

# „PSD2 – Wohin geht es? Evolution statt Revolution?“

**Lukas Korella, Bundesbank**

**Florian Preis, BaFin**

**Dr. Felix Strassmair-Reinshagen, BaFin**

# Inhalt

## 1) Woher kommen wir?

- PSD2
- Review-Prozess

## 2) Aktueller Stand: PSD3-E und PSR-E

- Vorschläge der KOM im Detail
- Erste Einordnungen zu ausgewählten Regelungsvorhaben

## 3) Wie geht es weiter?

- Ausblick auf den weiteren Gesetzgebungsprozess

# PSD2 als Meilenstein für Open Banking

Zweite Zahlungsdiensterichtlinie (Payment Services Directive 2 – PSD2) mit u.a.

- Verpflichtung zu starker Kundenauthentifizierung (**SKA**)
- Erfassung der bisher nicht regulierten Dienstleistungen **Kontoinformationsdienst (KID)** und **Zahlungsauslösedienst (ZAD)**: einerseits Einführung einer Erlaubnis- bzw. Registrierungspflicht, andererseits ausdrückliches Recht dieser neuen Zahlungsdienstleister auf den Zugang zu Zahlungskonten

Im Rahmen der Implementierung

- Hohe Zahl an neuen, beaufsichtigten Zahlungsdienstleistern
- Umstellung auf SKA bei Kreditkarten mit deutlicher Verzögerung
- Viele Auslegungsfragen, gerade in Bezug auf die Schnittstellen für Kontoinformations- und Zahlungsauslösedienstleister

# PSD2-Review

- **Review-Klausel** in der PSD2; auch Retail Payment Strategy der KOM kündigte "*comprehensive review of the application and impact of PSD2*" an
  - Review-Prozess **2022** gestartet, Bestandteile v.a.: Public consultation, Targeted consultation, EBA Call for Advice, Impact Assessment-Studie durch Beratungsunternehmen\*
  - Fokus des Reviews:
    - Evolution des Zahlungsverkehrsmarktes (neue Akteure und Produkte)
    - Sind Anwendungsbereich, Definitionen and Aufsichtsrahmen weiterhin angemessen?
    - Lehren aus Implementierung des Zugangs zu Zahlungskonten bzgl. Verbesserung Open Banking?
    - Verbraucherschutz, z.B. Transparenz- und Haftungsanforderungen sowie Betrugsprävention
- 28. Juni 2023: Veröffentlichung der Legislativvorschläge der KOM

\* Vgl. Bosch Chen, I., et al (2023): *A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*, FISMA/2021/OP/0002. European Commission,, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, VVA, CEPS.

# Überblick: Schwerpunkte des KOM-Vorschlags

- Neuordnung und Anpassung des regulatorischen Rahmens und des Aufsichtsregimes
- Erhöhung des Wettbewerbs bei elektronischen Zahlungen („leveling the playing field“)
- Weitere Förderung der Funktionsfähigkeit von Open Banking / Access-to-Accounts
- Anpassungen SKA und weitere Betrugsbekämpfungsmaßnahmen
- Stärkung des Verbraucherschutzes, Anpassungen im Haftungsregime
- Stärkung der Harmonisierung und Durchsetzbarkeit

## **Hauptziel:**

“...seeks to ensure the EU's financial sector is fit for purpose and capable of adapting to the ongoing digital transformation, and the risks and opportunities it presents – in particular for consumers.”

# Neuordnung des regulatorischen Rahmens

## Aufteilung in Verordnung und Richtlinie

- bisherige Richtlinie PSD2 wird in zwei nebeneinanderstehende Regelungen aufgespalten:
  - 1) angepasste **Richtlinie (Payment Services Directive, PSD3-E)**, vor allem zur Aufsicht speziell über Zahlungsinstitute
  - 2) neue **Verordnung (Payment Services Regulation, PSR-E)** mit aufsichts- und zivilrechtlichen Vorgaben für alle Zahlungsdienstleister
- Motiv für Wechsel zum Instrument der Verordnung: laut KOM vor allem eine uneinheitliche nationale Implementierung der PSD2

## Zusammenführung E-Geld-Richtlinie und Zahlungsdiensterichtlinie

- E-Geld-Richtlinie in PSD3-E überführt
- Zahlungsdienste und E-Geld Geschäft stehen „nebeneinander“

# Anpassungen im Aufsichtsrecht (PSD3-E)

- **Ausnahme** von der Erlaubnispflicht **für cash-withdrawal services** (Art. 37 PSD3-E)
  - Bargeldabhebungen bis 50 Euro auch ohne Erwerb von Waren oder Dienstleistungen
- Neue **Registrierungspflicht für Geldautomatenbetreiber**, die nicht gleichzeitig Zahlungskonten führen (Art. 38 PSD3-E)
- **Neuordnung der Zahlungsdienst-Tatbestände** und des E-Geld-Geschäfts (vgl. Anhang I und II zur PSD3-E)

## Hauptziel der KOM:

Zugang zu Bargeld soll erleichtert werden.

## Hinweis:

Artikel 38 PSD3-E sieht dafür ein analoges Verfahren vor, wie für die Registrierung als Kontoinformationsdienstleister nach § 34 ZAG.

# Anpassungen im Erlaubnisverfahren (Art. 3 PSD3-E)

- **Anpassung der Erlaubnisvoraussetzungen** bzgl. Informations- und Kommunikationstechnologie an Verordnung (EU) 2022/2554 (**DORA-VO**), insb. Art. 6, 7 DORA-VO (governance, risk management), Kapitel III DORA-VO (incident handling and reporting), Art. 11 Abs. 6 DORA-VO (BCM und response and recovery plans)
- **Einreichung eines Abwicklungsplans**, der eine geordnete Abwicklung im Rahmen der nationalen Gesetze ermöglicht (Art. 3 Abs. 3 lit. s PSD3-E)
- **Substitution** der **Berufshaftpflichtversicherung** durch 50.000 Euro **Anfangskapital** für ZAD/KID im Erlaubnis-/Registrierungsverfahren (nach Erlaubnis muss das Anfangskapital ohne schuldhaftes Zögern durch Versicherung ersetzt werden)
- **Inflationsbedingte Anpassung des Anfangskapitals** (Art. 5 PSD3-E)
  - Finanztransfergeschäft: 25.000 Euro
  - andere Zahlungsdienste: 150.000 Euro
  - E-Geld-Geschäft: 400.000 Euro

# Anpassungen in der laufenden Aufsicht (PSD3-E)

- **Absicherung der Kundengelder I:** Sicherungskonten bei Zentralbanken sollen ermöglicht werden (soll *de-risking* von KI entgegenwirken) (Art. 9 Abs. 1 PSD3-E)
- **Absicherung der Kundengelder II:** Recht auf Zugang zu Zahlungskonten bei Kreditinstituten soll für Zahlungsinstitute gestärkt werden (dazu später mehr)
- **Absicherung der Kundengelder III:** Konzentrationsrisiken soll entgegengewirkt werden; Absicherung der Kundengelder bei nur einer Bank soll vermieden werden; nach Möglichkeit soll mehr als eine Methode zur Absicherung verwendet werden (Art. 9 Abs. 2 PSD3-E)
- **Eigenmittelanforderungen:** Methode B wird Standardmethode (Art. 7 Abs. 2 PSD3-E)
- **Rezertifizierung** bestehender Erlaubnisse ggfs. notwendig (Art. 44, 45 PSD3-E; analog Einführung PSD2)

# Level Playing Field Banken & andere Zahlungsdienstleister

## **Bereitstellung von Zahlungskonten durch Kreditinstitute an Zahlungsinstitute (Art. 32 PSR-E)**

- Kreditinstitut darf Eröffnung Zahlungskonto für Zahlungsinstitut nur unter bestimmten, engen Voraussetzungen (z. B. Verdacht auf Geldwäsche o. ä. – vgl. Liste in Art. 32 Abs. 1 PSR-E) verweigern (ebenso bei Kündigung seitens der Bank)
- Ausdehnung der Regelung auf Antragsteller, Agenten und E-Geld-Agenten
- Regelung von Folgepflichten für Kreditinstitute: Ablehnung oder Kündigung muss detailliert begründet werden, u.a. unter Berücksichtigung spezifischer Risiken (Art. 32 Abs. 3 PSR-E), Beschwerdemöglichkeit für Zahlungsinstitute (Art. 32 Abs. 4 PSR-E), Standardmeldeweg (Art. 32 Abs. 5 PSR-E)

## Publikumsfrage

Die geplanten Änderungen zur Absicherung der Kundengelder werden die *de-risking* Problematik insgesamt:

- a) abmildern
- b) nicht beeinflussen
- c) verschlechtern (bspw. wegen Vorkehrungen zu Konzentrationsrisiken)

# Level Playing Field Banken & andere Zahlungsdienstleister

## Zugang zu Zahlungssystemen (Art. 31 PSR-E, Art. 46 PSD3-E)

- Änderung der Richtlinie 98/26/EG (Settlement Finality Directive – SFD); Einbezug von Zahlungsinstituten in den Institutsbegriff der SFD (Art. 46 PSD3-E)
- ermöglicht Zahlungsinstituten Teilnahme an Zahlungssystemen
- Zugang zu Zahlungssystemen: Systembetreiber sollen *non-discriminatory, transparent and proportionate rules* hierfür haben (Art. 31 Abs. 1 PSR-E)
- Systembetreiber darf Zugang nur ablehnen, wenn transparentes *risk assessment* ergibt, dass Stabilität des Systems gefährdet wäre (Art. 31 Abs. 1-3 PSR-E)

# Open Banking / Access-to-Account

## Novellierte API-Anforderungen

- Verpflichtung für Banken, eine API („*dedicated interface*“) bereitzustellen, dafür keine Verpflichtung mehr, ein *fallback interface* bereitzustellen (Art. 35 Abs. 2 PSR-E)
- Möglichkeit zur Befreiung von der API-Pflicht durch die Aufsicht (Art. 39 PSR-E)
- ZAD/KID dürfen bei Problemen mit der API (*failure or unavailability*) zur Wahrung ihrer *business continuity* mit Genehmigung ihrer Aufsicht über die Kundenschnittstelle zugreifen (Art. 38 Abs. 3-7 PSR-E)
- ZAD/KID muss sich immer identifizieren (vgl. u.a. Art. 38 Abs. 7 S. 2 PSR-E) – *fallback*-Verpflichtung durch die Hintertür?
- Verbot der Verwendung des *redirection*-Ansatzes als einzige Authentisierungsform (Art. 44 Abs. 1 lit. k PSR-E)
- Keine Begrenzung der Häufigkeit von KID-Zugriffen ohne Kundenaktivität (Art. 41 Abs. 2 PSR-E)

# Open Banking / Access-to-Account

## Mehr Möglichkeiten für ZAD

- Liste von zu unterstützenden Geschäftsfällen (Art. 36 Abs. 4 PSR-E), neu insbesondere die Lastschrift

## Dashboard für Kunden (Art. 43 PSR-E)

- Banken müssen Kunden *Dashboard* zum Überblick und Steuerung ihrer Kontozugriffsberechtigungen bereitstellen

Art. 36 (4) PSR-E: ASPSPs shall ensure that the dedicated interface allows PISP, at a minimum, to:

- (a) place and revoke a standing payment order or a direct debit;
- (b) initiate a single payment;
- (c) initiate and revoke a future dated payment;
- (d) initiate payments to multiple beneficiaries

[...]

## Übergang Authentifizierungspflicht auf KID (Art. 86 Abs. 3 und 4 PSR-E)

- Bei erstem Kontozugriff durch KID liegt die SKA-Pflicht beim kontoführenden PSP, danach Übergang Pflicht zu KID für eigene SKAs (für max. 180 Tage)

# SKA

## Klarstellungen zu SKA bei verschiedenen Zahlungsmethoden (Art. 85 PSR-E)

- SKA erforderlich für ein über Fernzugang erteiltes Lastschriftmandat, ebenso MIT-Mandat, wenn dabei der Zahlungsdienstleister des Zahlers eingebunden ist
- SKA nicht erforderlich für die eigentliche Lastschriftzahlung bzw. MIT (sofern keine weitere Interaktion mit dem Zahler erforderlich ist)
- Ebenso papierhafte oder telefonische Zahlungsaufträge, aber PSP mit Pflicht zu geeigneter (anderer) Authentifizierung

Für von Seiten Zahlungsempfänger initiierte Zahlungen acht Wochen unbedingtes Rückerstattungsrecht – auch bei MIT (Art. 61-63 PSR-E)

## Regulatory Technical Standards (Art. 89 PSR-E)

- EBA soll neue Regulatory Technical Standards entwickeln, u. a. zu Ausnahmen

# SKA

## SKA mit zwei Elementen der gleichen Kategorie?

- Bisher: SKA muss zwei (oder mehr) Authentifizierungselemente aus mindestens zwei der drei Kategorien Wissen, Besitz und Inhärenz enthalten.
- Vorschlag: Elemente müssen **nicht** aus verschiedenen Kategorien stammen, solange sie unabhängig voneinander sind.

Art. 85 (12) PSR-E: *The two or more elements ... on which SCA shall be based do not necessarily need to belong to different categories, as long as their independence is fully preserved.*

## Publikumsfrage

Die Kommission schlägt vor, dass die beiden Elemente einer SKA zukünftig aus ein und derselben Kategorie kommen können:

- a) befürworte ich
- b) lehne ich ab
- c) bin unentschieden

# SKA

## Barrierefreiheit (Art. 88 PSR-E)

- PSPs müssen mehrere SKA-Methoden anbieten, alle Kunden müssen in der Lage sein SKA durchzuführen
- Mindestens eine Methode auch für Personen ohne Zugang zu *digital channels*
- Besitz eines Smartphones darf keine Voraussetzung sein

# Weitere Betrugsbekämpfung

## **IBAN-Namen-Check (Art. 50 PSR-E)**

- Abgleich zwischen *unique identifier* (IBAN) und Name Überweisungsempfänger
- Vorgelagerte Prüfung bei Zahlungsauftrag, bei Abweichung Info an Kunden über den Grad der Abweichungen, Kunde kann Zahlung trotzdem initiieren
- IBAN-Namen-Check für Instant Payments voraussichtlich über IP-Verordnung eingeführt, PSR-E: Geltung für alle Überweisungen (alle EU-Währungen) (vgl. Art. 50 Abs. 8 PSR-E)

# Weitere Betrugsbekämpfung

## **Fraud data sharing (Art. 83 PSR-E)**

- Kommunikation von möglichen Betrugsfällen zwischen Zahlungsdienstleistern (*information sharing agreements*)
- Dedizierte, multilaterale Plattformen werden angeregt (*dedicated IT platforms*)

## **Informationspflichten zu Betrugsrisiken und Trends (Art. 84 PSR-E)**

- Zahlungsdienstleister müssen Kunden z. B. über neue Betrugsformen informieren und Mitarbeiter schulen (mind. jährlich)

# Anpassungen im Haftungsregime, u.a.

## **Verbraucherfreundlichere Erstattungsregeln für unautorisierte Zahlungen (Art. 56 PSR-E)**

- Im Fall von unautorisierten Zahlungen kann Erstattung durch Zahlungsdienstleister nur noch verweigert werden, wenn Zahler betrügerisch gehandelt hat (bisher auch bei grob fahrlässigem Handeln)
- Verkürzung Prüfungs- und Bearbeitungszeit bei begründetem Betrugsverdacht gegenüber Zahler auf 10 Tage (Art. 56 Abs. 2 PSR-E)

## **Neue Betrugsform: Impersonation fraud (Art. 59 PSR-E)**

- Betrüger gibt sich als Mitarbeiter eines Zahlungsdienstleisters aus (*Impersonation*) und manipuliert Verbraucher, sodass dieser autorisierte Zahlung initiiert
- Haftung des Zahlungsdienstleisters und Anspruch auf Erstattung, wenn Verbraucher Vorfall unverzüglich bei Polizei anzeigt und Zahlungsdienstleister informiert

# Weitere Vorschläge

## **Informationspflicht bei Zahlungen an Drittstaaten (Art. 20 PSR-E)**

- Information des Kunden durch PSP u. a. zu geschätzter Ausführungsfrist für Überweisungen außerhalb EU, geschätzten Währungsumrechnungsentgelten bei Abhebung/Zahlung außerhalb EU

## **Verbesserte Informationen z.B. auf Kontoauszügen (Art. 16, 25 PSR-E)**

- PSP soll Kunde auch *commercial trade name* des Zahlungsempfängers z. B. im Kontoauszug bereitstellen

## Publikumsfrage

Erste Einschätzung: Die Vorschläge der EU-Kommission:

- a) adressieren die wesentlichen Schwächen der PSD2
- b) gehen im wesentlichen an der Sache vorbei
- c) finde ich teilweise gut und teilweise weniger gut

# Wie geht es weiter?

- Ordentliches Gesetzgebungsverfahren
- Endgültige Fassungen wohl nicht vor 2025, Parlamentswahl im Mai 2024 könnte für Verzögerung sorgen
- PSD3 wäre in nationales Recht umzusetzen, PSR würde nach Übergangsfrist (vorgeschlagen 18 Monate) unmittelbar anwendbar sein
- Vergleich: Erster Vorschlag für PSD2 in 2013, Inkrafttreten in 2016, Umsetzung in nationales Recht bis Januar 2018 (Geltung zum Teil erst ab 2019)

# Diskussion



- **Wie bewerten Sie die Vorschläge?**
- **Adressiert die Regulierung die richtigen „Schmerzpunkte“?**
- **Wie ist Ihre Einschätzung zu einzelnen Artikeln im Legislativvorschlag?**

Vielen Dank für Ihre  
Aufmerksamkeit!

**Dr. Felix Strassmair-Reinshagen**

BaFin  
GIT 1 - Cybersicherheit in der  
Digitalisierung  
GIT1@bafin.de

**Florian Preis**

BaFin  
ZK 1 - Grundsatz ZAG-Aufsicht  
und Kryptoverwahrgeschäft  
Florian.Preis@bafin.de

**Lukas Korella**

Deutsche Bundesbank  
Z 10 - Strategie, Politik und  
Überwachung - Zahlungsverkehr  
und Wertpapierabwicklung  
Lukas.Korella@bundesbank.de