

AUSGABE DEZEMBER 2024



# VÖB ZAHLUNGSVERKEHR

## INHALT

|     |  |       |
|-----|--|-------|
| 1.  | Digitaler Euro: Neustart des Legislativpaketes                               | S. 2  |
| 2.  | Digitaler Euro: Arbeiten am Rulebook   | S. 3  |
| 3.  | SEPA-Echtzeitüberweisung: VoP im Fokus                                       | S. 3  |
| 4.  | SEPA-Echtzeitüberweisung: Auswirkungen auf Institute                         | S. 4  |
| 5.  | PSD3/PSR: Neue Vorschläge zulasten von Banken                                | S. 5  |
| 6.  | SEPA: Weitere Länder schließen sich an                                       | S. 6  |
| 7.  | Bundesbank: Einstellung des Telefax  | S. 6  |
| 8.  | Einstellung des Scheckverfahrens in 2027 geplant                             | S. 6  |
| 9.  | EBA/EZB: Betrugsstatistik  | S. 6  |
| 10. | ERPB: Maßnahmen gegen steigenden Betrug                                      | S. 7  |
| 11. | eIDAS 2.0: Vertrauen notwendig   | S. 7  |
| 12. | Künstliche Intelligenz: KI-Verordnung in Umsetzung                           | S. 8  |
| 13. | Künstliche Intelligenz: Multi-Stakeholder-Konsultation bis 11. Dezember 2024 | S. 9  |
| 14. | giroAPI-Scheme der DK: Nutzung ab 2025                                       | S. 9  |
| 15. | Kartensicherheit: Verbraucher sensibilisieren                                | S. 10 |
| 16. | DORA tritt in Kraft: Herausforderungen und offene Fragen                     | S. 10 |
| 17. | KRITIS Dachgesetz: starke Infrastrukturen schützen                           | S. 11 |
| 18. | VÖB-Fachtagung: „DORA-readiness im Praxis-Check“ am 12. Dezember 2024        | S. 12 |

Sehr geehrte Damen und Herren,

das Jahr 2024 neigt sich dem Ende. Was hat es aus Sicht des Zahlungsverkehrs und der Informationstechnologie gebracht, um die europäische Souveränität zu stärken, digitale Ökosysteme und Innovationen einer vom Markt getriebenen Wirtschaft nach vorne zu bringen? Was ist dafür seitens der europäischen Regulatorik in den kommenden Jahren notwendig und welche Schwerpunkte setzen wir bei unseren Aktivitäten im Jahr 2025? Eines wird deutlich: Neben Resilienz ist die Betrugsprävention über alle Kanäle hinweg notwendig, um das Vertrauen der Menschen in Europa aus wirtschaftlicher und gesellschaftlicher Sicht zu stärken.

Wir wünschen Ihnen eine interessante Lektüre.

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

## VÖB ZAHLUNGSVERKEHR

### 1. DIGITALER EURO: NEUSTART DES LEGISLATIVPAKETES

Nach Vorlage des Gesetzesvorschlages für einen digitalen Euro durch die EU-Kommission im Juni 2023 wurden Verhandlungen über den parlamentarischen Berichtsentwurf im Ausschuss für Wirtschaft und Währung (ECON-Ausschuss) des Parlaments bis zu den Europawahlen im Juni 2024 aufgenommen. Danach geriet der Prozess im ECON-Ausschuss ins Stocken. Wir erwarten einen Neustart der Verhandlungen voraussichtlich frühestens im 1. Quartal 2025. Ganz anders im Europäischen Rat: Ab 1. Januar 2025 übernimmt Polen die Ratspräsidentschaft, nach Ungarn ein weiteres Land ohne Euro. Die ungarische Ratspräsidentschaft hatte keine weitere wesentliche Positionierung im Europäischen Rat für das Jahr 2024 angekündigt und auch von Polen ist kaum eine Änderung im Rat zu erwarten.

Obwohl formal die grundsätzliche Entscheidung für einen digitalen Euro noch nicht gefallen ist, arbeitet auch die Europäische Zentralbank (EZB) mit Hochdruck an ihrem Konzept für ein eigenständiges hoheitliches Bezahlssystem in Europa. Das sich in Erarbeitung befindliche Rulebook definiert 93 Geschäftsvorfälle und sieht eine vollständige Zahlungsinfrastruktur vor. Das Rulebook soll Ende 2024 in einer vorläufigen Version vorliegen und in weniger als zwölf Monaten in die Beschlussfassung der Gremien der EZB eingebracht werden ([Project timeline and planning of 2024 ERPB – agenda item 6](#)).

Mit diesem beabsichtigten, europaweit einheitlichen Zahlungssystem ist nicht nur eine extreme Komplexität verbunden, auch die Herausforderungen, Auswirkungen und Abhängigkeiten sind bislang weder ausreichend ausformuliert noch gelöst.

Was ist notwendig, damit der digitale Euro ein Zugewinn für alle Marktteilnehmer werden kann? Was muss das Zahlungssystem leisten, damit das Ziel, Europa unabhängiger, wettbewerbsfähiger und resilienter zu machen, erreicht werden kann? Wichtige Kernforderungen sind:

#### Rollenverteilung sicherstellen

Zwingend notwendige Innovationspotentiale können nur durch eine enge Zusammenarbeit mit dem Privatsektor erschlossen werden. Die Bedürfnisse der Nutzer sind zu berücksichtigen. Entsprechend ist die Rollenverteilung wie folgt auszugestalten: Die EZB ist ausgebende Institution und stellt die Backend-Infrastruktur unter Einbindung bereits bestehender privatwirtschaftlicher Initiativen zur Verfügung; die Banken und Sparkassen stellen ihren Kunden den digitalen Euro über ein Frontend ihrer Wahl zur Verfügung.

#### Interessenskonflikte vermeiden

Im November 2021 hatte die EZB ihre Anforderungen an die Überwachung von elektronischen Zahlungsinstrumenten, Zahlungssystemen und sog. Zahlungsmodalitäten veröffentlicht (siehe [Eurosystem oversight framework for electronic payment instruments, schemes and arrangements](#)). Ziel ist, die Stabilität der Systeme über alle Ebenen zu gewährleisten. Wird der digitale Euro ebenfalls i.S. dieser Anforderungen mit der **EZB als Governance Body** betrieben werden? Nach welchen Kriterien und Prämissen wird das Zahlungssystem digitaler Euro dann letztlich betrieben?

Die Eurosystem bzw. die angeschlossenen nationalen Notenbanken sind für die Überwachung der in den jeweiligen Mitgliedsstaaten ansässigen Systeme und damit für die Überprüfung der Einhaltung der o.g. Anforderungen zuständig. Wie werden mögliche Wettbewerbsnachteile und Interessenskonflikte ausgeschlossen?

#### Komplexität reduzieren

Die hohe Anzahl von 93 Anwendungsfällen sollte auf Minimum-Anforderungen im Vergleich zur Nutzung von Bargeld reduziert werden. Eine vollständige Implementierung ist komplex und sehr kostenintensiv – neben der ergänzenden Erfüllung von regulatorischen Anforderungen. Entsprechend sind detaillierte Migrationspläne mit allen Beteiligten frühzeitig abzustimmen. Dies alles jenseits einer bislang nicht durchgeführten Kosten-Nutzen-Analyse. Je nach Ausgestaltung des Rulebooks sowie der Klärung weiterer Fragen erwarten wir – aus vielen Jahren Erfahrung im europäischen Zahlungsverkehr – einen mehrjährigen Zeitraum für die Implementierung. Gleichzeitig müssen in die Umsetzungsplanung weitere IT- und Zahlungsverkehrsprojekte ergänzend zu bestehenden regulatorischen Anforderungen integriert werden. Insofern ist sicherzustellen, dass die Institute ihre Wettbewerbsfähigkeit trotz dieser Mehrbelastung aufrechterhalten können.

#### Echte Mehrwerte schaffen

Wird der Kunde mit dem digitalen Euro am Kassenterminal bezahlen wollen? Bevorzugt vor allen ihm bislang gewohnten Bezahlmethoden? Letztere sind in den europäischen Ländern unterschiedlich ausgestaltet. Nach wie vor haben Kartenzahlungen den höchsten Anteil gefolgt von Barzahlungen. Diese privatwirtschaftlichen Zahlungsverkehrsangebote hat der digitale Euro zu komplementieren bzw. sind zu integrieren. Anderenfalls werden diese – in Deutschland ist die Debitkarte bevorzugtes Bezahlmittel am Point of Sale – vom Markt verdrängt. Inwieweit der Wettbewerb zugunsten des digitalen Euro steigt, bleibt abzuwarten. Ebenfalls, ob sich die hohen Investitionen amortisieren, wenn gleichzeitig für Zahlungsdienstleister nur begrenzt Geschäftsmodelle vorgesehen werden.

## VÖB ZAHLUNGSVERKEHR

Ohne **Vertrauen in ein Zahlungsmittel** und dessen Bereitsteller wird dieses nicht genutzt (siehe [Zahlungsverhalten in Deutschland 2023 | Deutsche Bundesbank](#)). Wie will das der digitale Euro schaffen? Es ist unerlässlich, dass sich die Ausgestaltung des digitalen Euro klar an der tatsächlichen Nachfrage am Markt ausrichtet. Hierbei sollte der Digitale Euro Zentralbankgeld dort verfügbar machen, wo Bargeld als Zahlungsmittel nicht verwendet werden kann, vornehmlich im digitalen Raum, im Sinne „Digital Only“.

### Regulatorik und mögliche Auswirkungen auf die Rechtsstaatlichkeit

Ein digitaler Euro wird nur dann erfolgreich sein, wenn er von den Bürgern und der Wirtschaft Europas akzeptiert wird.

Dies setzt voraus, dass der Rechtsrahmen zur Einführung des digitalen Euro rechtsstaatlichen Anforderungen genügt. Rechtssicherheit schafft Planungssicherheit. Diese Rechtssicherheit wird durch die neuen Haftungsregelungen von PSD3/PSR nicht zwingend hergestellt! Im Gegenteil: Banken sollen für sämtlichen Betrug haften, der Kunden in welcher Form auch immer entsteht. Es ist davon auszugehen, dass die Haftung auch bei Betrug, der im Zusammenhang mit der Nutzung des digitalen Euro entsteht, greift. Das beabsichtigte Zahlungsmittel erhöht somit die Risiken für die Beteiligten. Wie sich die EZB das Risikomanagement im Detail vorstellt, ob die bestehenden und neuen Maßnahmen zur Betrugsbekämpfung in Europa auch für das Bezahlsystem digitaler Euro relevant sind – s. bspw. Verification of Payee – auch das sind Fragen, die dringend beantwortet müssen.

Planungssicherheit geht mit Rechtssicherheit einher. Hier steht die EZB in der Verantwortung!

Der digitale Euro ist und bleibt eine Herausforderung für Europa – auch nach den Europawahlen. Die EZB möchte gern bereits im Herbst 2025 einen Beschluss für die Herausgabe des digitalen Euro auf der Grundlage des Rulebooks treffen. Ob bis dahin alle notwendigen Voraussetzungen für vorliegen, ist in erster Linie vom Stand des Legislativverfahrens abhängig. Bei letzterem sieht es aktuell parlamentsseitig nicht nach einem zügigen Fortschritt aus. Auch eine Rückgabe des Legislativvorschlages an die EU-Kommission ist im Gespräch.

## 2. DIGITALER EURO: ARBEITEN AM RULEBOOK

Den aktuellen Stand der Arbeiten am Rulebook hatte die EZB am 5. September 2024 veröffentlicht. Inzwischen wurde im Euro Retail Payments Board (ERPB) ein weiterer Workstream zum Thema „Integration des digitalen Euro in das Zahlungssystem“ etabliert. Konzentriert wird sich auf die Themen: Wettbewerb, Synergien und Geschäftsmodelle. Es gilt, Vorteile und potenzielle Risiken zu identifizieren sowie mögliche unbeabsichtigte Folgen eines nicht geeignet ausgestalteten Konzepts für einen digitalen Euro zu verringern.

Die Arbeiten werden sich voraussichtlich bis in das zweite Quartal 2025 erstrecken. Sie kommen etwas verspätet, dennoch sind diese zwingend notwendig, um weitere Entscheidungen in die richtige Richtung lenken. Die European Banking Federation (EBF) bringt sich in diese Arbeiten ebenfalls aktiv ein.

Die EZB selbst möchte das Rulebook für den digitalen Euro im Oktober 2025 fertigstellen. Über den Stand wurde zum 5. September informiert:

 [Update on the work of the digital euro scheme's Rulebook Development Group](#)

## 3. SEPA-ECHTZEITÜBERWEISUNG: VOP IM FOKUS

Die Regulierung zur Echtzeitüberweisung<sup>1)</sup> ist am 8. April 2024 in Kraft getreten. Der Zeitplan ist eng:

- 9. Januar 2025
  - Empfangen der Echtzeitüberweisungen ermöglichen
  - Deckelung der Entgelte für Echtzeitüberweisungen auf das Niveau der Überweisung
  - Prüfung gegen Embargo-Listen der EU
- 9. April 2025
  - Jährliche Berichte über Entgelte und Transaktionen; erstmaliger Bericht rückwirkend ab 26. Oktober 2022
- 9. Oktober 2025
  - Senden der Echtzeitüberweisungen anbieten
  - Empfänger überprüfen (Abgleich von IBAN und Name, Verification of Payee (VoP))

Kritisch in der Umsetzung ist der VoP. Beim VoP werden Institute verpflichtet, die IBAN und den Namen des Empfängers bei jeder

1) VERORDNUNG (EU) 2024/886 DES EUROPÄISCHEN PARLAMENTES 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

## VÖB ZAHLUNGSVERKEHR

einzelnen SEPA-Überweisung und SEPA-Echtzeitüberweisung abzugleichen. D.h. die Eingabe des Empfängernamens durch den Auftraggeber mit dem beim Empfängerinstitut hinterlegten Kontoinhaber wird buchstäblich abgeglichen.

Der European Payments Council (EPC) hat am 10. Oktober 2024 das im Frühjahr 2024 konsultierte „Verification Of Payee Scheme Rulebook“ veröffentlicht. Geregelt werden u.a. das Rollenmodell und weitere Mechanismen, damit für VoP zumindest technisch einheitliche Vorgaben für die Beteiligten bestehen. So hat der EPC ebenfalls Empfehlungen für das Matching für Namen grob formuliert: z. B.: u=ü=ue. Inwieweit diese Empfehlungen rechtlich bindend sind, ist unklar.

Bei EBICS sind bzgl. VoP die Verträge zwischen Service-Rechenzentren und Kunden insbesondere zur Haftung anzupassen. Ob eine aktive Benachrichtigung von Firmenkunden erfolgen soll, ist eine weitere kurzfristig zu klärende Frage.

Den technischen EPC Directory Service (EDS) für VoP wird SWIFT betreiben. Die Kosten werden über den EPC abgerechnet. Das VoP-Rulebook ist verpflichtend für alle SCT- und SCT-Inst-Teilnehmer des EPC. Ausgenommen werden können nur Institute, für die keine regulatorische Verpflichtung oder vergleichbare Gründe bestehen. Eine Ausnahme ist dem EPC bis Ende Januar 2025 per E-Mail an [vop@epc-cep.eu](mailto:vop@epc-cep.eu) anzuzeigen. Für alle übrigen Institute verbleiben weniger als zwölf Monate für die Implementierung von VoP.

### Verification of Payee kann Betrug nicht nachhaltig eindämmen!

Der IBAN-Namensabgleich soll Betrug verhindern, indem sich der Auftraggeber versichert, seine Zahlung auf das beabsichtigte Empfängerkonto zu tätigen. Stimmen die Angaben nicht oder teilweise überein, kann der Kunde entscheiden, ob er die Transaktion durchführen möchte. Wie das praktisch und – ohne den reibungslosen Massenzahlungsverkehr zu stören – funktionieren soll, ist fraglich. Allein in Deutschland wurden im Jahr 2023 mehr als 7 Milliarden Überweisungen getätigt.

Erfahrungen mit dem VoP liegen u. a. in den Niederlanden vor. Hier wurde VoP vor einigen Jahren etabliert, um gegen eine bestimmte Art von Betrug vorzugehen. Die Erfolge waren von kurzer Dauer. Heute sind die Niederlande nach der EBA/EZB-Statistik Europameister bei betrügerischen Überweisungen – auch in absoluten Zahlen. VoP wird daher nicht als nachhaltiges Instrument zur Betrugsbekämpfung angesehen. Damit ist VoP für neue Betrugszenarien nicht

zwingend geeignet und soll dennoch flächendeckend innerhalb der nächsten zehn Monate eingeführt werden. Ob die mit hohem Aufwand getätigten Investitionen betrügerische Transaktionen eingrenzen, bleibt fraglich. Klar ist hingegen, dass VoP die Kundenzufriedenheit bei Überweisungen beeinflusst.

 [EPC „Verification Of Payee Scheme Rulebook“](#)

 [EPC: EPC Recommendations for the Matching Processes under the VOP Scheme Rulebook](#)

## 4. SEPA-ECHTZEITÜBERWEISUNG: AUSWIRKUNGEN AUF INSTITUTE

Die SEPA-Echtzeitüberweisung werden absehbar Auswirkungen auf das Liquiditätsmanagement der Banken und Sparkassen haben. Damit die SEPA-Echtzeitüberweisungen auch für Institute unter Liquiditätsaspekten darstellbar wird, sind die Rahmenbedingungen für die Umsetzung der Verordnung zu verbessern. Die in der Deutschen Kreditwirtschaft zusammengeschlossenen kreditwirtschaftlichen Verbände haben folgende Forderungen an das Eurosystem sowie die Aufsichtsorgane gestellt, um die mit SEPA-Echtzeitüberweisung verbundenen Liquiditätsrisiken zu minimieren:

- TARGET muss in Richtung 24x7 zugänglich sein, um die Konten insbesondere in Bedarfsspitzen und bei Krisen verwalten zu können:
  - Die Liquidität zwischen den TARGET-Konten muss in Richtung 24x7 (bspw. mind. 22x7) übertragen werden können.
  - Zentralbankgeld muss zeitlich flexibler generiert werden können.
- Die Liquidität muss regelbasiert und automatisiert beispielsweise vom MCA auf das TIPS DCA übertragen werden können. Ein bereits länger vorliegender CR soll zügig umgesetzt werden.
- Die Liquidität auf den jeweiligen Konten (z. B. die für RT1 genutzt werden) muss automatisch über alle T2-Konten verzinst werden. Der Zinssatz für die Einlagenfazilität wird automatisch auf die Liquidität oberhalb der Mindestreserve angewendet. Dabei entfällt der Übertrag auf das Konto der Einlagenfazilität.

Darüber hinaus verpflichtet die Verordnung zur SEPA-Echtzeitüberweisung u. a. Institute dazu, auch eine papierhafte SEPA-Echtzeitüberweisung anzubieten. Daher wird nun zusätzlich auch die sog. Vordruckrichtlinie der DK angepasst.

## VÖB ZAHLUNGSVERKEHR

### 5. PSD3/PSR: NEUE VORSCHLÄGE ZULASTEN VON BANKEN

Die EU-Kommission hatte ihren Entwurf zur PSD3<sup>2)</sup> und der PSR<sup>3)</sup> bereits im letzten Jahr vorgelegt. Darin wurden u. a. neue Dienste gefordert:

- Lastschrift, Dauerauftrag und Sammler
- Die starke Kundenauthentifizierung (SKA) soll aufgeweicht und für Kontoinformationsdienste delegierbar werden: So sollen 2 Faktoren aus einer Kategorie für die SKA ausreichend sein.
- Zahlungsdienstleister müssen ein Dashboard für Kunden über ihre Einwilligungen bei Dritten vorhalten.

Seit den EU-Wahlen Mitte 2024 sind die weiteren Arbeiten ange laufen. Des Weiteren wurden neue Vorschläge vom ECON und dem EU-Rat eingebracht:

1. In die Definition der Autorisierung / Authentifikation sollen **subjektive Elemente** aufgenommen werden, d. h. Elemente, die die Absicht des Kunden berücksichtigen, eine Überweisung auszuführen. Subjektive Elemente sind objektiv nicht nachprüfbar. Ein subjektives Element kann die Absicht des Kunden sein, die Zahlung ausführen zu wollen – oder eben nicht. Im Streit- oder im Betrugsfall kann der Kunde immer behaupten, dass er die strittige Zahlung oder Kontobelastung gar nicht tätigen wollte.
2. Bei *Spoofing*, d. h. Angriffe, bei denen sich Betrüger z. B. als Bankmitarbeiter ausgeben, sollen Banken unmittelbar beim ersten Mal haften, sobald der Kunde den Betrug anzeigt.
3. Es ist weiterhin nicht möglich, dass **Entgelte** für die Dienste (bspw. zur Betrugsprävention) erhoben werden dürfen, um Schäden zu kompensieren.
4. Damit **Betrug effektiv bekämpft** werden kann, sind auch die **Telekommunikations- und Plattformanbieter einzubeziehen**. Dazu soll ein europäischer Round Table mit allen Stakeholdern einberufen werden. Parallel dazu wird sich die Deutsche Kreditwirtschaft mit den hier ansässigen Telekommunikations- und Plattformanbieter austauschen.

Nach Informationen der EU-Kommission sollen Banken ihren Kunden die SUA (Strong User Authentication) der eIDAS-Verordnung als Alternative zur SKA zur Autorisierung von Überweisungen ab Anfang 2027 anbieten müssen. Es ist nicht auszuschließen, dass damit auch eine Kontoneueröffnung ermöglicht werden muss.

Der weitere Zeitplan ist ungewiss. ECON und EU-Rat dürften sich im Trilog auf einen Kompromiss verständigen.

**Wird die „subjektive Theorie“ Gegenstand der Regelungen der PSD3 und PSR, wird sich das klassische Rechtsverständnis in Europa verändern – mit Folgen über die Kreditwirtschaft und die gesamte Finanzbranche hinaus.**

Was ist damit gemeint?

Nun, während es heute klare, objektive Regelungen im Zahlungsverkehr gibt, nach denen Kunden bestimmten (betrügerischen) Transaktionen widersprechen können, dürften künftig subjektive Behauptungen ausreichen: Man habe die Transaktionen gar nicht tätigen wollen, man habe nicht verstanden, dass es sich um eine Transaktion handele, dass das Konto belastet werden würde, der Betrag zu hoch sei usw. Der Phantasie dürften dabei kaum Grenzen gesetzt sein – so, wie eben der Einzelne bestimmte (Zahlungs-)situationen subjektiv wahrnimmt.

Dann wird reklamiert. Die Bank oder Sparkasse muss diesen Rückgabegrund gegen sich gelten lassen, die Rückabwicklung veranlassen und den Betrag erstatten. Die Aufwände hierfür muss sie selbst tragen. Was mit dem der Zahlungstransaktion zugrundeliegenden Grundgeschäft passiert, dürfte dann Sache des Kunden sein.

Wenn sich „subjektive Wahrnehmung“ künftig als Grund für das Bestreiten von weiteren Rechtsgeschäften (Kaufverträgen, Schenkungen, Grundstücksgeschäften usw.) gesetzlich etablieren sollte oder Kunden auf ihre „subjektiven Rechte“ bestehen, führt das zu Verwirrung und Chaos. Diese Verunsicherung kann sich auf weitere Bereiche erstrecken und Vertrauen reduzieren.

Doch ist nicht gerade Vertrauen in schwierigen Zeiten zwingend notwendig? Mit Vertrauen darf nicht gespielt werden – ebenso wenig wie mit Geld. Subjektive Wahrnehmung im Massenzahlungsverkehr auf gesetzlicher Grundlage gefährdet letztlich die Finanzstabilität in Europa.

**Wir** appellieren an die europäischen und an die nationalen Institutionen, an objektiven Regelungen in der PSD3/PSR festzuhalten. Es gilt, das Schlimmste zu verhindern!

2) PSD3: Dritte Zahlungsdiensterichtlinie

3) PSR neue Zahlungsdiensteverordnung (Payment Services Regulation)

## VÖB ZAHLUNGSVERKEHR

### 6. SEPA: WEITERE LÄNDER SCHLIESSEN SICH AN

Die EU-Kommission möchte weitere Länder außerhalb der Europäischen Union in den SEPA-Raum aufnehmen: Albanien, Bosnien Herzgowina, Georgien, Kosovo, Moldavien, Montenegro, Nord Mazedonien, Serbien sowie die Ukraine. Der EPC prüft die jeweiligen Beitrittsgesuche anhand der SEPA-Regularien auf der Grundlage der Comfort Letter der EU-Kommission. Als erstes weiteres SEPA-Land wird voraussichtlich Moldavien beitreten. Wir erwarten, dass dem Antrag stattgegeben wird.

Die Erweiterung des SEPA-Raumes erleichtert die Abwicklung des Zahlungsverkehrs mit den SEPA-Verfahren der beitretenden Länder. Gleichzeitig steigen mit zunehmender Teilnehmerzahl potentielle Risiken, neue Betrugsszenarien können auftreten. Wie sich die Aufnahme neuer Länder in den SEPA-Raum auf den Betrug auswirkt, bleibt abzuwarten.

### 7. BUNDESBANK: EINSTELLUNG DES TELEFAX

Die Bundesbank hat angekündigt, ihre Faxgeräte möglichst umgehend komplett abzuschaffen. Da das Fax z. B. immer noch im Interbankenband verpflichtend angegeben werden muss, ist es notwendig, eine Alternative zum Fax zu etablieren. Daher hatte die Bundesbank eine Sonderarbeitsgruppe zur Fax-Ablösung initiiert. Ziel ist es, das Fax als Übertragungsmedium abzuschaffen und ein adäquates Backup für das Fax zu finden.

Auf ihrer Webseite weist die Bundesbank bereits darauf hin, dass sie ab 31. Januar 2025 nicht mehr per Fax erreichbar ist. Dies gilt für die Kommunikation jenseits der im Zahlungsverkehr bislang per Fax verarbeiteten Daten.

### 8. EINSTELLUNG DES SCHECKVERFAHRENS IN 2027 GEPLANT

Klassische Schecks zur Verrechnung von Zahlungen werden immer weniger verwendet: In 2023 wurden rund 2,6 Millionen Scheckzahlungen in Deutschland durchgeführt; 20 Jahre zuvor waren es noch 131,8 Millionen (Quelle: Statista). In den kommenden Jahren wird ein weiterer Rückgang erwartet. Hierfür soll die notwendige Infrastruktur zeitnah zurückgebaut und das Scheck-clearing als auch die Verarbeitung von Schecks vollständig eingestellt werden. Geplant ist Ende des Jahres 2027.

Bestätigte Bankschecks werden bevorzugt bei Zwangsversteigerungen als Sicherheit hinterlegt. Damit wurden allein im ersten Halbjahr 2024 bei den zuständigen Amtsgerichten für knapp 7.000 Immobilien mit einem Verkehrswert von immerhin 2,2 Milliarden Euro aufgerufen. Diese Zahlen verdeutlichen – so die Ansicht der zuständigen Bundesministerien – die Bedeutung von Zwangsversteigerungen in Deutschland.

Gleichwohl halten die Deutsche Bundesbank als auch die Deutsche Kreditwirtschaft an einem Ausstieg aus dem Scheckverfahren Ende 2027 fest. Weitere Schritte werden eingeleitet, um die Bedenken auszuräumen. Wir gehen davon aus, dass im ersten Halbjahr 2025 über den Ausstieg entschieden wird.

Parallel, jedoch unabhängig von der beabsichtigten Einstellung des Scheckverfahrens, möchte die Bundesbank auch ihre eigenen Bundesbankschecks abschaffen.

### 9. EBA/EZB: BETRUGSSTATISTIK

Die EBA<sup>4)</sup> und die EZB haben die von den europäischen Zahlungsdienstleistern gem. PSD2<sup>5)</sup> zu meldenden Daten über Betrug (Q2/2022 bis Q1/2023) ausgewertet. Die Auswertung zeigt:

- Es werden Betrugszahlen zu Überweisungen, Lastschriften, Kartenzahlungen, Bargeldabhebungen und E-Geld-Transaktionen ausgewiesen. Eine Unterscheidung zwischen Echtzeit- und klassischer Überweisung erfolgt nicht. Dies kann daran liegen, dass die Betrugsfälle bei einer Echtzeitüberweisung deutlich höher als bei einer klassischen Überweisung sind.
- In 2022 belief sich der Betrug im Zahlungsverkehr auf 4,3 Mrd. Euro, im ersten Halbjahr 2023 auf 2,0 Mrd. Euro.
- Die höchsten Betrugsraten existieren bei Karten- und bei E-Geld-Zahlungen und sie sind um ein Vielfaches höher als bei Überweisungen.
- Missverständlich ist die Aussage im Management Summary: „... fraudulent credit transfers sent by PSPs ...”. - Banken versenden niemals betrügerische Überweisungen. Selbst in Verdachtsfällen, in denen die Bank den Kunden kontaktiert hat, dieser aber darauf bestand, die Überweisung zu senden, ist die Bank gesetzlich verpflichtet, diese Zahlung auszuführen.
- Die Manipulation des Zahlers ist Hauptursache von Betrug. Ebenso waren die meisten Fälle von Lastschriftbetrug auf nicht autorisierte Transaktionen zurückzuführen.

4) EBA: European Banking Authority

5) PSD2: Payment Services and Electronic Money Services Directive; Zahlungsdiensterichtlinie

## VÖB ZAHLUNGSVERKEHR

→ Der Betrag variiert stark nach Ländern. Die Niederlande führen die Betrugsstatistik in Europa an. Im direkten Vergleich ergibt sich u. a.

| Land | Überweisungen                             |                                  | Lastschriften                             |                                  |
|------|---|----------------------------------|---|----------------------------------|
|      | Wert betrügerischer Transaktionen in Euro | Anteil an gesamten Transaktionen | Wert betrügerischer Transaktionen in Euro | Anteil an gesamten Transaktionen |
| DE   | 147 Mio.                                  | 0,000 %                          | 3 Mio.                                    | 0,000 %                          |
| NL   | 162 Mio.                                  | 0,001 %                          | 60 Mio.                                   | 0,031 %                          |

Quelle: VÖB

Berücksichtigt man, dass die Niederlande den IBAN-Namensabgleich seit Jahren eingeführt haben, stellt sich die Frage nach der Wirksamkeit.

- Der Bericht unterstreicht die Wirksamkeit der SKA<sup>6)</sup> bei der Reduzierung von Betrug, insbesondere bei Kartenzahlungen.
- EBA und EZB planen jährlich aggregierte Betrugsdaten zu erheben. Künftige Berichte sollen detaillierte Erklärungen und Trends enthalten.

Bereits im 29. April 2024 hatte die EBA die Betrugsdaten für 2022 in ihrer „Draft EBA Opinion on new types of payment fraud and possible mitigants“ ausgewertet. Das Thema Betrug wird die Mitgliedstaaten der EU über die nächsten Jahrzehnte begleiten.

[EBA Fraud Bericht](#)

### 10. ERPB: MASSNAHMEN GEGEN STEIGENDEN BETRUG

Auch der Euro Retail Payments Board (ERPB) widmet sich dem Thema Betrug in Europa und mit welchen Maßnahmen Betrug begegnet werden könnte. Der Bericht der ERPB-Arbeitsgruppe geht darauf ein, dass Kriminelle psychologische Vorurteile und Taktiken für Identitäts- und Anlagebetrug verwenden. So werden öffentliche Institutionen und Behörden imitiert, das Vertrauen der Kunden wird ausgenutzt. Diese Gefahr und die damit einhergehende Komplexität und zeitliche Dauer von Betrug im Zahlungsverkehr wird sich in den kommenden Jahren erhöhen.

Demzufolge fordert der ERPB eine stärkere, sektorübergreifende und öffentlich-private Zusammenarbeit, um die derzeitigen und erwarteten Betrugsschäden für die Gesellschaft zu reduzieren.

Telekommunikations- und Plattformbetreiber sind in die gemeinsame Verantwortung zu nehmen und zur Betrugsprävention zu verpflichten. Zudem wird der EU-Kommission empfohlen, eine gemeinsame Plattform zur Betrugsprävention mit allen Stakeholdern zu etablieren.

[ERPB Arbeitsgruppen Präsentation](#)

[ERPB Fraud Bericht](#)

### 11. eIDAS 2.0: VERTRAUEN NOTWENDIG

Zu der am 20. Mai 2024 in Kraft getretenen Novelle der EU-Verordnung zur Schaffung eines europäischen Rahmens für eine digitale Identität (eIDAS 2.0) hatte die EU-Kommission im Sommer um erste Anmerkungen („Have your say“) zu Entwürfen von fünf Implementierungsrechtsakten (Implementing Acts) gebeten. Die ECSA's hatten dazu umfangreiche Empfehlungen u.a zum Architectural Reference Framework (ARF) und dessen Zusammenspiel mit den Implementierungsrechtsakten eingereicht. Mittlerweile sind modifizierte Versionen der eIDAS 2.0-Entwürfe der Durchführungsrechtsakte im Umlauf und auch verabschiedet worden. Seither läuft die Umsetzungsfrist, für die EUDI-Wallet bis Anfang 2027.

Mit eIDAS 2.0 soll der derzeit stark lokal fragmentierte Markt für digitale Dienste in der Europäischen Union vereinheitlicht werden. So sollen insbesondere natürliche Personen vollständig digital und vertrauensvoll mit Organisationen interagieren. Im Zentrum steht dabei die EUDI-Wallet, die natürlichen und juristischen Personen gleichermaßen zur Verfügung stehen soll. Im Entwicklungsprozess werden derzeit natürliche Personen allerdings deutlich priorisiert.

**Trotz der gründlichen Bemühungen bei der Erarbeitung des ARF gibt es grundsätzliche Bedenken hinsichtlich des Vertrauensniveaus.**

Ein großes Problem ist die unzureichende Bindung zwischen digitalen Daten und ihrem Subjekt. Diese kann möglicherweise Identitätsdiebstahl oder Betrug ermöglichen. Eine Lösung könnte in Form einer Identität mit Pass (Passport-Grade Identity) liegen, die schwer zu fälschende Sicherheitsmerkmale und Biometrie nutzt, um die Zuverlässigkeit zu gewährleisten. So soll es für Benutzer obligatorisch werden, während des Ausstellungsprozesses biometrische Daten zu den persönlichen Identifikationsdaten und diese den Zero Knowledge Proof-Systemen der EUDI-Wallet hinzuzufügen.

6) SKA: Strong Customer Authentication

## VÖB ZAHLUNGSVERKEHR

Die wachsenden Erwartungen an Komfort und hohe Sicherheit bei Online-Aktivitäten, wie z. B. der Ferneröffnung eines Bankkontos, unterstreichen die Bedeutung der Sicherheits- und Datenschutzaspekte von EUDI-Wallets, einschließlich der Zertifizierungsmechanismen. Der vorgesehene zweistufige Ansatz für die Zertifizierung wirft erhebliche Fragen auf, die auf ARF- und Implementierungsebene behandelt werden müssen.

Die Bedenken der ECSAs betreffen u.a. auch Registrierungs-, Zertifizierungs-, Synchronisierungs- und Abmeldeprozesse der vertrauenswürdigen Parteien im Rahmen der EUDI-Wallet. Diese Probleme erfordern weitere Klarstellungen und einheitliche Leitlinien, um einen reibungslosen und sicheren Betrieb für Unternehmen, einschließlich Banken, zu gewährleisten.

Diese drei Themen sind für das ARF und die Ausarbeitung der Durchführungsrechtsakte im Rahmen der EUDI-Wallet-Verordnung von entscheidender Bedeutung und bedingen einen kohärenten und harmonisierten Ansatz in der gesamten EU. Dieser liegt derzeit noch nicht vor.

### 12. KÜNSTLICHE INTELLIGENZ: KI-VERORDNUNG IN UMSETZUNG

Die neue KI-Verordnung der EU, d.h. die „Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz“ (kurz: AI Act/KI-VO), ist am 1. August 2024 in Kraft getreten. Die Verordnung sieht einen sektorübergreifenden, risikobasierten Ansatz mit vier Risikostufen für KI-Systeme vor. Der risikobasierte Ansatz soll verhindern, dass künstliche Intelligenz die Grundrechte von EU-Bürgern einschränkt oder verletzt.

Sechs Monate nach Inkrafttreten, am 2. Februar 2025, müssen verbotene KI-Anwendungen mit unannehmbar hohem Risiko abgeschaltet werden. Verboten sind KI-Anwendungen, wenn sie u.a. „... im Widerspruch zu den Werten der Union stehen, nämlich der Achtung der Menschenwürde, Freiheit, Gleichheit, Demokratie und Rechtsstaatlichkeit sowie der in der Charta verankerten Grundrechte, einschließlich des Rechts auf Nichtdiskriminierung, Datenschutz und Privatsphäre sowie der Rechte des Kindes ...“ stehen. Die Liste der in der KI-Verordnung verbotenen KI-Anwendungen soll regelmäßig überprüft werden.

#### Weitere Zeitplanung:

Zwölf Monate nach Inkrafttreten, am 2. August 2025, werden die Pflichten für KI mit allgemeinem Verwendungszweck (sog. GPAI/GenAI) wirksam und weitere zwölf Monate später, am 2. August 2026, gelten sämtliche Regelungen und Pflichten für KI-Hochrisikosysteme. Dazu gehören bspw. Kreditwürdigkeits- und Versicherungsprüfungen, da sie mit höherer Wahrscheinlichkeit Rechte von EU-Bürgern beeinträchtigen können.

Aktuell liegen nationale, branchenspezifische Spezifikationen noch nicht vor. Die Bundesnetzagentur wird in Deutschland sektorübergreifend als zentrale Behörde für die nationale Umsetzung und Überwachung der KI-VO zuständig sein. Zuständig für die sektorale finanzwirtschaftliche Umsetzung in Deutschland ist höchstwahrscheinlich die BaFin. Parallel dazu formuliert das Bundesamt für Sicherheit in der Informationstechnik (BSI) branchenspezifische Standards, u.a. im Rahmen von CEN/CENELEC. Diese sollen bis Mai 2025 veröffentlicht werden. Das neu geschaffene AI Office der EU-Kommission erarbeitet die konkreten Regeln und Pflichten zu KI mit allgemeinem Verwendungszweck und ist für deren Überwachung in Europa zuständig.

Der erste Regelungsschritt in Europa ist getan. Damit eine liberale Nutzung von KI zum Wohle Europas im globalen Wettbewerb mit einer nicht zu restriktiven, aber eindeutigen Auslegung des AI Acts gewährleistet ist, ist wichtig:

- Eine klare, eindeutige Definition von KI ist essenziell, damit die Erstellung eines KI-Inventars in den Instituten entsprechend der KI-VO überhaupt erst ermöglicht wird und die Auswirkungen von Risikomodellen begrenzt werden können.
- Die Detailregelungen für die Schulungen von Mitarbeitern im Umgang mit KI sowie die notwendige menschliche Überwachung sind bereitzustellen.
- Es braucht praxisgerechte, rechtssichere Leitplanken, die eine angemessene Umsetzung der KI-VO frühzeitig erleichtern.
- Längere Umsetzungsfristen sind nötig, damit die Compliance der KI-Governance angemessen gewährleistet werden kann.
- Die sehr umfangreichen Transparenz-, Monitoring- und Berichtspflichten für verschiedene Risikoklassen erschweren die Umsetzung und sind möglichst praxisgerecht auszugestalten.
- Es sind allgemeine Guidelines für die praktische Nutzung und ethische Umsetzung, insbesondere für GPAI, bereitzustellen. Gerade diese KI-Modelle sind sehr beliebt und verbreiten sich schnell, sodass den zu erwartenden Codes of Practice des AI

## VÖB ZAHLUNGSVERKEHR

Office eine besondere Bedeutung für die tägliche Praxis der Institute zukommt.

- Die vom BSI angekündigte Publikation zur Standardisierung sollte zügig bereitgestellt werden, damit der eigenverantwortliche Einsatz von KI unterstützt wird.
- Der pragmatische Ansatz der BaFin bei der Prüfung von KI-Modellen in der Banksteuerung ist zu begrüßen. KI wird hier als eine von vielen Technologien behandelt, die Banken testen und verantwortlich einsetzen.

### Die europäische KI-Verordnung setzt neue Maßstäbe in Europa

Der Rechtsrahmen in all seiner Komplexität hat weitreichende Auswirkungen auf Industrie und Wirtschaft, auf die Gesellschaft und damit – so die Zielsetzung – auf das gute Zusammenleben der Menschen in Europa. Er soll Rechtssicherheit aber auch Schutz für die Gesellschaft, für alle Bevölkerungsschichten und für jeden Einzelnen schaffen.

Werden die klassischen gesetzlichen Vorgaben und Ausführungsbestimmungen ausreichen, um diese weitreichenden Ziele zu erreichen? Bietet nicht die Schnelllebigkeit digitaler Technologien bis hin zu vorsätzlichem Verhalten nicht immer wieder auf's Neue, durch KI besonders befeuerte Angriffspunkte und Verletzbarkeiten für unser Zusammenleben?

Die größte Herausforderung bleibt: Das Vertrauen in KI-Technologien flächendeckend und breit aufzubauen. Vertrauen, für das man im elektronischen Zahlungsverkehr einige Jahrzehnte benötigt hat, um eine breite Bevölkerung zu erreichen. Das dürfte in einer zunehmend digitalisierten Welt für KI hoffentlich nicht ganz so lange dauern.

Es liegt demnach auch an uns selbst, täglich achtsam mit der digitalen und medialen Welt umzugehen – selbstverständlich auch jenseits der hier aus der Sicht der Banken und Sparkassen betrachteten neuen KI-Verordnung.

 [Zur KI-Verordnung](#)

### 13. KÜNSTLICHE INTELLIGENZ: MULTI-STAKEHOLDER-KONSULTATION BIS 11. DEZEMBER 2024

Das Europäische AI-Office als Teil der EU-Kommission hat am 13. Oktober 2024 eine breit angelegte Multi-Stakeholder-Konsultation veröffentlicht, bei der

1. zu Fragen der Definition eines KI-Systems einschl. deren Anwendung sowie
2. zu im Gesetz über die Künstliche Intelligenz festgelegten verbotenen KI-Praktiken

Stellung genommen werden kann. Zielgruppe der Konsultation sind verschiedene Stakeholder-Kategorien, einschließlich Anbieter und Nutzer von KI-Systemen wie Unternehmen (also auch Banken), Behörden und anderen Organisationen, akademische- und Forschungseinrichtungen, Gewerkschaften, zivilgesellschaftliche Organisationen, öffentliche Aufsichtsbehörden sowie die allgemeine Öffentlichkeit.

Die Teilnehmer werden ermutigt, Erklärungen und konkrete Beispiele als Teil ihrer Antworten beizufügen, um die praktische Anwendbarkeit der Leitlinien zu unterstützen.

Die Konsultation wurde am 13. November 2024 gestartet und endet am 11. Dezember 2024. Sie ist ausschließlich auf Englisch verfügbar.

 [Zur Konsultation](#)

### 14. giroAPI-SCHEME DER DK: NUTZUNG AB 2025

giroAPI ist eine Initiative der Deutschen Kreditwirtschaft, die Bank-Dienste für Dritte innerhalb eines sogenannten Schemes definiert. Auf die Dienste der Banken können Dritte über eine API-Schnittstelle zugreifen und ihren Kunden eigene Dienste anbieten.

giroAPI erweitert die verpflichtenden Dienste der Zahlungsdienstrichtlinie (PSD2). Banken können für das Nutzen der Dienste Entgelte erheben. Mit giroAPI wird ein neues digitales Ökosystem geschaffen, von dem sowohl Anbieter als auch Abnehmer profitieren.

Über die notwendigen einheitlichen funktionalen und technischen Schnittstellen und Anforderungen an den Betrieb dieses giroAPI-Schemes haben sich die kreditwirtschaftlichen Verbände verständigt. Der Start des giroAPI-Schemes ist für Anfang 2025 geplant. Dann wird jedes Mitgliedsinstitut eines Verbandes individuell dem giroAPI-Scheme beitreten können. Das Interesse bei den Dritten ist groß und wir erwarten eine rege Beteiligung an giroAPI.

## VÖB ZAHLUNGSVERKEHR

### 15. KARTENSICHERHEIT: VERBRAUCHER SENSIBILISIEREN

Auch im girocard-System werden die Aktivitäten ausgebaut, um Kunden praxisnah beim sorgfältigen Umgang mit ihren Credentials zu schützen. Auf [www.kartensicherheit.de](http://www.kartensicherheit.de) gibt die EURO Kartensysteme GmbH seit vielen Jahren nicht nur wertvolle Tipps im Umgang mit PIN und Karte sondern darüber hinaus. Konkrete Maßnahmen, die Kunden selbst zum Schutz ihrer Credentials vor Betrügern vornehmen können, werden auf der Webseite und in einer Vielzahl von Printmedien veröffentlicht. Dabei wird auf Aufklärung, Vernetzung und Kommunikation gesetzt. Damit unterstützt die EURO Kartensysteme die kartenausgebenden Banken und Sparkassen bei der Kundeninformation in der breiten Öffentlichkeit.



Die aktuelle Awareness-Kampagne „#Datendrang“ sensibilisiert für die Gefahren durch Social Engineering und klärt über verschiedene Betrugsformen auf. Die bereitgestellten Werbemittel unterstützen ein kritisches sowie sensibles Bewusstsein und bieten aktiv Hilfe an.

#### Aufklärung und Sensibilisierung zur Betrugsprävention sind eine gesamtgesellschaftliche Aufgabe!

Es ist doch gar nicht so schwierig. Sollte man meinen. Doch tatsächlich ist Social Engineering eine der wesentlichen Ursachen für Betrug. Kunden werden getäuscht und so zur Herausgabe persönliche Credentials verleitet. Manchmal sind die Tricks der Betrüger täuschend echt und schwer zu erkennen. – Doch Hand auf´s Herz, hier geht es um die Finanzen jedes Einzelnen. Da sollte besondere Vorsicht herrschen bzw. ein Grundverständnis und das Wissen, dass Banken und Sparkassen niemals zur Herausgabe von Credentials auffordern.

Vertrauen ist gut, Kontrolle ist besser! – Das gilt insbesondere beim Umgang mit Geld, im Online- oder mobile Banking sowie über weitere elektronische Kanäle bis hin zur Haustür. Auch wenn

öffentliche Institutionen oder Telekommunikationsanbieter als seriös angesehen werden – geht es um die eigenen Finanzen, sind ausschließlich Banken und Sparkassen bzw. die jeweiligen Anbieter zuständig.

Dies zu vermitteln, kann und darf nicht allein in den Händen der Institute liegen. Die geplanten Änderungen der Haftungsregelungen gem. PSD3/PSR veranlassen die Kunden umso mehr, sich noch weniger um ihre persönlichen finanziellen Mittel Gedanken zu machen.

**Wir** sprechen uns explizit und weiterhin für breite, öffentlichkeitswirksame Aktivitäten und Aufklärung aus. Diese sind durch alle Marktbeteiligten und gemeinsam mit Ministerien und Behörden sowie öffentlichen und privaten Initiativen konsequent und dauerhaft durchzuführen. Betrug wird erst dann eingedämmt werden können, wenn ALLE dazu beitragen.

 [Die Werbemittel der EURO Kartensysteme stehen zum Download bereit](#)

### 16. DORA TRITT IN KRAFT: HERAUSFORDERUNGEN UND OFFENE FRAGEN

Am 17. Januar 2025 endet die zweijährige Übergangsfrist – DORA (Digital Operational Resilience Act) wird in der EU vollumfänglich wirksam. Trotz der nahenden Umsetzung bleiben viele Unsicherheiten bestehen, die auf zwei zentrale Themenfelder zurückzuführen sind:

Der gesetzliche Rahmen ist sowohl auf EU- als auch auf nationaler Ebene noch nicht finalisiert.

#### Europäische Ebene

Im Oktober 2024 lehnte die EU-Kommission den Entwurf des Technischen Implementierungsstandards (ITS) zum Informationsregister erst ab und veröffentlichte am 29.11.2024 den angepassten Text. Der Vorschlag hätte es Finanzinstituten ermöglicht, den Legal Entity Identifier (LEI) oder den European Unique Identifier (EUID) zur Identifikation von IKT-Drittparteien zu nutzen. Die European Supervisory Authorities (ESAs – EBA, EIOPA und ESMA) kritisierten, dass dies zu unnötiger Komplexität führt und die Zielsetzung, die kritischsten Dienstleister unter den DORA-Überwachungsrahmen zu stellen, verzögern könnte.

In ihrer [Pressemittteilung](#) vom 15. November 2024 veröffentlichten die ESAs ihre Entscheidung, die regelt, welche Informationen von den

## VÖB ZAHLUNGSVERKEHR

zuständigen Behörden im Rahmen von DORA an die ESAs bis zum 30. April 2025 gemeldet werden müssen, um kritische IKT-Drittanbieter zu benennen.

Eine Übersicht der bereits verabschiedeten delegierten Rechtsakte bietet die [BaFin-Website](#).

### Nationale Ebene:

In Deutschland befinden sich das NIS2-Umsetzungsgesetz, das KRITIS-Dachgesetz und das Finanzmarktdigitalisierungsgesetz noch im Gesetzgebungsprozess. Da sie bislang nicht durch den Bundestag verabschiedet wurden, bleibt unklar, ob eine Entscheidung vor den anstehenden Neuwahlen erfolgt.

Finanzinstitute sehen sich bei der praktischen Umsetzung von DORA mit erheblichen Herausforderungen konfrontiert:

### Kritische oder wichtige Funktionen:

Die DORA-Verordnung definiert „kritische oder wichtige Funktionen“ auf Basis potenzieller Auswirkungen eines Ausfalls. Dies unterscheidet sich von der Wesentlichkeitsbestimmung bei Auslagerungen nach MaRisk. Die BaFin betont, dass eine umfassende Risikoanalyse erforderlich ist, auch wenn die delegierte Verordnung bewusst auf detaillierte Spezifikationen verzichtet hat, um Flexibilität zu wahren. Ein Industriestandard hat sich bislang nicht etabliert.

### Vertragsanpassungen:

Viele bestehende Verträge mit IKT-Dienstleistern erfüllen die neuen DORA-Vorgaben nicht und erfordern Anpassungen – eine Mammutaufgabe bis zum Stichtag im Januar 2025. Verzögerungen könnten Sanktionen nach sich ziehen. Standardvertragsklauseln, die laut Artikel 30 (4) von Behörden bereitgestellt werden sollen, fehlen bislang, was ineffiziente individuelle Vertragslösungen notwendig macht.

### Kontrolle von Dienstleistern:

Eine weitere Herausforderung liegt in der tatsächlichen Überwachung von IKT-Dienstleistern und deren Unterauftragnehmern. Reine Zertifizierungen reichen unter DORA nicht mehr aus. Branchenübergreifende Koordination – etwa über Plattformen, Audit-Pools oder Zertifizierungsmechanismen – könnte die Umsetzung effizienter gestalten. Einheitliche Modelle fehlen jedoch noch.

### Begriffsunsicherheiten:

Unklar bleibt auch, ob regulierte Finanzinstitute, die IT-Dienstleistungen für andere Finanzinstitute erbringen, als IKT-Dienstleister eingestuft werden könnten. Die Branche fordert daher Klarstellungen, dass regulierte Finanzdienstleistungen nicht unter den Begriff „IKT-Dienstleistungen“ fallen sollen.

Die praktische Umsetzung von DORA wird für viele Finanzinstitute auch im Jahr 2025 eine zentrale Priorität bleiben.

Mit zunehmender Anwendung und Prüfungen könnte sich die Transparenz erhöhen, sodass unterschiedliche Vorgehensweisen verglichen und harmonisiert werden können. Eine stärkere Klarheit und Konsistenz bei der Auslegung und Anwendung der Vorgaben wäre essenziell, um die Resilienz der Finanzbranche nachhaltig zu stärken.

## 17. KRITIS DACHGESETZ: STARKE INFRASTRUKTUREN SCHÜTZEN

Mit dem am 6. November 2024 im Bundeskabinett beschlossenen „Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen“ sollte die EU-Richtlinie über die Resilienz kritischer Einrichtungen aus dem Jahr 2022 in nationales Recht umgesetzt und erstmalig bundeseinheitliche rechtliche Regelungen für den Schutz kritischer Infrastrukturen, zu denen auch die Finanzbranche gehört, festgelegt werden.

Die für die Finanzbranche bereits geltenden Anforderungen werden durch das Gesetz weitestgehend berücksichtigt. So gibt es Ausnahmen der Anforderungen bspw. für das Risikomanagement und die Resilienz, die bereits DORA festgelegt sind. Es bleibt abzuwarten, ob bis zur Regierungsneubildung dieses Gesetz noch das parlamentarische Verfahren durchlaufen wird.

 [Zum Entwurf des KRITIS-Dachgesetz](#)

## VÖB ZAHLUNGSVERKEHR

### 18. VÖB-FACHTAGUNG: „DORA-READINESS IM PRAXIS-CHECK“ AM 12. DEZEMBER 2024

Die Implementierung der Anforderungen aus dem Digital Operations Resilience Act (DORA) stellt Institute vor erhebliche Herausforderungen bei der Implementierung. Daher lädt der VÖB gemeinsam mit der Academy of Finance der VÖB-Service GmbH zu einer virtuellen Fachtagung ein. Diese Veranstaltung wird praxisrelevante Fragestellungen vor dem Start von DORA beleuchten:

- die Bestimmung kritischer oder wichtiger Funktionen,
- Anpassungen von Verträgen,
- Meldepflichten und Informationsregister,
- Anforderungen an Verschlüsselung und Test,
- Threat Led Penetration Testing (TLPT).

Die Fachtagung findet am **Donnerstag, den 12. Dezember 2024, von 09:30 Uhr bis 14:30 Uhr**. **Anmeldungen** sind hier auch noch kurzfristig möglich:

 [VÖB-Service GmbH](#)

### 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](mailto:presse@voeb.de). Geben Sie einfach den Betreff „Anmeldung VÖB Zahlungsverkehr“ an.

Alle VÖB-Newsletter können Sie unter [www.voeb.de/publikationen](http://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](mailto:presse@voeb.de) | Internet: [www.voeb.de](http://www.voeb.de)  
Redaktion: Team Zahlungsverkehr und Informationstechnologie  
Redaktionsschluss: 28. November 2024  
Registernummer im Transparenz-Register der EU: 0767788931-41