AUSGABE JULI 2026

VÖB ZAHLUNGSVERKEHR & DIGITALES

INHALT

Sehr geehrte Damen und Herren,

ein Blick in die Geschichte verdeutlicht: Die technologischen Innovationen in der heutigen digital vernetzten Welt waren noch nie so umfangreich und dynamisch. Dies stellt die europäische Banken- und Finanzindustrie vor komplexe Herausforderungen – nicht nur in Bezug auf die zunehmenden regulatorischen Anforderungen. Digitale Souveränität, regulatorische Compliance und operative Resilienz sind mit Innovationsfähigkeit eng zu verknüpfen.

Zu diesen Themen sowie über aktuelle Entwicklungen im Zahlungsverkehr berichten wir in unserer neuen Ausgabe der VÖB Zahlungsverkehr & Digitales.

Wir wünschen Ihnen eine interessante Lektüre.

Ihr Bundesverband Öffentlicher Banken Deutschlands, VÖB, Bereich Zahlungsverkehr und Informationstechnologie

Ausgabe Juli 2026

VÖB ZAHLUNGSVERKEHR & DIGITALES

1. DIGITALE SOUVERÄNITÄT – HANDLUNGSFÄHIGKEIT BEWAHREN

Souveränität erhält immer mehr Einzug in die Gesetzesvorhaben. Dies zeigt sich beispielsweise bei den aktuellen Gesetzesvorschlägen wie dem Tech Sovereignty Package und Cloud and AI Development Act oder auch dem Cyber Security Act 2. Diese beeinflussen die gesamte Wertschöpfungskette. Banken sind gefordert, Herausforderungen und Strategien für digitale Souveränität und Cloud-Architekturen mit den ggfs. auch weiteren regulatorischen Rahmenbedingungen in Einklang zu bringen.

Unverändert wichtig bleibt es, die Entscheidungshoheit über Daten, Infrastruktur und Anwendungen beizubehalten. Denn es gilt, sicher, resilient und flexibel in einer global vernetzten IT-Landschaft zu agieren.

Wesentliche Aspekte und Herausforderungen sowie welche Anpassungsbedarfe Banken und Sparkassen an die Gesetzgebung haben, hat der VÖB in einem Positionspapier zusammengestellt.

Regulatorische Herausforderungen neuer Technologien:
Neue Technologien verändern Bankprozesse grundlegend, bestehende Regelwerke stoßen an ihre Grenzen. Bankprozesse sind flexibel und risikoorientiert umzusetzen. Banken benötigen flexible Spielräume, um Innovationen zu fördern, ohne die Sicherheit zu gefährden. Die Anforderungen an Kontrolle, Dokumentation und Meldewesen müssen an neue Technologien angepasst werden.

Regulatorische Kohärenz und Entlastung:
Die Vielzahl an IT-bezogenen Regelungen führt zu Redundanzen und erhöhtem Aufwand. Um operative Belastungen zu reduzieren, braucht es u. a. eine einheitliche europäische Aufsichtspraxis, neue Vorgaben nur bei tatsächlichem Regelungsbedarf sowie offene Standards und Interoperabilität statt zusätzlicher Zertifikate. Europäische Technologiekompetenzen sind durch steuerliche Anreize und Förderprogramme aufzubauen.

Bedeutung der Cloud-Strategien für digitale Handlungsfähigkeit:
Hybride und Multi-Cloud-Modelle stärken die Resilienz, erfordern aber eine bewusste Steuerung und Kontrolle der Infrastruktur. Entsprechend müssen Banken die Infrastruktur weiterhin und trotz wachsender Komplexität kontrollieren können. Neue Abhängigkeiten durch KI, Automatisierung und innovative Features müssen transparent gemanagt werden.

Governance- und Risikomanagementstrukturen:
Regulatorische Vorgaben sollten auf bewährte Governance-, Kontroll- und Risikomanagementstrukturen setzen. So sollten übermäßige Detailvorgaben in Rechtsakten vermieden und risikobasierte Ermessensspielräume in der Aufsicht stärker genutzt werden. Mehrfachprüfungen sollten systematisch vermieden werden.

Regulatorische Kohärenz und europäische Harmonisierung:
Die Vielzahl an Regulierungen führt zu Redundanzen und Komplexität. Alle regulatorischen Anforderungen sind auf Notwendigkeit und Praxistauglichkeit zu prüfen.

Es braucht eine Gesamtstrategie für eine zukunftsfähige Finanzregulierung, denn nur eine integrierte, proportionale und praxisnahe Regulierung stärkt die Resilienz und Wettbewerbsfähigkeit.

Das vollständige VÖB-Positionspapier zur digitalen Souveränität finden Sie hier zum Download.

2. DORA – WIE KANN DIE EU-VERORDNUNG PRAXISNAHER UMGESETZT WERDEN?

Der Digital Operations Resilience Act (DORA) der EU-Kommission aus dem Jahr 2022 hat einen einheitlichen europäischen Rahmen für das Management von IKT-Risiken geschaffen. Banken begrüßen DORA grundsätzlich. Der Anwendungsbereich ist sehr detailliert. Die Umsetzung, einschließlich Dokumentation, Drittparteienmanagement und Meldepflichten, führt zu erheblichen Aufwänden. Große Institute sind besonders stark betroffen.

Wichtige Aspekte aus den ersten Erfahrungen mit DORA, die für die weitere praxisnahe DORA-Anwendung relevant sind, hat der VÖB in seinem Positionspapier zusammengefasst:

Auszüge aus den VÖB-Petita zu einer praxisnahen DORA-Anwendung, Stand April 2026:

1. Eine mittlere Anforderungskategorie für Institute einführen, die nicht systemrelevant, aber groß und komplex sind, damit diese die DORA-Anforderungen in reduziertem, proportionalem Umfang erfüllen können.
2. Bestehende Informationssicherheitsstandards für die mittlere Anforderungskategorie anerkennen, damit Doppelprüfungen vermieden werden.
3. Risikoorientierte Dokumentationsanforderungen differenzieren:

Detailtiefe für stabile, etablierte Prozesse reduzieren; auf risikorelevante Informationen fokussieren anstatt auf vollständige Lieferketten.
4. Single Entry Point nutzen – als Instrument, um Meldungen zu entschlacken, zu harmonisieren und zu vereinheitlichen.
5. Vorfallmeldungen differenzieren: zwischen internen Betriebsstörungen und externen Sicherheitsvorfällen klar ex ante abgrenzen; Schwellenwerte bzw. explizite Ausnahmen für interne Störungen, die innerhalb der definierten RTO/RPO behoben werden können, erhöhen.
6. Wochenend- und Feiertagsmeldungen flexibilisieren: Meldepflichten sollen an das Risikoprofil des Instituts angepasst und mit anderen Meldefristen (z. B. GDPR) harmonisiert werden.
7. Keine pauschalen Prüf- und Auditpflichten gerade bei marktmächtigen Anbietern, sofern standardisierte, anerkannte Nachweise vorliegen und keine konkreten Risikohinweise bestehen.
8. Vertragsbausteine für Drittdienstleister standardisieren und aufsichtlich abgestimmte Muster bereitstellen, damit Rechts- und Abstimmungsaufwände reduziert werden.
9. Mandate der 2nd Level-Rechtsakte nicht überschreiten – Proportionalität bei Dokumentationstiefe, Testzyklen und Berichtspflichten konkret leben.
10. Dreistufige Anerkennungs- und Prüfarchitektur für IKT-Drittdienstleister/Kritische IKT-Drittdienstleister.

3. AI FRONTIER MODELLE WIE MYTHOS ODER „DIE NEUE GESCHWINDIGKEIT VON RISIKO“

Spätestens mit DORA wird operationale Resilienz als ganzheitliche Steuerungsaufgabe verstanden. Wie notwendig dieser Ansatz ist, zeigt sich auch in der aktuellen Diskussion um KI und resiliente Systeme am Beispiel von AI Frontier-Modellen. Hier verstärken sich Technologie- und Risikodynamiken in bisher ungewohnter Geschwindigkeit gegenseitig. Mit dem „Claude-Mythos“ – stellvertretend für AI Frontier Models – wurde im April 2026 erneut deutlich, dass moderne KI-Systeme zugleich Produktivitäts- und Angriffswerkzeug sind. Dual Use wird damit zur Grundcharakteristik:

Dieselben Modelle, die Effizienz und Automatisierung erhöhen, beschleunigen auch die Skalierung von Angriffen. KI muss damit zunehmend auch zur Verteidigung gegen KI eingesetzt werden.

Für Banken ist der Umgang mit AI Frontier Models kein IT-Thema, sondern eine Frage der Gesamtsteuerung von Risiko, Resilienz und Stabilität der Geschäftsmodelle. Denn die Technologie wirkt nicht isoliert in Systemen, sondern entlang der gesamten Wertschöpfungskette: in Kundenprozessen, Entscheidungslogiken, Drittparteienbeziehungen und zunehmend auch in der operativen Stabilität kritischer Services.

Damit verschiebt sich KI von einem Innovations- zu einem systemischen Betriebs- und Sicherheitsfaktor.

Parallel dazu können Banken auf bestehende Rahmenwerke wie DORA, IT- und Auslagerungsregime zurückgreifen. Für Banken bedeutet das: Keine neue Systematik, jedoch verschärfen sich bestehende Anforderungen an Geschwindigkeit, Abhängigkeiten und operative Reaktionsfähigkeit deutlich.

Der zentrale Wandel liegt in der Dynamik des Risikos. Mit der zunehmenden Allgegenwärtigkeit von Large Language Models (also große Sprachmodelle, die für das Training von KI essenziell sind) sinkt die Zeit, in der Schwachstellen möglicherweise ausgenutzt werden. Die Aufsichtsbehörden gehen daher davon aus, dass gezielte Triage-Entscheidungen und temporäre Ausfälle im Rahmen beschleunigter Patch- und Update-Zyklen künftig Teil des regulären Betriebs sein können. Patching wird damit zu einem kontinuierlichen, hochfrequenten Steuerungsprozess.

Damit verschiebt sich der Fokus von einzelnen Schwachstellen hin zu einem strukturellen Resilienzproblem.
Entscheidend ist nicht mehr, nur bekannte Risiken zu identifizieren, sondern die Fähigkeit, neue Angriffspfade schnell zu erkennen, zu bewerten und operativ umzusetzen.

Legacy-Systeme geraten dabei besonders unter Druck: Schwachstellenscanning, Security-by-Design und automatisiertes Testing müssen deutlich ausgebaut werden – inklusive konsequenter Bewertung auch niedriger Risiko-Scores.

Ein zentraler Hebel liegt in der starken Abhängigkeit von Drittparteien. Schwachstellenmanagement endet nicht an der Institutsgrenze. Banken müssen Lieferketten aktiv einbinden und kontinuierlich Informationen zu Schwachstellen, Patches und Exploits ihrer Dienstleister einfordern. Drittparteienresilienz wird damit zu einem kollektiven Lern- und Geschwindigkeitssystem, nicht zu einer rein vertraglichen Steuerungsfrage.

Operativ beschleunigen sich Patch- und Change-Prozesse, Tests werden stärker automatisiert, IT, Security und Betrieb werden enger verzahnt; risikobasierte Entscheidungslogiken geraten unter Zeitdruck.

DORA bleibt dabei der zentrale Rahmen – proportional, risikobasiert und pragmatisch in der Anwendung, im engen Schulterschluss zwischen Industrie und Aufsicht. Entscheidend ist nicht, neue Prinzipien einzuführen, sondern konsequent fähig zu sein, bestehende Anforderungen an die Resilienz auf einen hochdynamischen, KI-getriebenen Bedrohungsraum zu übertragen.

4. DIGITALER EURO: STUFENWEISER ANSATZ

Am 28. Oktober 2025 hatte der Hauptberichterstatter des Europäischen Parlaments für den digitalen Euro (ECON-Ausschuss), Fernando Navarrete, seinen Berichtsentwurf zum Legislativvorschlag über die Einführung eines digitalen Euro vorgelegt.

Im Kern sah der Bericht einen konditionalen Zwei-Stufen-Ansatz bei der Einführung des digitalen Euro vor: Zunächst sollte ausschließlich die Offline-Variante des digitalen Euro als digitales Bargeld (Tokenized Cash) eingeführt werden. Nur wenn nach einer Prüfung durch die EU-Kommission festgestellt worden wäre, dass keine privatwirtschaftliche Retail-Zahlungslösung den gesamten Euroraum abdeckt, hätte die Kommission die Einführung der Online-Variante verfügen können. Diese Konditionalklausel, die auf den ersten Blick Raum für privatwirtschaftliche Lösungen geschaffen hätte, war im Parlament jedoch nicht mehrheitsfähig. Stattdessen näherten sich die Abgeordneten im ECON-Ausschuss des EU-Parlaments immer mehr der bereits seit Ende 2025 bestehenden Ratsposition an, den digitalen Euro von Beginn an vollumfänglich zu emittieren.

Der Trilog zwischen der Ratsposition und der Parlamentsposition kann nach bisheriger Planung in der zweiten Jahreshälfte 2026 gestartet und bestenfalls bis Jahresende abgeschlossen werden.

Neben Fragen zur Governance des Haltelimits, dem Kompensationsmodell und zu Modalitäten des Open Fundings sind auch Verhandlungen zu den Zuständigkeiten des Eurosystems im Trilog zu erwarten. Sowohl im Rat als auch im Parlament wird eine Pflicht für Banken, eine EZB-App anbieten zu müssen, abgeschwächt. Eigene Lösungen in Bank-Wallets sollen möglich sein.

Wir plädieren für eine gestaffelte Einführung des digitalen Euro unter vollumfänglicher Nutzung bereits vorhandener Zahlungsverkehrsstandards, um Komplexität und Kosten von Anfang an zu reduzieren.

5. DIGITALER EURO: PILOTIERUNG WIRD VORBEREITET

Ende Oktober 2025 hatte die Europäische Zentralbank (EZB) beschlossen, ihre zweijährige Vorbereitungsphase abzuschließen und nun vor allem die technischen Anforderungen zu konkretisieren. Damit soll die Grundlage für die weitere Entscheidung für den digitalen Euro geschaffen werden.

Bei der technischen Umsetzung ist die EZB bemüht, die Kosten zu dämpfen. Sie setzt dabei u. a. auf offene, nicht-proprietäre Standards (z. B. CPACE, EPC-QR, nexo, Berlin Group), damit der digitale Euro über alle Komponenten hinweg interoperabel verarbeitet werden kann.

Diese sowie weitere Aspekte sollen in einer Pilotphase für den digitalen Euro erprobt werden. Bereits Ende Juni 2026 soll das entsprechende „Participation Agreement“ mit ausgewählten Banken im Euroraum unterzeichnet werden. Im Fokus stehen Retailbanken und das Privatkundengeschäft. Bislang sind vier P2P- bzw. P2B-Anwendungsfälle auf dem jeweiligen Gelände der Zentralbanken und der EZB vorgesehen. Insgesamt haben gut 50 Banken, darunter auch einige deutsche Banken, Interesse signalisiert, an der Pilotphase teilzunehmen. Der Handel soll gesondert zur Teilnahme aufgerufen werden.

Im Rahmen der vorausgegangenen Konsultation des „digital Euro scheme rulebook“ waren über 1.200 Kommentare eingegangen. Das Feedback der EZB wurde in einem aktualisierten Regelwerk, Version 0.91, eingearbeitet, die neuste Version 0.92 wird im Juli 2026 erwartet. Eine „draft rulebook version for consultation (0.98)“ wird erst 2027 erwartet. Zahlreiche Aspekte einer Offline-Variante des digitalen Euro wurden bislang noch nicht ausreichend berücksichtigt.

Der Ausschuss für Wirtschaft und Währung des Europäischen Parlaments (ECON) hat am 23. Juni 2026 seine Position zur Verordnung über die Einführung des digitalen Euro beschlossen und damit den Weg für interinstitutionelle Verhandlungen mit Rat und Europäischer Kommission, dem Trilog, geebnet. Die formale Bestätigung dieser Verhandlungsposition durch das Plenum des Europäischen Parlaments wird für Anfang Juli 2026 erwartet. Damit tritt das Gesetzgebungsverfahren in eine entscheidende Phase ein; die Trilogverhandlungen könnten ab Mitte Juli 2026 aufgenommen werden und bestenfalls bis Jahresende abgeschlossen werden.

Weitere Zeitplanung:
Wenn die Verordnung zum digitalen Euro durch Parlament und Rat bis Ende des Jahres 2026 verabschiedet wird, soll die einjährige Pilotierung und Erprobung der ersten Transaktionen durch die EZB bereits ab Mitte 2027 stattfinden.

Das Eurosystem bereitet sich auf eine mögliche Erstausgabe des digitalen Euro im Verlauf des Jahres 2029 vor.

Wohin geht die Reise des digitalen Euro?
Es dürfte unumstritten sein: Der digitale Euro wird kommen! Alle Marktteilnehmer sind aufgefordert, sich mit den Anforderungen und der neuen Welt des digitalen Euro spätestens jetzt auseinanderzusetzen. Die Nachfrage bzgl. der Teilnahme am Piloten zeigt, dass sich die europäischen Banken durchaus Mehrwerte erhoffen und diese in ihre strategischen Überlegungen einbeziehen.

Interessant ist diese Entwicklung, denn der digitale Euro fordert Investitionen. Diese sind langfristig zu denken, und damit stehen einige Institute vor grundsätzlichen Entscheidungen, auf welche Standards und Infrastrukturen sie künftigen setzen müssen. Dies dürfte zunächst vor allem europaweit agierende Institute sowie Banken mit starkem Privatkundengeschäft betreffen.

Aktuell immer noch wahrgenommene Unsicherheiten beim digitalen Euro hemmen weitere, dringend notwendige Investitionsentscheidungen bereits jetzt. Daher stellt sich durchaus die Frage, ob die von der EZB vorgegebenen Standards richtungsweisend für die Zahlungsverkehrsinfrastruktur in Europa sind. Wäre dies schädlich? Die Nachteile proprietärer Standards gerade im Zahlungsverkehr sind hinlänglich bekannt. Daher ist es nicht verwunderlich, dass sich die EZB in den vergangenen Monaten mit den teils seit Jahrzehnten erfolgreich betriebenen Standardisierungsinitiativen aktiv ausgetauscht hat.

Welche langfristigen Folgen dieses Engagement der EZB auf die Zahlungsverkehrsabwicklung haben wird, bleibt abzuwarten.

Der digitale Euro wird im Markt angeboten werden. Wann, in welcher Form und zu welchen Konditionen – die Ergebnisse der Pilotphase dürften hierfür hinreichende Aussagen bereitstellen.

Regelwerk für den digitalen Euro

Zur DK-Stellungnahmevom 23. Juni 2026

6. KI: NEUE MEILENSTEINE UND ZAHLREICHE LEITLINIEN

Seit dem 2. August 2025 gelten die „Pflichten für KI mit allgemeinem Verwendungszweck (GPAI)“ nach dem AI Act. Ursprünglich sollten zum 2. August 2026 sämtliche Regelungen und Pflichten für Hochrisikosysteme aus Anhang III (Liste der Anwendungsfälle mit hohem Risiko – wozu auch die Kreditwürdigkeitsprüfung gehört) in Kraft treten.

In den Trilogverfahren zum KI-Omnibus über Anpassungen am europäischen AI Act wurde am 7. Mai 2026 eine vorläufige Einigung erzielt: Die Vorschriften für Künstliche Intelligenz sollen gestrafft werden. Eine vorläufige Kompromissfassung des Rates ist am 13. Mai 2026 erschienen. Verbindlich wird die Änderungsverordnung erst nach Veröffentlichung im Amtsblatt und einer kurzen Frist bis zum tatsächlichen Inkrafttreten.

Der Kompromiss soll u. a. doppelte Prüf- und Dokumentationsprozesse vermeiden und bringt eine zweifache Fristverschiebung für Hochrisiko-KI-Systeme: Sie sollen nun ab dem 2. Dezember 2027 für eigenständige Hochrisiko-KI-Systeme (Annex III) und ab dem 2. August 2028 für Hochrisiko-KI-Systeme, die in Produkte eingebettet sind (Annex I), gelten.

Auch die Umsetzungsfrist von Transparenzlösungen für künstlich erzeugte Inhalte für Bestandssysteme wurde um vier Monate verlängert – als neue Frist wurde der 2. Dezember 2026 festgesetzt.

Das AI Office der EU-Kommission hat bereits 2025 fünf Leitlinien zur Umsetzung der Regularien des AI Acts (rechtlich noch nicht bindend) veröffentlicht, u. a. zu verbotenen KI-Praktiken, zur Anwendung der KI-Definition oder zum Living Repository zur Förderung des Lernens und des Austauschs über KI-Kompetenz.

Folgende Leitlinien werden noch erwartet oder bereits konsultiert:

1. Leitlinien für die Meldung von schwerwiegenden Vorfällen (Art. 73(7) KI-VO) – EU KOM Konsultation 26.09.-07.11.2025 – geplant in Q1 2026 – derzeit verspätet
2. Leitlinien zur Einstufung von HRKI-Systemen (Art. 6(5) KI-VO) – Frist 02.02.2026 – in Konsultation bis 15. Juni 2026
3. Leitlinien zum Verhältnis der KI-VO mit anderen sektoralen Rechtsvorschriften (Art. 96(1)(e) KI-VO) – vssl. Q3 2026
4. Leitlinien zur praktischen Anwendung der Transparenzanforderungen gemäß Art. 50 KI-VO – vssl. Q3 2026 – in Konsultation bis 15. Juni 2026

5. Leitlinien zu den Anforderungen an HRKI-Systeme (Art. 8 -15 KI-VO) – vssl. Q3 2026
6. Fragebogen zur Grundrechte-Folgenabschätzungen (Art. 27(5) KI-VO) – vssl. Q3 2026
7. Leitlinien für die praktische Durchführung der Bestimmungen über wesentliche Veränderungen (Art. 96(1)(c) KI-VO) – vssl. Q3 2026
8. Leitlinien zur praktischen Anwendung der Vorschriften für die Verantwortlichkeiten entlang der KI-Wertschöpfungskette – vssl. Q3 2026
9. Leitlinien zu den Elementen des Qualitätsmanagementsystems, die KMU und SMC in vereinfachter Form einhalten können

Weitere Unterstützungsmaterialien des AI Office der EU-Kommission (rechtlich nicht bindend) sind ebenfalls verfügbar:

- → März 2025: FAQs zum Thema General Purpose AI (GPAI) Model – gerade aktualisiert
- → August 2025: FAQs zur AI Literacy aktualisiert
- → Oktober 2025: FAQs zum AI Act allgemein und dessen Umsetzung
- → Oktober 2025: AI Help Desk im AI Office der Europäischen Kommission

Voraussichtlich noch im Jahr 2026 soll CEN/CENELEC Standardisierungs- und Prüfkriterien veröffentlichen.

Zum Referentenentwurf zur nationalen Umsetzung des AI Act des Bundesministeriums für Digitalisierung und Staatsmodernisierung liegt eine Stellungnahme der Deutschen Kreditwirtschaft vom Oktober 2025 vor.

Die Bafin hat eine Orientierungshilfe zu Cloudauslagerungen von KI im Hinblick auf IKT-Risiken und DORA veröffentlicht.

Kann eine KI die Umsetzungsleitfäden auch selbst erstellen?
Warum nicht, sollte man meinen? Beim genaueren Hinblicken stellt man fest: KI kann sicherlich unterstützend eingesetzt werden, aber Probleme z. B. bei der Definition oder Klassifizierung nicht selbst beheben. Dazu bräuchte es klare Gesetze und eine praktische Anleitung zu den Interpretationen der Gesetzestexte, im Sinne einer technischen Übersetzung, seitens der Aufsichtsbehörden.

7. KI: ANFORDERUNGEN DES ZAHLUNGSVERKEHRS

Aus Sicht des Zahlungsverkehrs gibt es weitere Anforderungen, damit künstliche Intelligenz im Zahlungsverkehr gut und i. S. des europäischen AI Act auch praktisch gelingen kann. Wie z. B.:

- → KI-Definition schärfen, Überklassifizierung vermeiden: Nicht-lernende und vollständig transparente statistische Modelle (z. B. lineare/logistische Regression) sind explizit aus der Definition von KI auszunehmen, echte KI-Risiken sind zu adressieren.
- → Rollen und Haftung klarer definieren: „Provider vs. Deployer" sind abzugrenzen; zu bestätigen ist, dass reine Deployer nicht in die verschuldensunabhängige PLD-Haftung geraten – sonst wird selbst sichere KI nicht skaliert.
- → Hochrisiko-Fälle im Finanzbereich ausdrücklich differenzieren: Kreditwürdigkeitsprüfungen sind durch echte KI im Anwendungsbereich beizubehalten, gleichzeitig ist die ausdrückliche Ausnahme für Betrugsprävention zu bewahren: Diese Tools dienen meist der Mustererkennung und nicht als automatisierte Rechtsentscheidungen. Dies scheint durch den Omnibus for AI zunächst so zu sein, gleichzeitig bleibt Art. 6 Abs. 3 AI Act als mögliche Ausnahme für Annex-III-Systeme wichtig, wenn ein System keine signifikanten Risiken verursacht und nur eng begrenzte Verfahrensaufgaben erfüllt.
- → „One supervisor, one playbook": Bestehende Finanzaufsichten sind als AI-Marktaufsichten für Banken zu benennen und in die Sekundärrechtsetzung des AI Office einzubinden – das verhindert zersplitterte Aufsicht und widersprüchliche Auslegungen. Doppelregulierungen sind auszuschließen.
- → Überschneidungen mit Sektorrecht abbauen. Vor KI-Sonderauflagen systematisch Lücken/Überlappungen gegen CRR/CRD, DORA, PSD2, AMLR, IPR etc. mappen und Doppelregulierungen vermeiden. Ein EBA-Mapping hierzu liegt mittlerweile vor.
- → FRIA ↔ DPIA abbilden & Datenregeln klären. Gegenseitige Anerkennung/Vorlagen zwischen der Grundrechts-Folgenabschätzung (FRIA) des AI-Act und der DSGVO-DPIA bereitstellen; Rechtsstatus pseudonymisierter Daten für KI-Training zügig präzisieren. Hierzu zeichnen sich Ansätze im Omnibus for AI ab, allerdings stehen die versprochenen Vorlagen für die konkrete Umsetzung durch das AI Office noch aus.
- → Stufenweise Umsetzung und Interimsinstrumente. Massive Verzögerungen bei Normen (CEN/CENELEC; GPAI-Leitlinien) anerkennen. Mit gestuften Fristen oder Zwischeninstrumenten (z. B. GPAI Code of Practice) Rechtssicherheit wahren, bis

Sicherungsmechanismen ausgereift sind. Die Verzögerungen halten an, der Omnibus verspricht auch deshalb neue gestaffelte Fristen; aber den Zwischeninstrumenten fehlt es häufig an Eindeutigkeit.

Der „**Digitale Omnibus für KI**“ – ein Oberbegriff der EU-Kommission – beinhaltet ein Gesetzespaket, das die europäische KI-Verordnung vereinfachen und aktualisieren sollte, aber letztlich den Finanzinstituten außer kleineren Firstverlängerungen keine wesentlichen Erleichterungen gebracht hat.

8. DIGITALE IDENTITÄTEN: REGIERUNGSENTWURF BESCHLOSSEN

Das Bundeskabinett hat Mitte Mai 2026 den Regierungsentwurf für das „Gesetz zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Brieftasche für die Digitale Identität sowie zur Änderung anderer Rechtsvorschriften“ (DIdG) beschlossen.

Gegenüber dem Referentenentwurf wurden beispielsweise elektronische Attributsbescheinigungspflichten klargestellt. Diese Attributsbescheinigungen stellen 24 Monate nach Gesetzesverkündigung einen Nachweis gegenüber Behörden des Bundes (bei Anwendung von Bundesrecht) dar, der in dieser Funktion der gesetzlich vorausgesetzten Schriftform gleichsteht. Es sei denn, elektronische Verfahren sind gesetzlich ausgeschlossen oder mit weiteren Voraussetzungen verbunden (qualifizierte elektronische Signatur). Weitere durch das Kabinett angepasste Aspekte betreffen die verpflichtende Interoperabilität mit Nutzerkonten und NOOTS sowie die Erhöhung des Schutzniveaus im Datenschutzrecht mittels gesetzlicher Grundlage, und es wurden die Anforderungen an eine Beleihung und die Herabsenkung des eID-Mindestalters für Onboarding und einen digitalen PIN-Rücksetzdienst konkretisiert.

Die Kritikpunkte aus der Stellungnahme der Deutschen Kreditwirtschaft (DK) zum Referentenentwurf werden nur punktuell und in der Gesetzesbegründung adressiert. Aus Sicht der DK ist es nicht notwendig, dass sich die Anwendbarkeit von bestimmten Regelungen zur eID auf die EUDI-Wallet in § 15 Abs. 2 des DIdG erstreckt. In der Kabinettsfassung wird gleichwohl die Grundregel des § 15 unverändert beibehalten, in der Gesetzesbegründung wird dazu auf Spezialitätsgrundsatz sowie sachgerechte Anwendung verwiesen. Auch die Änderungen des GwG in Art. 6 wurden beibehalten.

Ebenfalls beibehalten ist in der Kabinettsfassung die nationale Umsetzung von Art. 5f eIDAS. Grenzüberschreitende Pflichten werden systematisch auf Inlandssachverhalte übertragen, die EUDI-Wallet soll funktional dem bisherigen eID-Regime gleichgestellt werden. Private Diensteanbieter sollen ihre Systeme breit anpassen. Nicht enthalten sind ein konkreter und verbindlicher Migrationsfahrplan sowie technische Roadmaps oder Übergangsfristen.

9. EUDI-WALLET: EIN NEUES ZAHLUNGSMITTEL?

Voraussichtlich ab dem 2. Januar 2027 soll die EUDI-Wallet der Bundesregierung in einer ersten Ausbaustufe an den Start gehen. Den entsprechenden Entwurf für das Digitale Identitätengesetz (DIdG) hat das Bundeskabinett im Mai 2026 beschlossen. Die EUDI-Wallet ermöglicht Bürgerinnen und Bürgern, ihre Identität künftig sowohl per Smartphone nachzuweisen als auch digitale Dokumente zu nutzen und auch einzelne Daten aus diesen Dokumenten digital und vertrauensvoll zu übermitteln. Die neue Smartphone-App soll grenzüberschreitend in Europa einsetzbar sein.

Die EUDI-Wallet wird digitale Identitäten mit dem Alltag verbinden, indem sie vielfältige Nachweise (z. B. Personalausweis, Führerschein) digital abbildet und perspektivisch persönliche Zertifikate, qualifizierte elektronische Signaturen, pseudonyme Logins und Zahlungsfunktionen unterstützen soll.

Quelle: Bundesministerium für Digitales und Staatsmodernisierung.

Ob und in welcher Form die EUDI-Wallet – zumindest in Deutschland – für Zahlungen genutzt werden wird, ist Gegenstand von intensiven Gesprächen mit den zuständigen Behörden. Die Überlegungen und Planungen reichen von der Möglichkeit, die starke Kundenauthentifizierung (konform zum Zahlungsdiensteaufsichtgesetz (ZAG)) für das Auslösen von Zahlungen jedweder Art nutzen zu können, bis hin dazu, dass die EUDI-Wallet selbst als Akzeptanzstelle dient. Offline-Zahlungen, wie sie beispielsweise der digitale Euro fordert, werden hingegen schwieriger umzusetzen sein.

Fragen zu Haftung, Betrugsprävention sowie Interoperabilität stehen ebenfalls auf der Agenda der Gespräche. Inwieweit Verbraucher die EUDI-Wallet mit ihren Funktionen nutzen werden, hängt vor allem auch davon ab, welche Unternehmen und Institutionen die neue Wallet nutzen und wie nutzerfreundlich und einfach die Bedienung in der Wallet gestaltet werden wird.

Zum Kabinettsentwurf

10. PSD3/PSR: ZEITPLAN VERZÖGERT SICH

Der Zeitplan für das mit Spannung erwartete neue Zahlungsverkehrspaket der EU hat sich verschoben: Nachdem sich das EU-Parlament und der Europäische Rat am 27. November 2025 politisch auf die Payment Services Regulation (PSR) und die Payment Services Directive 3 (PSD3) geeinigt hatten, schien der Weg frei. Doch nun kommt es zu Verzögerungen.

Ursprünglich sollte die finale Fassung des Gesetzespakets im Mai 2026 vom Europäischen Rat verabschiedet und anschließend vom EU-Parlament beschlossen werden. Aufgrund von Verzögerungen bei den Übersetzungen in die Amtssprachen wurde dieser Zeitplan nun verworfen:

- → Dezember 2026: voraussichtliche Verabschiedung des Gesetzespakets durch das EU-Parlament.
- → Anschluss: Veröffentlichung im Amtsblatt der Europäischen Union (frühestens nach der Verabschiedung).
- → Inkrafttreten: Das Gesetz tritt 20 Tage nach der Veröffentlichung im Amtsblatt sowie einer anschließenden 21-monatigen Übergangsfrist in Kraft.
- → Ergebnis: Mit einer Anwendung der neuen Regeln ist damit frühestens in Q3 2028 zu rechnen.

Kritische Punkte und deutliche Fortschritte in den aktuellen Entwürfen:

- → Kritik an der Haftungsausweitung: Die im Paket vorgesehene Ausweitung der Haftung von Banken ist weiterhin nicht sachgerecht.
- → Erfolg bei der Betrugsbekämpfung: Positiv zu bewerten ist, dass mit der PSR künftig der Austausch von Betrugsdaten innerhalb eines Schemes ermöglicht wird. Datenschutzrechtliche Bedenken treten dadurch in den Hintergrund. Dies erlaubt eine europaweit effektivere Betrugsbekämpfung.

11. WIRD OCT INST VERPFLICHTEND?

Die Diskussion um den One Leg Out Instant Credit Transfer (OCT Inst), d.h., Echtzeitzahlungen aus Europa in andere nichteuropäische Länder zu ermöglichen, gewinnt zunehmend an Dynamik.

OCT Inst orientiert sich am europäischen SEPA-Echtzeitverfahren (SCT Inst). Damit stellt es eine wichtige Weiterentwicklung im grenzüberschreitenden Zahlungsverkehr dar. Die Initiative des European Payment Council (EPC) ist politisch geprägt. Sie geht maßgeblich auf den G20-Gipfel sowie die Retail Payments Strategy der EU-Kommission aus dem Jahr 2020 zurück. Die G20-Finanzminister und -Zentralbankchefs hatten konkrete Ziele formuliert, um internationale Zahlungen schneller, günstiger und transparenter zu machen und damit den Marktzugang zu verbessern: Bis Ende 2027 sollen rund 75 Prozent der grenzüberschreitenden Transaktionen innerhalb einer Stunde abgewickelt werden. Der daraufhin veröffentlichte globale Fahrplan umfasst 19 Maßnahmenbereiche, darunter die Ausweitung der Betriebszeiten von Echtzeit-Bruttoabwicklungssystemen (RTGS-Systemen). Damit sollen sich die Beteiligten international besser vernetzen.

In Europa wird dies durch Anpassungen im TARGET-System sowie durch das seit 2018 bestehende TARGET Instant Payment Settlement (TIPS) unterstützt. TIPS soll schon bald sekundenschnelle Währungsumrechnungen ermöglichen. Ergänzend verfolgt die EU-Kommission das Ziel, Echtzeitzahlungen als internationalen Standard zu etablieren, weshalb der EPC im März 2023 das OCT Inst Rulebook veröffentlichte.

In der aktuellen Marktdiskussion zeigt sich jedoch, dass das Vorhaben mit erheblichen Herausforderungen verbunden ist. Da die Teilnahme am OCT Inst bislang freiwillig ist, beteiligen sich nur wenige Institute. Um einer möglichen strengeren Regulierung zuvorzukommen, erörtert der EPC intensiv eine verpflichtende Einführung für Kundenbanken. Eine freiwillige Verpflichtung wird kaum unterstützt.

Strategisch betrachtet bewegt sich die Debatte in zwei Richtungen: Zum einen geht es um die globale Anbindung an Zahlungsdienstleister, um die Ziele der G20 umzusetzen. Dabei stehen derzeit insbesondere Transaktionen mit Indien und den USA im Mittelpunkt. Einige Institute transformieren Auslandszahlungen heute bereits in günstige SEPA-Zahlungen. Es fehlen jedoch belastbare Daten zu diesen Missbräuchen, sodass eine abschließende Bewertung spekulativ bleibt.

Zum anderen wird die Ausweitung des Systems auf europäische Nicht-Euro-Länder über TARGET und TIPS vorangetrieben. Die dänische Krone ist bereits vollständig in TARGET integriert. Die Projekte in Schweden und Norwegen laufen und sind teilweise schon über TIPS erreichbar.

Kritisch bewertet wird vor allem die fehlende Reziprozität, da eine unzureichende Gegenseitigkeit negative Auswirkungen auf den Markt haben kann.

Zum EPC OCT Inst rulebook

12. FIDA: RÜCKNAHME GEFORDERT

Die Diskussion um die Financial Data Access-Verordnung (FiDA) hat sich in den vergangenen Monaten deutlich zugespitzt. Bereits im Juli 2025 forderte die European Banking Federation (EBF) umfassende Änderungen am Entwurf. Die EBF bezeichnet eine vollständige Rücknahme als sachgerechte Option, sollte keine substanzielle Überarbeitung erfolgen.

Der ursprünglich für 2026 geplante Fortgang des Trilogs, der im zweiten Quartal 2025 begonnen hatte, ist inzwischen ins Stocken geraten. Bemerkenswert ist, dass die Kritik mittlerweile auch innerhalb der Europäischen Kommission selbst an Gewicht gewinnt: Valdis Dombrovskis, Kommissar für Wirtschaft und Produktivität, Umsetzung und Vereinfachung, äußerte sich öffentlich kritisch und schloss nicht mehr aus, den Entwurf zurückzunehmen. Zudem haben mindestens zwei weitere Generaldirektionen interne Fragen zum Vorschlag aufgeworfen. Gleichzeitig hält die Generaldirektion Finanzstabilität, Finanzdienstleistungen und Kapitalmarktunion (GD FISMA), unter anderem vertreten durch das Kabinett von Maria Luís Albuquerque, weiterhin an FiDA fest.

Auch auf nationaler Ebene wächst der Widerstand. Mehrere Verbände der Finanzwirtschaft, darunter auch der VÖB, haben sich in einem gemeinsamen Schreiben an das Bundesministerium der Finanzen (BMF) gewandt und die Rücknahme der Verordnung gefordert. Bemängelt wird, dass die vorgesehenen Vereinfachungen nicht ausreichen und zentrale Fragen weiterhin ungelöst bleiben.

Als wesentliche Kritikpunkte werden benannt:

- fehlende Antworten auf zentrale Risiken,
- zusätzliche bürokratische Belastungen,
- die Gefahr, dass der Finanzstandort Europa im globalen Wettbewerb geschwächt wird und
- dass die Ziele einer innovativen, wettbewerbsfähigen europäischen Finanzindustrie verfehlt werden.

Auch im Europäischen Rat haben sich Deutschland und Frankreich gegen eine Weiterverfolgung des FiDA-Entwurfs ausgesprochen.

13. WERTPAPIERABWICKLUNG DER EZB: PONTES & APPIA

Die EZB hat zwei Modelle für die zukünftige Wertpapierabwicklung vorgestellt. Diese werden den europäischen Markt in den kommenden Jahren maßgeblich prägen: **Pontes** und **Appia.**

Während Pontes als kurzfristige Übergangslösung konzipiert ist und voraussichtlich zwischen 2026 und 2028 zur Verfügung stehen soll, bildet Appia die langfristige Zielarchitektur, deren Umsetzung erst in den 2030er Jahren erwartet wird.

Pontes basiert auf dem Grundprinzip, dass sich beide an einer Transaktion beteiligten Parteien auf ein gemeinsames Abwicklungssystem festlegen müssen – entweder auf TARGET2 Securities (T2S) oder auf Pontes; ein paralleler Betrieb ist nicht vorgesehen. Die Abwicklungssicherheit wird zunächst über ein Prefunding-Modell gewährleistet, das im weiteren Verlauf ausgebaut werden soll. Zudem sind die Betriebszeiten aktuell auf 8:00 Uhr bis 17:00 Uhr begrenzt, was insbesondere für die operative Planung der Institute relevant sein dürfte.

Die EZB hat eine Pontes Market Contact Group eingerichtet und bereits einen Call for Interest gestartet. Die Teilnahmebedingungen stehen fest. Die technischen Anforderungen werden aktuell ausgearbeitet. Klar ist, dass der Zugang künftig nicht über SWIFT, sondern über moderne API-Schnittstellen erfolgen wird.

14. GIROAPI-NUTZERVERANSTALTUNG IM ZEICHEN VON ZAAB

Die giroAPI-Community hat am 2. Juni 2026 in ihrer Nutzerversammlung nächste Meilensteine im Open Banking erörtert: Der neue Use Case „Zahlungen aus autorisiertem Budget“ (ZaaB) – im internationalen Kontext besser bekannt als Variable Recurring Payments (VRP) – stand im Mittelpunkt.

Was macht ZaaB so innovativ?
ZaaB ist ein alltagsrelevanter und zukunftsweisender Anwendungsfall, der neues Level an Flexibilität und Sicherheit bietet. Ein vorab vereinbartes Limit spart dem Kunden aufwendige Einzelfreigaben bei jedem Zahlvorgang und ermöglicht zugleich dem Zahlungsdienstleister eine prozessoptimierte Abwicklung der einzelnen Zahlvorgänge.

Wie viel Potenzial und Interesse in diesem Modell steckt, zeigt der Blick nach Großbritannien: Die dortige Open Banking-Initiative hat speziell für diesen Geschäftsvorfall ein eigenes Scheme ins Leben gerufen, das sich als echte, Konto- und API-basierte Alternative zu den internationalen Kartensystemen positioniert.

Im Ergebnis der Nutzerversammlung sollen die bestehenden Geschäftsvorfälle der giroAPI gezielt weiterentwickelt werden.

Weitere namhafte Institute und Zahlungsdienstleister haben offiziell ihre Absicht erklärt, dem giroAPI Scheme noch in diesem Jahr beizutreten. Mit Blick auf 2027 wird neben den schon beigetretenen Genossenschaftsbanken mit dem erwarteten Beitritt der Sparkassen das Bankennetz voraussichtlich die kritische Masse durchbrechen.

Fazit
Die Dynamik um giroAPI zeigt deutlich: Es entstehen attraktive, neue Geschäftsmodelle – und zwar für beide Seiten, sowohl für Banken als auch für Zahlungsdienstleister.

Zum giroAPI Scheme

15. BUNDESLAGEBILD CYBERCRIME 2025

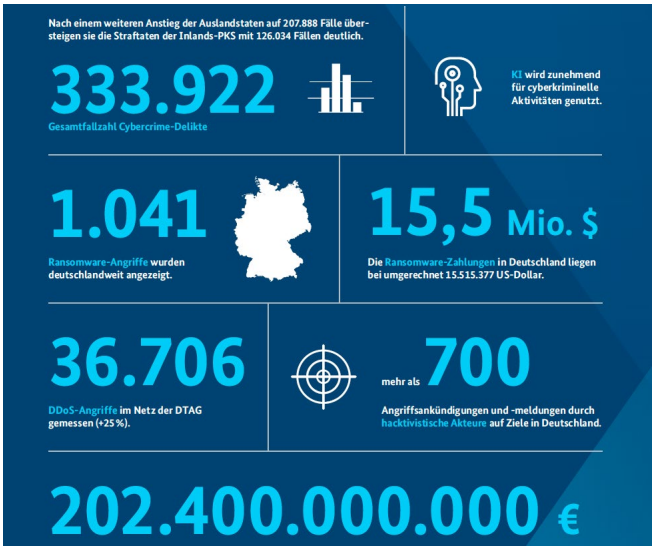
Das Bundeslagebild Cybercrime 2025, das im Mai 2026 vom Bundesministerium des Innern (BMI) veröffentlicht wurde, verdeutlicht, wie notwendig Maßnahmen zum Schutz der kritischen Infrastruktur und der Gesellschaft sind:

„Das geschätzte Schadensvolumen für die deutsche Wirtschaft liegt bei 202,4 Milliarden Euro und entspricht damit rund 4,5 Prozent des Bruttoinlandsprodukts. 2025 wurden rund 334.000 Fälle von Cybercrime im engeren Sinne registriert. Zwei Drittel der Taten (207.888) wurden aus dem Ausland oder von unbekannten Tatorten aus begangen. Die tatsächliche Bedrohung dürfte aufgrund eines erheblichen Dunkelfeldes deutlich höher liegen."
Quelle: BMI

Nicht verwunderlich ist, dass künstliche Intelligenz die Bedrohungslage verschärft. Die Sicherheitsbehörden sind sich bewusst, ihre Fähigkeiten zur Cyberabwehr zu stärken.

Zur Pressemitteilung des BMI

Zum Bundeslagebild Cybercrime 2025



Quelle: Cybercrime Bundeslagebild, Bundeslagebild 2025, Seite 5

16. BETRUGSPRÄVENTION IM ZAHLUNGSVERKEHR: DIE GESELLSCHAFT IST GEFORDERT

Professionell und anpassungsfähig agiert die organisierte Kriminalität, um Verbraucher, Unternehmen und die öffentliche Hand gezielt zu Zahlungen auf betrügerische Konten zu veranlassen. Phishing-Kampagnen, sei es beispielsweise über Telefonanrufe, wirken – teils unter Nutzung von Künstlicher Intelligenz – täuschend echt. Banken und Sparkassen arbeiten permanent an den notwendigen Abwehrmaßnahmen.

Doch Betrug setzt bereits an der Quelle an und ist daher auch über die gesamte Kette hinweg zu bekämpfen. Dazu gehören:

- Verbraucher umfangreich sensibilisieren
- Neue Handlungsoptionen erarbeiten und Hindernisse identifizieren
- Organisatorisch-rechtliche Grundlagen bereitstellen, damit ein übergreifender Austausch betrugsrelevanter Daten unter Berücksichtigung der Datenschutzaspekte möglich ist

Einige dieser Themen werden im Rahmen des im November 2025 etablierten Bundesbank-Roundtables zur Betrugsbekämpfung behandelt. Unter der Schirmherrschaft der Deutschen Bundesbank tauschen sich dort Vertreter der Finanzindustrie, privater Unternehmen und Vereine sowie öffentlicher Institutionen aus und entwickeln gemeinsame Maßnahmen zur Betrugsprävention. Die Arbeiten schreiten voran, sodass bereits dieses Jahr erste öffentlichkeitswirksame Maßnahmen erwartet werden.

Unsere Positionen zur Betrugsbekämpfung im Zahlungsverkehr:

Relevante Akteure sind gesetzlich zu verpflichten: Betrugsbekämpfung setzt an der Quelle an. In die Betrugskette eingebundene Marktakteure – darunter Banken, Telekommunikationsanbieter, Postdienstleister und digitale Plattformen – müssen auf gesetzlicher Grundlage Betrugsprävention unterstützen.

Es gilt, datenbasiert zusammenzuarbeiten: Informationen über Betrugsversuche und tatsächliche Betrugsfälle sind zeitnah und strukturiert zwischen den beteiligten Akteuren über eine zentrale Austauschplattform als sektorenübergreifende Plattform auszutauschen.

Die Haftung ist differenziert zu gestalten: Die Haftung bei Betrug darf nicht einseitig bei der Bank oder bei der Sparkasse liegen. Insbesondere dann, wenn diese – wie so oft – keine Möglichkeit hatten, den Betrug zu verhindern. Eine Haftung darf nur dann greifen, wenn ein Institut tatsächlich fahrlässig gehandelt oder technische Schutzmöglichkeiten ungenutzt gelassen hat.

Die Eigenverantwortung jedes Einzelnen ist zu stärken – im beruflichen wie auch im privaten Umfeld: Jeder Einzelne kann zur Betrugsprävention beitragen. Dabei helfen deutschlandweit breit und dauerhaft angelegte und niederschwellige Aufklärungskampagnen, um Verbraucher zu sensibilisieren. Diese Kampagnen sind gemeinsam durch Wirtschaftsunternehmen, Organisationen sowie öffentliche Institutionen zu finanzieren und zu unterstützen.

Eine Vollkaskomentalität ist zu vermeiden: Nicht jeder Betrugsfall darf automatisch von beteiligten Institutionen ersetzt werden. Bewusster und sicherheitsorientierter Umgang mit sensiblen Zugangsdaten ist u. a. durch flächendeckende und konsequente Aufklärung zu fördern.

17. BARGELD-VERORDNUNG: TRILOG-START NACH DER SOMMERPAUSE MÖGLICH

Der Europäische Rat hatte den Kommissionsvorschlag zum „Entwurf einer Verordnung über die Rolle von Euro-Bargeld (Banknoten und Münzen) als gesetzliches Zahlungsmittel“ bereits 2025 bewertet und am 19. Dezember 2025 veröffentlicht. Der Kommissionsvorschlag hat sich im Rat nicht grundlegend verändert. Neu und hervorzuheben ist ein Cash Resilience Plan in Art. 8 a der Ratsposition. Dieser befasst sich mit Krisenszenarien und damit, wie der Zugang zu Bargeld auch in Krisenfällen sichergestellt wird.

Als letzter Trilog-Teilnehmer wird das Europäische Parlament seine Position zum Kommissionsentwurf voraussichtlich im Juli 2026 abschließen. Der Trilog von EU-Kommission, Europäischem Parlament und Europäischem Rat würde danach starten. Gemäß aktuell vorliegenden Informationen bleibt es beim „Single Currency Package“ aus Bargeld-Verordnung und digitalem Euro. In Abhängigkeit zum Verlauf der weiteren Gespräche bezgl. des digitalen Euro ist ein Inkrafttreten der Bargeld-Verordnung voraussichtlich Mitte 2027 denkbar.

Über VÖB Zahlungsverkehr & Digitales
Mit dieser Publikation informieren wir über ausgewählte Schwerpunkte im Zahlungsverkehr auf nationaler und europäischer Ebene sowie über Digitalisierungsthemen.

Sie wollen VÖB Zahlungsverkehr & Digitales abonnieren?
Dann schreiben Sie bitte eine E-Mail an presse@voeb.de. Geben Sie den Betreff „Anmeldung VÖB Zahlungsverkehr & Digitales“ an.

Alle VÖB-Publikationen können Sie unter www.voeb.de/publikationen lesen, downloaden und bestellen.

IMPRESSUM
Bundesverband Öffentlicher Banken Deutschlands, VÖB
Lennéstraße 11, 10785 Berlin
Telefon: +49 30 8192 166
E-Mail: presse@voeb.de | Internet: www.voeb.de
Redaktion: Team Zahlungsverkehr und Informationstechnologie
Redaktionsschluss: 29. Juni 2026
Registernummer im Transparenz-Register der EU: 0767788931-41