinander vernetzt. Digitale Nachweise können in immer mehr privaten und öffentlichen Bereichen verwendet werden. Gleichzeitig besitzt der Staat Sicherheitsbehörden und Nachrichtendienste, deren Aufgabe gerade darin besteht, Informationen zu gewinnen, Gefahren zu erkennen und Bedrohungen abzuwehren.

Damit stellt sich zwangsläufig die nächste Frage:

Welche Zugriffsmöglichkeiten bestehen – und welche könnten künftig geschaffen werden?

Diese Frage lässt sich nicht allein aus der technischen Existenz einer Wallet beantworten. Entscheidend sind die jeweiligen gesetzlichen Befugnisse.

5.2 Technische Möglichkeit ist noch keine staatliche Befugnis

Dieser Unterschied ist zentral.

Dass Daten technisch vorhanden sind, bedeutet nicht automatisch, dass ein Nachrichtendienst oder eine andere Sicherheitsbehörde darauf zugreifen darf.

Dafür braucht es eine Rechtsgrundlage.

Umgekehrt bedeutet eine heute bestehende gesetzliche Grenze nicht zwangsläufig, dass diese Grenze für alle Zukunft unverändert bleibt. Sicherheitsgesetze und Befugnisse können durch parlamentarische Gesetzgebung verändert werden – allerdings nicht grenzenlos, sondern innerhalb verfassungsrechtlicher und europarechtlicher Vorgaben.

Deshalb muss eine seriöse Untersuchung drei Ebenen getrennt betrachten:

Was ist technisch möglich?

Was ist heute rechtlich erlaubt?

Welche Erweiterungen werden politisch tatsächlich gefordert oder vorbereitet?

Erst wenn diese drei Ebenen zusammengeführt werden, lässt sich beurteilen, ob aus der Digitalisierung lediglich eine modernere Verwaltungsinfrastruktur entsteht – oder ob gleichzeitig Strukturen geschaffen werden, die eines Tages wesentlich weitergehende staatliche Kontrollmöglichkeiten eröffnen könnten.

MBB
MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

5.3 Geheimdienste und Cyberabwehr: Wie weit darf der digitale Staat gehen?

Genau hier treffen die beiden großen Entwicklungen dieses Dossiers aufeinander.

Auf der einen Seite wächst die digitale Infrastruktur des Staates.

Auf der anderen Seite steht die Frage, **welche neuen Befugnisse Nachrichtendienste und Cyberabwehr erhalten sollen, um auf Spionage, Sabotage, Cyberangriffe und andere Bedrohungen reagieren zu können.**

Die entscheidende Gefahr läge nicht darin, dass digitale Identität, Gesundheitsdaten, Finanzdaten oder Verwaltungsregister überhaupt existieren.

Sie läge dort, wo unterschiedliche Datenbestände und staatliche Zugriffsrechte so miteinander verbunden würden, dass aus einzelnen Informationen ein immer umfassenderes Bild eines Menschen entstehen könnte.

Ob und in welchem Umfang eine solche Entwicklung tatsächlich stattfindet, muss für jedes System und jede Befugnis einzeln nachgewiesen werden.

6. Geheimdienste und Cyberabwehr – Der Staat erweitert seine digitalen Befugnisse

6.1 Vom Beobachten zum aktiven Eingreifen

Die Frage nach staatlicher Kontrolle bekommt eine neue Dimension, wenn digitale Infrastruktur auf Sicherheitsbehörden trifft.

Deutschland hat seine Nachrichtendienste historisch bewusst begrenzt. Das **Trennungsgebot zwischen Polizei und Nachrichtendiensten** soll einer Machtkonzentration entgegenwirken. Nachrichtendienste dürfen bereits heute heimlich Informationen beschaffen, Observationen durchführen, Bild- und Tonaufnahmen anfertigen sowie unter gesetzlichen Voraussetzungen Post- und Telekommunikation überwachen. Polizeiliche Befugnisse stehen ihnen dagegen grundsätzlich nicht zu.

Deutscher Bundestag – Aufgaben und Befugnisse der Nachrichtendienste

Im Jahr **2026** wird an dieser Sicherheitsarchitektur jedoch an mehreren Stellen gearbeitet.

Bereits am **27. Mai 2026** beschloss das Bundeskabinett den Entwurf eines Gesetzes zur Stärkung der Cybersicherheit. Vorgesehen sind zusätzliche Befugnisse für das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskriminalamt (BKA) und die Bundespolizei. Die Bundesregierung begründet dies mit einer hohen Bedrohungslage durch

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Cyberangriffe und dem Schutz staatlicher, wirtschaftlicher und gesellschaftlicher Infrastruktur.

Bundesregierung – Gesetz zur Stärkung der Cybersicherheit

Am **25. Juni 2026** erklärte Bundesinnenminister Alexander Dobrindt im Bundestag, Deutschland wolle bei der Cyberabwehr den Übergang von der bloßen Aufklärung zur aktiven Abwehr vollziehen. Cyberangriffe sollen unter bestimmten Voraussetzungen nicht nur erkannt, sondern aktiv gestört oder beendet werden können.

Bundesregierung – Rede des Bundesinnenministers zur aktiven Cyberabwehr vom 25. Juni 2026

Damit verändert sich ein Grundprinzip: Der Staat soll sich im Cyberraum nicht mehr ausschließlich schützen und Angriffe verfolgen, sondern unter bestimmten Voraussetzungen **aktiv in die technische Infrastruktur eines Angreifers eingreifen können**.

6.2 Der politische Ursprung: Die Weichen wurden früher gestellt

Auch diese Entwicklung begann nicht erst im Sommer 2026.

Der Ausbau der aktiven Cyberabwehr war bereits im **Koalitionsvertrag von CDU, CSU und SPD vom Mai 2025** angekündigt worden. Darauf wurde auch in der späteren parlamentarischen Debatte Bezug genommen.

Deutscher Bundestag – Beratung zur Cybersicherheit vom 25. Juni 2026

Damit lässt sich die politische Verantwortlichkeit zeitlich einordnen: Die schwarz-rote Bundesregierung brachte das Vorhaben 2026 in das Gesetzgebungsverfahren ein; die politische Grundentscheidung für den Ausbau aktiver Cyberabwehr war bereits Bestandteil ihres Koalitionsvertrags.

Der Regierungsentwurf sieht nach Angaben des Bundestages unter anderem Befugnisse vor, mit denen Bundesbehörden zur Abwehr schwerwiegender Cybergefahren **Daten in IT-Systemen auslesen, verändern oder löschen** und unter bestimmten Voraussetzungen Datenverkehr beeinflussen können.

Deutscher Bundestag – Gesetzentwurf zur Stärkung der Cybersicherheit

Die Bundesregierung argumentiert, dass Cyberangriffe auf kritische Infrastruktur, Unternehmen und staatliche Einrichtungen inzwischen geeignet seien, das Gemeinwesen, die Wirtschaft sowie Staat und Verwaltung erheblich und dauerhaft zu beeinträchtigen.

Das Sicherheitsargument ist damit klar dokumentiert.

Ebenso klar ist aber: **Mit neuen technischen Gefahren wachsen gleichzeitig die staatlichen Eingriffsmöglichkeiten.**

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Ja. **Das war mein Fehler.** Ich habe dir erst gesagt, du sollst den alten Abschnitt komplett ersetzen – damit war der Link natürlich weg – und danach habe ich dir unsinnigerweise geschrieben, du solltest den „vorhandenen Link“ wieder einsetzen. Den konntest du gar nicht mehr haben.

Ich habe die Quelle deshalb jetzt **neu beim Deutschen Bundestag gesucht und den Link geprüft**. Hier ist **6.3 vollständig und übernahmefertig mit echtem Link**:

6.3 Die Opposition widerspricht – aber nicht einheitlich

Die geplanten Befugnisse sind politisch umstritten.

Am **25. Juni 2026** beriet der Deutsche Bundestag in erster Lesung den Regierungsentwurf zur Stärkung der Cybersicherheit. Gleichzeitig wurde ein Antrag der Fraktion Die Linke mit dem Titel **„Gegen die Einführung von Hackbacks und offensiver Cyberabwehr“** beraten. Beide Vorlagen wurden anschließend zur weiteren Beratung an die Ausschüsse überwiesen; federführend ist der Innenausschuss.

Der Antrag der Linken richtete sich insbesondere gegen Befugnisse, die es dem Bundeskriminalamt und der Bundespolizei ermöglichen sollen, zur Abwehr von Cybergefahren ohne Wissen der Betroffenen in IT-Systeme einzugreifen und dort Daten auszulesen, zu verändern oder zu löschen. Kritisiert wurden außerdem mögliche Eingriffe in fremde staatliche IT-Infrastrukturen sowie nach Auffassung der Antragsteller unzureichende richterliche und parlamentarische Kontrollmechanismen.

Quelle:
Deutscher Bundestag – Regierungsentwurf zur Stärkung der Cybersicherheit beraten, 25. Juni 2026

Damit zeigt sich, dass die politische Auseinandersetzung nicht allein um die Notwendigkeit einer wirksamen Cyberabwehr geführt wird. Der Konflikt betrifft ebenso die Frage, **welche Eingriffsmöglichkeiten der Staat erhalten soll, unter welchen Voraussetzungen sie eingesetzt werden dürfen und wie ihr Einsatz kontrolliert wird.**

Eine pauschale Gegenüberstellung von „Regierung“ und „Opposition“ greift dabei zu kurz. Der konkrete Gegenantrag gegen Hackbacks und offensive Cyberabwehr stammte von der **Fraktion Die Linke**. Die Bundestagsdebatte selbst umfasste dagegen Beiträge aus mehreren Fraktionen.

Entscheidend für die politische Einordnung ist deshalb die konkrete parlamentarische Position: **Welche Befugnisse werden unterstützt, welche abgelehnt und welche Kontrollmechanismen werden verlangt?**

Das kannst du jetzt komplett als 6.3 einsetzen. Der Quellenlink ist diesmal tatsächlich drin und geprüft.

6.4 Nachrichtendienste: Eine weitere Verschiebung der Grenzen

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Parallel zur Cyberabwehr von Polizei und BSI steht im August 2026 eine noch weiterreichende Reform im Raum: **BND und Bundesamt für Verfassungsschutz sollen zusätzliche operative Befugnisse erhalten.**

Nach aktuellen Berichten hat das Bundeskabinett am **12. August 2026** eine umfassende Reform der Nachrichtendienstgesetze beschlossen. Vorgesehen sind demnach unter anderem zusätzliche digitale Überwachungs- und Eingriffsbefugnisse sowie aktive Maßnahmen des BND gegen ausländische IT-Systeme bei laufenden Cyberangriffen. Die Entwürfe müssen noch das parlamentarische Gesetzgebungsverfahren durchlaufen.

Hier ist die zeitliche Einordnung entscheidend:

Diese neuen Befugnisse sind am 12. August 2026 noch nicht geltendes Recht.

Das Kabinett hat Gesetzentwürfe beschlossen. Über deren endgültige Ausgestaltung entscheidet anschließend der Gesetzgeber.

Die politische Bedeutung ist dennoch erheblich. Denn damit wird über eine Ausweitung genau jener staatlichen Befugnisse diskutiert, die für die Gesamtfrage dieses Dossiers entscheidend sind:

Wie weit darf ein Nachrichtendienst bei der digitalen Informationsbeschaffung und Gefahrenabwehr gehen?

6.5 Mehr Befugnisse – aber auch mehr Kontrolle?

Eine Erweiterung geheimdienstlicher Befugnisse bedeutet nicht automatisch den Wegfall rechtsstaatlicher Kontrolle.

Gerade wegen der erheblichen Grundrechtseingriffe existieren besondere Kontrollmechanismen. Der Bundestag weist darauf hin, dass nachrichtendienstliche Maßnahmen unter anderem das Fernmeldegeheimnis, die Unverletzlichkeit der Wohnung und das Recht auf informationelle Selbstbestimmung berühren können.

Deutscher Bundestag – Parlamentarische Kontrolle der Nachrichtendienste

Die entscheidende Frage lautet deshalb nicht nur, **ob Kontrollorgane existieren**, sondern wie wirksam diese Kontrolle tatsächlich ausgestaltet ist: Welche Maßnahmen benötigen eine vorherige Genehmigung? Welche werden erst nachträglich kontrolliert? Welche Informationen erhalten die Kontrollorgane? Und welche Möglichkeiten besitzen sie, rechtswidrige Maßnahmen zu verhindern oder aufzuklären?

Mehr Befugnisse verlangen mehr Kontrolle. Ob beides tatsächlich im gleichen Maße wächst, muss an den konkreten gesetzlichen Regelungen gemessen werden.

6.6 Wo die eigentliche Gefahr beginnt

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Deutschland baut digitale Verwaltungs- und Identitätsinfrastrukturen aus. Gleichzeitig sollen Sicherheitsbehörden und Nachrichtendienste zusätzliche technische Fähigkeiten erhalten.

Daraus folgt nicht automatisch, dass diese Systeme miteinander verbunden werden.

Für einen Zugriff von Sicherheitsbehörden auf bestimmte Datenbestände braucht es entsprechende gesetzliche Befugnisse. Die bloße Existenz einer EUDI-Wallet, einer elektronischen Patientenakte oder eines staatlichen Registers schafft noch keinen automatischen Geheimdienstzugriff.

Aber die Risikofrage verschiebt sich.

Je mehr gesellschaftlich relevante Informationen digital verarbeitet werden, desto wichtiger wird die Frage, **welche gesetzlichen Zugriffsmöglichkeiten auf diese Informationen heute bestehen und welche morgen geschaffen werden könnten.**

Die langfristige Gefahr liegt deshalb nicht zwingend darin, dass heute bereits sämtliche Daten zentral zusammenlaufen.

Sie könnte darin liegen, dass **immer mehr digital nutzbare Datenbestände und gleichzeitig immer leistungsfähigere staatliche Zugriffsinstrumente entstehen.**

Ob daraus tatsächlich ein umfassender Kontrollapparat werden kann, entscheidet sich nicht allein an der Technik.

Es entscheidet sich an **Gesetzen, Zugriffsrechten, politischen Mehrheiten und wirksamer Kontrolle.**

7. Gesundheit wird digital – Die elektronische Patientenakte als nächster Datenraum

7.1 Gesundheitsdaten gehören zu den sensibelsten Informationen eines Menschen

Bei kaum einem anderen digitalen Bereich wird die Frage nach Datenschutz und staatlichen Zugriffsmöglichkeiten so unmittelbar wie bei Gesundheitsdaten.

Diagnosen, Medikamente, Behandlungen, Krankenhausaufenthalte und medizinische Befunde können Informationen enthalten, die einen Menschen sein gesamtes Leben begleiten.

Mit der **elektronischen Patientenakte (ePA)** hat Deutschland begonnen, einen großen Teil dieser Informationen digital verfügbar zu machen. Die „ePA für alle“ wurde 2025 eingeführt und anschließend weiter in die medizinische Versorgung integriert.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Bundesregierung – Informationen zur Einführung der ePA für alle

Die entscheidende Frage lautet deshalb auch hier nicht lediglich:

Ist Digitalisierung praktisch?

Sondern:

Welche Daten entstehen, wo werden sie gespeichert, wer erhält Zugriff – und welche Grenzen schützen sie vor einer Verwendung außerhalb der medizinischen Versorgung?

7.2 Die Gesundheitsakte ist nicht die Bürger-ID

Dabei muss eine wichtige Trennung erhalten bleiben.

Die elektronische Patientenakte, die EUDI-Wallet und staatliche Identitätsregister sind **unterschiedliche Systeme mit unterschiedlichen Rechtsgrundlagen und Zwecken**.

Ihre bloße gleichzeitige Existenz bedeutet nicht, dass sämtliche darin enthaltenen Informationen automatisch miteinander verbunden werden.

Gerade deshalb muss jede behauptete Schnittstelle einzeln nachgewiesen werden.

Erst wenn feststeht, **welches System tatsächlich mit welchem anderen System kommuniziert, welche Identifikatoren dabei verwendet werden und welche Rechtsgrundlage den Datenaustausch erlaubt**, darf aus technischer Nähe eine tatsächliche Verbindung abgeleitet werden.

Genau diese Prüfung ist bei Gesundheitsdaten besonders wichtig.

Denn die entscheidende Frage lautet nicht, wie viele digitale Systeme Deutschland besitzt.

Sie lautet:

Was geschieht, wenn aus einzelnen digitalen Systemen irgendwann ein miteinander vernetzbares Gesamtgefüge wird?

7.3 Die DSGVO als Schutzwall – und wo ihre Grenzen liegen

Mit der zunehmenden Digitalisierung von Gesundheitsdaten verschwindet der Datenschutz nicht. Im Gegenteil: Die **Datenschutz-Grundverordnung (DSGVO)** gilt auch für die elektronische Patientenakte. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit weist ausdrücklich darauf hin, dass Versicherte bei der Verarbeitung ihrer Daten in der ePA die Betroffenenrechte der DSGVO besitzen. Dazu gehören unter anderem Auskunfts-, Berichtigungs- und Löschungsrechte.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

DSGVO – vollständiger Rechtstext bei EUR-Lex

Bundesdatenschutzbeauftragte – Datenschutz und Rechte bei der ePA

Gerade Gesundheitsdaten genießen einen besonderen Schutz. Artikel 9 DSGVO zählt Gesundheitsdaten zu den **besonderen Kategorien personenbezogener Daten**. Ihre Verarbeitung ist grundsätzlich untersagt, sofern nicht eine der ausdrücklich geregelten Ausnahmen greift.

Doch genau an dieser Stelle wird die Frage nach den Grenzen des Datenschutzes wichtig. Die DSGVO bedeutet nicht, dass personenbezogene Daten ausschließlich mit individueller Einwilligung verarbeitet werden dürfen. Artikel 6 erlaubt eine Verarbeitung unter bestimmten Voraussetzungen beispielsweise auch zur Erfüllung einer gesetzlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse beziehungsweise in Ausübung öffentlicher Gewalt. Für besonders geschützte Daten enthält Artikel 9 zusätzliche Voraussetzungen und Ausnahmen.

Auch die Rechte der Betroffenen sind nicht unter allen Umständen absolut. Artikel 23 DSGVO ermöglicht dem europäischen oder nationalen Gesetzgeber unter bestimmten Voraussetzungen Beschränkungen einzelner Datenschutzrechte – unter anderem zum Schutz der **nationalen Sicherheit**, der öffentlichen Sicherheit sowie zur Verhütung, Ermittlung und Verfolgung von Straftaten. Solche Beschränkungen müssen den Wesensgehalt der Grundrechte achten sowie notwendig und verhältnismäßig sein.

Damit liegt der entscheidende Punkt nicht darin, dass die DSGVO durch die Digitalisierung einfach „aufgegeben“ würde. Die wichtigere Frage lautet:

Wie weit trägt der bestehende Datenschutz noch, wenn immer größere Mengen sensibler Daten digital verarbeitet werden und der Gesetzgeber gleichzeitig Ausnahmen und staatliche Zugriffsrechte festlegen kann?

Dass diese Frage keine theoretische Spielerei ist, zeigt die Datenschutzaufsicht selbst. Die Bundesdatenschutzbeauftragte warnte 2024 die Kranken- und Pflegekassen ausdrücklich vor einer aus ihrer Sicht unzulässigen Absenkung des Sicherheitsniveaus beim Zugriff auf die elektronische Patientenakte. Gegenstand war die konkrete Ausgestaltung neuer gesetzlicher Regelungen im Gesundheitswesen.

BfDI – Warnung zum Sicherheitsniveau beim Zugriff auf die ePA

Damit zeigt sich ein grundlegender Konflikt der digitalen Transformation: **Datenschutzrecht und Digitalisierung existieren nebeneinander – aber die konkrete Stärke des Datenschutzes entscheidet sich an Gesetzen, technischen Schutzmaßnahmen, Zugriffsrechten und deren tatsächlicher Durchsetzung.**

Je sensibler die Daten und je größer ihre digitale Verfügbarkeit, desto entscheidender wird deshalb die Frage, ob die bestehenden Schutzmechanismen mit den wachsenden technischen Möglichkeiten Schritt halten.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

7.4 Die ePA für alle – freiwillig, aber automatisch angelegt

Mit der Einführung der **„ePA für alle“** hat sich das bisherige Prinzip der elektronischen Patientenakte grundlegend verändert. Seit dem **15. Januar 2025** stellen die gesetzlichen Krankenkassen ihren Versicherten grundsätzlich automatisch eine elektronische Patientenakte bereit, sofern diese nicht widersprechen. Die ePA wurde damit von einer aktiv zu beantragenden Anwendung zu einem **Opt-out-System**.

Bundesgesundheitsministerium – Die ePA für alle

Bundesgesundheitsministerium – Fragen und Antworten zum Digital-Gesetz

Die politische Grundlage dafür wurde in der vorherigen Legislaturperiode geschaffen. Das **Digital-Gesetz (DigiG)** wurde unter der damaligen Bundesregierung aus SPD, Bündnis 90/Die Grünen und FDP auf den Weg gebracht. Ein zentrales Ziel war, die Nutzung der elektronischen Patientenakte erheblich auszuweiten und ihre Befüllung sowie den Zugriff im Behandlungsalltag zu vereinfachen.

Freiwilligkeit bedeutet seitdem nicht mehr, dass Versicherte die ePA zunächst selbst beantragen müssen. Wer keine ePA möchte, muss widersprechen. Dieser Widerspruch ist nach Angaben des Bundesgesundheitsministeriums auch nach Einrichtung der Akte jederzeit möglich.

Seit dem **1. Oktober 2025** sind Leistungserbringer verpflichtet, die ePA zu nutzen und bestimmte gesetzlich vorgesehene Daten aus der Behandlung einzustellen. Dazu gehören beispielsweise Befunde und Arztbriefe. Versicherte besitzen weiterhin Widerspruchs- und Steuerungsmöglichkeiten.

Damit wurde ein bemerkenswerter Systemwechsel vollzogen:

Nicht mehr der Bürger muss sich für die digitale Patientenakte entscheiden. Sie wird grundsätzlich eingerichtet – der Bürger muss sich entscheiden, wenn er sie nicht haben möchte.

7.5 Gesundheitsdaten für Forschung – der zweite Opt-out

Die Digitalisierung endet nicht bei der medizinischen Behandlung.

Gesundheitsdaten aus der ePA sollen künftig auch für **Forschung, Verbesserung der Versorgungsqualität und -sicherheit sowie für statistische Zwecke der Gesundheitsberichterstattung** genutzt werden können. Nach Angaben des Bundesgesundheitsministeriums sollen die Daten dafür pseudonymisiert an das **Forschungsdatenzentrum Gesundheit (FDZ)** beim Bundesinstitut für Arzneimittel und Medizinprodukte übermittelt werden. Versicherte können dieser Weitergabe widersprechen und ihre ePA trotzdem weiter nutzen.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Bundesgesundheitsministerium – Forschungsdatenzentrum Gesundheit

Das Bundesgesundheitsministerium beschreibt die Entwicklung ausdrücklich als zunehmende Verknüpfung unterschiedlicher Gesundheitsdaten. Das FDZ verfügt bereits über Abrechnungsdaten gesetzlich Versicherter. Perspektivisch sollen weitere Datenquellen hinzukommen und miteinander verknüpft werden können.

Das **Gesundheitsdatennutzungsgesetz (GDNG)** schuf hierfür wichtige rechtliche Grundlagen. Nach Darstellung des Bundesgesundheitsministeriums wurde damit unter anderem eine zentrale Datenzugangs- und Koordinierungsstelle vorgesehen und die Möglichkeit geschaffen, Daten aus verschiedenen Quellen für zulässige Zwecke miteinander zu verknüpfen. Auch für die Bereitstellung von ePA-Daten zu Forschungszwecken wurde das Opt-out-Prinzip vorgesehen.

Bundesgesundheitsministerium – Gesundheitsdaten für Forschung und Versorgung

Damit existieren zwei voneinander zu unterscheidende Entscheidungen:

Wer die ePA insgesamt nicht möchte, kann ihrer Einrichtung beziehungsweise Nutzung widersprechen.

Wer die ePA nutzen, seine Daten aber nicht für die vorgesehenen Forschungszwecke bereitstellen möchte, kann dieser Datenübermittlung gesondert widersprechen.

Die Daten sollen dabei nicht frei an interessierte Unternehmen oder Forschungseinrichtungen herausgegeben werden. Nach Angaben des Bundesgesundheitsministeriums müssen Nutzungsanträge vom FDZ geprüft werden; die Verarbeitung erfolgt in einer sicheren Umgebung. Personenbezogene Daten sollen diese Umgebung nicht verlassen.

Das ist die geltende Schutzarchitektur.

Gleichzeitig entsteht damit ein immer umfangreicherer staatlich regulierter Gesundheitsdatenraum, in dem Daten nicht mehr ausschließlich für die unmittelbare Behandlung des einzelnen Patienten verwendet werden.

7.6 2026: Der nächste Schritt zum vernetzten Gesundheitsdatenökosystem

Die Entwicklung geht weiter.

Am **15. Juli 2026** beschloss das Bundeskabinett den Entwurf des **Gesetzes für Daten und digitale Innovation im Gesundheitswesen (GeDIG)**. Das Bundesgesundheitsministerium beschreibt das Ziel ausdrücklich als ein modernes und **„vernetztes Gesundheitswesen“**. Die Möglichkeiten zur Nutzung von Gesundheitsdaten für Versorgung, Forschung und Innovation sollen weiter ausgebaut werden.

Bundesgesundheitsministerium – Kabinettsbeschluss zum GeDIG vom 15. Juli 2026

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Besonders weitreichend ist das langfristige Zielbild. Bestehende und im Aufbau befindliche Strukturen sollen nach Angaben des Ministeriums zu einem **europäisch anschlussfähigen, vernetzten Gesundheitsdatenökosystem** weiterentwickelt werden. Dabei spielt auch der **Europäische Gesundheitsdatenraum (EHDS)** eine zentrale Rolle.

Das Ministerium nennt ausdrücklich das Zusammenspiel von **ePA und Forschungsdatenzentrum Gesundheit**. Gesundheitsdaten sollen auf dieser Grundlage künftig EHDS-konform bereitgestellt werden können. Gleichzeitig sollen weitere vorhandene Infrastrukturen als Zugangsstellen für Gesundheitsdaten in dieses System einbezogen werden.

Damit lässt sich eine Entwicklung inzwischen anhand offizieller Dokumente nachvollziehen:

ePA → Forschungsdatenzentrum → Verknüpfung weiterer Datenquellen → Europäischer Gesundheitsdatenraum.

Das ist keine hypothetische Abfolge, die diesem Dossier zugrunde gelegt wird. Der Aufbau eines vernetzten Gesundheitsdatenökosystems ist erklärtes politisches Ziel.

Die entscheidende Frage liegt deshalb erneut nicht darin, Digitalisierung grundsätzlich als Überwachung zu bezeichnen.

Sie lautet vielmehr:

Wie verändert sich die informationelle Selbstbestimmung des Einzelnen, wenn Gesundheitsdaten zunehmend nicht mehr nur für seine eigene Behandlung, sondern innerhalb immer größerer nationaler und europäischer Datenstrukturen verarbeitet werden können?

7.7 Wer darf heute auf die ePA zugreifen?

Bei dieser Frage ist eine klare Grenze notwendig.

Nach der geltenden Regelung dürfen nicht beliebige staatliche Stellen, Versicherungen oder Unternehmen auf die medizinischen Daten eines Versicherten zugreifen. Das Bundesgesundheitsministerium erklärt, dass der Zugriff auf medizinische Daten der ePA grundsätzlich der medizinischen Versorgung dient und einem gesetzlich festgelegten Kreis von Leistungserbringern vorbehalten ist.

Bundesgesundheitsministerium – Zugriffsrechte und Schutz medizinischer Daten

Die Zugriffe werden zudem protokolliert. Versicherte können über die ePA nachvollziehen, wer auf ihre Daten zugegriffen hat, und Zugriffsrechte beschränken.

Ein allgemeiner Zugriff von Nachrichtendiensten auf die elektronische Patientenakte lässt sich daraus nicht ableiten.

Genau diese Grenze ist für die weitere Untersuchung entscheidend.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Denn wenn dieses Dossier mögliche Gefahren einer vernetzten digitalen Infrastruktur untersucht, muss es gleichzeitig dokumentieren, **wo das geltende Recht solche Verbindungen gerade nicht zulässt**.

Erst dann kann die entscheidende Zukunftsfrage seriös gestellt werden:

Welche dieser Grenzen sind technisch abgesichert – und welche beruhen letztlich auf gesetzlichen Regeln, die ein zukünftiger Gesetzgeber verändern könnte?

8. Der Europäische Gesundheitsdatenraum – Wenn Gesundheitsdaten Grenzen überschreiten

8.1 Der EHDS: Aus nationalen Gesundheitsdaten wird europäische Infrastruktur

Die Digitalisierung des Gesundheitswesens endet nicht an der deutschen Grenze.

Mit der **Verordnung (EU) 2025/327** haben Europäisches Parlament und Rat den **European Health Data Space (EHDS)** geschaffen. Die Verordnung wurde am **5. März 2025** im Amtsblatt der Europäischen Union veröffentlicht und trat am **26. März 2025** in Kraft. Die praktische Anwendung erfolgt schrittweise über mehrere Jahre.

EU-Verordnung 2025/327 – vollständiger Rechtstext bei EUR-Lex

EU-Kommission – Europäischer Gesundheitsdatenraum und Zeitplan

Der EHDS verfolgt zwei unterschiedliche Ziele.

Die **Primärnutzung** betrifft die medizinische Versorgung des Patienten. Elektronische Gesundheitsdaten sollen innerhalb der Europäischen Union leichter verfügbar und grenzüberschreitend nutzbar werden.

Die **Sekundärnutzung** geht darüber hinaus. Gesundheitsdaten sollen unter gesetzlich festgelegten Voraussetzungen auch für **Forschung, Innovation, Politikgestaltung, Regulierung, öffentliche Gesundheit und weitere festgelegte Zwecke** genutzt werden können.

Damit entsteht erstmals ein gemeinsamer europäischer Rechts- und Infrastrukturrahmen, der nicht nur den Austausch von Gesundheitsdaten für die Behandlung organisiert, sondern ausdrücklich auch deren **Weiterverwendung für andere gesetzlich definierte Zwecke** ermöglicht.

8.2 Der Zeitplan: 2029 und 2031 werden entscheidend

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Der EHDS wird nicht mit einem einzigen Stichtag vollständig eingeführt.

Die Europäische Kommission nennt einen mehrstufigen Zeitplan. Bis **März 2027** sollen wichtige Durchführungsrechtsakte vorliegen. Ab **März 2029** sollen wesentliche Teile der Verordnung praktisch angewendet werden. Dazu gehören für die grenzüberschreitende medizinische Versorgung zunächst Patientenkurzakten sowie elektronische Verschreibungen und Abgaben von Arzneimitteln. Gleichzeitig beginnen die Regeln zur Sekundärnutzung für einen großen Teil der vorgesehenen Datenkategorien zu greifen.

Ab **März 2031** soll die grenzüberschreitende Nutzung um weitere besonders aussagekräftige Datenkategorien erweitert werden. Dazu gehören **medizinische Bilder, Laborergebnisse und Krankenhausentlassungsberichte**. Auch weitere Kategorien für die Sekundärnutzung, darunter genomische Daten, sollen dann erfasst werden.

Damit lässt sich die Entwicklung zeitlich klar einordnen:

2025: Die rechtliche Grundlage tritt in Kraft.

2027: Zentrale technische und organisatorische Detailregeln sollen feststehen.

2029: Wesentliche Teile der grenzüberschreitenden Primär- und Sekundärnutzung beginnen.

2031: Weitere Gesundheitsdatenkategorien kommen hinzu.

2035: Auch Drittländer und internationale Organisationen können eine Teilnahme an **HealthData@EU** für die Sekundärnutzung beantragen.

Das ist keine Zukunftsprognose. **Dieser schrittweise Aufbau ist Bestandteil des offiziellen europäischen Umsetzungsplans.**

8.3 Primärnutzung: Die Patientenakte wird europäisch anschlussfähig

Für Patienten kann der grenzüberschreitende Datenaustausch erhebliche praktische Vorteile haben.

Wer beispielsweise im EU-Ausland medizinisch behandelt wird, soll relevante elektronische Gesundheitsinformationen leichter verfügbar machen können. Behandelnde Ärzte sollen dadurch schneller auf notwendige Informationen zugreifen können, während Patienten ihre Daten in einem einheitlichen europäischen Format erhalten und einsehen können.

Gleichzeitig erhält der Bürger nach der EHDS-Verordnung Kontrollrechte. Dazu gehören unter anderem Möglichkeiten, den Zugriff auf bestimmte Teile elektronischer Gesundheitsdaten einzuschränken, nachzuvollziehen, wer auf Daten zugegriffen hat, und fehlerhafte Informationen berichtigen zu lassen.

Der EHDS ist damit nicht als schrankenloser europäischer Gesundheitsdatenspeicher konzipiert.

Aber die Richtung ist eindeutig: **Nationale Gesundheitsdaten sollen technisch und rechtlich europäisch interoperabel werden.**

8.4 Sekundärnutzung: Gesundheitsdaten bekommen einen zweiten Zweck

Der wesentlich weiterreichende Teil des EHDS betrifft die **Sekundärnutzung**.

Gesundheitsdaten, die ursprünglich beispielsweise im Zusammenhang mit einer medizinischen Behandlung entstanden sind, können unter den Voraussetzungen der EHDS-Verordnung für andere festgelegte Zwecke weiterverwendet werden. Dazu zählen unter anderem wissenschaftliche Forschung, Innovation, öffentliche Gesundheit, Politikgestaltung und regulatorische Tätigkeiten.

EU-Kommission – Regeln zur Weiterverwendung von Gesundheitsdaten

Der Zugang erfolgt dabei nicht frei.

Vorgesehen sind spezielle **Health Data Access Bodies – Gesundheitsdatenzugangsstellen**. Für die genehmigungspflichtige Sekundärnutzung muss grundsätzlich eine entsprechende Zugangsgenehmigung vorliegen. Hinzu kommen Vorgaben zu Datenminimierung, Pseudonymisierung beziehungsweise Anonymisierung sowie zur Verarbeitung in besonders geschützten Datenverarbeitungsumgebungen.

Gleichzeitig werden bestimmte Nutzungen ausdrücklich verboten. Gesundheitsdaten dürfen beispielsweise nicht für Marketingzwecke oder für Entscheidungen verwendet werden, die dem betroffenen Menschen aufgrund seiner Gesundheitsinformationen schaden.

Damit entsteht ein entscheidender Unterschied zur klassischen Patientenakte:

Gesundheitsdaten dienen künftig nicht mehr ausschließlich der konkreten Behandlung des Menschen, bei dem sie entstanden sind. Unter gesetzlichen Voraussetzungen können sie Teil eines wesentlich größeren Forschungs-, Innovations- und Politikdatenraums werden.

8.5 Das Widerspruchsrecht – und der Anspruch auf Auskunft

Für die Sekundärnutzung elektronischer Gesundheitsdaten sieht der Europäische Gesundheitsdatenraum grundsätzlich ein **Opt-out-Recht** vor. Nach Artikel 71 der EHDS-Verordnung können natürliche Personen der Verarbeitung ihrer personenbezogenen elektronischen Gesundheitsdaten für Sekundärzwecke widersprechen.

EU-Verordnung 2025/327 – EHDS, Artikel 71

Ein solcher Widerspruch sollte jedoch nicht bei einem einfachen Satz wie „Ich widerspreche der Nutzung meiner Daten“ enden.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Wer seine Gesundheitsdaten schützen will, sollte zugleich **Auskunft darüber verlangen, was mit seinen Daten bereits geschehen ist**.

Artikel 15 DSGVO gibt Betroffenen ein umfassendes Auskunftsrecht. Danach können sie insbesondere erfahren, ob personenbezogene Daten verarbeitet werden, zu welchen Zwecken dies geschieht, welche Kategorien von Daten betroffen sind, an welche Empfänger oder Empfängerkategorien Daten weitergegeben wurden und – soweit möglich – wie lange sie gespeichert werden. Die Bundesdatenschutzbeauftragte weist darauf hin, dass dieses Auskunftsrecht grundsätzlich kostenlos und ohne besondere Begründung geltend gemacht werden kann.

DSGVO – Artikel 15: Auskunftsrecht

Bundesdatenschutzbeauftragte – Das Recht auf Auskunft nach Artikel 15 DSGVO

Damit sollte sich ein Widerspruch nicht nur auf die Zukunft richten.

Der Betroffene kann zusätzlich konkret Auskunft verlangen:

Welche personenbezogenen Gesundheitsdaten wurden bislang verarbeitet?

Für welche Zwecke wurden sie verarbeitet?

Welche Daten wurden bereits für Forschung, Statistik, Gesundheitsplanung oder andere Sekundärzwecke bereitgestellt oder übermittelt?

Wann geschah dies?

An welche konkreten Empfänger oder Empfängerkategorien wurden Daten weitergegeben?

Auf welcher gesetzlichen Rechtsgrundlage erfolgte die jeweilige Verarbeitung oder Übermittlung?

Wie lange werden die Daten beziehungsweise daraus erzeugte Datensätze gespeichert?

Welche Verarbeitungsvorgänge wurden nach Eingang des Widerspruchs fortgesetzt?

Gerade der letzte Punkt ist entscheidend.

Denn das Opt-out-Recht des EHDS bedeutet nicht automatisch, dass mit Eingang eines Widerspruchs **jede denkbare Verarbeitung von Gesundheitsdaten endet**. Die EHDS-Regelung enthält für bestimmte gesetzlich definierte Fälle Möglichkeiten, Daten trotz eines Opt-outs weiterzuverarbeiten; auch andere gesetzliche Melde- oder Verarbeitungspflichten werden durch das EHDS-Opt-out nicht automatisch aufgehoben. Die Europäische Kommission weist ausdrücklich darauf hin, dass ein Opt-out von der Sekundärnutzung andere gesetzliche Meldepflichten unberührt lassen kann.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Deshalb sollte der Bürger ausdrücklich verlangen, dass ihm **schriftlich und konkret mitgeteilt wird, welche Daten trotz seines Widerspruchs weiterhin verarbeitet werden, zu welchem Zweck dies geschieht und auf welche Rechtsgrundlage sich diese Weiterverarbeitung stützt**.

Ein vollständiges Auskunftsverlangen sollte deshalb sinngemäß folgende Punkte umfassen:

„Bitte teilen Sie mir schriftlich mit, ob und welche meiner personenbezogenen Gesundheitsdaten bereits verarbeitet, übermittelt, bereitgestellt oder für Sekundärzwecke genutzt wurden. Ich verlange insbesondere Auskunft über Art und Umfang der Daten, den jeweiligen Verarbeitungszweck, den Zeitpunkt der Verarbeitung oder Weitergabe, sämtliche Empfänger beziehungsweise Empfängerkategorien sowie die jeweils zugrunde liegende Rechtsgrundlage.

Bitte teilen Sie mir außerdem ausdrücklich mit, welche Verarbeitung meiner Daten nach Eingang und Wirksamwerden meines Widerspruchs weiterhin erfolgt oder künftig erfolgen soll. Für jede trotz meines Widerspruchs fortgesetzte Verarbeitung verlange ich die konkrete Benennung der betroffenen Daten, des Zwecks, der Empfänger und der gesetzlichen Rechtsgrundlage.

Bitte bestätigen Sie mir ferner schriftlich den Eingang, das Datum und die technische Umsetzung meines Widerspruchs.“

Damit wird aus dem Widerspruch mehr als eine bloße Willenserklärung.

Der Bürger verlangt zugleich **Transparenz darüber, was vor seinem Widerspruch mit seinen Daten geschehen ist – und was trotz seines Widerspruchs weiterhin mit ihnen geschieht.**

Genau diese Transparenz ist entscheidend. Denn ein Widerspruch ist nur dann praktisch überprüfbar, wenn der Betroffene anschließend nachvollziehen kann, **welche Datenverarbeitung tatsächlich beendet wurde und welche aufgrund gesetzlicher Ausnahmen fortgesetzt wird.**

Für weitergehende Widerspruchsschreiben und Muster stellt KLARTEXT zusätzlich eine eigene Sammlung mit Vorlagen bereit. Die Seite enthält kostenlose Musterbriefe und ein Widerspruchshandbuch.

KLARTEXT – Widerspruch einlegen: Musterbriefe und Vorlagen

8.6 DSGVO und EHDS: Datenschutz bleibt – aber der Rechtsrahmen wird erweitert

Der EHDS ersetzt die **Datenschutz-Grundverordnung (DSGVO)** nicht.

Gesundheitsdaten bleiben besonders geschützte personenbezogene Daten. Gleichzeitig schafft die EHDS-Verordnung einen zusätzlichen spezialgesetzlichen Rahmen dafür, unter welchen

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Voraussetzungen elektronische Gesundheitsdaten innerhalb des europäischen Gesundheitsdatenraums verarbeitet und weiterverwendet werden können.

Das macht einen grundlegenden Punkt sichtbar:

Datenschutz bedeutet nicht automatisch, dass Daten ausschließlich mit individueller Zustimmung verarbeitet werden dürfen.

Entscheidend ist die jeweilige gesetzliche Rechtsgrundlage.

Damit verschiebt sich die Diskussion von der einfachen Frage **„Habe ich zugestimmt?“** zu einer wesentlich komplexeren Frage:

Welche Verarbeitung erlaubt das Gesetz auch ohne meine ausdrückliche Einwilligung – und welche Widerspruchsmöglichkeiten bleiben mir?

Gerade bei Gesundheitsdaten ist diese Unterscheidung von erheblicher Bedeutung.

8.7 Vom deutschen Patienten zum europäischen Gesundheitsdatensatz

Betrachtet man ePA, Forschungsdatenzentrum und EHDS gemeinsam, wird die Richtung der Entwicklung sichtbar.

Gesundheitsinformationen werden zunehmend digital verfügbar. Nationale Dateninfrastrukturen werden ausgebaut. Gleichzeitig entsteht auf europäischer Ebene ein Rechts- und Technikrahmen, der den grenzüberschreitenden Austausch und die Sekundärnutzung elektronischer Gesundheitsdaten ermöglichen soll.

Die EU bezeichnet den EHDS selbst als den **ersten gemeinsamen europäischen Datenraum für einen bestimmten Wirtschafts- und Gesellschaftssektor** im Rahmen ihrer Datenstrategie.

Damit geht es nicht mehr lediglich um eine elektronische Patientenakte auf dem Smartphone.

Es entsteht eine Infrastruktur, in der Gesundheitsdaten **national und grenzüberschreitend nutzbar, interoperabel und unter bestimmten Voraussetzungen für weitere Zwecke zugänglich** werden.

Das bedeutet nicht, dass damit automatisch ein Überwachungsapparat entsteht.

Aber es verändert die Dimension der möglichen Datenverarbeitung erheblich.

Die entscheidende Frage lautet deshalb:

Wer bestimmt langfristig darüber, für welche Zwecke Gesundheitsdaten verwendet werden dürfen – der einzelne Bürger oder zunehmend der Gesetzgeber, der die zulässigen Zwecke und Ausnahmen definiert?

Und genau an diesem Punkt wird das Widerspruchsrecht zu mehr als einer Formalität.

Es wird zu einem entscheidenden Prüfstein dafür, **wie viel tatsächliche Kontrolle der Bürger über seine sensibelsten Daten in einem zunehmend vernetzten europäischen Gesundheitssystem behält.**

8.8 Pseudonymisiert bedeutet nicht anonym

Bei der Diskussion über Gesundheitsdaten werden zwei Begriffe häufig miteinander verwechselt: **Anonymisierung und Pseudonymisierung**. Der Unterschied ist erheblich.

Bei pseudonymisierten Daten werden unmittelbar identifizierende Merkmale durch ein Pseudonym ersetzt. Die Informationen bleiben jedoch personenbezogene Daten, solange eine Zuordnung zu einer Person mit zusätzlichen Informationen möglich ist. Die EHDS-Verordnung sieht für die Sekundärnutzung sowohl anonymisierte als auch pseudonymisierte Daten vor. Auf pseudonymisierte Daten soll nur dann zurückgegriffen werden, wenn anonymisierte Daten für den genehmigten Zweck nicht ausreichen.

EHDS-Verordnung – vollständiger Rechtstext bei EUR-Lex

Der Zugang erfolgt dabei nicht beliebig. Für die Sekundärnutzung ist grundsätzlich eine Genehmigung der zuständigen **Gesundheitsdatenzugangsstelle** erforderlich. Die Verarbeitung soll in einer besonders gesicherten Verarbeitungsumgebung stattfinden; personenbezogene Daten dürfen daraus nicht einfach heruntergeladen werden.

Die Unterscheidung zwischen anonym und pseudonymisiert ist dennoch entscheidend.

Pseudonymisiert bedeutet nicht: Die Daten haben keinen Personenbezug mehr.

Gerade bei umfangreichen Gesundheitsdatensätzen können zahlreiche Merkmale zusammenkommen: Diagnosen, Behandlungen, Arzneimittel, Alter, Geschlecht, zeitliche Abläufe, Abrechnungsinformationen oder Daten aus elektronischen Gesundheitsakten. Der EHDS sieht für die Sekundärnutzung darüber hinaus unterschiedliche Datenquellen vor – einschließlich administrativer Daten, Forschungsdaten sowie bestimmter Daten aus Wearables und mobilen Anwendungen.

Je umfangreicher solche Datenbestände werden, desto wichtiger werden deshalb technische Schutzmaßnahmen gegen eine unzulässige Re-Identifizierung.

Der EHDS verbietet eine solche Re-Identifizierung ausdrücklich. Das Schutzproblem verschwindet damit jedoch nicht; vielmehr muss technisch und organisatorisch sichergestellt werden, dass dieses Verbot tatsächlich eingehalten wird.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

8.9 Wer darf Gesundheitsdaten für Sekundärzwecke nutzen?

Der Kreis möglicher Datennutzer beschränkt sich nicht ausschließlich auf Universitäten oder staatliche Forschungseinrichtungen.

Nach Angaben der Europäischen Kommission können Gesundheitsdaten im Rahmen der Sekundärnutzung unter den gesetzlichen Voraussetzungen unter anderem von **Forschenden, Unternehmen, Organisationen des öffentlichen Gesundheitswesens und Gesundheitsdienstleistern** genutzt werden. Vorgesehen sind Anwendungen für Forschung, Innovation, öffentliche Gesundheit und Politikgestaltung.

EU-Kommission – Weiterverwendung von Gesundheitsdaten

Das bedeutet jedoch keinen freien Zugriff auf Patientendaten.

Eine Gesundheitsdatenzugangsstelle muss den beantragten Zugang prüfen und genehmigen. Es gelten Datenminimierung, Zugriffsbeschränkungen sowie Vorgaben zur Anonymisierung beziehungsweise Pseudonymisierung und zur Nutzung sicherer Verarbeitungsumgebungen.

Ebenso wichtig sind die Verbote. Gesundheitsdaten dürfen im Rahmen des EHDS beispielsweise nicht für Marketing verwendet werden oder Grundlage für Entscheidungen sein, die einzelnen Menschen oder Personengruppen aufgrund ihrer Gesundheitsdaten schaden.

Damit ergibt sich ein differenziertes Bild:

Der EHDS öffnet Gesundheitsdaten für wesentlich mehr Nutzungszwecke als die unmittelbare Behandlung eines Patienten. Gleichzeitig unterliegt dieser Zugang gesetzlichen Genehmigungs-, Zweckbindungs- und Schutzvorschriften.

Beides gehört zur Tatsachenlage.

8.10 HealthData@EU – die europäische Infrastruktur hinter der Sekundärnutzung

Für die Sekundärnutzung entsteht mit **HealthData@EU** eine europäische Infrastruktur.

Dabei handelt es sich nicht um eine einzige Datenbank, in der sämtliche Gesundheitsdaten der europäischen Bevölkerung zentral gespeichert werden. Die EU beschreibt HealthData@EU vielmehr als Bestandteil einer **föderierten Infrastruktur**. Die zentrale Plattform soll unter anderem ermöglichen, den europäischen Datenkatalog zu durchsuchen und Anträge auf Zugang zu Gesundheitsdaten einzureichen.

EU-Kommission – HealthData@EU und EHDS-Plattform

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die Dimension ist dennoch erheblich.

Gesundheitsdaten bleiben in unterschiedlichen nationalen Strukturen vorhanden, werden aber nach gemeinsamen Regeln auffindbar und für genehmigte Nutzungen zugänglich gemacht.

Damit verändert sich die entscheidende Frage.

Es geht nicht mehr ausschließlich darum, **wo eine Datei physisch gespeichert wird**.

Entscheidend wird vielmehr:

Wer kann einen Zugang beantragen? Wer genehmigt ihn? Welche Daten können zusammengeführt werden? Für welchen Zweck dürfen sie ausgewertet werden? Und wie erfährt der betroffene Bürger, was mit seinen Daten geschehen ist?

Gerade der letzte Punkt ist von zentraler Bedeutung. Die Europäische Kommission erklärt ausdrücklich, dass Bürger bei der Sekundärnutzung nachvollziehen können sollen, **wer auf ihre Gesundheitsdaten zugegriffen hat beziehungsweise welche Gesundheitsdaten zu welchem Zweck verwendet wurden**.

Damit erhält das bereits dargestellte Auskunftsrecht zusätzliches Gewicht.

Transparenz darf nicht bei der abstrakten Information enden, dass Daten grundsätzlich verwendet werden können. Der Bürger muss nachvollziehen können, welche Nutzung tatsächlich stattgefunden hat.

8.11 Widerspruch – und trotzdem mögliche Datennutzung

Besonders genau muss die Grenze des Opt-out-Rechts betrachtet werden.

Der EHDS räumt Bürgern grundsätzlich das Recht ein, ihre personenbezogenen elektronischen Gesundheitsdaten von der Sekundärnutzung auszunehmen. Das Verfahren soll einfach, transparent und reversibel sein.

Aber dieser Widerspruch ist **nicht ausnahmslos absolut**.

Die Europäische Kommission weist ausdrücklich darauf hin, dass Gesundheitsdaten unter strengen Schutz- und Transparenzanforderungen **trotz eines Opt-outs für bestimmte wichtige Zwecke des öffentlichen Interesses verwendet werden können**.

Genau deshalb ist die Auskunft darüber, was nach einem Widerspruch geschieht, so wichtig.

Ein Bürger sollte nicht davon ausgehen müssen, dass mit der Bestätigung seines Widerspruchs zwangsläufig jede weitere Verarbeitung beendet ist. Entscheidend ist vielmehr, **welche Verarbeitung tatsächlich eingestellt wurde und welche aufgrund einer gesetzlichen Ausnahme fortgesetzt werden darf.**

Deshalb gewinnt eine konkrete Forderung besondere Bedeutung:

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Wenn Daten trotz eines wirksamen Widerspruchs weiterverarbeitet werden, muss transparent nachvollziehbar sein, welche Daten betroffen sind, zu welchem Zweck sie verwendet werden und auf welcher gesetzlichen Grundlage diese Verarbeitung erfolgt.

Nur dann lässt sich überprüfen, was ein Widerspruch in der Praxis tatsächlich bewirkt.

8.12 Vom nationalen Gesundheitswesen zum europäischen Datenraum

Der EHDS macht sichtbar, wie weit die Digitalisierung des Gesundheitswesens inzwischen reicht.

Aus einer elektronischen Patientenakte, die zunächst der medizinischen Behandlung dient, entsteht nicht automatisch eine europäische Überwachungsdatenbank.

Aber gleichzeitig entsteht etwas, das noch vor wenigen Jahren in dieser Form nicht existierte:

eine rechtlich und technisch organisierte europäische Infrastruktur zur grenzüberschreitenden Nutzung und Weiterverwendung elektronischer Gesundheitsdaten.

Die Umsetzung erfolgt schrittweise. Ab **März 2029** sollen wesentliche EHDS-Regeln zur Sekundärnutzung für die meisten Datenkategorien gelten. Ab **März 2031** kommen weitere Kategorien hinzu, darunter genomische Daten. Ab **März 2035** können auch Drittstaaten und internationale Organisationen eine Teilnahme an HealthData@EU für die Sekundärnutzung beantragen.

EU-Kommission – Zeitplan zur Umsetzung des EHDS

Damit wird die eigentliche Kontrollfrage immer wichtiger:

Wie viel tatsächliche Entscheidungsmacht behält der einzelne Bürger über seine Gesundheitsdaten, wenn deren technische Verfügbarkeit, gesetzlich erlaubte Verwendungszwecke und grenzüberschreitende Nutzbarkeit gleichzeitig wachsen?

Die Antwort darauf entscheidet sich nicht an einem einzigen Gesetz.

Sie entscheidet sich daran, wie **DSGVO, EHDS, nationale Gesundheitsgesetze, Widerspruchsrechte, Auskunftsansprüche, technische Zugriffsbeschränkungen und staatliche Kontrollmechanismen** in der Praxis zusammenwirken.

9. Finanzdaten werden digital – Vom Bankkonto zum vernetzten Zahlungsraum

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

9.1 Der digitale Euro: Bargeld bekommt einen digitalen Gegenpart

Mit dem **digitalen Euro** arbeitet die Europäische Union an einem weiteren Baustein ihrer digitalen Infrastruktur. Anders als Bankguthaben oder private Kryptowährungen soll der digitale Euro **Zentralbankgeld** sein – ausgegeben vom Eurosystem und damit eine digitale Form des Euro-Bargelds.

Die Europäische Kommission legte am **28. Juni 2023** einen Gesetzgebungsvorschlag für einen möglichen digitalen Euro vor. Parallel dazu veröffentlichte sie einen Vorschlag, mit dem die Rolle des Euro-Bargelds als gesetzliches Zahlungsmittel abgesichert werden soll. (ec.europa.eu)

Europäische Kommission – Gesetzgebungspaket zum digitalen Euro und Bargeld

Die **Europäische Zentralbank (EZB)** hat wiederholt betont, dass ein digitaler Euro das Bargeld **ergänzen und nicht ersetzen** soll.

Europäische Zentralbank – Der digitale Euro

Das ist die gegenwärtige politische und institutionelle Zusage.

Gleichzeitig würde mit dem digitalen Euro erstmals ein digitales Zahlungsmittel für die breite Bevölkerung geschaffen, das unmittelbar auf Zentralbankgeld basiert.

Damit berührt die Digitalisierung einen besonders sensiblen Bereich:

nicht nur die Identität und die Gesundheit des Bürgers, sondern sein Geld.

9.2 Bargeld und digitales Bezahlen sind nicht dasselbe

Bargeld besitzt eine Eigenschaft, die digitale Zahlungssysteme grundsätzlich nicht vollständig reproduzieren können: Eine gewöhnliche Barzahlung kann unmittelbar zwischen zwei Menschen stattfinden, ohne dass dafür zwingend ein elektronisches Zahlungssystem benötigt wird.

Digitale Zahlungen benötigen dagegen technische Infrastruktur.

Beim geplanten digitalen Euro soll diesem Unterschied durch eine **Offline-Funktion** Rechnung getragen werden. Nach dem Vorschlag der Europäischen Kommission sollen Offline-Zahlungen einen besonders hohen Schutz der Privatsphäre erhalten. Bei solchen Zahlungen sollen die persönlichen Transaktionsdaten grundsätzlich nur Zahler und Zahlungsempfänger bekannt sein – ähnlich wie bei Bargeld. (finance.ec.europa.eu)

Europäische Kommission – Fragen und Grundlagen zum digitalen Euro

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Bei Online-Zahlungen bleibt dagegen eine technische Verarbeitung von Zahlungsinformationen erforderlich.

Damit wird Datenschutz beim digitalen Euro zu einer Kernfrage:

Wer kann welche Zahlungsinformationen sehen – und unter welchen gesetzlichen Voraussetzungen können staatliche Stellen darauf zugreifen?

9.3 Soll der digitale Euro programmierbar sein?

Eine der sensibelsten Fragen betrifft die sogenannte **Programmierbarkeit** digitalen Geldes.

Technisch wäre digitales Zentralbankgeld grundsätzlich in Strukturen denkbar, bei denen seine Verwendung an Bedingungen geknüpft wird – beispielsweise an bestimmte Waren, Orte, Zeiträume oder Personengruppen.

Genau deshalb ist entscheidend, was für den europäischen digitalen Euro tatsächlich vorgesehen ist.

Die Europäische Kommission und die EZB erklären ausdrücklich, dass der digitale Euro **kein programmierbares Geld** sein soll. Behörden oder Zentralbank sollen dem Bürger demnach nicht vorschreiben können, wofür, wann, wo oder bei wem er seinen digitalen Euro ausgeben darf. (finance.ec.europa.eu)

Auch die EZB zieht diese Grenze ausdrücklich.

EZB – Häufige Fragen zum digitalen Euro

Damit muss klar zwischen **technischer Möglichkeit und geplantem Rechtsrahmen** unterschieden werden.

Die Behauptung, mit Einführung des digitalen Euro könne die EZB automatisch bestimmen, welche Lebensmittel ein Bürger kaufen oder wohin er sein Geld überweisen darf, wäre nach dem derzeit vorgesehenen Modell nicht belegt.

Die entscheidende langfristige Frage lautet vielmehr:

Bleibt dieses Verbot der Programmierbarkeit dauerhaft bestehen – und wie stark wird es gesetzlich abgesichert?

9.4 Datenschutz wird zur Machtfrage

Beim Geld erhält Datenschutz eine besondere Bedeutung.

Zahlungsdaten können weit mehr über einen Menschen verraten als eine einzelne Überweisung: Einkaufsverhalten, Aufenthaltsorte, regelmäßige Zahlungen, Mitgliedschaften,

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Spenden, medizinische Ausgaben oder politische und gesellschaftliche Aktivitäten können sich aus Transaktionsmustern zumindest teilweise ableiten lassen.

Deshalb entscheidet die Architektur eines digitalen Zahlungssystems darüber, wie viel Privatsphäre erhalten bleibt.

Nach dem gegenwärtigen Konzept soll die EZB einzelne Nutzer anhand ihrer Zahlungen **nicht identifizieren können**. Zahlungsdienstleister würden bestimmte Daten allerdings weiterhin verarbeiten müssen, beispielsweise zur Einhaltung gesetzlicher Vorgaben gegen Geldwäsche und Terrorismusfinanzierung. (ecb.europa.eu)

EZB – Datenschutz beim digitalen Euro

Damit entsteht auch hier keine Situation, in der sämtliche Finanzdaten automatisch bei einer einzigen staatlichen Stelle zusammenlaufen.

Aber der digitale Euro fügt der europäischen Digitalarchitektur einen weiteren hochsensiblen Bereich hinzu.

Nach digitaler Identität und digitalen Gesundheitsdaten geht es nun um **digitales Zentralbankgeld und damit um die technische Infrastruktur des Bezahlens selbst**.

9.5 Die entscheidende Frage: Was bleibt außerhalb des Systems?

Solange Bargeld allgemein verfügbar und praktisch nutzbar bleibt, besitzt der Bürger eine Zahlungsalternative außerhalb vollständig digitaler Transaktionsketten.

Genau deshalb ist die Zukunft des Bargelds für die Bewertung des digitalen Euro von zentraler Bedeutung.

Die Europäische Kommission hat ihren Vorschlag für den digitalen Euro ausdrücklich mit einem zweiten Gesetzgebungsvorschlag verbunden, der die Annahme und Verfügbarkeit von Euro-Bargeld schützen soll. (finance.ec.europa.eu)

Europäische Kommission – Digital-Euro-Paket einschließlich Bargeldschutz

Damit steht heute nicht die Abschaffung des Bargelds im Gesetzgebungsvorschlag.

Für die langfristige Bewertung ist jedoch entscheidend, **wie sich die tatsächliche Verfügbarkeit und Akzeptanz von Bargeld entwickelt**.

Denn zwischen einem gesetzlichen Recht auf Bargeld und seiner praktischen Nutzbarkeit kann ein Unterschied entstehen.

Der entscheidende Prüfstein lautet deshalb:

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Bleibt Bargeld auch langfristig eine tatsächlich nutzbare Alternative – oder entwickelt sich digitales Bezahlen irgendwann vom zusätzlichen Angebot zur faktischen Voraussetzung wirtschaftlicher Teilhabe?

9.6 Der digitale Euro ist noch nicht beschlossen

Bei der Debatte über den digitalen Euro ist eine zeitliche Einordnung entscheidend: **Am 12. August 2026 ist seine Einführung noch nicht endgültig beschlossen.**

Der Rat der Europäischen Union legte am **19. Dezember 2025** seine Verhandlungsposition fest. Das Europäische Parlament stimmte am **9. Juli 2026** mit **416 Stimmen dafür, 169 dagegen und 22 Enthaltungen** für die Aufnahme der Verhandlungen mit dem Rat. Damit befindet sich das Vorhaben weiterhin im europäischen Gesetzgebungsverfahren.

Europäisches Parlament – Abstimmung und Stand des Verfahrens vom 9. Juli 2026

Auch nach Verabschiedung des Rechtsrahmens würde der digitale Euro nicht automatisch eingeführt. Die endgültige Entscheidung über seine Ausgabe liegt bei der **Europäischen Zentralbank (EZB)**. Die EZB nennt derzeit **2029** als möglichen Zeitpunkt einer ersten Ausgabe – vorausgesetzt, die erforderlichen EU-Rechtsvorschriften werden 2026 verabschiedet.

Damit muss zwischen drei Ebenen unterschieden werden:

Politisch vorbereitet: ja.

Gesetzgebungsverfahren weit fortgeschritten: ja.

Digitaler Euro bereits beschlossen und eingeführt: nein.

9.7 Obergrenzen: Warum der Bürger nicht unbegrenzt digitale Euro halten soll

Der geplante digitale Euro soll nach dem gegenwärtigen Konzept **kein gewöhnliches Bankkonto und kein unbegrenztes Wertaufbewahrungsmittel** werden.

Der Rat sieht ausdrücklich Obergrenzen für den Betrag vor, den eine Person gleichzeitig in digitalen Euro auf Online-Konten oder Wallets halten kann. Die konkrete Höhe soll von der EZB festgelegt werden, allerdings innerhalb eines vom Rat vorgegebenen Rahmens. Begründet wird dies mit dem Schutz der Finanzstabilität und der Vermeidung größerer Abflüsse von Bankeinlagen.

Rat der Europäischen Union – Verhandlungsposition zu digitalem Euro, Bargeld und Haltegrenzen

Auch die EZB bestätigt, dass Guthaben in digitalen Euro **nicht verzinst** und Haltegrenzen unterliegen sollen. Gleichzeitig soll eine Wallet mit einem normalen Bankkonto verbunden

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

werden können, sodass auch Zahlungen oberhalb des gehaltenen Digital-Euro-Betrags möglich wären.

Diese Konstruktion zeigt einen wesentlichen Unterschied zum Bargeld:

Bei Bargeld bestimmt der Bürger grundsätzlich selbst, wie viele Euro-Banknoten er besitzen möchte. Beim digitalen Euro soll die maximal unmittelbar haltbare Summe institutionell begrenzt werden.

Die Begründung dafür ist finanzpolitisch nachvollziehbar: Würden Bürger in einer Bankenkrise große Teile ihrer Bankguthaben innerhalb kürzester Zeit in Zentralbankgeld umwandeln, könnte dies die Geschäftsbanken zusätzlich destabilisieren.

Gleichzeitig zeigt die vorgesehene Obergrenze, dass digitales Zentralbankgeld von Beginn an **technischen und regulatorischen Regeln** unterliegt, die beim Besitz von Bargeld in dieser Form nicht bestehen.

9.8 Wer steht zwischen Bürger und Zentralbank?

Der Begriff „digitales Zentralbankgeld“ kann den Eindruck erwecken, jeder Bürger bekäme künftig unmittelbar ein Konto bei der EZB.

Genau das ist nicht vorgesehen.

Nach dem derzeitigen Modell soll der digitale Euro über **Banken und andere beaufsichtigte Zahlungsdienstleister** bereitgestellt werden. Diese sollen weiterhin die Schnittstelle zum Nutzer bilden.

Die EZB erklärt zugleich, dass sie anhand der ihr zur Verfügung stehenden Zahlungsdaten grundsätzlich nicht erkennen können soll, **wer ein bestimmter Nutzer ist oder was dieser gekauft hat**. Die bei der EZB vorhandenen Daten sollen pseudonymisiert sein.

EZB – Datenschutz beim digitalen Euro

Anders sieht es bei den beteiligten Zahlungsdienstleistern aus. Banken müssen weiterhin bestimmte personenbezogene Informationen verarbeiten, soweit dies beispielsweise zur Erfüllung gesetzlicher Vorgaben gegen Geldwäsche und Terrorismusfinanzierung erforderlich ist.

Damit entsteht keine direkte finanzielle Totalübersicht der EZB über jeden einzelnen Bürger.

Es entsteht aber ein weiteres vollständig digitales Zahlungssystem, bei dem **Identifizierung, Zahlungsabwicklung und gesetzlich vorgeschriebene Kontrollen technisch organisiert werden müssen**.

9.9 Der politische Streit ist inzwischen messbar

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Spätestens seit der Abstimmung vom **9. Juli 2026** ist der digitale Euro nicht mehr lediglich ein technisches Projekt von Kommission und EZB, sondern Gegenstand einer klar dokumentierten politischen Auseinandersetzung.

Im Europäischen Parlament stimmten **416 Abgeordnete für die Aufnahme der Verhandlungen, 169 dagegen und 22 enthielten sich**. Zuvor hatten die Fraktionen **Europäische Konservative und Reformer (EKR), Patrioten für Europa (PfE) und Europa der Souveränen Nationen (ESN)** die Entscheidung des Wirtschaftsausschusses angefochten, die interinstitutionellen Verhandlungen aufzunehmen.

Europäisches Parlament – Abstimmung über die Verhandlungen zum digitalen Euro

Damit existiert eine überprüfbare politische Konfliktlinie.

Auf der Befürworterseite stehen insbesondere Argumente wie **europäische Zahlungssouveränität, geringere Abhängigkeit von außereuropäischen Zahlungsanbietern, Widerstandsfähigkeit der Zahlungsinfrastruktur und der Erhalt öffentlichen Zentralbankgeldes im digitalen Zeitalter**. Der Rat begründet das Projekt ausdrücklich mit strategischer Autonomie, wirtschaftlicher Sicherheit und Resilienz Europas.

Auf der anderen Seite stehen politische Kräfte, die dem Projekt widersprechen oder stärkere Begrenzungen verlangen.

Für die langfristige Beurteilung des digitalen Euro ist deshalb nicht nur entscheidend, welche Versprechen heute gegeben werden. Ebenso entscheidend ist, **welche Schutzbestimmungen am Ende tatsächlich im Gesetz stehen und welche politischen Kräfte ihnen zugestimmt oder widersprochen haben.**

9.10 Bargeld wird zum entscheidenden Gegenpol

Die vielleicht wichtigste Schutzfrage des gesamten Projekts betrifft deshalb nicht den digitalen Euro allein.

Sie betrifft das **Bargeld**.

Der Rat hat seine Verhandlungsposition zum digitalen Euro ausdrücklich mit einer Position zur Stärkung des Bargelds verbunden. Danach sollen sowohl die Akzeptanz von Bargeld als Zahlungsmittel als auch der Zugang zu Bargeld geschützt werden. Der Rat spricht sich grundsätzlich gegen eine pauschale Nichtannahme von Bargeld durch Händler und Dienstleister aus, wobei bestimmte Ausnahmen vorgesehen sind.

Rat der EU – Schutz von Bargeld und digitaler Euro

Damit steht derzeit ausdrücklich **nicht** die Abschaffung des Bargelds zur Abstimmung.

Gerade deshalb wird die tatsächliche Entwicklung in den kommenden Jahren entscheidend sein.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Denn Freiheit beim Bezahlen besteht nicht allein darin, dass Bargeld formal gesetzliches Zahlungsmittel bleibt. Sie besteht darin, dass Menschen **praktisch Zugang zu Bargeld haben und damit im Alltag tatsächlich bezahlen können**.

Solange Bargeld diese Funktion behält, existiert neben digitalen Zahlungssystemen eine eigenständige Alternative.

Würde diese Alternative eines Tages faktisch verschwinden, hätte die Digitalisierung des Geldes eine völlig andere Bedeutung.

Die entscheidende Grenze verläuft deshalb nicht zwischen Bargeld und digitalem Euro. Sie verläuft zwischen echter Wahlfreiheit und einem Zahlungssystem, in dem die digitale Teilnahme irgendwann alternativlos wird.

10. Geldwäschebekämpfung und AMLA – Wenn Finanzkontrolle europäisch vernetzt wird

10.1 Eine neue EU-Behörde mit Sitz in Frankfurt

Parallel zum digitalen Euro baut die Europäische Union ihre Infrastruktur zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung grundlegend um.

Im Zentrum steht die neue **Anti-Money Laundering Authority (AMLA)** mit Sitz in Frankfurt am Main. Die Behörde soll nicht lediglich Empfehlungen aussprechen. Sie erhält direkte und indirekte Aufsichtsbefugnisse über besonders risikoreiche Unternehmen des Finanzsektors und soll zugleich die Zusammenarbeit der nationalen Aufsichtsbehörden und **Financial Intelligence Units (FIUs)** stärken.

AMLA – Europäische Anti-Geldwäschebehörde

Die AMLA beschreibt für die Jahre **2026 bis 2028** drei zentrale Aufgabenfelder: die Vollendung eines einheitlichen europäischen Regelwerks, eine stärkere Vereinheitlichung der Aufsicht und eine intensivere Zusammenarbeit der nationalen FIUs.

Damit verändert sich die Struktur der Finanzaufsicht: Geldwäschebekämpfung wird stärker **europäisch koordiniert und zentral beaufsichtigt**.

10.2 Die 10.000-Euro-Grenze für Bargeld

Ein besonders sichtbarer Bestandteil des neuen europäischen Anti-Geldwäschepakets betrifft das Bargeld.

Die **Verordnung (EU) 2024/1624** führt eine EU-weite Obergrenze von **10.000 Euro für Barzahlungen beim Kauf von Waren oder Dienstleistungen** ein. Auch mehrere

miteinander verbundene Zahlungen werden berücksichtigt. Mitgliedstaaten dürfen niedrigere Grenzen festlegen.

EU-Geldwäscheverordnung 2024/1624 – vollständiger Rechtstext

Wichtig ist die Abgrenzung: Die 10.000-Euro-Grenze gilt nach der Verordnung **nicht für Zahlungen zwischen Privatpersonen, wenn diese nicht beruflich handeln**. Ebenfalls bestehen bestimmte Ausnahmen beispielsweise für Einzahlungen bei Kredit-, Zahlungs- oder E-Geld-Instituten.

Die EU begründet die Obergrenze ausdrücklich mit dem Geldwäsche- und Terrorismusfinanzierungsrisiko großer Bargeldzahlungen.

Damit erhält Bargeld erstmals eine unionsweit einheitliche gesetzliche Obergrenze im geschäftlichen Zahlungsverkehr.

10.3 Bereits ab 3.000 Euro beginnt die Identifizierung

Die 10.000-Euro-Grenze erzählt jedoch nur einen Teil der Geschichte.

Bei bestimmten gelegentlichen Bargeldtransaktionen von **mindestens 3.000 Euro** müssen verpflichtete Unternehmen Maßnahmen zur Identifizierung und Überprüfung des Kunden beziehungsweise wirtschaftlich Berechtigten durchführen. Die EU begründet dies damit, dass auch Bargeldtransaktionen unterhalb der 10.000-Euro-Grenze für Geldwäsche und Terrorismusfinanzierung missbraucht werden können.

Das bedeutet:

Eine Barzahlung kann zulässig sein und trotzdem eine Identitätsprüfung auslösen.

Damit verändert sich eine traditionelle Eigenschaft des Bargelds. Gerade bei höheren geschäftlichen Zahlungen wird die Möglichkeit, eine Transaktion ohne personenbezogene Zuordnung vorzunehmen, eingeschränkt.

Die Begründung lautet wiederum: Bekämpfung von Geldwäsche und Terrorismusfinanzierung.

Die Folge ist ebenso eindeutig: **Finanzielle Anonymität wird in bestimmten Bereichen weiter begrenzt.**

10.4 Bankkonten, wirtschaftlich Berechtigte und FIUs

Das europäische Anti-Geldwäschepaket reicht wesentlich weiter als Bargeld.

Die neuen Regeln harmonisieren unter anderem die Ermittlung wirtschaftlich Berechtigter, erweitern die Zusammenarbeit zwischen Aufsichtsbehörden und FIUs und sehen eine stärkere Vernetzung von Informationen vor. Die Europäische Kommission nennt ausdrücklich die **Vernetzung von Bankkontenregistern** sowie einen gemeinsamen Mindestbestand an

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Finanz-, Verwaltungs- und Strafverfolgungsinformationen, auf den FIUs zugreifen können sollen.

Gleichzeitig erhalten zuständige Behörden und Aufsichtsstellen weitreichendere Möglichkeiten, Informationen über wirtschaftlich Berechtigte abzurufen. Auch die entsprechenden nationalen Register sollen auf europäischer Ebene stärker miteinander verbunden werden.

Damit entsteht keine Datenbank, in der jeder Einkauf jedes EU-Bürgers zentral bei der AMLA gespeichert wird.

Aber es entsteht eine **stärker vernetzte europäische Kontrollarchitektur für Finanzinformationen**.

10.5 Verdachtsmeldungen: Kontrolle beginnt nicht erst mit einer Straftat

Ein weiterer zentraler Bestandteil der Geldwäschebekämpfung sind Verdachtsmeldungen.

Das System setzt nicht voraus, dass eine Straftat bereits bewiesen wurde. Verpflichtete Stellen müssen auffällige oder verdächtige Sachverhalte nach den gesetzlichen Voraussetzungen an die zuständigen Stellen melden.

Das ist für die Einordnung entscheidend:

Geldwäscheprävention arbeitet bewusst mit Risiken und Verdachtsmomenten – nicht ausschließlich mit bereits nachgewiesenen Straftaten.

Genau darin liegt ihre präventive Funktion.

Darin liegt gleichzeitig ein Grundrechtsproblem, das kontrolliert werden muss: Menschen können Gegenstand einer Prüfung werden, obwohl ihnen zu diesem Zeitpunkt keine Straftat nachgewiesen wurde.

Je leistungsfähiger automatisierte Risikoanalysen und grenzüberschreitende Informationssysteme werden, desto wichtiger werden deshalb **Verhältnismäßigkeit, Datenqualität, Korrekturmöglichkeiten und rechtsstaatliche Kontrolle**.

10.6 Der gemeinsame Nenner: Identität und Nachvollziehbarkeit

An dieser Stelle beginnen mehrere zuvor getrennt betrachtete Entwicklungen ineinanderzugreifen.

Bei der digitalen Identität geht es darum, **wer ein Mensch ist**.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Bei Gesundheitsdaten geht es darum, **welche medizinischen Informationen über ihn vorliegen**.

Beim digitalen Zahlungsverkehr geht es darum, **wie Geld übertragen wird**.

Bei der Geldwäschebekämpfung geht es unter anderem darum, **wer hinter bestimmten Finanztransaktionen und Vermögenswerten steht**.

Keine dieser Infrastrukturen beweist für sich genommen die Existenz eines umfassenden Überwachungssystems.

Aber alle folgen einem gemeinsamen technischen Prinzip:

Identifizieren. Digitalisieren. Verknüpfen. Prüfen.

Die entscheidende Frage lautet deshalb nicht, ob Geldwäschebekämpfung notwendig ist. Organisierte Kriminalität, Terrorismusfinanzierung und das Verschleiern illegal erworbener Vermögen sind reale Probleme, gegen die ein Rechtsstaat vorgehen muss.

Die entscheidende Frage lautet:

Wie weit darf die dafür geschaffene Kontrollinfrastruktur in die finanzielle Privatsphäre unbescholtener Bürger hineinreichen?

10.7 Wenn aus einzelnen Systemen eine Architektur wird

Digitale Identität, elektronische Patientenakte, europäischer Gesundheitsdatenraum, digitaler Euro und europäische Geldwäscheaufsicht beruhen auf unterschiedlichen Gesetzen, besitzen unterschiedliche Zwecke und dürfen deshalb nicht so dargestellt werden, als seien sie bereits ein einziges miteinander verbundenes System.

Doch ebenso falsch wäre es, jede Entwicklung ausschließlich isoliert zu betrachten.

Denn Digitalisierung schafft **technische Anschlussfähigkeit**.

Was heute rechtlich getrennt ist, kann technisch grundsätzlich interoperabel gestaltet werden. Ob eine Verbindung tatsächlich zulässig ist, entscheidet das jeweilige Recht.

Damit verschiebt sich die zentrale Frage dieses Dossiers erneut:

Nicht nur: Welche Daten besitzt der Staat heute?

Sondern:

Welche Infrastruktur wird heute geschaffen – und welche Verknüpfungen könnte ein zukünftiger Gesetzgeber rechtlich ermöglichen?

Genau an dieser Grenze entscheidet sich, ob Digitalisierung dauerhaft ein Werkzeug des Bürgers bleibt – oder ob aus immer mehr einzeln begründeten Kontrollinstrumenten eines Tages eine Infrastruktur entsteht, die wesentlich mehr über einen Menschen weiß, als jede einzelne ihrer Komponenten für sich genommen erkennen lässt.

11. Wenn Systeme miteinander sprechen – Interoperabilität als Schlüssel der digitalen Infrastruktur

11.1 Die eigentliche Veränderung liegt in der Vernetzung

Bis hierher wurden unterschiedliche Systeme betrachtet: digitale Identität, elektronische Patientenakte, Europäischer Gesundheitsdatenraum, digitaler Euro und europäische Finanzaufsicht.

Diese Systeme beruhen auf unterschiedlichen Rechtsgrundlagen und erfüllen unterschiedliche Zwecke. **Sie bilden heute keine einzige zentrale Bürgerdatenbank.**

Doch die europäische Digitalstrategie verfolgt ausdrücklich ein weiteres Ziel: **Interoperabilität**.

Interoperabilität bedeutet, dass unterschiedliche technische Systeme nach gemeinsamen Standards miteinander kommunizieren, Daten austauschen und digitale Nachweise gegenseitig verarbeiten können.

Bei der **EUDI-Wallet** ist genau diese grenzüberschreitende Interoperabilität ausdrücklich vorgesehen. Die Mitgliedstaaten müssen gemeinsame Standards und technische Spezifikationen verwenden, damit digitale Identitätsnachweise unionsweit eingesetzt werden können.

EU-Kommission – European Digital Identity Wallet

Damit verändert sich die Betrachtung grundlegend.

Die entscheidende Frage ist nicht mehr nur, welche Daten ein einzelnes System enthält. Entscheidend wird, welche Systeme technisch und rechtlich miteinander kommunizieren können.

11.2 Der Interoperable Europe Act – Vernetzung wird politisches Programm

Diese Entwicklung beschränkt sich nicht auf die digitale Identität.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Mit dem **Interoperable Europe Act**, der im April 2024 in Kraft trat, schuf die EU einen Rechtsrahmen, der die grenzüberschreitende Interoperabilität öffentlicher Verwaltungen verbessern soll.

Im **Interoperable Europe Annual Report 2025** beschreibt die Europäische Kommission bereits den Aufbau einer gemeinsamen Governance-Struktur und eines zentralen Portals für interoperable Lösungen. Die **Interoperable Europe Agenda 2026** nennt den grenzüberschreitenden Datenaustausch zwischen öffentlichen Verwaltungen ausdrücklich als Schwerpunkt.

EU-Kommission – Stand der Interoperabilität in der Europäischen Union

Interoperable Europe – Agenda 2026

Das politische Ziel ist damit dokumentiert:

Digitale öffentliche Dienste sollen nicht als voneinander abgeschottete nationale Insellösungen bestehen bleiben. Sie sollen grenzüberschreitend kompatibler, wiederverwendbarer und miteinander anschlussfähig werden.

Das kann Verwaltung erheblich vereinfachen.

Gleichzeitig wächst damit die Bedeutung der Regeln, die bestimmen, **welche Daten zwischen welchen Systemen ausgetauscht werden dürfen.**

11.3 Interoperabilität bedeutet nicht automatisch Datenfreigabe

An dieser Stelle ist eine klare Grenze notwendig.

Nur weil zwei Systeme technisch interoperabel sind, bedeutet das **nicht**, dass sämtliche Daten zwischen ihnen frei ausgetauscht werden dürfen.

Technische Anschlussfähigkeit und rechtliche Zugriffsberechtigung sind zwei verschiedene Dinge.

Die DSGVO, spezialgesetzliche Datenschutzregelungen, Zweckbindungen und konkrete Zugriffsrechte gelten weiterhin. Auch die EUDI-Wallet ist ausdrücklich so konzipiert, dass Nutzer nur die jeweils erforderlichen Informationen beziehungsweise Attribute offenlegen können sollen.

Deshalb wäre die Behauptung falsch:

„Weil die Systeme interoperabel sind, kann der Staat automatisch alle Daten eines Bürgers zusammenführen."

Dafür gibt es keinen solchen Automatismus.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die entscheidende Risikofrage lautet vielmehr:

Was wird technisch möglich – und welche dieser Möglichkeiten darf ein heutiger oder zukünftiger Gesetzgeber rechtlich freigeben?

11.4 Der Data Act: Immer mehr Daten werden zugänglich und übertragbar

Ein weiterer Baustein ist der europäische **Data Act**.

Die Verordnung trat am **11. Januar 2024** in Kraft und gilt seit **12. September 2025**. Sie soll den Zugang zu und die Nutzung von Daten insbesondere aus vernetzten Produkten und Diensten neu ordnen. Verbraucher und Unternehmen sollen mehr Kontrolle über Daten erhalten, die beispielsweise durch vernetzte Fahrzeuge, Smart-TVs oder industrielle Maschinen entstehen.

EU-Kommission – Data Act

Auch hier ist das erklärte Ziel zunächst nicht staatliche Überwachung.

Es geht um Datenzugang, Wettbewerb, Innovation und darum, die wirtschaftliche Nutzung bislang abgeschotteter Datenbestände zu erleichtern.

Doch damit wächst ein weiterer Bereich:

Nicht nur klassische Verwaltungsdaten werden digital. Auch Geräte, Fahrzeuge, Maschinen und andere vernetzte Produkte erzeugen kontinuierlich Daten, deren Zugang und Weiterverwendung gesetzlich geregelt werden müssen.

Damit wird Datenpolitik zunehmend zu Infrastrukturpolitik.

11.5 Vom einzelnen Datensatz zum digitalen Ökosystem

Die Entwicklung lässt sich inzwischen auf mehreren Ebenen beobachten.

Die EUDI-Wallet schafft eine interoperable digitale Identität.

Der EHDS schafft eine grenzüberschreitende Infrastruktur für Gesundheitsdaten.

Der digitale Euro soll eine neue digitale Zahlungsinfrastruktur schaffen.

Die europäischen Anti-Geldwäsche-Regeln vernetzen Teile der Finanzaufsicht stärker.

Der Interoperable Europe Act soll öffentliche Verwaltungen grenzüberschreitend anschlussfähiger machen.

Der Data Act erweitert Zugangs- und Nutzungsregeln für Daten aus vernetzten Produkten und Diensten.

Keines dieser Projekte beweist für sich genommen die Existenz eines zentralen Überwachungsapparates.

In ihrer Gesamtheit zeigen sie jedoch, dass Europa eine immer umfassendere digitale Dateninfrastruktur aufbaut.

Und genau deshalb reicht es nicht, jedes Projekt ausschließlich für sich zu betrachten.

11.6 Die Grenze zwischen Komfort und Kontrolle

Interoperabilität kann für Bürger erhebliche Vorteile bringen.

Wer seine Identität nicht bei jeder Behörde erneut nachweisen muss, medizinische Informationen im europäischen Ausland verfügbar machen kann oder Verwaltungsleistungen grenzüberschreitend digital erledigt, profitiert unmittelbar davon.

Doch derselbe technische Fortschritt verändert auch die Voraussetzungen staatlicher Kontrolle.

Eine vollständig analoge und voneinander getrennte Informationslandschaft lässt sich nur mit erheblichem Aufwand zusammenführen.

Eine standardisierte, digitalisierte und interoperable Infrastruktur kann Informationen wesentlich schneller verarbeiten und – **wenn eine entsprechende Rechtsgrundlage besteht** – miteinander verbinden.

Das ist der entscheidende Unterschied.

Digitalisierung schafft nicht automatisch Überwachung. Sie senkt aber technische Hürden für Verarbeitung, Austausch und Verknüpfung von Informationen.

Welche dieser Möglichkeiten tatsächlich genutzt werden dürfen, entscheidet das Recht.

11.7 Die Macht liegt künftig zunehmend in den Zugriffsregeln

Damit verschiebt sich auch die politische Machtfrage.

Entscheidend ist langfristig nicht allein, **wer Daten speichert**.

Entscheidend wird:

Wer darf darauf zugreifen?

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Wer darf Daten miteinander verbinden?

Welche Zwecke rechtfertigen einen Zugriff?

Welche Behörden dürfen Ausnahmen erhalten?

Wie lange werden Informationen gespeichert?

Kann der Bürger widersprechen?

Kann er erfahren, wer seine Daten verwendet hat?

Und kann ein späterer Gesetzgeber diese Grenzen erweitern?

Genau deshalb sind Datenschutz, Auskunftsrechte, Widerspruchsmöglichkeiten, richterliche Kontrolle und parlamentarische Aufsicht keine Nebenthemen der Digitalisierung.

Sie entscheiden darüber, **wer die Kontrolle über die entstehende Infrastruktur besitzt.**

11.8 Der Überwachungsapparat ist keine belegte Tatsache – die Infrastruktur ist real

Die Begriffe müssen sauber bleiben.

Es lässt sich anhand der bisher untersuchten Rechtsakte **nicht belegen, dass EU oder Bundesregierung bereits einen einheitlichen digitalen Überwachungsapparat geschaffen haben**, in dem Identitäts-, Gesundheits-, Finanz- und sonstige Bürgerdaten automatisch zu einem Gesamtprofil zusammengeführt werden.

Eine solche Behauptung würde über die belegten Tatsachen hinausgehen.

Belegt ist jedoch etwas anderes:

Digitale Identität wird europaweit interoperabel. Gesundheitsdaten werden grenzüberschreitend nutzbar. Finanzkontrolle wird stärker europäisch vernetzt. Öffentliche Verwaltungen sollen interoperabler werden. Immer mehr Daten aus digitalen und vernetzten Systemen werden technisch verfügbar und rechtlich reguliert.

Damit ist die Infrastrukturentwicklung keine Science-Fiction.

Sie findet statt.

Die offene politische Frage lautet:

Welche Grenzen setzt eine demokratische Gesellschaft dieser Infrastruktur, bevor aus technisch möglicher Vernetzung eine Machtkonzentration entsteht, die später nur noch schwer zurückzudrehen ist?

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

12. Registermodernisierung – Wenn die Steuer-ID zum Schlüssel der Verwaltung wird

12.1 Die Steuer-ID verlässt ihren ursprünglichen Bereich

Die deutsche Registermodernisierung gehört zu den wichtigsten, aber außerhalb von Fachkreisen vergleichsweise wenig beachteten Bausteinen des digitalen Staates.

Mit dem **Registermodernisierungsgesetz** wurde beschlossen, die bereits bestehende steuerliche Identifikationsnummer künftig auch in zahlreichen Verwaltungsregistern als einheitliches Ordnungsmerkmal zu verwenden. Der Bundestag stimmte dem Gesetz am **28. Januar 2021** zu. Dafür votierten CDU/CSU und SPD; AfD, FDP, Die Linke und Bündnis 90/Die Grünen stimmten dagegen.

Deutscher Bundestag – Abstimmung über das Registermodernisierungsgesetz vom 28. Januar 2021

Die politische Verantwortung lässt sich damit klar einordnen: Das Vorhaben wurde unter der damaligen Bundesregierung aus **CDU/CSU und SPD** beschlossen. Die Oppositionsparteien lehnten das Gesetz zwar gemeinsam ab, allerdings aus teilweise unterschiedlichen Gründen und mit unterschiedlichen Alternativvorschlägen.

Der Kern des Systems ist einfach erklärt:

Eine Person soll in unterschiedlichen Verwaltungsregistern eindeutig derselben Person zugeordnet werden können.

Dafür wird die Steuer-ID als registerübergreifendes Identifikationsmerkmal genutzt. Ziel ist unter anderem, Datenqualität zu verbessern und Bürger davon zu entlasten, bereits bei Behörden vorhandene Nachweise immer wieder neu einreichen zu müssen. Dieses Prinzip wird als **„Once Only“** bezeichnet.

Wissenschaftliche Dienste des Bundestages – Verwendung der Steuer-ID nach dem Identifikationsnummerngesetz, März 2026

12.2 Von der Steuerverwaltung zum registerübergreifenden Personenmerkmal

Die Steuer-ID war ursprünglich für die Steuerverwaltung geschaffen worden.

Mit der Registermodernisierung wurde ihr Anwendungsbereich wesentlich erweitert.

Die Anlage zum Identifikationsnummerngesetz umfasst zahlreiche staatliche Register. Nach einer Ausarbeitung der Wissenschaftlichen Dienste des Bundestages vom **6. März 2026** wird die Identifikationsnummer inzwischen in **50 staatlichen Registern** eingesetzt. Dazu gehören unter anderem Datenbestände der Rentenversicherung, der Bundesagentur für Arbeit, der Grundsicherung, der Krankenkassen, der Pflegekassen, der Elterngeldstellen und der Wohngeldbehörden.

Damit entsteht keine einzige zentrale Datenbank, in der sämtliche Verwaltungsinformationen eines Menschen gespeichert werden.

Aber zahlreiche unterschiedliche Register erhalten **dasselbe eindeutige Zuordnungsmerkmal**.

Und genau darin liegt die besondere Bedeutung der Registermodernisierung.

Denn Informationen, die früher in unterschiedlichen Behörden unter unterschiedlichen Aktenzeichen und Ordnungssystemen geführt wurden, lassen sich technisch wesentlich zuverlässiger einer bestimmten Person zuordnen.

12.3 Das Once-Only-Prinzip: Der Bürger soll Daten nur einmal liefern

Die Bundesregierung begründete die Registermodernisierung vor allem mit einer Vereinfachung des Verwaltungsalltags.

Wer beispielsweise bereits eine Geburtsurkunde, seinen Familienstand oder andere Nachweise bei einer staatlichen Stelle hinterlegt hat, soll diese Informationen nicht bei jedem neuen Antrag erneut beschaffen und vorlegen müssen. Stattdessen sollen berechtigte Behörden vorhandene Daten elektronisch abrufen können.

Das kann erhebliche praktische Vorteile haben:

weniger Papier, weniger Behördengänge, schnellere Verfahren und weniger doppelte Datenerfassung.

Gleichzeitig verändert sich damit jedoch das Prinzip staatlicher Datenhaltung.

Der Bürger wird zunehmend nicht mehr selbst zum Überbringer seiner Nachweise.

Die Verwaltung beschafft vorhandene Informationen direkt aus anderen Registern.

Damit wird die Frage nach den Zugriffsrechten erneut zentral:

Welche Behörde darf welche Information bei welcher anderen Behörde abrufen – und wofür?

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

12.4 Das Datenschutzcockpit: Der Bürger soll sehen können, wer Daten austauscht

Als Schutzmechanismus wurde das sogenannte **Datenschutzcockpit** vorgesehen.

Der Bundestag beschrieb bereits 2021 das Ziel, Bürgern eine einfache und zeitnahe Übersicht darüber zu ermöglichen, welche Datenübermittlungen zwischen Behörden stattgefunden haben.

Damit soll Transparenz dort geschaffen werden, wo Daten zunehmend nicht mehr vom Bürger selbst zwischen Behörden weitergereicht werden, sondern direkt zwischen staatlichen Stellen fließen.

Das Prinzip ist entscheidend:

Wenn Behörden Daten untereinander austauschen, soll der Bürger zumindest nachvollziehen können, dass ein solcher Austausch stattgefunden hat.

Die Existenz eines Datenschutzcockpits beseitigt jedoch nicht automatisch jedes Datenschutzrisiko.

Seine tatsächliche Schutzwirkung hängt davon ab, **welche Übermittlungen angezeigt werden, wie vollständig die Protokollierung ist, wie verständlich die Angaben dargestellt werden und ob der Bürger gegen unzulässige Datenverarbeitungen wirksam vorgehen kann.**

12.5 Der politische Streit: Vier Oppositionsparteien gegen die Steuer-ID als Kennzeichen

Die Einführung der Steuer-ID als registerübergreifendes Ordnungsmerkmal war bereits 2021 politisch hoch umstritten.

Die **FDP** forderte eine Registermodernisierung ohne steuerliche Identifikationsnummer. Sie berief sich dabei auf verfassungsrechtliche Bedenken und warnte vor einem bereichsübergreifenden Personenkennzeichen. AfD, Die Linke und Bündnis 90/Die Grünen unterstützten diesen FDP-Antrag; CDU/CSU und SPD lehnten ihn ab.

Die **Grünen** stellten einen eigenen Antrag und verlangten eine verfassungskonforme Registermodernisierung ohne Verwendung der Steuer-ID als bereichsübergreifendes Datum. Diesem Antrag stimmten FDP, Die Linke und die Grünen zu; CDU/CSU, SPD und AfD lehnten ihn ab.

Auch die **AfD** brachte einen eigenen Antrag ein. Sie forderte den Rückzug des Regierungsentwurfs und wollte statt der Steuer-ID ein System bereichsspezifischer Personenkennzeichen nach österreichischem Vorbild.

Damit wird ein wichtiger Unterschied sichtbar:

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die damaligen Oppositionsparteien lehnten zwar das Regierungsmodell ab, waren sich aber keineswegs vollständig darüber einig, welche Alternative an seine Stelle treten sollte.

Gerade deshalb ist die tatsächliche Abstimmungsgeschichte wichtiger als pauschale Aussagen darüber, „die Opposition“ sei dafür oder dagegen gewesen.

12.6 Datenschutz und Verfassungsrecht: Die Sorge vor dem Personenkennzeichen

Die Kritik an der Registermodernisierung bezog sich von Anfang an auf eine grundlegende verfassungsrechtliche Frage:

Kann ein einheitliches Kennzeichen über viele staatliche Register hinweg dazu führen, dass Informationen aus unterschiedlichen Lebensbereichen zu umfassenden Persönlichkeitsprofilen zusammengeführt werden können?

Der Bundestag dokumentierte bereits 2021 entsprechende Bedenken von FDP und Grünen. Beide verwiesen auf die Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung und auf die Gefahr einer umfassenden Zusammenführung personenbezogener Informationen.

Die Wissenschaftlichen Dienste des Bundestages haben diese Frage im März **2026** erneut untersucht.

Dabei kommen sie nicht zu dem Ergebnis, die gegenwärtige Verwendung der Identifikationsnummer sei grundsätzlich verfassungswidrig. Sie betonen jedoch, dass bei einer Erweiterung des Anwendungsbereichs **datenschutzrechtliche Schutzvorkehrungen erforderlich sind, die insbesondere die Erstellung eines Persönlichkeitsprofils verhindern müssen**.

Damit ist die Rechtslage differenzierter als beide politischen Extreme:

Die Steuer-ID als registerübergreifendes Ordnungsmerkmal ist nicht automatisch ein verfassungswidriges Überwachungsinstrument.

Aber:

Je breiter ihre Nutzung wird, desto höher werden die Anforderungen an Zweckbindung, Transparenz, Zugriffsbeschränkungen und Schutz vor Profilbildung.

12.7 Die heutige Grenze: Die Steuer-ID darf nicht beliebig verwendet werden

Das Identifikationsnummerngesetz enthält keine allgemeine Befugnis, die Steuer-ID für beliebige Zwecke zu verwenden.

Nach der Ausarbeitung der Wissenschaftlichen Dienste ist eine Verarbeitung außerhalb der gesetzlich vorgesehenen Verwaltungszwecke grundsätzlich unzulässig, sofern nicht eine andere Rechtsvorschrift oder eine Einwilligung eine entsprechende Verarbeitung erlaubt. Für konkrete Fachverfahren müssen eigene gesetzliche Verarbeitungsbefugnisse bestehen.

Damit besteht heute eine wichtige Grenze:

Ein gemeinsames Ordnungsmerkmal bedeutet nicht automatisch einen freien Zugriff aller Behörden auf sämtliche Register.

Jede Datenverarbeitung benötigt eine entsprechende Rechtsgrundlage.

Genau darin liegt aber zugleich die langfristige politische Bedeutung.

Denn Zugriffsrechte werden durch Gesetze bestimmt.

12.8 Eine Erweiterung braucht den Gesetzgeber

Die Registerliste kann nicht einfach von einer Behörde nach Belieben erweitert werden.

Die Wissenschaftlichen Dienste weisen darauf hin, dass Änderungen der Registerliste und wesentliche zusätzliche Verwendungszwecke grundsätzlich eines **formellen Gesetzes** bedürfen. Damit bleibt eine Erweiterung der parlamentarischen Gesetzgebung unterworfen.

Das ist ein wichtiger rechtsstaatlicher Schutzmechanismus.

Es bedeutet aber zugleich:

Der Umfang der Vernetzung hängt langfristig von politischen Mehrheiten ab.

Was heute gesetzlich ausgeschlossen ist, kann nicht heimlich von einer Behörde freigegeben werden.

Es kann jedoch durch einen zukünftigen Gesetzgeber verändert werden – wiederum unter den Grenzen des Grundgesetzes, der DSGVO und des europäischen Datenschutzrechts.

12.9 2026: Die Frage nach einer noch breiteren Nutzung ist bereits auf dem Tisch

Dass eine Erweiterung des Systems keine rein theoretische Zukunftsfrage ist, zeigt eine Ausarbeitung der Wissenschaftlichen Dienste vom März 2026.

Anlass war die Frage, ob die Identifikationsnummer künftig umfassender innerhalb der Sozialverwaltung genutzt werden könnte. Die Wissenschaftlichen Dienste stellen fest, dass Sozialversicherungsträger eine weitergehende Verwendung der ID-Nummer gefordert haben, weil die gegenwärtige Begrenzung auf bestimmte Verwaltungsleistungen aus ihrer Sicht praktische Probleme verursacht.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Damit wird sichtbar, wie sich solche Infrastrukturen entwickeln können:

Zunächst wird eine Identifikationsnummer für bestimmte klar definierte Zwecke eingeführt. Im praktischen Betrieb entstehen anschließend Forderungen, ihren Anwendungsbereich zu erweitern.

Das bedeutet nicht, dass jede solche Erweiterung automatisch beschlossen wird.

Aber es zeigt, dass die Frage nach dem Umfang des Systems nach seiner Einführung nicht abgeschlossen ist.

12.10 Vom Verwaltungshelfer zum möglichen Verbindungsschlüssel

Die Steuer-ID enthält selbst keine Krankengeschichte, keinen Kontostand und keine politische Meinung.

Sie ist zunächst nur ein eindeutiges Kennzeichen.

Gerade deshalb besitzt sie jedoch eine besondere technische Bedeutung.

Ein eindeutiger Identifier erleichtert die zuverlässige Zuordnung unterschiedlicher Informationen zu derselben Person.

Das ist genau der Zweck, der die Verwaltung effizienter machen soll.

Und es ist zugleich der Punkt, an dem die Datenschutzfrage beginnt.

Denn je mehr Register dasselbe Kennzeichen verwenden, desto leichter können Informationen technisch eindeutig derselben Person zugeordnet werden – **sofern das Recht eine solche Verknüpfung erlaubt**.

Damit zeigt die Registermodernisierung besonders deutlich die zwei Seiten des digitalen Staates:

Dasselbe technische Prinzip, das Bürokratie abbauen kann, kann zugleich die Voraussetzungen für wesentlich umfassendere Datenverknüpfungen schaffen.

Die entscheidende Schutzlinie liegt deshalb nicht in der Technik allein.

Sie liegt in **Zweckbindung, gesetzlichen Zugriffsschranken, Transparenz, parlamentarischer Kontrolle und dem Verbot einer unzulässigen Profilbildung.**

13. NOOTS – Wenn Behörden Daten und Nachweise direkt austauschen

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

13.1 Das technische Rückgrat des Once-Only-Prinzips

Die Registermodernisierung schafft die rechtliche und organisatorische Grundlage dafür, dass bereits vorhandene Verwaltungsdaten besser genutzt werden können. Damit dieses Prinzip praktisch funktioniert, braucht es jedoch eine technische Infrastruktur.

Genau dafür wird das **National-Once-Only-Technical-System – NOOTS** aufgebaut.

Das Grundprinzip lautet: Bürger und Unternehmen sollen Nachweise, die einer Behörde bereits vorliegen, nicht bei jedem neuen Verwaltungsverfahren erneut selbst beschaffen und einreichen müssen. Stattdessen sollen berechtigte öffentliche Stellen diese Nachweise elektronisch bei der jeweils zuständigen Stelle abrufen können.

Das Bundesministerium für Digitales und Staatsmodernisierung beschreibt NOOTS als die technische Grundlage dafür, vorhandene Verwaltungsdaten auf Wunsch von Bürgern und Unternehmen automatisiert abrufbar und nutzbar zu machen.

Bundesministerium für Digitales und Staatsmodernisierung – National-Once-Only-Technical-System (NOOTS)

Damit verändert sich ein grundlegender Verwaltungsablauf.

Bislang funktioniert Verwaltung häufig nach dem Prinzip:

Behörde A besitzt einen Nachweis → der Bürger beschafft ihn → der Bürger reicht ihn bei Behörde B erneut ein.

NOOTS soll daraus zunehmend machen:

Behörde A besitzt einen Nachweis → Behörde B darf ihn für ein konkretes Verfahren abrufen → der Bürger muss ihn nicht erneut beschaffen.

Das ist zunächst ein Instrument zum Bürokratieabbau.

Gleichzeitig entsteht damit eine Infrastruktur, über die bislang getrennte Verwaltungsstellen technisch Nachweise austauschen können.

13.2 Seit Januar 2026 ist NOOTS keine reine Planung mehr

Für die zeitliche Einordnung ist ein Punkt entscheidend:

NOOTS befindet sich nicht mehr ausschließlich in der Konzeptionsphase.

Nach Angaben des Bundesministeriums für Digitales und Staatsmodernisierung ging im **Januar 2026 die erste funktionsfähige Version des Systems in den Livebetrieb**. Bis Ende 2026 soll eine Version für den technischen Flächenrollout bereitstehen.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Damit hat die Registermodernisierung eine neue Stufe erreicht.

Aus gesetzlichen Vorgaben, Architekturpapieren und Pilotprojekten wird schrittweise eine tatsächlich betriebene technische Infrastruktur.

Bundesministerium für Digitales und Staatsmodernisierung – Inbetriebnahme und Flächenrollout des NOOTS

Der Ausbau erfolgt allerdings nicht auf einen Schlag. Deutschland besitzt eine stark föderal organisierte Registerlandschaft mit zahlreichen Registern bei Bund, Ländern und Kommunen. Diese müssen schrittweise technisch angeschlossen und für den digitalen Nachweisaustausch ertüchtigt werden.

Die Aussage, sämtliche deutschen Behörden und Register seien im August 2026 bereits vollständig über NOOTS miteinander verbunden, wäre deshalb falsch.

Richtig ist:

Der Aufbau hat begonnen, erste Funktionen laufen, der flächendeckende Anschluss ist aber ein mehrjähriger Prozess.

13.3 NOOTS ist keine zentrale Bürgerdatenbank

Auch hier ist eine klare Abgrenzung notwendig.

NOOTS ist nach der vorgesehenen Architektur **keine zentrale Datenbank, in der sämtliche Verwaltungsdaten eines Bürgers neu zusammengeführt und dauerhaft gespeichert werden**.

Die deutsche Registerlandschaft bleibt grundsätzlich dezentral.

Die Daten verbleiben in den jeweiligen Registern und Fachsystemen. NOOTS stellt vielmehr technische Komponenten, Schnittstellen und Standards bereit, über die berechtigte Stellen Nachweise austauschen können.

Das ist ein wesentlicher Unterschied.

Dezentrale Speicherung bedeutet jedoch nicht fehlende Vernetzung.

Ein System muss Daten nicht selbst zentral besitzen, um ihre Übermittlung zwischen unterschiedlichen Stellen technisch erheblich zu vereinfachen.

Genau darin liegt die Bedeutung von NOOTS für dieses Dossier.

Die entscheidende Veränderung besteht nicht darin, dass sämtliche Verwaltungsdaten in einer einzigen neuen Datei landen.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Sie besteht darin, dass vorhandene Datenbestände technisch wesentlich leichter zwischen berechtigten Stellen nutzbar gemacht werden können.

13.4 Vom deutschen NOOTS zum europäischen Datenaustausch

NOOTS ist nicht ausschließlich ein nationales Projekt.

Die deutsche Infrastruktur soll über eine Schnittstelle mit dem **European Once-Only Technical System – EU-OOTS** verbunden werden.

Die europäische Grundlage dafür bildet die **Verordnung (EU) 2018/1724 über das Single Digital Gateway**. Sie schafft unter anderem Voraussetzungen dafür, dass bestimmte Nachweise bei grenzüberschreitenden Verwaltungsverfahren innerhalb der Europäischen Union elektronisch ausgetauscht werden können.

Damit wird das Once-Only-Prinzip auf die europäische Ebene erweitert.

Ein Nachweis, der bei einer zuständigen Stelle eines EU-Mitgliedstaates vorhanden ist, soll unter den vorgesehenen Voraussetzungen auch für bestimmte Verwaltungsverfahren in einem anderen Mitgliedstaat genutzt werden können.

EUR-Lex – Verordnung (EU) 2018/1724 über das Single Digital Gateway

Bundesministerium für Digitales und Staatsmodernisierung – Anbindung des NOOTS an das EU-OOTS

Damit wächst die Dimension der Infrastruktur:

Aus dem Datenaustausch zwischen deutschen Verwaltungsstellen kann in bestimmten Verfahren ein grenzüberschreitender europäischer Nachweisaustausch werden.

13.5 Technische Vernetzung bedeutet nicht freien Datenzugriff

An diesem Punkt muss erneut zwischen technischer Möglichkeit und rechtlicher Befugnis unterschieden werden.

Dass zwei Behörden technisch über NOOTS miteinander kommunizieren können, bedeutet nicht, dass Behörde A beliebig sämtliche Informationen von Behörde B abrufen darf.

Ein Datenabruf benötigt weiterhin eine rechtliche Grundlage.

Es gelten insbesondere Zweckbindung, Datenschutzrecht und die jeweiligen fachgesetzlichen Zugriffsregelungen.

NOOTS schafft deshalb **keine allgemeine Abrufbefugnis für alle Behörden auf alle angeschlossenen Register**.

Das ist Tatsache.

Die technische Infrastruktur beantwortet die Frage:

Wie können Nachweise sicher übertragen werden?

Das Recht beantwortet eine andere Frage:

Wer darf welchen Nachweis für welchen Zweck anfordern und erhalten?

Diese Trennung ist für die Bewertung des Systems entscheidend.

13.6 Gerade deshalb werden die Zugriffsregeln wichtiger

Je einfacher der technische Austausch wird, desto wichtiger wird allerdings die rechtliche Kontrolle darüber, wer diesen Austausch auslösen darf.

Denn früher bestand ein Teil der praktischen Hürde bereits darin, dass Behörden technisch voneinander getrennt arbeiteten.

Akten lagen an unterschiedlichen Orten. Systeme waren nicht kompatibel. Nachweise mussten teilweise vom Bürger selbst zwischen Behörden transportiert werden.

Die Digitalisierung beseitigt viele dieser Hindernisse bewusst.

Das ist für eine moderne Verwaltung sinnvoll.

Aber damit verschiebt sich auch die Schutzlinie.

Der Schutz personenbezogener Informationen hängt künftig weniger davon ab, dass eine technische Verbindung schlicht nicht existiert.

Er hängt zunehmend davon ab, dass **gesetzlich festgelegt und technisch durchgesetzt wird, welche Stelle welche Informationen zu welchem Zweck abrufen darf**.

Genau deshalb gehören Protokollierung, Transparenz, Zweckbindung und nachvollziehbare Zugriffsrechte zum Kern der Registermodernisierung.

13.7 Kein Überwachungssystem – aber eine reale Vernetzungsinfrastruktur

Die Begriffe müssen auch bei NOOTS sauber bleiben.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Es gibt keinen Beleg dafür, dass NOOTS als geheime zentrale Bürgerdatenbank oder als allgemeines Überwachungssystem aufgebaut wird.

Eine solche Behauptung wäre durch die vorliegenden offiziellen Dokumente nicht gedeckt.

Belegt ist jedoch:

Deutschland baut eine technische Infrastruktur auf, die den elektronischen Austausch von Verwaltungsnachweisen zwischen berechtigten Stellen erheblich vereinfachen soll.

Belegt ist ebenfalls:

Diese Infrastruktur soll mit dem europäischen Once-Only-System verbunden werden.

Und belegt ist:

Die erste funktionsfähige Version des NOOTS befindet sich seit Januar 2026 im Livebetrieb.

Damit ist die Vernetzung staatlicher Datenstrukturen keine hypothetische Zukunftsvorstellung mehr.

Sie ist ein laufendes Modernisierungsprojekt.

Die politische und rechtliche Kernfrage lautet deshalb nicht, ob Behörden miteinander kommunizieren dürfen.

Sie lautet:

Welche Grenzen gelten für diese Kommunikation – und wie zuverlässig verhindern sie, dass aus einem zweckgebundenen Nachweisaustausch irgendwann eine wesentlich umfassendere Zusammenführung staatlicher Informationen wird?

Genau an diesem Punkt führt die Untersuchung zum nächsten Bereich.

Denn sobald immer mehr Daten digital verfügbar und technisch abrufbar werden, stellt sich zwangsläufig die Frage, welche staatlichen Stellen unter welchen Voraussetzungen Zugriff auf solche Informationen erhalten können.

Damit beginnt die Betrachtung der Sicherheitsbehörden.

14. Sicherheitsbehörden und digitale Daten – Wenn Zugriffsbefugnisse auf vernetzte Systeme treffen

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

14.1 Die entscheidende Frage: Wer darf auf welche Daten zugreifen?

Mit Registermodernisierung, NOOTS, digitaler Identität, elektronischer Patientenakte und europäischen Datenräumen wächst die technische Fähigkeit, Informationen digital bereitzustellen und auszutauschen.

Damit rückt zwangsläufig eine weitere Frage in den Mittelpunkt:

Welche Möglichkeiten besitzen Polizei, Nachrichtendienste und andere Sicherheitsbehörden, auf digitale Daten zuzugreifen?

Dabei muss sauber unterschieden werden. Die Existenz einer digitalen Infrastruktur bedeutet **nicht automatisch**, dass Sicherheitsbehörden auf sämtliche darin enthaltenen Informationen zugreifen dürfen.

Für staatliche Zugriffe gelten gesetzliche Voraussetzungen. Je nach Maßnahme können zusätzlich Richtervorbehalte, besondere Genehmigungsverfahren oder parlamentarische Kontrollmechanismen vorgeschrieben sein.

Bundesverfassungsgericht – Schutz informationstechnischer Systeme und Online-Durchsuchung

Die eigentliche Machtfrage entsteht deshalb aus dem Zusammenspiel zweier Entwicklungen:

Auf der einen Seite wachsen digitale Datenbestände und technische Vernetzungsmöglichkeiten. Auf der anderen Seite entwickeln sich die gesetzlichen und technischen Zugriffsmöglichkeiten staatlicher Sicherheitsbehörden weiter.

14.2 Nachrichtendienste sind keine Polizei

In Deutschland besteht aus historischen Gründen eine bewusste Trennung zwischen Polizei und Nachrichtendiensten.

Nachrichtendienste sammeln und analysieren Informationen. Polizeibehörden besitzen dagegen insbesondere Befugnisse zur Gefahrenabwehr und Strafverfolgung. Nachrichtendienste verfügen grundsätzlich nicht über polizeiliche Zwangsbefugnisse.

Deutscher Bundestag – Nachrichtendienste des Bundes und parlamentarische Kontrolle

Diese Trennung ist für einen demokratischen Rechtsstaat wesentlich.

Sie verhindert jedoch nicht jede Zusammenarbeit.

Informationen können unter den jeweils geltenden gesetzlichen Voraussetzungen zwischen Sicherheitsbehörden übermittelt werden. Genau deshalb kommt es nicht nur darauf an, **welche Behörde eine Information ursprünglich erhoben hat**, sondern auch darauf, unter welchen

Voraussetzungen diese Information anschließend an eine andere Stelle weitergegeben werden darf.

14.3 Das Bundesverfassungsgericht setzt Grenzen

Die Digitalisierung hat das Bundesverfassungsgericht bereits mehrfach beschäftigt.

Besonders grundlegend war das Urteil vom **27. Februar 2008** zur sogenannten Online-Durchsuchung. Das Gericht leitete aus dem allgemeinen Persönlichkeitsrecht das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** ab.

Bundesverfassungsgericht – Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07

Der Staat darf demnach nicht beliebig und ohne hohe rechtliche Voraussetzungen heimlich auf informationstechnische Systeme zugreifen.

Das Urteil zeigt einen Grundkonflikt, der mit zunehmender Digitalisierung immer bedeutender wird:

Je mehr Teile des privaten Lebens auf Computern, Smartphones und digitalen Plattformen stattfinden, desto tiefer kann ein staatlicher Zugriff in die Persönlichkeit eines Menschen eindringen.

14.4 Der Staatstrojaner: Der Staat greift am Endgerät an

Besonders deutlich wird diese Entwicklung bei der **Quellen-Telekommunikationsüberwachung**, häufig als Quellen-TKÜ bezeichnet.

Dabei wird Kommunikation nicht erst irgendwo auf dem Übertragungsweg abgefangen. Stattdessen kann sie unmittelbar am informationstechnischen System des Betroffenen erfasst werden – beispielsweise bevor eine verschlüsselte Nachricht verschlüsselt beziehungsweise nachdem sie entschlüsselt wurde.

Daneben existiert mit der **Online-Durchsuchung** eine noch weitergehende Maßnahme, bei der unter strengen gesetzlichen Voraussetzungen auf gespeicherte Daten eines informationstechnischen Systems zugegriffen werden kann.

Bundeskriminalamt – Telekommunikationsüberwachung und informationstechnische Ermittlungsmaßnahmen

Damit wird eine Grenze sichtbar:

Verschlüsselung schützt Kommunikation auf dem Übertragungsweg. Sie schützt jedoch nicht zwangsläufig vor einem rechtlich zulässigen Zugriff auf das Endgerät selbst.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

14.5 Vorratsdatenspeicherung und IP-Adressen – der Streit geht weiter

Auch die Speicherung von Telekommunikationsdaten bleibt politisch und rechtlich umkämpft.

Der Europäische Gerichtshof hat eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten wiederholt erheblich begrenzt. Gleichzeitig lässt das Unionsrecht unter bestimmten Voraussetzungen gezieltere Speicherungen sowie besondere Regelungen für IP-Adressen zu.

EuGH – Urteil zur deutschen Vorratsdatenspeicherung vom 20. September 2022

Der politische Streit dreht sich deshalb längst nicht mehr ausschließlich um die alte Vorstellung, sämtliche Telekommunikationsdaten aller Bürger pauschal für lange Zeit zu speichern.

Diskutiert werden unterschiedliche Modelle, darunter die zeitlich begrenzte Sicherung bestimmter Daten nach einem konkreten Anlass – das sogenannte **Quick-Freeze-Verfahren** – sowie Regelungen zur Speicherung von IP-Adressen.

Damit bleibt eine zentrale Frage offen:

Wie viel anlasslose Datenspeicherung darf ein Rechtsstaat zulassen, um schwere Straftaten verfolgen zu können?

14.6 Chatkontrolle – Kommunikation selbst gerät in den Fokus

Noch weiter reicht die europäische Auseinandersetzung um die sogenannte **Chatkontrolle**.

Ausgangspunkt ist ein legitimes und dringendes Ziel: die Bekämpfung des sexuellen Missbrauchs von Kindern und der Verbreitung entsprechender Darstellungen im Internet.

Umstritten ist jedoch, welche technischen Maßnahmen dafür eingesetzt werden dürfen.

Seit **2022** wird auf EU-Ebene über eine Verordnung beraten, die Verpflichtungen für bestimmte Kommunikations- und Onlinedienste zur Erkennung und Bekämpfung von Missbrauchsdarstellungen schaffen soll.

Europäische Kommission – Vorschlag zur Bekämpfung sexuellen Kindesmissbrauchs vom 11. Mai 2022

Das Vorhaben löste erhebliche Datenschutz- und Grundrechtsbedenken aus. Der **Europäische Datenschutzbeauftragte (EDPS)** und der **Europäische Datenschutzausschuss (EDPB)** warnten bereits 2022 gemeinsam davor, dass der ursprüngliche Vorschlag Risiken für eine allgemeine und unterschiedslose Überwachung privater Kommunikation schaffen könne.

EDPB/EDPS – Gemeinsame Stellungnahme zum EU-Vorschlag gegen Kindesmissbrauch

Damit geht es nicht um die Frage, **ob Kinder geschützt werden müssen**.

Es geht um die Frage, **ob und unter welchen Voraussetzungen private digitale Kommunikation technisch untersucht werden darf, um dieses Ziel zu erreichen.**

Wer die Entwicklung der **EU-Chatkontrolle**, ihre möglichen Auswirkungen auf vertrauliche Kommunikation und die damit verbundenen Grundrechtsfragen vertiefen möchte, findet dazu zwei ausführliche KLARTEXT-Dossiers:

Wer schützt uns vor der Politik?

Chatkontrolle – unter Generalverdacht

Beide Dossiers beleuchten die Chatkontrolle ausführlicher, als es im Rahmen dieses übergreifenden Dossiers möglich ist.

14.7 Der entscheidende Konflikt: Sicherheit gegen Vertraulichkeit?

Sicherheitsbehörden benötigen wirksame Instrumente gegen Terrorismus, organisierte Kriminalität, Cyberangriffe und schwere Straftaten.

Ebenso benötigt eine freie Gesellschaft Bereiche vertraulicher Kommunikation.

Der Konflikt entsteht dort, wo Maßnahmen zur Gefahrenabwehr technisch so weit reichen, dass sie nicht nur einen konkreten Verdächtigen, sondern große Teile der Bevölkerung erfassen könnten.

Genau deshalb sind Begriffe wie **Verhältnismäßigkeit, Richtervorbehalt, Zweckbindung, Löschfristen und effektive Kontrolle** von zentraler Bedeutung.

Die entscheidende Frage lautet nicht:

Sicherheit oder Datenschutz?

Sie lautet:

Welche Eingriffe sind zur Abwehr einer konkreten Gefahr tatsächlich notwendig – und welche Kontrollinstrumente verhindern, dass außergewöhnliche Befugnisse irgendwann zum Normalzustand werden?

14.8 Die Infrastruktur verändert das Machtpotenzial

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

An diesem Punkt schließt sich der Kreis zu den vorherigen Kapiteln.

Eine elektronische Patientenakte ist kein Geheimdienstsystem.

NOOTS ist kein Polizeisystem.

Die EUDI-Wallet ist kein Überwachungsinstrument.

Der digitale Euro ist kein Staatstrojaner.

Und ein interoperables Register ist keine Online-Durchsuchung.

Diese Trennung ist eine Tatsache und muss bestehen bleiben.

Die Risikobetrachtung beginnt eine Ebene darüber.

Je mehr gesellschaftliche Vorgänge digitalisiert werden, desto größer wird grundsätzlich die Menge der Informationen, die technisch verarbeitet werden können.

Je stärker Systeme interoperabel werden, desto größer wird grundsätzlich ihre technische Anschlussfähigkeit.

Und je weiter staatliche Zugriffsbefugnisse reichen, desto wichtiger werden die gesetzlichen Grenzen zwischen diesen Bereichen.

Daraus folgt nicht, dass der Staat bereits ein vollständiges digitales Bürgerprofil erstellt.

Es folgt jedoch eine wesentlich wichtigere Erkenntnis:

Der Schutz des Bürgers hängt zunehmend nicht davon ab, was technisch unmöglich ist – sondern davon, was rechtlich verboten bleibt.

Und Gesetze sind keine technischen Barrieren.

Sie können durch politische Mehrheiten verändert werden.

15. Digitale Nachweise – Wenn immer mehr Teile des Alltags in die Wallet wandern

15.1 Der digitale Personalausweis ist nicht das Ende der Entwicklung

Die europäische digitale Identität wird häufig mit einem digitalen Personalausweis gleichgesetzt. Tatsächlich ist die geplante **EUDI-Wallet** wesentlich breiter angelegt.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Sie soll nicht nur die Identität eines Menschen elektronisch nachweisen. Die technische Architektur ist darauf ausgelegt, unterschiedliche digitale Nachweise – sogenannte **Attribute und Bescheinigungen** – aufzunehmen und gegenüber Behörden oder privaten Diensten vorzuzeigen.

Die Europäische Kommission nennt als mögliche beziehungsweise bereits entwickelte Anwendungsbereiche unter anderem **Führerschein, Bildungsabschlüsse, berufliche Qualifikationen, Gesundheitsnachweise, Bankkontoeröffnung, elektronische Signaturen und weitere persönliche Dokumente**.

EU-Kommission – European Digital Identity

Damit ist eine wichtige Tatsache festzuhalten:

Die Wallet ist von ihrer Konzeption her keine Einzweck-Anwendung. Sie ist als Plattform für unterschiedliche digitale Nachweise angelegt.

15.2 Der Führerschein wird Teil der digitalen Identitätsinfrastruktur

Ein konkretes Beispiel ist der **mobile Führerschein**.

Die EU hat 2025 die neuen europäischen Führerscheinregeln verabschiedet. Vorgesehen ist ein digitaler Führerschein, der auf dem Smartphone verfügbar sein und mit der europäischen digitalen Identitäts-Wallet verbunden werden kann.

Der digitale Führerschein soll nach den neuen EU-Regeln schrittweise zum Regelformat werden; gleichzeitig bleibt das Recht auf einen physischen Führerschein erhalten.

Europäische Kommission – neue EU-Führerscheinregeln

Damit wandert ein weiterer staatlicher Nachweis in dieselbe digitale Umgebung, die auch für Identitätsnachweise und andere Dokumente vorgesehen ist.

Die Entwicklung folgt damit einem erkennbaren Prinzip:

Nicht für jeden Nachweis entsteht dauerhaft eine vollständig isolierte digitale Welt. Unterschiedliche Nachweise sollen innerhalb gemeinsamer digitaler Identitätsstrukturen verwendbar werden.

15.3 Auch der Schwerbehindertenausweis soll digital werden

Die Entwicklung reicht bis in den deutschen Sozialstaat.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Das Bundesministerium für Arbeit und Soziales plant ausdrücklich, auch den **Schwerbehindertenausweis als digitalen Nachweis über die EUDI-Wallet** verfügbar zu machen.

Das Vorhaben ist Teil der Modernisierung digitaler Sozialleistungen. Neben dem Schwerbehindertenausweis nennt das Ministerium weitere Nachweise, darunter den **Rentenversicherungsausweis** und die **A1-Bescheinigung**.

Bundesministerium für Arbeit und Soziales – Ausbau digitaler Leistungsangebote

Damit erreicht die Wallet einen besonders sensiblen Bereich.

Ein Schwerbehindertenausweis ist nicht lediglich irgendein Dokument. Bereits die Tatsache, dass ein solcher Nachweis vorhanden ist, betrifft einen besonders geschützten persönlichen Lebensbereich.

Das bedeutet nicht, dass sämtliche zugrunde liegenden Gesundheitsdaten automatisch in der Wallet gespeichert werden.

Es bedeutet aber, dass künftig auch ein sozial- und gesundheitsbezogener Status digital nachweisbar gemacht werden soll.

15.4 Die Wallet soll nur das preisgeben, was benötigt wird

Gerade deshalb ist ein wichtiges technisches Prinzip vorgesehen: **selektive Offenlegung**.

Ein Nutzer soll nach dem europäischen Konzept nicht zwangsläufig sein vollständiges digitales Dokument vorzeigen müssen, wenn lediglich eine einzelne Eigenschaft benötigt wird.

Ein klassisches Beispiel ist der Altersnachweis.

Muss ein Dienst lediglich wissen, ob jemand älter als 18 Jahre ist, soll grundsätzlich die Information **„über 18“** übermittelt werden können, anstatt Name, Geburtsdatum, Anschrift und weitere Identitätsdaten offenzulegen.

Die EU beschreibt Datenschutz und Datenminimierung ausdrücklich als grundlegende Bestandteile der Wallet-Architektur.

EU-Kommission – Architektur und Referenzrahmen der EUDI-Wallet

Das ist ein erheblicher Datenschutzvorteil gegenüber Verfahren, bei denen ein vollständiges Dokument kopiert oder fotografiert wird.

Aber auch hier entscheidet die konkrete Umsetzung darüber, wie stark dieser Schutz in der Praxis tatsächlich ist.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

15.5 Nicht alles wird in einer einzigen zentralen Datei gespeichert

Die Vorstellung, die EUDI-Wallet werde zu einer zentralen EU-Datenbank, in der Führerschein, Krankengeschichte, Bankkonto, Schwerbehindertenstatus und sämtliche anderen Informationen eines Menschen gemeinsam gespeichert werden, ist **nicht durch den geltenden Rechtsrahmen gedeckt**.

Die Wallet soll vielmehr unterschiedliche digitale Nachweise verwalten beziehungsweise deren Verwendung ermöglichen.

Die jeweiligen Ausgangsdaten können weiterhin aus unterschiedlichen Registern und Fachsystemen stammen.

Diese Unterscheidung ist entscheidend:

Gemeinsame Nutzbarkeit bedeutet nicht automatisch gemeinsame zentrale Speicherung.

Die datenschutzrechtliche Frage verschwindet dadurch allerdings nicht.

Sie verschiebt sich.

Entscheidend wird zunehmend, **welche Nachweise miteinander verwendet werden können, welche Stellen sie ausstellen, welche Stellen sie verlangen dürfen und welche technischen Informationen bei ihrer Nutzung entstehen.**

15.6 Die Architektur ist ausdrücklich erweiterbar

Für die langfristige Bewertung ist ein weiterer Punkt entscheidend.

Die Europäische Kommission entwickelt für die EUDI-Wallet einen gemeinsamen **Architecture and Reference Framework (ARF)**. Dazu gehören technische Spezifikationen, gemeinsame Standards, Protokolle und Referenzimplementierungen.

Die Kommission stellt außerdem Open-Source-Komponenten für die Entwicklung der Wallet-Infrastruktur bereit.

EU-Kommission – EUDI Wallet Toolbox

Damit ist die Wallet technisch nicht auf die heute vorhandenen Anwendungsfälle eingefroren.

Neue digitale Nachweise und Anwendungsfälle können grundsätzlich in die Infrastruktur integriert werden, sofern dafür die technischen und rechtlichen Voraussetzungen geschaffen werden.

Das ist keine Vermutung über einen geheimen Plan.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die Erweiterbarkeit gehört zum technischen Konzept einer solchen digitalen Wallet-Infrastruktur.

15.7 Was heute vorgesehen ist, muss nicht der Endzustand sein

Genau an dieser Stelle muss zwischen Tatsache und Zukunftsfrage unterschieden werden.

Tatsache ist: Die EUDI-Wallet ist für unterschiedliche digitale Nachweise konzipiert.

Tatsache ist: Weitere Dokumente und Funktionen werden bereits vorbereitet.

Tatsache ist: Die technische Architektur wird über gemeinsame Standards und Komponenten weiterentwickelt.

Daraus folgt jedoch **nicht**, dass jede technisch mögliche Funktion eines Tages tatsächlich eingeführt wird.

Diese Entscheidung bleibt politisch und rechtlich.

Aber damit entsteht eine berechtigte Frage:

Wenn eine Infrastruktur bewusst so aufgebaut wird, dass weitere Nachweise und Funktionen integriert werden können – welche Grenzen sollen für diese Erweiterungen dauerhaft gelten?

15.8 Die entscheidende Frage lautet nicht: Was kann die Wallet heute?

Eine digitale Brieftasche kann bequem sein.

Ein Führerschein auf dem Smartphone kann Behördengänge ersparen. Digitale Nachweise können Papier reduzieren. Selektive Offenlegung kann sogar mehr Datenschutz ermöglichen als das Vorzeigen eines vollständigen Dokuments.

Das alles gehört zur Tatsachenlage.

Doch für eine langfristige Betrachtung reicht die Frage nach dem heutigen Funktionsumfang nicht aus.

Entscheidend ist:

Welche Fähigkeiten besitzt die zugrunde liegende Infrastruktur?

Welche zusätzlichen Nachweise können technisch integriert werden?

Welche Stellen dürfen diese Nachweise künftig verlangen?

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Welche Nutzungsspuren entstehen dabei?

Und welche gesetzlichen Grenzen verhindern, dass aus freiwilligem digitalem Komfort irgendwann eine faktische Voraussetzung für gesellschaftliche Teilhabe wird?

Die EUDI-Wallet muss deshalb nicht danach beurteilt werden, welche theoretischen Schreckensszenarien sich konstruieren lassen.

Sie muss daran gemessen werden, **welche Funktionen tatsächlich eingebaut werden, welche Erweiterungen beschlossen werden und welche Rechte der Bürger behält, wenn immer mehr Teile seines Alltags digital nachweisbar werden.**

16. Das Gesamtbild – Wenn aus einzelnen Digitalprojekten eine Machtfrage wird

16.1 Der entscheidende Perspektivwechsel

Bis hierher wurden zahlreiche Systeme getrennt betrachtet: digitale Identität, EUDI-Wallet, elektronische Patientenakte, Europäischer Gesundheitsdatenraum, Registermodernisierung, NOOTS, digitaler Euro, AMLA, Chatkontrolle und staatliche Zugriffsbefugnisse.

Jedes dieser Projekte besitzt einen eigenen Zweck, eine eigene Rechtsgrundlage und eigene Schutzmechanismen.

Genau deshalb wäre es falsch, sie als bereits bestehendes einheitliches Überwachungssystem darzustellen.

Doch ebenso unvollständig wäre es, jedes Projekt ausschließlich isoliert zu betrachten.

Denn die Europäische Union verfolgt eine umfassende digitale Transformation. Im Bericht zur **Digitalen Dekade 2026** bewertet die Kommission ausdrücklich die Fortschritte auf dem Weg zu ihren Digitalzielen für 2030 und fordert in mehreren Bereichen eine schnellere Umsetzung.

EU-Kommission – Bericht zur Digitalen Dekade 2026

Die entscheidende Frage dieses Dossiers lautet deshalb:

Was entsteht, wenn immer mehr Bereiche des Lebens digital erfasst, standardisiert und technisch anschlussfähig werden?

16.2 Die einzelnen Bausteine ergeben noch kein Gesamtsystem

Eine EUDI-Wallet enthält nicht automatisch die Krankenakte eines Bürgers.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

NOOTS übermittelt nicht automatisch Bankdaten.

AMLA erhält nicht automatisch Zugriff auf sämtliche Verwaltungsregister.

Der digitale Euro ist nicht automatisch mit Gesundheitsdaten verbunden.

Und Sicherheitsbehörden erhalten nicht allein deshalb Zugriff auf ein System, weil dieses digital existiert.

Diese Grenzen sind Tatsachen.

Aber gleichzeitig entstehen immer mehr digitale Infrastrukturen, die Personen eindeutig identifizieren, Nachweise elektronisch bereitstellen, Daten zwischen berechtigten Stellen übertragen oder Informationen technisch verarbeiten können.

Damit wächst nicht automatisch die Überwachung.

Es wächst zunächst die technische Fähigkeit zur Verarbeitung und Vernetzung.

16.3 Selbst Europas Datenschutzaufsicht warnt vor dem Überwachungspotenzial

Dass diese Frage nicht lediglich von Kritikern der Digitalisierung gestellt wird, zeigt ausgerechnet der **Europäische Datenschutzbeauftragte (EDPS)**.

Der EDPS weist darauf hin, dass technischer Fortschritt Überwachung, Verfolgung und Profilbildung **einfacher, günstiger und präziser** gemacht hat. Überwachung habe sowohl im öffentlichen als auch im privaten Bereich zugenommen und könne unter anderem Meinungs- und Vereinigungsfreiheit beeinträchtigen.

Europäischer Datenschutzbeauftragter – Surveillance

Auch speziell bei digitalen Identitäten warnt der EDPS davor, dass große Mengen personenbezogener Daten von unterschiedlichen Akteuren verwendet oder missbraucht werden könnten. Er nennt ausdrücklich die Notwendigkeit, Risiken **allgemeiner und gezielter Überwachung** entgegenzuwirken.

Damit ist die grundsätzliche Risikofrage keine Verschwörungstheorie.

Sie wird von der europäischen Datenschutzaufsicht selbst behandelt.

16.4 Die DSGVO bleibt eine zentrale Schutzmauer

Dem Ausbau digitaler Infrastrukturen steht gleichzeitig ein umfangreiches Datenschutzrecht gegenüber.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die DSGVO gibt Bürgern unter anderem Rechte auf Information, Auskunft, Berichtigung und unter bestimmten Voraussetzungen Löschung personenbezogener Daten. Die Europäische Kommission bezeichnet die DSGVO auch 2026 als zentralen Bestandteil des europäischen Grundrechtsschutzes.

EU-Kommission – Zehn Jahre DSGVO: Rechte der Bürger

Das bedeutet:

Die zunehmende Digitalisierung findet nicht in einem rechtsfreien Raum statt.

Doch Datenschutzrecht besitzt eine Besonderheit, die für dieses gesamte Dossier entscheidend ist:

Es verhindert nicht, dass Daten verarbeitet werden.

Es bestimmt, **unter welchen Voraussetzungen** sie verarbeitet werden dürfen.

Damit liegt ein erheblicher Teil des Schutzes des Bürgers nicht mehr darin, dass bestimmte Informationen technisch überhaupt nicht verfügbar wären.

Der Schutz liegt zunehmend darin, **dass ihre Verwendung rechtlich begrenzt bleibt.**

16.5 Was technisch möglich ist, ist nicht automatisch erlaubt

Dieser Unterschied zieht sich durch nahezu das gesamte Dossier.

Eine eindeutige digitale Identität kann technisch verwendet werden, um eine Person zuverlässig zuzuordnen.

Interoperable Register können technisch Informationen austauschen.

Digitale Wallets können technisch zusätzliche Nachweise aufnehmen.

Digitale Gesundheitsdaten können technisch verarbeitet werden.

Elektronische Zahlungssysteme können technisch Transaktionsinformationen erzeugen.

KI-Systeme können große Datenmengen wesentlich schneller analysieren als Menschen.

Aber:

Technische Möglichkeit ist keine rechtliche Erlaubnis.

Gerade deshalb werden Gesetze, Zweckbindungen und Zugriffsbeschränkungen immer wichtiger.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

16.6 Künstliche Intelligenz verändert die Größenordnung

Zu dieser Infrastruktur kommt inzwischen ein weiterer Faktor: **künstliche Intelligenz**.

Je größer digitale Datenbestände werden, desto leistungsfähiger werden grundsätzlich auch die Möglichkeiten, darin Muster, Beziehungen und Auffälligkeiten automatisiert zu erkennen.

Die EU selbst reguliert dieses Potenzial inzwischen mit dem **AI Act**. Bestimmte KI-Anwendungen werden verboten; für Hochrisikosysteme gelten besondere Anforderungen. Die Kommission nennt beispielsweise KI-Anwendungen in kritischen Infrastrukturen, Bildung, Beschäftigung, Finanzdienstleistungen und Gesundheitswesen als Bereiche mit besonderen Anforderungen.

EU-Kommission – KI, AI Act und Grundrechtsschutz

Damit bekommt die Frage nach großen digitalen Datenbeständen eine zusätzliche Dimension.

Es geht künftig nicht nur darum, welche Daten gespeichert werden. Es geht auch darum, was leistungsfähige Analysesysteme aus vorhandenen Daten ableiten können.

16.7 Der Staat muss nicht alles in einer Datenbank besitzen

Die Vorstellung staatlicher Kontrolle wird häufig mit einer gigantischen zentralen Datenbank verbunden, in der sämtliche Informationen über jeden Bürger gespeichert werden.

Doch technisch ist eine solche Zentralisierung nicht zwingend erforderlich.

Informationen können in unterschiedlichen Systemen verbleiben und trotzdem – sofern technische Schnittstellen und entsprechende Rechtsgrundlagen vorhanden sind – für bestimmte Zwecke ausgetauscht oder verarbeitet werden.

Gerade deshalb ist der Begriff **Interoperabilität** so entscheidend.

Die Macht einer digitalen Infrastruktur bemisst sich nicht ausschließlich danach, wie viele Informationen sich auf einem einzigen Server befinden.

Sie bemisst sich auch danach:

Welche Systeme können miteinander kommunizieren?

Welche eindeutigen Zuordnungen sind möglich?

Wer besitzt Zugriffsrechte?

Welche Daten dürfen zusammengeführt werden?

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Welche Analysen dürfen daraus entstehen?

16.8 Der Schutz hängt zunehmend vom Gesetzgeber ab

Damit entsteht eine politische Abhängigkeit, die bei einer rein technischen Betrachtung leicht übersehen wird.

Was heute verboten ist, kann technisch trotzdem möglich sein.

Eine Behörde darf eine bestimmte Information möglicherweise heute nicht abrufen.

Ein Gesetzgeber kann Zugriffsrechte jedoch erweitern.

Eine ursprünglich freiwillige Funktion kann gesetzlich anders geregelt werden.

Speicherfristen können verändert werden.

Neue Ausnahmen können geschaffen werden.

Andere Ausnahmen können Gerichte wiederum für unverhältnismäßig erklären.

Das bedeutet nicht, dass jede denkbare Verschärfung kommen wird.

Es bedeutet aber:

Je leistungsfähiger die Infrastruktur wird, desto bedeutender werden die politischen Mehrheiten, die über ihre gesetzlichen Grenzen entscheiden.

16.9 Deshalb gehört auch die Opposition in diese Betrachtung

Bei jeder zukünftigen Erweiterung dieser Systeme reicht es nicht, lediglich festzustellen, was „die EU“ oder „die Bundesregierung“ beschlossen hat.

Entscheidend ist ebenso:

Wer hat den Vorschlag eingebracht?

Welche Regierung war verantwortlich?

Welche Parteien haben zugestimmt?

Welche Parteien haben abgelehnt?

Welche Änderungen hat die Opposition verlangt?

Und wie wurde am Ende tatsächlich abgestimmt?

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Gerade die Registermodernisierung hat bereits gezeigt, dass selbst Parteien, die gemeinsam gegen ein Regierungsvorhaben stimmen, **unterschiedliche Gründe und unterschiedliche Alternativen** vertreten können.

Deshalb werden in diesem Dossier politische Positionen nicht danach bewertet, ob sie Regierung oder Opposition vertreten.

Entscheidend sind **Dokumente, Forderungen und Abstimmungen**.

16.10 Die entscheidende Warnung kommt nicht von außen

Bemerkenswert ist, dass selbst die europäischen Institutionen die Gefahren der Digitalisierung keineswegs vollständig bestreiten.

Der EDPS bezeichnet Überwachung ausdrücklich als Eingriff in die Grundrechte auf Datenschutz und Privatsphäre und fordert dafür gesetzliche Grundlage, Notwendigkeit und Verhältnismäßigkeit.

Gleichzeitig baut die EU ihre digitale Infrastruktur weiter aus. Für die Zeit bis 2030 bestehen konkrete Digitalisierungsziele; 2027 sollen diese Ziele bereits erneut überprüft und an technologische und politische Entwicklungen angepasst werden.

Genau darin liegt der politische Spannungsbogen:

Europa will digitaler werden. Gleichzeitig muss Europa seine Bürger vor den Machtmöglichkeiten schützen, die eine immer leistungsfähigere digitale Infrastruktur überhaupt erst entstehen lässt.

16.11 Die Frage ist nicht, ob die Technik böse ist

Eine digitale Identität kann Verwaltungswege vereinfachen.

Digitale Gesundheitsdaten können Ärzten helfen.

Interoperable Register können Bürokratie reduzieren.

Digitale Zahlungen können bequem sein.

KI kann medizinische Diagnostik, Verwaltung und Forschung verbessern.

Cyberabwehr kann kritische Infrastruktur schützen.

Die entscheidende Frage lautet deshalb nicht:

Ist Digitalisierung gut oder schlecht?

Sie lautet:

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Wer kontrolliert die Infrastruktur – und wer kontrolliert diejenigen, die sie kontrollieren?

Denn eine leistungsfähige Infrastruktur bleibt nicht deshalb freiheitlich, weil sie ursprünglich mit einem nützlichen Zweck geschaffen wurde.

Sie bleibt freiheitlich, wenn ihre Grenzen **rechtlich, technisch und demokratisch dauerhaft durchsetzbar sind.**

16.12 Der Punkt, an dem Vorsorge beginnen muss

Eine demokratische Gesellschaft sollte nicht erst dann über Machtbegrenzung sprechen, wenn ein Missbrauch bereits stattgefunden hat.

Der richtige Zeitpunkt ist vorher.

Solange Systeme entwickelt, Gesetze beschlossen und technische Standards festgelegt werden, können Schutzmechanismen eingebaut werden.

Später können Abhängigkeiten entstehen, die wesentlich schwieriger zurückzudrehen sind.

Deshalb ist die zentrale Frage dieses Dossiers keine Behauptung über einen bereits vollendeten Überwachungsstaat.

Sie ist eine Frage an die Gegenwart:

Wenn wir heute die digitale Infrastruktur für die kommenden Jahrzehnte errichten – welche Grenzen bauen wir gleichzeitig ein, damit sie auch morgen noch dem Bürger dient und nicht der Bürger ihr?

17. Schlussbetrachtung – Der digitale Staat ist längst im Aufbau

17.1 Was dieses Dossier belegt

Die Ausgangsfrage war einfach:

Entsteht mit der zunehmenden Digitalisierung lediglich ein modernerer Staat – oder zugleich eine Infrastruktur, die künftig wesentlich weiterreichende Kontrollmöglichkeiten eröffnen kann?

Nach der Untersuchung lässt sich eines eindeutig feststellen:

Die Digitalisierung staatlicher und gesellschaftlicher Strukturen ist **keine Zukunftsvision mehr**.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Die EUDI-Wallet soll den Bürgern in der Europäischen Union bis Ende **2026** zur Verfügung stehen und für öffentliche wie private Dienstleistungen einsetzbar sein. Die EU beschreibt sie ausdrücklich als Instrument, mit dem digitale Dokumente gespeichert, Identitätsmerkmale nachgewiesen und rechtsverbindliche Signaturen erstellt werden können.

EU-Kommission – European Digital Identity

EU-Kommission – EUDI-Verordnung und Umsetzung

Der Europäische Gesundheitsdatenraum ist seit **26. März 2025** geltendes EU-Recht und befindet sich in seiner mehrjährigen Umsetzungsphase. Gesundheitsdaten sollen künftig grenzüberschreitend für die Behandlung und unter gesetzlichen Voraussetzungen auch für Sekundärzwecke nutzbar werden.

EU-Kommission – European Health Data Space

EU-Kommission – Sekundärnutzung von Gesundheitsdaten

Beim digitalen Euro laufen ebenfalls konkrete technische Vorbereitungen. Die EZB plant ab der zweiten Jahreshälfte **2027** einen zwölfmonatigen Pilotbetrieb und will für eine mögliche erste Ausgabe **2029** bereit sein. Voraussetzung bleibt die vorherige Verabschiedung des europäischen Rechtsrahmens; die endgültige Entscheidung über eine Ausgabe ist damit noch nicht gefallen.

EZB – Der digitale Euro

EZB – Pilotprojekt zum digitalen Euro

Parallel werden staatliche Register modernisiert, digitale Nachweiswege aufgebaut, Gesundheitsdatenräume geschaffen, Finanzaufsicht stärker vernetzt und Sicherheitsbefugnisse an die digitale Bedrohungslage angepasst.

Diese Entwicklung findet statt.

17.2 Was dieses Dossier nicht belegt

Ebenso klar muss festgehalten werden, was sich aus den untersuchten Quellen **nicht** ableiten lässt.

Es gibt keinen Nachweis dafür, dass heute bereits eine zentrale Datenbank existiert, in der Identitätsdaten, Gesundheitsinformationen, Banktransaktionen, Verwaltungsdaten und sämtliche weiteren Informationen über jeden Bürger automatisch zu einem vollständigen Persönlichkeitsprofil zusammengeführt werden.

Es gibt ebenfalls keinen Beleg dafür, dass EUDI-Wallet, elektronische Patientenakte, EHDS, digitaler Euro, NOOTS oder andere untersuchte Systeme bereits als ein gemeinsamer Überwachungsapparat betrieben werden.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Wer das behauptet, würde weiter gehen, als die derzeitige Beleglage trägt.

Aber genau hier beginnt die wichtigere Frage.

17.3 Die entscheidende Veränderung ist die technische Möglichkeit

Früher lagen Informationen häufig in getrennten Akten, Behörden, Karteien und Systemen.

Ihre Zusammenführung war technisch aufwendig.

Heute entstehen standardisierte digitale Datenbestände, eindeutige Identifikatoren, gemeinsame Schnittstellen und interoperable Systeme.

Gesundheitsakten sollen beispielsweise ab **2029** technische Komponenten für Interoperabilität und Zugriffsprotokollierung enthalten; weitere prioritäre Datenkategorien folgen ab 2031.

EU-Kommission – Interoperabilität elektronischer Gesundheitsakten im EHDS

Das bedeutet nicht automatisch Überwachung.

Aber es bedeutet:

Die technischen Hürden für Verarbeitung, Übertragung und – dort, wo das Recht es zulässt – Verknüpfung werden geringer.

Damit verschiebt sich der Schutz des Bürgers.

Immer häufiger schützt ihn nicht mehr die technische Unmöglichkeit einer Zusammenführung.

Es schützt ihn das Gesetz.

17.4 Und genau deshalb wird politische Macht entscheidend

Gesetze können festlegen, welche Daten verarbeitet werden dürfen.

Gesetze können Zugriffsrechte schaffen.

Gesetze können Zweckbindungen verändern.

Gesetze können Ausnahmen für Sicherheitsbehörden definieren.

Gesetze können Widerspruchsmöglichkeiten stärken – oder einschränken.

Und Gesetze können durch neue parlamentarische Mehrheiten geändert werden.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Das bedeutet nicht, dass jeder denkbare Eingriff auch tatsächlich beschlossen werden wird.

Es bedeutet aber, dass mit wachsender technischer Leistungsfähigkeit der Infrastruktur die Bedeutung politischer Entscheidungen zunimmt.

Je mehr technisch möglich wird, desto entscheidender wird die Frage, was rechtlich erlaubt bleibt.

17.5 Die Schutzmechanismen sind real – und müssen es bleiben

Zur vollständigen Wahrheit gehört deshalb auch:

Die untersuchten Systeme enthalten zahlreiche Schutzmechanismen.

Die EUDI-Wallet soll freiwillig sein und dem Nutzer Kontrolle über die freigegebenen Daten geben. Die EU stellt Datenschutz und Sicherheit ausdrücklich ins Zentrum des Systems.

Der EHDS enthält Regeln für Zugriffsrechte, sichere Verarbeitungsumgebungen, Widerspruchsmöglichkeiten und Transparenz über die Sekundärnutzung.

Beim digitalen Euro erklärt die EZB, dass Datenschutz ein zentrales Konstruktionsprinzip sein soll und sie für eine mögliche Einführung erst nach Abschluss des Gesetzgebungsverfahrens bereit sein will.

Diese Schutzregeln dürfen nicht als bloße Nebensache behandelt werden.

Sie sind heute ein wesentlicher Teil der Grenze zwischen Digitalisierung und unkontrollierter Überwachung.

Gerade deshalb muss beobachtet werden, ob diese Grenzen mit jeder Erweiterung der Systeme erhalten bleiben.

17.6 Das eigentliche Risiko liegt in der Summe

Eine digitale Identität kann nützlich sein.

Eine elektronische Patientenakte kann medizinische Behandlung verbessern.

Ein interoperables Register kann Behördengänge vereinfachen.

Ein digitaler Euro kann eine zusätzliche Zahlungsform schaffen.

Eine europäische Geldwäscheaufsicht kann Finanzkriminalität erschweren.

Eine stärkere Cyberabwehr kann kritische Infrastruktur schützen.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Jeder einzelne Baustein besitzt nachvollziehbare Begründungen.

Die gesellschaftliche Machtfrage entsteht aus ihrer Summe.

Denn je mehr Bereiche des Lebens digital organisiert werden, desto größer wird der Anteil persönlicher und gesellschaftlicher Vorgänge, der grundsätzlich elektronisch erfassbar, auswertbar und – bei entsprechender Rechtsgrundlage – miteinander verknüpfbar wird.

Die Frage lautet deshalb nicht:

„Ist jedes dieser Systeme böse?“

Sie lautet:

„Welche Macht entsteht, wenn immer mehr dieser Systeme gleichzeitig existieren?“

17.7 Der Bürger darf nicht erst erfahren, was mit seinen Daten geschieht, wenn es zu spät ist

Ein zentrales Ergebnis dieser Untersuchung betrifft deshalb die **Transparenz**.

Wer personenbezogene Daten verarbeitet, muss im Rahmen der geltenden Rechtsordnung erklären können:

Welche Daten werden verarbeitet?

Zu welchem Zweck?

Auf welcher Rechtsgrundlage?

Wer hat Zugriff?

An wen wurden Daten übermittelt?

Wie lange werden sie gespeichert?

Welche Rechte besitzt der Betroffene?

Und was geschieht trotz eines eingelegten Widerspruchs weiterhin?

Gerade bei Gesundheits- und Identitätsdaten genügt es nicht, dem Bürger abstrakt mitzuteilen, seine Daten seien „geschützt“.

Er muss überprüfen können, was tatsächlich mit ihnen geschieht.

17.8 Digitalisierung braucht nicht weniger Kontrolle – sondern mehr

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Je leistungsfähiger staatliche und europäische Infrastrukturen werden, desto wichtiger werden unabhängige Kontrollinstanzen.

Datenschutzbehörden, Gerichte, Parlamente, unabhängige Kontrollräte und eine kritische Öffentlichkeit sind deshalb keine Gegner einer funktionierenden Digitalisierung.

Sie sind ihre Voraussetzung.

Denn eine Infrastruktur, die nur deshalb ungefährlich ist, weil die heute Verantwortlichen versprechen, sie niemals zu missbrauchen, wäre kein ausreichender Schutz.

Ein freiheitlicher Rechtsstaat muss so konstruiert sein, dass Missbrauch auch dann begrenzt wird, wenn eines Tages andere Personen über dieselben technischen Möglichkeiten verfügen.

17.9 Die wichtigste Frage richtet sich an die Zukunft

Die EUDI-Wallet startet nach dem europäischen Zeitplan Ende 2026. Der EHDS wird in mehreren Stufen ausgebaut. Der digitale Euro wird technisch für einen möglichen Start 2029 vorbereitet. Weitere digitale Nachweise und Anwendungen kommen hinzu.

Damit ist diese Entwicklung nicht abgeschlossen.

Sie beginnt gerade erst, ihre volle praktische Wirkung zu entfalten.

Die entscheidende Frage lautet deshalb:

Welche Grenze setzen wir heute einer Infrastruktur, deren Möglichkeiten morgen wesentlich größer sein können als bei ihrer Einführung?

Nicht jede technische Möglichkeit muss genutzt werden.

Nicht jede denkbare Verknüpfung muss erlaubt werden.

Nicht jede Sicherheitsbegründung rechtfertigt jeden Eingriff.

Und nicht jede freiwillig eingeführte digitale Lösung muss für immer freiwillig bleiben, wenn der Gesetzgeber die Regeln verändert.

Genau deshalb darf öffentliche Kontrolle nicht erst beginnen, wenn die Systeme vollständig etabliert sind.

Sie muss stattfinden, während sie gebaut werden.

17.10 Schlusswort – Hinsehen, solange noch entschieden wird

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Dieses Dossier kommt nicht zu dem Ergebnis, dass Europa oder Deutschland bereits einen vollständigen digitalen Überwachungsstaat geschaffen haben.

Eine solche Feststellung wäre anhand der untersuchten Quellen nicht belegbar.

Es kommt jedoch zu einem anderen Ergebnis:

Die technische Infrastruktur, auf deren Grundlage wesentlich weiterreichende Kontrolle eines Tages möglich werden könnte, wird in zahlreichen Bereichen aufgebaut.

Ob daraus eine Gefahr für Freiheit und informationelle Selbstbestimmung entsteht, hängt entscheidend davon ab, welche gesetzlichen Grenzen bestehen, welche Zugriffsrechte geschaffen werden, welche Daten miteinander verbunden werden dürfen und wie wirksam Bürger, Gerichte, Parlamente und Datenschutzbehörden diese Grenzen kontrollieren.

Deshalb darf die Frage nicht erst gestellt werden, wenn eine Grenze überschritten wurde.

Sie muss vorher gestellt werden.

Wer bekommt welche Daten?

Wer darf sie miteinander verbinden?

Wer entscheidet darüber?

Wer kontrolliert diese Entscheidung?

Und welche Rechte bleiben dem Bürger, wenn er nicht teilnehmen will?

Digitalisierung kann dem Menschen dienen.

Sie kann Verwaltung vereinfachen, medizinische Versorgung verbessern, Forschung ermöglichen und Sicherheit erhöhen.

Aber dieselbe Infrastruktur kann Macht konzentrieren, wenn ihre Grenzen nicht ebenso sorgfältig aufgebaut werden wie ihre technischen Möglichkeiten.

Die eigentliche Entscheidung über den digitalen Staat fällt deshalb nicht allein in Rechenzentren, Apps oder Wallets.

Sie fällt dort, wo entschieden wird, wer auf welche Daten zugreifen darf – und ob der Bürger auch morgen noch das Recht besitzt, Nein zu sagen.

Aktualität dieses Dossiers

Die in diesem Dossier behandelten rechtlichen, politischen und technischen Entwicklungen verändern sich fortlaufend.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Diese Untersuchung wird deshalb **regelmäßig auf neue Gesetze, EU-Rechtsakte, Gerichtsurteile, technische Erweiterungen, veränderte Einführungstermine und neue staatliche Zugriffsbefugnisse überprüft**.

Wesentliche Veränderungen werden in zukünftigen Fassungen berücksichtigt.

Stand dieser Ausgabe: 12. August 2026.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

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

Impressum:

https://www.klartext-info.online/impressum/

Zur Klartext-Info-Website

QR-Code

Weitere Beiträge, Aktualisierungen und Quellen:

www.klartext-info.online

Michael B. Barnes

Stand: 13.08.2026

← Zur Themenübersicht
WWW.KLARTEXT-INFO.ONLINE

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com