AUSGABE JULI 2025

VÖB ZAHLUNGSVERKEHR

INHALT

1. Digitaler Euro: nicht nur Kosten auf dem Prüfstand *S. 2*
2. Digitaler Euro: Zeitplanung des Eurosystems *S. 2*
3. Digitaler Euro: Legislativvorschlag des Europäischen Rates *S. 3*
4. Digitaler Euro: Geopolitik verändert den Blick *S. 3*
5. Verification of Payee: Störungen im Zahlungsverkehr erwartet *S. 4*
6. giroAPI-Scheme: erfolgreicher Start 2025 *S. 5*
7. PSD3/PSR: Art. 59 weiterhin kritisch *S. 6*
8. Betrugsprävention im Zahlungsverkehr: Was ist zu tun? *S. 6*
9. Bundesbank: Abschalten des Telefax Ende 2025 *S. 7*
10. Einstellung des Scheckverfahrens in 2027 geplant *S. 8*
11. Künstliche Intelligenz: KI-Verordnung in Umsetzung *S. 8*
12. DORA: mehr digitale Resilienz, weniger Komplexität *S. 8*
13. Cyber Resilience Act (CRA): Unterstützung für den „Stop the Clock“-Vorschlag der polnischen Ratspräsidentschaft *S. 9*
14. ECPA: europäische Kartensysteme stärken *S. 9*
15. Europa zertifiziert Cybersicherheit von IT-Produkten gemäß Common Criteria *S. 10*
16. DsiN: Sicherheitsindex 2025 *S. 10*
17. Regulatorik: KMU sollen entlastet werden *S. 10*

Sehr geehrte Damen und Herren,

Sommer und Urlaubszeit lassen uns kurz durchatmen. In den ersten Monaten des Jahres haben wir unerwartete geopolitische Veränderungen erfahren. Diese veranlassen die Branche, sich neu zu positionieren. Die Souveränität Europas im Zahlungsverkehr und bei der IT in der Finanzbranche erscheint notwendiger denn je. Sie sind ein Teil der kritischen Infrastruktur. Robuste und agile Strukturen sowie ein eigenständiger Betrieb der Systeme gewährleisten Resilienz und stützen das Vertrauen der Verbraucher. Während Banken und Sparkassen die gesetzten Anforderungen an IT-Sicherheit und Resilienz bereits umsetzen, sind Grundsatzfragen zur Machbarkeit des digitalen Euros als europäisches Bezahlsystem nicht geklärt. Die (finanzielle) Last von Betrug im Zahlungsverkehr tragen noch immer die Banken, obwohl geeignete Werkzeuge durch Dritte genutzt werden könnten.

Ursachen und Hintergründe dazu sowie zu weiteren Themen lesen Sie in unserem heutigen Newsletter.

Wir wünschen Ihnen eine interessante Lektüre.

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

Ausgabe Juli 2025

VÖB ZAHLUNGSVERKEHR

1. DIGITALER EURO: NICHT NUR KOSTEN AUF DEM PRÜFSTAND

Im Auftrag von drei europäischen Bankenverbänden wurden erstmals Investitionskosten für Banken und Sparkassen in Europa geschätzt, sollte der digitale Euro wie geplant als Bezahlsystem im Privatkundengeschäft etabliert werden müssen. Die im Juni 2025 veröffentlichte Studie von PricewaterhouseCoopers (PwC) kommt zu dem Schluss, dass die Einführung eines digitalen Euros mit erheblichen Kosten verbunden sein dürfte. So werden Umstellungskosten von bis zu 18 Milliarden Euro auf Seiten der europäischen Banken und Sparkassen für den gesamten Euroraum geschätzt.

Zentrale Kostentreiber wären zu 75 % der Gesamtkosten technische Anpassungen, die u. a. für die Herausgabe des digitalen Euros als Zahlungsmittel für die Kunden und die damit bankseitig vorzuhaltende Infrastruktur vorzunehmen wären.

Zusätzlich würden ca. 46 % der notwendigen personellen Kapazitäten über mehrere Jahre gebunden; anderweitige Investitions- und Innovationsvorhaben – sowohl für die eigene Geschäftstätigkeit als auch für die bereits heute bekannten regulatorischen Umsetzungsprojekte – würden stark eingeschränkt. Ausgegangen wird zunächst von einem Zeitraum von vier Jahren.

Die Studie, für die 19 Institute in Europa befragt wurden, gibt erste Anhaltspunkte für die durch die europäische Kreditwirtschaft zu stemmenden Investitionssummen.

Im Ergebnis formuliert die Studie strategische Empfehlungen zu:

- Kostenreduktion
- Effizienzsteigerung
- Sicherstellung der Wettbewerbsfähigkeit europäischer Banken und Sparkassen

Weitere Untersuchungen, die explizit bspw. die Kosten der Akzeptanzseite sowie der Zahlungsdienstleister beinhalten, sowie weitere Detaillierungen dürften notwendig sein, um die Gesamtlast, die Europa infolge der Einführung des digitalen Euros zu tragen hat, beziffern zu können.

Grundsatzfrage

Der digitale Euro soll vom Handel als Zahlungsmittel akzeptiert werden können, Nutzer sollen mit dem digitalen Euro gebührenfrei bezahlen können. Banken und Sparkassen als Herausgeber sollen die Kosten der ihrerseits benötigten Infrastruktur einschließlich Kosten für Betrugshaftung und Risikomanagement weitestgehend selbst tragen – dauerhaft.

Wenn das Eurosystem an dieser Vorstellung festhält, widerspricht dies dem Gedanken der freien Marktwirtschaft. Banken und Sparkassen müssten ihre unternehmerische Geschäftstätigkeit neu ausrichten – zu Lasten ihrer Kunden.

Eine deutlich eingeschränkte Innovationskraft und ggf. nicht vorhandene personelle und fachliche Ressourcen werden die Finanzbranche voraussichtlich europaweit schwächen.

Es liegt nahe, dass das Eurosystem jenseits des technisch-organisatorischen Konzepts die seinerseits gesetzten Ziele mit Blick auf Marktrelevanz, Praxistauglichkeit, Resilienz, Autonomie und Wettbewerb überdenkt.

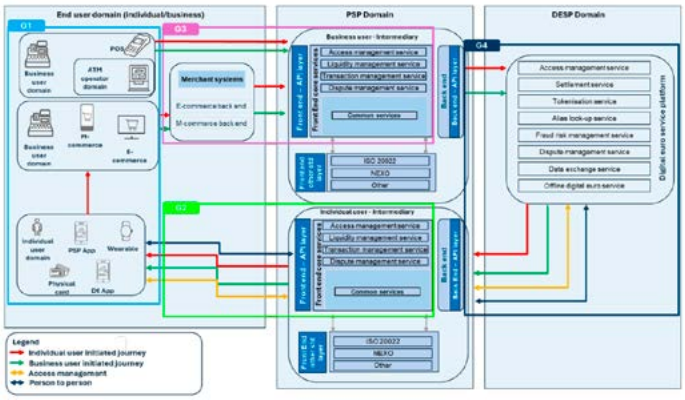
Zur Kostenstudie von PwC

2. DIGITALER EURO: ZEITPLANUNG DES EUROSYSTEMS

Die Arbeiten am Digital Euro Scheme Rulebook der gleichnamigen Development Group der EZB schreiten zügig voran. Ein Update des Rulebooks in der Version 0.9 wurde Anfang Juli 2025 veröffentlicht. In der Vorgängerversion waren bereits über 2.000 Kommentare berücksichtigt worden. Die neue Version geht ebenfalls in Konsultation. Die Architektur für den digitalen Euro ist komplex und unterscheidet sich von bestehenden Bezahlsystemen und Bezahlanwendungen. Zu begrüßen sind die Bemühungen, auf bestehende Standards (bspw. Berlin Group, nexo, CPACE oder EPC QR), auf existierende Zertifizierungsinfrastrukturen und somit auf vorhandene Infrastrukturen aufzusetzen. Allein alle potenziellen Anwendungsfälle kanalübergreifend und europaweit abzudecken, erscheint nach wie vor anspruchsvoll. Insofern laufen die Arbeiten in allen Workstreams zum digitalen Euro auf Hochtouren.

Nach aktueller Planung soll der ECON-Bericht zum digitalen Euro im Oktober 2025 erscheinen. Ebenfalls im Oktober 2025 soll der

Abb. 1: Die funktionale Architektur, die die Bereiche des digitalen Euros und ihre Schnittstellen spezifiziert



Quelle: Update on the work of the digital euro scheme's Rulebook Development Group

Governing Council der EZB über die bis dahin laufende Vorbereitungsphase für den digitalen Euro entscheiden. Wir erwarten nach derzeitigem Stand, dass das aktuelle Rulebook in der Version 0.9 lediglich als Annex und nicht vollständig als Ganzes in diese Entscheidung einfließen wird. Die Themen Adherence Model, Governance und Offline-Nutzung werden voraussichtlich nicht Teil dieser Version sein. Sie hängen stark vom Stand des Legislativverfahrens ab.

3. DIGITALER EURO: LEGISLATIVVORSCHLAG DES EUROPÄISCHEN RATES

Eines der wichtigen Themen, die die europäischen Banken und Sparkassen beschäftigen, sind zum einen deren Rolle in der aktuell beabsichtigten Abwicklungsstruktur und zum anderen die Finanzierung sowie das Kompensationsmodell. Das heißt, wie können die Aufwände für die Bereitstellungen eines „Digitaler-Euro-Zahlungskontos" kompensiert werden? So ist vorgesehen, dass die Banken und Sparkassen solch ein „Digitaler-Euro-Zahlungskonto" zusätzlich zu einem bestehenden Zahlungskonto vorhalten und beide Kontoarten miteinander verknüpfen müssen. Nach dem aktuellen Open-Funding-Ansatz ist vorgesehen, dass auch andere Zahlungsdienstleister ein „Digitaler-Euro-Konto" in ihrer Wallet anbieten können. Die Verknüpfung ist zwischen allen PSPs, die ein D€-Zahlungskonto unterhalten, nur mühsam sicherzustellen und impliziert eine Aufteilung der Kompensationsentgelte zwischen den verschiedenen PSPs. Diese werden ohnehin gedeckelt. Verschiedene Akteure in Europa haben dazu ihre Vorstellungen im Europäischen Rat eingebracht. Der Vorschlag des Rates beinhaltet im Moment ein vom Händler an dessen Acquirer zu zahlendes Entgelt sowie ein Entgelt der Händlerbank an die Kundenbank. Die genaue Höhe und prozentuale Verteilung zwischen diesen beiden Entgeltarten bleiben nach wie vor umstritten. Wir plädieren deshalb dafür, gemeinsam mit der Deutschen Kreditwirtschaft (DK), den Open-Funding-Ansatz nicht aufrechtzuerhalten, so dass nur das kontoführende Institut den digitalen Euro ausgeben und den dazugehörenden Account führen können soll. Diese Diskussion über Open Funding und das überkomplexe Kompensationsmodell prägt die derzeit laufenden Gespräche der DK auf europäischer Ebene sehr stark.

Mit welchen Fragen sich Verbraucher beim digitalen Euro beschäftigen, hat der Deutsche Sparkassen- und Giroverband e.V. im Rahmen einer qualitativen Studie untersuchen lassen: Im Wesentlichen wird erwartet, dass ein digitaler Euro genauso sicher, einfach und benutzerfreundlich ist, wie es bisher genutzte Systeme sind, und zusätzlich noch einen Mehrwert bieten muss – dieser wird bisher noch nicht gesehen".

Zur qualitativen Wirkungsanalyse

4. DIGITALER EURO: GEOPOLITIK VERÄNDERT DEN BLICK

Eines der Ziele für die Einführung eines digitalen Euros durch das Eurosystem und die Europäische Kommission war, eine elektronische Form von Bargeld für digitale Zahlungen bereitzustellen – überall verfügbar, nutzerfreundlich und weitestgehend kostenlos für die Nutzer. Ziel war auch, die Währungshoheit des Euroraums aus strategischen Gründen zu stärken und widerstandsfähiger auszugestalten.

Diese Ziele gelten weiterhin uneingeschränkt – mit Blick auf die rasant und nahezu täglich zunehmenden Bedrohungen und Unsicherheiten dürfte der digitale Euro eine neue Bedeutung erhalten. Aufgrund dieser neuen (politischen) Rahmenbedingungen sind die Prioritäten zu überdenken.

So verstärkt die wachsende Besorgnis über die Souveränität des Zahlungsverkehrs in Europa das Gefühl, unverzüglich und konkret handeln zu müssen – unter hohem Zeitdruck. Wettbewerbsfähigkeit (u.a. durch Vereinfachung), strategische Autonomie sowie Resilienz sind zu stärken. Dies wird auch von politischen Entscheidungsträgern wiederholt betont.

Alle am Projekt „Digitaler Euro“ Beteiligten sollten sich zügig über die Perspektiven sowie Grundsatzfragen verständigen und konstruktiv, kompromissbereit und kompromissfähig zusammenarbeiten.

So ist der digitale Euro für die Kreditwirtschaft in Europa dann attraktiv, wenn sinnvolle kommerzielle Rahmenbedingungen geschaffen werden. Dies schließt durch die Kreditwirtschaft heute bereits vorgehaltene oder sich in Umsetzung befindliche Lösungen ein.

Nur eine gemeinsame Lösung bzw. eine geteilte Vision kann von den europäischen Banken und Sparkassen mitgetragen werden.

Eurosystem und europäischer Gesetzgeber sind aufgefordert, dies zu ermöglichen.

5. VERIFICATION OF PAYEE: STÖRUNGEN IM ZAHLUNGSVERKEHR ERWARTET

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), die Deutsche Bundesbank und die Deutsche Kreditwirtschaft (DK) erwarten Störungen des Zahlungsverkehrs aufgrund der Einführung des Verification of Payee (VoP) ab Oktober 2025. Auch regionale Rechenzentren gehen von Zahlungsausfällen aus, da Verbraucher aufgrund der VoP-Warnungen verunsichert werden.

Denn ab 9. Oktober 2025 müssen Banken und Sparkassen bei jeder einzelnen SEPA-Überweisung und SEPA-Echtzeitüberweisung auf ein Zahlungskonto die IBAN und den Namen des Zahlungsempfängers kontrollieren. Die beim Empfängerinstitut hinterlegten Daten des Kontoinhabers sind mit den vom Auftraggeber eingegebenen Angaben abzugleichen. Entsprechendes regelt die am 8. April 2024 in Kraft getretene Regulierung zur Echtzeitüberweisung.[1)]

Im ersten Halbjahr 2024 wurden in Europa ca. 16 Milliarden Überweisungen getätigt (Quelle: Eurosystem). Für Einzeltransaktionen gilt künftig, dass Kunden zusätzlich und vor Zahlungsfreigabe das Ergebnis des VoP, das mit Grün, Gelb, Rot, Grau oder Weiß gekennzeichnet ist, bestätigen müssen:

VoP	Bedeutung	Hinweise für Aktion durch den Kunden
Grün	Übereinstimmung	Zahlung wird ausgeführt, keine Nachfrage beim Kunden
Gelb	Teilweise Übereinstimmung	Hinweis an den Kunden und Bitte um Prüfung/Freigabe/Ablehnung
Rot	Keine Übereinstimmung	Hinweis an den Kunden und Bitte um Prüfung/Freigabe/Ablehnung
Weiß	Service beim Empfänger nicht vorhanden, kein Abgleich möglich	Hinweis an den Kunden und Bitte um Prüfung/Freigabe/Ablehnung
Grau	Technischer Fehler, kein Abgleich möglich	Hinweis an den Kunden und Bitte um Prüfung/Freigabe/Ablehnung

VoP gilt für die oben genannten Überweisungen zwischen Zahlungskonten von Privat- und Firmenkunden sowie für die öffentliche Hand.

Weitere Regeln sind:

- Bei SCT / SCT-Inst von Verbrauchern ist immer ein VoP durchzuführen (Opt-in).
- Bei Sammlern mit SCT / SCT-Inst mit mehr als einer Transaktion dürfen Nicht-Verbraucher VoP abwählen.
- Bei Sammlern (SCT / SCT-Inst) mit einer Transaktion muss immer ein VoP durchgeführt werden (Opt-in).
- Bei Daueraufträgen besteht Bestandsschutz. Neu angelegte oder Änderungen bestehender Daueraufträge unterliegen dem VoP.

Technische Grundlage für VoP ist das VoP-Rulebook des European Payment Council (EPC). Das VoP-Rulebook ist verpflichtend für alle SCT- und SCT-Inst-Teilnehmer des EPC. Den technischen EPC Directory Service (EDS) für VoP betreibt SWIFT. Die Kosten werden über den EPC abgerechnet. Der EPC stellt aktuell Anforderungen zusammen, damit die Institute ab Oktober notwendige VoP-Statistiken einliefern können und müssen.

1) Verordnung (EU) 2024/886 des Europäischen Parlaments und des Rates vom 13. März 2024 zur Änderung der Verordnungen (EU) Nr. 260/2012 und (EU) 2021/1230 und der Richtlinien 98/26/EG und (EU) 2015/2366 zur Echtzeitüberweisungen in Euro.

Wie ist der Stand der Umsetzung?

Die Umsetzung in den Häusern ist aufwendig, Anpassungen sind sowohl an den Kundenschnittstellen im Online- und Mobile-Banking notwendig als auch in den Hintergrundsystemen und an den Schnittstellen zu Dritten. Die Vorbereitungen laufen auf Hochtouren; den Instituten verbleiben noch drei Monate.

Des Weiteren müssen Verbraucher und Firmenkunden über VoP informiert werden. Die Firmen müssen Aliasse vergeben und über die Konsequenzen von VoP aufgeklärt werden. Wenn viele Kunden von den VoP-Warnungen abgeschreckt werden, kann dies zu Zahlungsausfällen und ggf. zu Liquiditätsengpässen führen. Daher müssen Institute ihre Kunden rechtzeitig informieren. Die AGB- und DFÜ-Vereinbarungen müssen aktualisiert werden. Wir gehen davon aus, dass Verbraucher diese Verträge kaum lesen und daher kaum verstehen werden, was sie Anfang Oktober erwartet. Firmen, Behörden und öffentliche Kassen sollten ebenfalls unterstützen und ihre Kunden informieren, um Zahlungsausfälle zu vermeiden.

Ist Verification of Payee das richtige Mittel, um Betrug einzudämmen?

VoP kann nur in wenigen Szenarien von Betrug diesen auch effektiv eindämmen. Doch bei VoP müssen Kosten und Nutzen gegenübergestellt werden. Die Betrugsindustrie reagiert flexibel auf Gegenmaßnahmen. VoP ist aufwendig und teuer. Die Betrugsindustrie kann voraussichtlich mit einfachen Mitteln ausweichen.

Es gibt kaum Nachweise, Projekte oder Statistiken, nach denen VoP nachweislich Betrug eindämmt oder verhindert. Betrüger sind raffiniert und nutzen jegliche Umstellung von Bankprozessen aus, um Kunden zu täuschen und neue Betrugsmuster zu etablieren. Die erwartete Verunsicherung von Kunden bei Überweisungen ab Oktober und eine erhöhte Nachfrage bei Zahlungsempfängern könnten Betrüger für neue Betrugsszenarien ausnutzen.

Der Versuch, Betrug über VoP einzudämmen, könnte konterkariert werden. Die Verunsicherung wäre perfekt, Kunden geschädigt, Banken und Sparkassen würden einen Vertrauensverlust erleiden. Jeder Betrug ist anzuzeigen, auf Polizei- und Kriminalbehörden käme Mehrarbeit auf Kosten der Steuerzahler zu. Damit dieses theoretische Szenario nicht praxisrelevant wird, setzen wir uns für eine Zusammenarbeit zwischen allen Stakeholdern ein.

Zum EPC „Verification Of Payee Scheme Rulebook“

Zu den EPC Recommendations for the Matching Processes under the VOP Scheme Rulebook

6. GIROAPI-SCHEME: ERFOLGREICHER START 2025

Das giroAPI-Scheme der vier kreditwirtschaftlichen Verbände BdB, BVR, DSGV und VÖB ist Anfang des Jahres erfolgreich gestartet! Eine entsprechende Vereinbarung, die den Aufbau, den Betrieb und die Weiterentwicklung der „giroAPI-Schnittstelle“ regelt, wurde geschlossen. Über die giroAPI-Schnittstelle können Daten für die Erbringung von Dienstleistungen übertragen werden. Zwei Sub-Schemes sind verfügbar:

- Payment (bspw. Zahlung mit Disposition und Ausführung, Teilzahlungen, Micro-Payments, Bestätigung IBAN-Zugriffsmöglichkeit)
- Financial Information

Stand Juni 2025 sind bereits 190 genossenschaftliche Banken und ein Asset Broker (Abnehmer der Daten) – die Token GmbH – beigetreten. Weitere Beitritte auch europäischer Unternehmen werden zum 13. August 2025 erwartet. Das Interesse und die Nachfrage nach einem Beitritt sind groß. Wir erwarten, dass sich giroAPI zeitnah erfolgreich am Markt etablieren wird. Das giroAPI-Scheme der DK ist das erste API-Scheme in Europa!

Sechs Jahre nach der Einführung der PSD2 ist damit erstmals ein produktives Scheme live gegangen, das die Idee von Open Finance in Europa konkret umsetzt. Für beide Seiten – Banken und Asset Broker – ergibt sich daraus eine echte Win-win-Situation. Mit giroAPI wird eine neue Kundenklientel erschlossen. Die neue Kundenklientel muss als Partner und Kunde verstanden werden, so wie heute beispielsweise internationale Kartenherausgeber. Übrigens, diese haben schon Interesse an giroAPI bekundet. Auch hinter der Token GmbH steht ein Milliardenkonzern, der gern mit Banken und Sparkassen kooperieren möchte.

Sämtliche vertraglichen Dokumente, technischen Spezifikationen und Beitrittsanforderungen sind öffentlich verfügbar.

Informationen, Dokumente zum Download

7. PSD3/PSR: ART. 59 WEITERHIN KRITISCH

Der Ausschuss der Ständigen Vertreter der Mitgliedstaaten bei der EU hat am 18. Juni 2025 die Position des Rates zu PSR2/PSD3 gebilligt. Der Trilog soll bereits Mitte Juli 2025 beginnen. Nach vorsichtiger Einschätzung der DG FISMA könnte eine Einigung im EU-Parlament bis Weihnachten 2025 erzielt werden.

Seitens vieler Mitgliedstaaten wird weiterhin der Art. 59 kritisiert. Dieser Artikel besagt, dass Banken für Betrug im Zahlungsverkehr uneingeschränkt und ausschließlich haften sollen – selbst dann, wenn die Ursache des Betrugs außerhalb ihres Verantwortungsbereichs und ihrer (technischen) Möglichkeiten liegt und Betrug auch jenseits technischer Maßnahmen nicht verhinderbar ist. Banken sollen haften, wenn sich Betrüger gegenüber Verbrauchern als Bankmitarbeitende ausgeben. Das Europäische Parlament möchte die Haftung der Banken sogar auf alle Formen des Social Engineerings ausweiten.

Diese (berechtigte) Kritik ist mit konkreten Vorschlägen verbunden, wie die Haftungsbestimmungen angepasst werden können:

- Anwendungsbereich des Art. 59 erweitern und Anbieter elektronischer Kommunikationsdienste und Telekommunikationsdienstleister ausdrücklich einbinden bzw. zu Betrugspräventionsmaßnahmen verpflichten,
- technische Maßnahmen zur Betrugsprävention eindeutig definieren,
- Zahlungsdienstleistern unter bestimmten Voraussetzungen die Möglichkeit einräumen, Anbieter elektronischer Kommunikationsdienste haftbar zu machen,
- statt einer pauschalen Rückerstattungspflicht den Schwerpunkt auf präventive Maßnahmen legen, indem bspw. Mechanismen ausgebaut und so manipulative Angriffe aufgedeckt werden,
- Datenaustausch zwischen PSPs verstärken und dadurch gemeinschaftlich Betrug bekämpfen,
- weitere Formen von Identitätsbetrug ausdrücklich berücksichtigen sowie
- explizites Zwei-Faktor-Verfahren für Mobile Banking einführen und verbindlich regeln.

Diese Vorschläge sind realistisch umsetzbar. Telekommunikations- und Plattformanbieter halten bereits technische Werkzeuge vor und können damit Betrug effektiv bekämpfen. Eine gesetzliche Änderung, die einen Datenaustausch zwischen den Beteiligten explizit für den Zweck der Betrugsbekämpfung vorsieht, ist notwendig.

Vorläufiger Art. 59 – eine Art Subvention von Betrug im Zahlungsverkehr!

Vieles ist bereits gesagt, viele Argumente und Vorschläge sind bereits vorgebracht worden. Unverständlich ist weiterhin, warum der Regulator und die Politik eine verschuldensunabhängige Haftung zulasten von Banken und Sparkassen gesetzlich vorgeben? Es ist nicht nachvollziehbar, warum Banken und Sparkassen bspw. im Falle grober Fahrlässigkeit des Kunden haften sollen.

Der Art. 59 schafft es nicht, die organisierte Kriminalität einzudämmen, im Gegenteil. In der Folge dürften Verbraucher noch nachlässiger mit sensiblen Daten umgehen. Die Anzahl der Betrugsfälle und die Belastung für die Strafverfolgung steigen.

Wir erwarten einen Vertrauensverlust gegenüber digitalen Medien aufgrund des ansteigenden Betrugs. Dies gefährdet die digitale Transformation. Dieses Worst-Case-Szenario ist inakzeptabel.

Wir halten es für eine Pflicht des Regulators und der Politik, durch verursachungsgerechte Haftungsregeln – soweit sie überhaupt erforderlich sind – Verantwortung zu übernehmen. Wir plädieren dafür, Verbraucher zu einem verantwortungsbewussten Umgang mit zahlungsrelevanten Informationen und Medien zu bewegen, anstatt Kunden weitreichende Freiräume für einen weniger sorgfältigen Umgang bei Zahlungstransaktionen einzuräumen.

Bleibt der Art. 59 unverändert, wirkt er wie ein Freibrief, um unbekümmert und weniger verantwortungsvoll Dienstleistungen und Produkte von Banken und Sparkassen zu nutzen. Durch den Ansatz, dass die Bank den Schaden des Kunden zu ersetzen hat, droht eine Art Vollkasko-Mentalität zu entstehen.

Wir appellieren weiterhin an die europäischen und an die nationalen Institutionen, an objektiven Regelungen in der PSD3/PSR festzuhalten.

8. BETRUGSPRÄVENTION IM ZAHLUNGSVERKEHR: WAS IST ZU TUN?

Die Statistik des Bundeskriminalamtes ist alarmierend. Der Verbraucherzentrale Nordrhein-Westfalen wurden im Jahr 2024 ca. 400.000 Phishing-E-Mails gemeldet – im Fokus der kriminellen Aktivitäten ist weiterhin die Kreditwirtschaft. Banken und Sparkassen, zunehmend nicht nur Zahlungskonten von Privat- und Firmenkunden, sondern bspw. auch Depotkonten,

für den Zahlungsverkehr im Inland und mit dem Ausland, sind betroffen.

Eines ist klar: Betrug im Zahlungsverkehr hat eine neue Stufe der Professionalität erreicht. Es handelt sich um eine Betrugsindustrie, die organisiert und flexibel auf Abwehrmaßnahmen reagiert. Maßnahmen des europäischen Gesetzgebers – wie beispielsweise der Verification of Payee – sind zu unflexibel und werden von der Betrugsindustrie mit einfachen Mitteln umgangen. Deutschland scheint stärker betroffen zu sein als andere europäische Länder.

Die Schadensumme steigt ins Unermessliche: Laut BKA-Lagebild und Daten der Bitkom soll 2024 ein wirtschaftlicher Schaden infolge von Cyberkriminalität von insgesamt ca. 178 Milliarden Euro entstanden sein. Zum Vergleich: Der Entwurf für den Bundeshaushalt 2025 sieht Ausgaben von etwa 503 Milliarden Euro vor (*Bundeshaushalt 2025: Fragen und Antworten | Bundesregierung*).

Betrugsszenarien stellen heute überwiegend auf die Manipulation von Kunden oder von Mitarbeitern in Unternehmen oder auch öffentlichen Institutionen ab, die durch das sogenannte Social Engineering zu einer Zahlung bewegt werden sollen. Dieser Prozess der Manipulation beginnt mit einer E-Mail, einem Brief, einer SMS, einer WhatsApp oder einem Anruf. Die Zahlung steht am Ende des Betrugsprozesses, der über Tage, Wochen oder sogar Monate dauern kann. Sich nur auf Banken als letztes Glied in der Kette zu konzentrieren oder diese für sämtliche Schäden haftbar zu machen, ist nicht sachgerecht. Im Gegenteil: Nützliche Informationen, wie ein sich anbahnender Betrug frühzeitig zu erkennen ist, sind denjenigen Stellen unverzüglich bereitzustellen, die diesen einschränken oder letztlich tatsächlich verhindern können. Daher sind und müssen auch die Anbieter von E-Mails, Postdiensten, Social Media und Telefondiensten aktiv und bewusst in die Maßnahmen zur Betrugsprävention einbezogen werden.

Auch Strafverfolgungsbehörden sind in die Betrugsprävention einzubinden. Diese müssen verstärkt gegen die Betrugsindustrie vorgehen und ihrerseits verfügbare Angaben und erkennbare Entwicklungen frühzeitig mit betroffenen Institutionen teilen.

Damit Betrugsprävention wirksam gelingt, ist diese über den gesamten Prozess zu verfolgen. Eine Zusammenarbeit zwischen diesen drei Parteien erscheint notwendig:

- Behörden, insbesondere das Bundeskriminalamt und die Landeskriminalämter
- Post-, Telekommunikations- und Plattformanbieter
- Banken und Sparkassen

Ein Austausch von Daten über die Grenzen von Telekommunikationsunternehmen, Postdienstleistern, Plattformanbietern und Banken hinweg ist heute nicht möglich.

Der Austausch von Daten über Betrug ist auf zahlreiche Schultern zu verteilen, die jeweiligen Ressorts sind zu vernetzen. Ein runder Tisch allein reicht dafür nicht aus. Um notwendige Daten auszutauschen, sind gesetzliche Regelungen bereitzustellen – mit Augenmaß und unter Berücksichtigung des Datenschutzes. Geht es um Betrugsprävention, sind die Regeln des Datenschutzes angemessen auszugestalten. Ohne Zutun des Gesetzgebers wird die Betrugsindustrie nicht wirksam bekämpft werden können; Schäden werden steigen, Betroffene sowie die breite Öffentlichkeit werden Vertrauen nicht nur in Banken und Sparkassen verlieren. Denn auch wenn das Ziel der Betrüger immer ein Geldbetrag ist, als Mittel zum Zweck werden Phishing-E-Mails auch im Namen vermeintlicher Kriminalbehörden, Lieferdienste, Behörden, Ärzte, Wohltätigkeitsorganisationen usw. verschickt. Die Kreativität der Kriminellen kennt keine Grenzen, ein Ende von Betrug im Zahlungsverkehr ist nicht in Sicht.

Es gilt, die Souveränität Europas und seine Wettbewerbsfähigkeit auch im Bereich der Betrugsprävention im Zahlungsverkehr zu stärken. Wir fordern, die notwendigen gesetzlichen Grundlagen für einen sektorübergreifenden Austausch von Daten zwischen Kreditwirtschaft, Plattformanbietern, Strafverfolgungsbehörden, Telekommunikations- und Postdienstleistern zu schaffen.

9. BUNDESBANK: ABSCHALTEN DES TELEFAX ENDE 2025

Die Bundesbank wird zum Ende des Jahres 2025 das Fax zur Kommunikation größtenteils abschalten und auf eine gesicherte E-Mail umstellen. Betroffen sind u. a. folgende Dienste:

- TARGET2
  - Für Änderung der Liquiditätsbereitstellung in ECONS II
- SEPA-Clearer
  - Bei Problemen oder Störungen auf Kundenseite an den SEPA-Clearer
  - Beim Wechsel des Kommunikationskanals des Teilnehmers bei Störung

10. EINSTELLUNG DES SCHECKVERFAHRENS IN 2027 GEPLANT

Die Deutsche Kreditwirtschaft und die Deutsche Bundesbank halten weiterhin daran fest, das Scheck- und Reisescheckabkommen zum Ende des Jahres 2027 zu kündigen. Während Auslandsschecks nicht betroffen wären, würde spätestens ab dem Jahr 2028 kein Scheckinkasso in Deutschland mehr durchgeführt werden.

Scheckzahlungen sind seit Jahren rückläufig. Rund 2,6 Millionen Scheckzahlungen wurden im Jahr 2023 abgewickelt, 2022 waren es noch 3,6 Millionen (Quelle: Statista). Für die kommenden beiden Jahre wird mit einem weiteren Rücklauf gerechnet. Entsprechend werden Vorbereitungen getroffen, die für die Scheckabwicklung vorgehaltene Infrastruktur und die damit vergleichsweise hohen Kosten zeitnah zurückzubauen und Clearing und Verarbeitung vollständig Ende 2027 einzustellen.

11. KÜNSTLICHE INTELLIGENZ: KI-VERORDNUNG IN UMSETZUNG

Der regulatorische Rahmen für Künstliche Intelligenz (KI) wird derzeit sowohl auf europäischer als auch auf deutscher Ebene aufgebaut. Die KI-Verordnung der Europäischen Union (AI Act) – am 1. August 2024 in Kraft getreten – soll gestaffelt über die nächsten zwei Jahre umgesetzt werden. Der AI Act selbst soll sicherstellen, dass die Grundrechte der EU-Bürger bei Einsatz von KI gewahrt bleiben. Zugleich werden grundlegende Anforderungen für den Einsatz generativer KI formuliert.

Wichtige Punkte bleiben noch ungeklärt:

Es fehlt weiterhin eine klare Definition von KI, die den Status der Kreditwürdigkeitsprüfung in der Bankenanwendung eindeutig regeln würde. Die im April 2025 versprochenen europäischen Standardisierungen sowie die Leitlinien für generative KI stehen noch aus. Das macht die Einhaltung der gesetzlich vorgesehenen Umsetzungsfristen fast unmöglich. Hier sind zügig praxisgerechte, rechtssichere Leitplanken bereitzustellen. In diesem Zusammenhang wird eine Verschiebung der Anwendungsfristen und eine Vereinfachung ausgewählter Einzelregelungen sowie die verstärkte Unterstützung von Unternehmen bei der Implementierung der KI-Verordnung (insbesondere von KMU) sowohl auf europäischer als auch auf deutscher Ebene heiß diskutiert.

Ein deutsches Umsetzungsgesetz ist bisher nicht verabschiedet. Daher ist der pragmatische Ansatz der BaFin bei der Prüfung von KI-Modellen in der Banksteuerung zu begrüßen. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Prüfkatalog für vertrauenswürdige KI in der Finanzwirtschaft veröffentlicht. Dadurch wird der eigenverantwortliche Einsatz von KI zumindest auf nationaler Ebene unterstützt.

Im Zusammenhang mit der Implementierung von KI stellen sich Herausforderungen, wie mit bestehenden IKT-Risiken unter DORA umzugehen sein wird. Hierzu dürfte mit einer Mitteilung der BaFin im 4. Quartal 2025 zu rechnen sein.

12. DORA: MEHR DIGITALE RESILIENZ, WENIGER KOMPLEXITÄT

Schon mit dem Inkrafttreten des Digital Operational Resilience Act (DORA) zum 17. Januar 2025 nach zweijähriger Übergangsfrist ist Bedarf für Entlastung hörbar. Denn obwohl DORA verhältnismäßig verankert wurde, wird er in der praktischen Auslegung und in den technischen Regulierungsstandards (RTS/ITS) nicht konsequent durchdekliniert:

- Pflichten, wie das Erstellen eines vollständigen Registers aller IKT-Dienstleister, umfangreiche IT-Dokumentationen oder vielfach redundante Meldepflichten aus DORA, NIS2 und DSGVO erzeugen Aufwand – ohne entsprechenden Sicherheitsgewinn.
- Sinnvolle Schwellenwerte – etwa nach Kritikalität, Auslagerungsvolumen oder Relevanz für die Geschäftsfortführung – und langfristig standardisierte Meldeplattformen mit automatisiertem Datenabruf könnten hier gezielt entlasten. So würden Ressourcen auf tatsächliche Risiken gelenkt, statt in formalistischer Pflichterfüllung gebunden zu werden.

Auch wenn der Review von DORA erst bis zum 17. Januar 2028 erfolgen muss, ist das Zeitfenster unter dem aktuellen Stichwort „Simplifizierung“ günstig, um grundsätzliche Aspekte zu überprüfen und ggf. neu zu bewerten.

Der VÖB hat seine Positionen in einem Positionspapier zusammengefasst und setzt sich für diese im Dialog mit Politik und Aufsicht ein. Im Zentrum stehen dabei klare Anforderungen für eine tatsächlich risikoorientierte Umsetzung, die nach dem Prinzip „weniger ist mehr“ echte Resilienz ermöglicht.

Zum VÖB-Positionspapier

13. CYBER RESILIENCE ACT (CRA): UNTERSTÜTZUNG FÜR DEN „STOP THE CLOCK"-VORSCHLAG DER POLNISCHEN RATSPRÄSIDENTSCHAFT

Mit dem Cyber Resilience Act will die EU die Cybersicherheit digitaler Produkte verbessern – ein wichtiges Ziel, das wir ausdrücklich teilen. Gleichwohl birgt der aktuelle Zeitplan Risiken für Rechtssicherheit und Umsetzbarkeit.

Wir unterstützen daher den Vorschlag der polnischen Ratspräsidentschaft, einen „Stop the Clock"-Mechanismus einzuführen: Die Übergangsfrist soll erst dann starten, wenn alle wesentlichen Durchführungsrechtsakte vorliegen.

Warum das wichtig ist – gerade für die Finanzindustrie:

- → DORA ist Lex specialis: Finanzunternehmen unterliegen bereits heute sehr spezifischen Anforderungen an digitale Resilienz. Diese Spezialisierung muss auch im CRA berücksichtigt werden.
- → Branchenspezifik ernst nehmen: Der CRA stuft Zahlungsverkehrskarten als kritische Produkte mit gesonderten Anforderungen ein, obwohl diese bereits heute höchsten Sicherheitsanforderungen unterliegen (s. EUCC). Durch die Geltung des CRA für eine große Bandbreite digitaler Produkte – vom Online-Spiel bis zu komplexen Kartenlösungen –, ist es umso wichtiger, dass Banken und Consumer-Anwendungen nicht pauschal gleichbehandelt werden.
- → Doppelte Pflichten vermeiden: Es drohen Überlappungen bei Meldepflichten und Sicherheitsanforderungen – z. B. zwischen CRA, DORA und NIS2. Hier braucht es Klarheit statt Komplexität.

Wir unterstützten daher den Vorschlag der polnischen Ratspräsidentschaft und setzen uns für eine Herausnahme der Finanzindustrie aus dem CRA ein.

14. ECPA: EUROPÄISCHE KARTENSYSTEME STÄRKEN

Europäische Kartensysteme, d. h. Kartensysteme mit eigener Governance in Europa, haben im Jahr 2024 mit 263,1 Millionen sich im Umlauf befindlichen Karten knapp 31,5 Milliarden Transaktionen abgewickelt. Grund genug, dass die European Card Payment Association (ECPA) in einem Whitepaper fordert, die Souveränität der europäischen Kartenzahlungssysteme zu stärken. Die ECPA unterstreicht die bewährten Grundlagen von Resilienz, Kosteneffizienz und marktspezifischen Lösungen sowie deren wesentliche Rolle und ihren Beitrag zur europäischen Souveränität.

Das Whitepaper adressiert Forderungen an politische Entscheidungsträger in Europa:

- → Es ist sicherzustellen, dass Verbraucher und Unternehmen in der Europäischen Union über mindestens ein in der EU gesteuertes Zahlungsinstrument verfügen können. Hierdurch wird die – von der Politik erwartete – europäische Souveränität im Zahlungsverkehr gewährleistet.
- → Vorhandene europäische Standards, wie bspw. CPACE, und deren Nutzung sind zu unterstützen.
- → Maßnahmen der Regulierung im Zahlungsverkehr müssen sicherstellen, dass gleiche Wettbewerbsbedingungen zwischen den europäischen Kartenzahlungssystemen und international agierenden Akteuren gelten.
- → Um die Reichweite europäischer Kartensysteme auszubauen und weiterhin den Schwerpunkt auf die bestehenden nationalen Märkte (hier werden über 90 % der Transaktionen abgewickelt!) setzen zu können, sind grenzüberschreitende Aktivitäten für den Ausbau der notwendigen Infrastruktur zu unterstützen.
- → Initiativen für europäische Lösungen, die die grenzüberschreitende Interoperabilität europäischer Kartensysteme ermöglichen, sind zu unterstützen.

Europäische Kartenzahlungssysteme sind für die Souveränität Europas unverzichtbar!

Die über teils viele Jahrzehnte fest im Tagesgeschäft von Verbrauchern und Unternehmen etablierten europäischen Kartensysteme stemmen den überwiegenden Teil der alltäglichen Bezahltransaktionen – reibungslos, effizient und vertraut.
Die europäischen Kartensysteme wissen – nicht zuletzt aufgrund von langer Erfahrung und spezifischem Know-how im Kartengeschäft – um die Feinheiten und die Komplexität beim Bezahlen wie auch bei Bargeldverfügungen an Geldautomaten. Hier werden keine Rosinen herausgepickt und die erzielbaren Margen halten sich aufgrund bestehender Regulatorik in Grenzen. Dies freut den Handel und der Verbraucher kann sich auf eine breite Akzeptanzinfrastruktur verlassen.
Der Regulierer in Europa tut gut daran, bewährte und verlässliche Praktiken als Beitrag zur Souveränität Europas zu stärken.
Die Forderungen der ECPA sind zu unterstützen.

Zum Pressestatement der ECPA

15. EUROPA ZERTIFIZIERT CYBERSICHERHEIT VON IT-PRODUKTEN GEMÄSS COMMON CRITERIA

Das heutige SOGIS-Scheme für Zertifizierungen auf Basis von Common Criteria wurde im März 2025 auf das neue EUCC-Scheme migriert. Damit sind die Voraussetzungen für ein in Europa einheitliches Schema für die Zertifizierung der Cybersicherheit von IT-Produkten geschaffen. EUCC steht für European Union Cybersecurity Certification.

Im Zahlungsverkehr, insbesondere dem girocard-System, ist die Zertifizierung von Point-of-Sale-Terminals gemäß Common Criteria bereits seit vielen Jahren etabliert. Gemeinsam mit UK Payments hatte die Deutsche Kreditwirtschaft als Betreiberin des girocard-Systems vor zehn Jahren eine gemeinsame Infrastruktur für die Zertifizierung geschaffen. Seitdem wurde die Hardware und Firmware für fast 200 Endgeräte – Points of Interaction (POI) – gemäß Common Criteria und auf Grundlage von Protection Profiles für POI evaluiert und zertifiziert. UK Payments und DK prüfen derzeit, wie bestehende Prozesse in EUCC so überführt werden können, dass sowohl das für die Kartenzahlungen notwendige Sicherheitsniveau erhalten bleibt als auch die Abläufe eine zügige Zertifizierung im Interesse der Hersteller und der Systeme gewährleisten.

Im neuen EUCC-Scheme wurden bestehende internationale Common-Criteria-Standards hinsichtlich europäischer Anforderungen angepasst – ein Schritt zu mehr Unabhängigkeit im Interesse der Sicherheit.

Zu Common.SECC

Zu ENISA

16. DSIN: SICHERHEITSINDEX 2025

Der vom Verein Deutschland sicher im Netz e.V. (DsiN) im Juni 2025 veröffentlichte „Sicherheitsindex 2025“ bewertet erneut die digitale Sicherheitslage von Verbrauchern in Deutschland. Das Ergebnis überrascht nicht: Während die Bedrohungslage steigt, nimmt das Verhalten in puncto Sicherheit ab. Einzelne ausgewählte Beispiele zeigen dies.

Der digitale Wandel, d. h. der Übergang von bislang von Verbrauchern genutzten Hardware-gestützten Geräten hin zu technologisch flexiblen Medien, führt zu unbedarfterer Nutzung und weniger Sensibilität im Umgang mit diesen. Fehlendes, jedoch notwendiges Wissen verleitet Verbraucher dazu, Risiken zu unterschätzen und somit eher auf Betrüger hereinzufallen.

Der Sicherheitsindex 2025 des DsiN kommt richtigerweise zu dem Ergebnis, dass technische Schutzmaßnahmen zu nutzen sind. Hierfür ist Aufklärung notwendig. Im Gegensatz zu den Bestrebungen der EU-Kommission in der PSD3/PSR, Verbraucher von Haftung im Falle von Betrug (im Zahlungsverkehr) freizustellen und damit vor finanziellen Schäden zu schützen, setzt der DsiN auf vorhandene Möglichkeiten und den „Schutz“ von Verbrauchern, indem diese selbst aktiv werden.

Effektive Schutzmaßnahmen sind unerlässlich!

Dieses Ergebnis des DsiN ist wichtig. Es unterstützt unser Verständnis, dass vorhandene technische Maßnahmen, bspw. das Blocken massenhaft versendeter Phishing-E-Mails durch Telekommunikationsdienstleister, gesetzlich ermöglicht werden müssen. Darüber hinaus sind dazwischengeschaltete Dienstleister zu verpflichten, ihrerseits mögliche technische Schutzmaßnahmen vorzuhalten.

Sensibilisierung von Verbrauchern und Unternehmen allein reicht nicht aus. Gezielte Aufklärung über notwendige Schutzmaßnahmen ist unerlässlich.

Zum Sicherheitsindex 2025

17. REGULATORIK: KMU SOLLEN ENTLASTET WERDEN

Die polnische Ratspräsidentschaft der Europäischen Union setzt Zeichen: Im digitalen Sektor sollen regulatorische Anforderungen vereinfacht werden. Dadurch sollen Innovationen insbesondere für kleine und mittlere Unternehmen gefördert werden. Vorgeschlagen und relevant für das Finanzwesen sind:

→ Artificial Intelligence Act (AI Act)

→ Cyber Resilience Act (CRA)

- Definitionen von CRA, NIS2 und DORA sollen harmonisiert werden
- Meldepflichten von CRA und NIS2 sollen gegenseitig anerkannt werden
- Vorhandene Zertifizierungen sollen anerkannt, sektorspezifische Zertifizierungen ermöglicht werden

- Fristen für die Umsetzung sollen verlängert werden („Stop the clock“-Mechanismus)

→ Datenschutz-Grundverordnung (DSGVO)

- Sandboxes mit Datenschutzbehörden und KI-Aufsichtsbehörden, unterstützt durch eine gemeinsame Plattform
- Stärkere institutionelle Zusammenarbeit zwischen AI-Office, AI-Board und dem Europäischen Datenschutzausschuss (EDPB)
- Vereinfachte Anwendung der DSGVO auf Trainingsdaten der KI im Rahmen einer allgemeinen Flexibilisierung der Datenschutzgrundsätze, z. B. die Anerkennung von Anonymisierung als zulässigen Verarbeitungszweck
- Konsolidierung der Transparenzpflichten durch Entwicklung eines einheitlichen, standardisierten Rahmens für digitale Dienste

Über VÖB Zahlungsverkehr
Mit VÖB Zahlungsverkehr informieren wir über ausgewählte Schwerpunkte im Zahlungsverkehr auf nationaler und europäischer Ebene.

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

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

Weitere Newsletter des VÖB:
- → *VÖB Aktuell*
- → *VÖB Digital*
- → *VÖB Aktienmarktprognose*
- → *VÖB Kapitalmarktprognose*

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: 16. Juli 2025
Registernummer im Transparenz-Register der EU: 0767788931-41