Positionspapier

August 2025

Auf dem Weg zu einem widerstandsfähigen, vertrauenswürdigen und betrugssicheren digitalen Binnenmarkt

Eine integrierte Perspektive auf künstliche Intelligenz, Betrugsprävention und operationelle IT-Resilienz für den EU-„Digital Omnibus“

Warum auf diese drei Säulen fokussieren?

Das bevorstehende „Digital Omnibus“-Paket bietet eine seltene Gelegenheit, die dringendsten digitalen Politikfelder Europas zu einem kohärenten Ganzen zu verweben. Unter den vielen diskutierten Themen ragen Künstliche Intelligenz (KI), Betrugsprävention und operationelle IT-Resilienz aus drei Gründen heraus:

1. Wechselseitig verstärkende Risiken – Hochentwickelte KI-Modelle beschleunigen Innovationen, können aber auch Betrugsvektoren verstärken und die Auswirkungen von IT-Ausfällen vergrößern, wenn sie tief in kritische Infrastrukturen eingebettet sind.
2. Gemeinsame regulatorische Stellhebel – Alle drei Bereiche hängen von Datenverfügbarkeit, Aufsichtskooperation und angemessenen Schutzmaßnahmen ab. Ihre Verzahnung verhindert Doppelarbeit, schließt Lücken und schafft gleiche Wettbewerbsbedingungen für Unternehmen jeder Größe.
3. Strategische Autonomie und Wettbewerbsfähigkeit – Sichere KI-Einführung, wirksame Zusammenarbeit bei der Betrugsbekämpfung und robuste digitale Resilienz sind unverzichtbar, wenn Europa global wettbewerbsfähig bleiben und gleichzeitig die Souveränität über sein Finanzsystem wahren will.

Der folgende Text behandelt die drei Säulen daher als Teile eines zusammenhängenden Politikrahmens und nicht als isolierte Dossiers. Er enthält gezielte Empfehlungen, um das EU-Regelwerk zu vereinfachen, abzustimmen und zukunftssicher zu gestalten – passend für die Debatte zum „Digital Omnibus“.

1. Smarte KI-Regulierung – kohärent, verhältnismäßig, praktikabel

1.1 Klärung von Geltungsbereich und Definitionen

Eine prägnante, risikoorientierte Definition von KI ist entscheidend. Die derzeitige Formulierung des KI-Gesetzes lässt zu viel Raum für mehrdeutige Auslegungen transparenter, regelbasierter Modelle wie linearer oder logistischer Regression, die weder die Intransparenz- noch die Lernrisiken moderner KI-Systeme bergen. Der Ausschluss nicht-lernender oder vollständig transparenter statistischer Modelle würde den Aufsichtsfokus schärfen und Compliance-Ressourcen schonen.

Bundesverband Öffentlicher Banken Deutschlands, VÖB, e.V.
Lennéstraße 11, 10785 Berlin
www.voeb.de

Präsident: Eckhard Forst
Stellvertretender Präsident: Rainer Neske
Hauptgeschäftsführerin und geschäftsführendes Vorstandsmitglied: Iris Bethge-Krauß

1.2 Unterscheidung von Hochrisiko-Anwendungsfällen

Im Finanzwesen wird KI häufig für operative Aufgaben (Betrugserkennung, Anomalieerkennung, Musteranalyse) eingesetzt und nicht für Entscheidungen mit unmittelbarer Rechtswirkung auf Einzelpersonen. Der Hochrisikokatalog in Anhang III sollte daher den ausdrücklichen Ausschluss von Betrugspräventionstools beibehalten, während Bonitätsentscheidungen auf Basis echter KI-Modelle im Geltungsbereich bleiben.

1.3 Ein Aufseher, ein Regelwerk

Zersplitterte Aufsicht würde den Binnenmarkt untergraben. Die primäre Verantwortung sollte bestehenden Finanzaufsichtsbehörden (z. B. EZB/SSM, EBA-koordinierte nationale zuständige Behörden) zugewiesen werden, um Doppelstandards zu vermeiden und die KI-Aufsicht nahtlos mit der prudentiellen Aufsicht zu verzahnen.

1.4 Beseitigung von Überschneidungen mit sektoraler Regulierung

Bevor zusätzliche KI-spezifische Kontrollen auferlegt werden, muss eine Überschneidungs- und Lückenanalyse gegenüber CRR/CRD, DORA, PSD 2, IPR, AMLR und bestehenden EBA-Leitlinien erfolgen. Gleichwertige Schutzmaßnahmen sollten standardmäßig als konform gelten.

1.5 Integration von Berichtswegen und Tools

Anstatt separate Kanäle aufzubauen, können Vorfallmeldungen und Compliance-Bestätigungen bestehende Portale wie die Europäische einheitliche Aufsichtsberichterstattungsplattform (MVP) nutzen. Ein modulares Self-Assessment-Tool, das maßgeschneiderte Compliance-Leitlinien gemäß der vierstufigen Risikoklassifizierung des KI-Gesetzes ausgibt, würde die Hürden für KMU erheblich senken.

1.6 Angleichung an Datenschutzrecht

Gemeinsame EBA-EDPB-Leitlinien sollten Vorgaben zu Bias-Minderung, Datenminimierung und Genauigkeit harmonisieren sowie die Grundrechtsfolgenabschätzung des KI-Gesetzes auf die Datenschutz-Folgenabschätzung gemäß DSGVO abbilden. Der Rechtsstatus pseudonymisierter Daten für KI-Trainingszwecke muss dringend geklärt werden.

1.7 Realistische Zeitpläne respektieren

Die Politik hat den Zeitbedarf für Standardisierung unterschätzt. Das gesamte Rahmenwerk verzögert sich, und die Industrie kann nicht rechtzeitig planen. Verbindliche Standards über CEN/CENELEC sind bereits ein Jahr im Verzug; Aufsichtsleitlinien zu General Purpose AI (GPAI) liegen noch im Entwurf vor. Eine gestaffelte Umsetzung oder die ausdrückliche Nutzung von Übergangsinstrumenten (z. B. GPAI-Verhaltenskodex) bis zur Reife formaler Standards würde Rechtssicherheit wahren, ohne Schutzmaßnahmen zu verwässern.

2. Betrugsbekämpfung durch Kooperation entlang der gesamten Kette

2.1 Die sich wandelnden Betrugsbedrohungen

Betrug gegenüber Kunden und Unternehmen wird zunehmend professionell. Wir haben es mit einer Betrugsindustrie zu tun, die organisiert ist und flexibel auf Gegenmaßnahmen reagiert. Maßnahmen wie Verification of Payee sind für diese Industrie zu starr und lassen sich leicht mit simplen Taktiken umgehen. Wir brauchen daher wirksame Betrugsprävention auf Basis einer Zusammenarbeit zwischen verschiedenen Marktakteuren und Behörden..

2.2 Bestandsaufnahme des heutigen Betrugs

Heutiger Betrug basiert oft auf der Manipulation von Kunden oder Unternehmensmitarbeitern, die zu betrügerischen Zahlungen verleitet werden (Social Engineering). Der Manipulationsprozess beginnt typischerweise mit einer E-Mail, einem Brief, einer SMS, WhatsApp-Nachricht oder einem Anruf. Die Zahlung ist der letzte Schritt in einem möglicherweise wochen- oder monatelangen Prozess. Wer sich nur auf Banken – das letzte Glied in der Kette – konzentriert, verpasst wertvolle Informationen aus den frühen Betrugsphasen. Deshalb müssen auch E-Mail-Provider, Postdienste, soziale Medien und Telekommunikationsunternehmen eingebunden werden.

2.3 Silos aufbrechen

Da die Betrugswege mehrere Kommunikationsschichten durchlaufen, ist es ein Fehler, ausschließlich Banken als Endpunkt anzugehen. Ein wirksames Modell muss zusammenbringen:

- → Strafverfolgungsbehörden – Bundes- und Landeskriminalämter (BKA/LKA)
- → Kommunikations- und Plattformanbieter – E-Mail-Provider, Postdienste, Telekommunikationsunternehmen, soziale Netzwerke
- → Banken und Zahlungsdienstleister

2.4 Was blockiert heute die Zusammenarbeit?

Derzeit gibt es keine Möglichkeit zum Datenaustausch zwischen Telekommunikationsunternehmen, Postdienstleistern, Plattformbetreibern und Banken. Die Verantwortung für den Austausch betrugsrelevanter Daten ist fragmentiert. Der Digital Omnibus bietet die Chance, diese sektorübergreifende Zusammenarbeit zu ermöglichen. Es gibt zwar zahlreiche Gremien, aber keine sektorübergreifende Rechtsgrundlage für den Echtzeitaustausch kontextbezogener Daten, die für die vollständige Rückverfolgung betrügerischer Kampagnen notwendig sind.

2.5 Digital Omnibus als Chance für wirksame Betrugsprävention und Strafverfolgung!

Der Digital Omnibus ist Europas beste Gelegenheit, sektorübergreifende Zusammenarbeit gegen Betrug zu ermöglichen. Er sollte daher einen Rahmen schaffen, der verhältnismäßigen, zweckgebundenen Datenaustausch zur Betrugsprävention erlaubt.

Gestaltungsprinzipien:

- → Gezielte DSGVO-Ausnahme für betrugsrelevante Daten
  Eine klare Ausnahmegrundlage, ergänzt durch Zugriffskontrollen und Prüfprotokolle. Aufbewahrungsfristen sowie Bedingungen für Weitergabe und Löschung müssen rechtssicher definiert sein.
- → Verpflichtender Informationsaustausch über Betrug und Gegenmaßnahmen
  Regelmäßige Treffen, bei denen Strafverfolgungsbehörden, Online-Plattformen, Telekommunika-

tions- und Postdienste sowie Banken gemeinsam neue Betrugsarten analysieren und geeignete Maßnahmen beschließen.

→ Safe-Harbour-Schutz
Schutz der Teilnehmer vor zivil- oder aufsichtsrechtlicher Haftung, wenn sie in gutem Glauben auf geteilte Warnmeldungen reagieren.

Ohne diese Regelungen werden weiterhin Milliarden durch Betrug in der EU verloren gehen, und Steuerzahler werden geschädigt. Betrug untergräbt das Vertrauen in die digitale Agenda und belastet Bürger sowie Wirtschaft. Wenn Europa echte digitale Souveränität und Wettbewerbsfähigkeit will, muss nahtloser Datenaustausch ein Eckpfeiler seiner Betrugsabwehrstrategie werden.

3. DORA zweckmäßig machen – proportionale Resilienz

3.1 Lex specialis und Vereinfachung

DORA steht kurz davor, die Lex specialis für Cyber-Resilienz im Finanzsektor zu werden. Um Überschneidungen zu vermeiden, sollten Finanzinstitute ausdrücklich von der horizontalen Cyber Resilience Act ausgenommen werden, wenn DORA gilt.

3.2 Abgestufte Anforderungen

DORAs One-Size-fits-all-Ansatz birgt die Gefahr von „Gold Plating“ durch abweichende nationale Auslegungen. Ein gestuftes Rahmenwerk, z.B. angelehnt an CRR-Segmente (G-SIBs, O-SII, nicht-systemische Institute, Berücksichtigung der besonderen Rolle der Förderbanken), würde Pflichten wie Dokumentationstiefe, Testfrequenz und Vorfallschwellen an die tatsächliche Wirkung auf den Finanzmarkt anpassen. Förderbanken mit öffentlichem Auftrag und moderatem Risikoprofil könnten von reduzierten Meldefrequenzen profitieren. Unabhängig davon ist und bleibt der gelebte Grundsatz der Proportionalität und eines risikobasierten Ansatzes elementar.

3.3 Intelligentere Vorfallmeldung

Unkritische Ausfälle und geringe Kundenauswirkungen überlasten Aufsichtsressourcen. Eine Anhebung der Kundenschwellenwerte (z. B. 200 000 oder 5 % der Basis) und eine Ausweitung der meldepflichtigen Ausfallzeit für unkritische Systeme von einer auf vier Stunden würde den Fokus auf wesentliche Ereignisse richten.

3.4 Effizientere Drittparteien-Aufsicht

Continuous bespoke audits of hyperscale cloud or SaaS providers are unrealistic for smaller banks. DORA should formally recognise EU wide certifications (e.g. the forthcoming EUCS for cloud) and joint audit models. A single annual outsourcing overview centred on SLA compliance could replace disparate, overlapping questionnaires.

3.5 Risikobasiertes Testen

Threat-Led Penetration Testing (TLPT) ist ressourcenintensiv und sollte auf systemische oder hoch exponierte Institute beschränkt sein. Niedrigrisikoinstitute könnten auf Red-Team-Übungen, Planspiele oder sektorweite TLPT-Teilnahmen setzen, mit einem zweijährigen bis dreijährigen Testzyklus für unkritische Systeme.

Fazit – Ein einheitlicher Fahrplan für den Digital Omnibus

Die Behandlung von KI-Governance, Betrugsprävention und IT-Resilienz als getrennte Silos würde Bürokratie vervielfachen, Lücken offenlassen und Innovation verlangsamen. Ein vereinfachtes, verhältnismäßiges und interoperables Regelwerk über diese drei Säulen hinweg wird:

- → Vertrauen stärken – Bürger gewinnen Sicherheit, dass KI-Innovationen sicher sind, Betrugsrisiken eingedämmt werden und essenzielle Dienste verfügbar bleiben.
- → Kosten senken – Unternehmen vermeiden doppelte Prüfungen, überlappende Berichte und inkonsistente Aufsichtsanforderungen.
- → Souveränität stärken – Europa schafft sich einen Wettbewerbsvorteil durch sichere, verantwortungsvolle digitale Infrastruktur statt durch regulatorische Zersplitterung.

Die obigen Empfehlungen weisen einen pragmatischen Weg: Definitionen klären, zentrale Aufsicht benennen, gezielten Datenaustausch zur Betrugsbekämpfung ermöglichen und DORA-Pflichten risikoadäquat kalibrieren. Ihre Verankerung im Digital Omnibus wird politische Ambitionen in operative Kohärenz umsetzen – und damit das Fundament für einen widerstandsfähigen, innovativen und betrugssicheren europäischen Finanzsektor legen.

Der Bundesverband Öffentlicher Banken Deutschlands, VÖB, ist ein Spitzenverband der deutschen Kreditwirtschaft. Er vertritt die Interessen von 64 Mitgliedern, darunter die Landesbanken sowie die Förderbanken des Bundes und der Länder. Die Mitgliedsinstitute des VÖB haben eine Bilanzsumme von rund 3.200 Milliarden Euro und bilden damit etwa ein Viertel des deutschen Bankenmarktes ab. Die öffentlichen Banken nehmen ihre Verantwortung für Mittelstand, Unternehmen, die öffentliche Hand und Privatkunden wahr und sind in allen Teilen Deutschlands fest in ihren Heimatregionen verwurzelt. Mit 57 Prozent sind die ordentlichen VÖB-Mitgliedsbanken Marktführer bei der Kommunalfinanzierung und stellen zudem rund 22 Prozent aller Unternehmenskredite in Deutschland zur Verfügung. Die Förderbanken im VÖB haben im Jahr 2024 Förderdarlehen in Höhe von knapp 60 Milliarden Euro bereitgestellt. Als einziger kreditwirtschaftlicher Verband übt der VÖB die Funktion eines Arbeitgeberverbandes für seine Mitgliedsinstitute aus. Die tarifrechtlichen Aufgaben, insbesondere der Abschluss von Tarifverträgen, werden von der Tarifgemeinschaft Öffentlicher Banken wahrgenommen. Ihr gehören rund 65.000 Beschäftigte der VÖB-Mitgliedsinstitute an.

Weitere Informationen unter www.voeb.de