ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

OPEN BANKING UND STARKE KUNDENAUTHENTIFIZIERUNG

Mag. Philipp Großfurtner, MiM
Dr. Anna Muri, MBA

FMA, 21.11.2019

INHALTSVERZEICHNIS

RECHTSGRUNDLAGEN

RECHTSGRUNDLAGEN – PSD2

RL (EU) 2015/2366 (PSD2/ZDRL II) – AUSGEWÄHLTE BEWEGGRÜNDE

- Digitalisierung
- Neue Geschäftsmodelle
- Verbraucherschutz; Sicherheit
- Technischer Fortschritt

NEUE PLAYER: SOG THIRD PARTY PROVIDER (TPP)

- Zahlungsauslösedienstleister und Kontoinformationsdienstleister

GEREGELTER ZUGANG ZU KUNDENKONTEN (DEDIZIERTE SCHNITTSTELLEN – API)

STARKE KUNDENAUTHENTIFIZIERUNG

RECHTSGRUNDLAGEN – DELVO (EU) 2018/389 UND ZADIG 2018

DELVO (EU) 2018/389

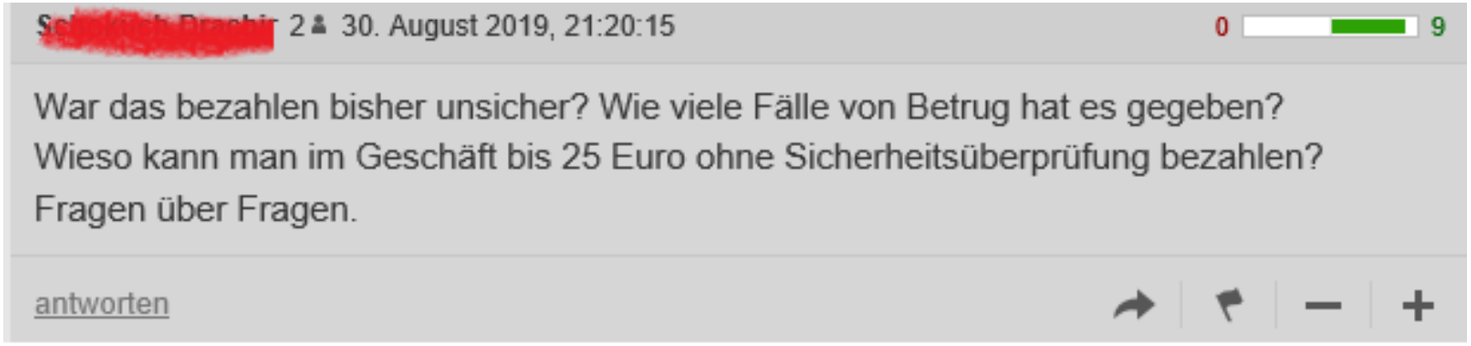
- Konkrete Vorgaben für starke Kundenauthentifizierung und dedizierte Schnittstellen

ZADIG 2018

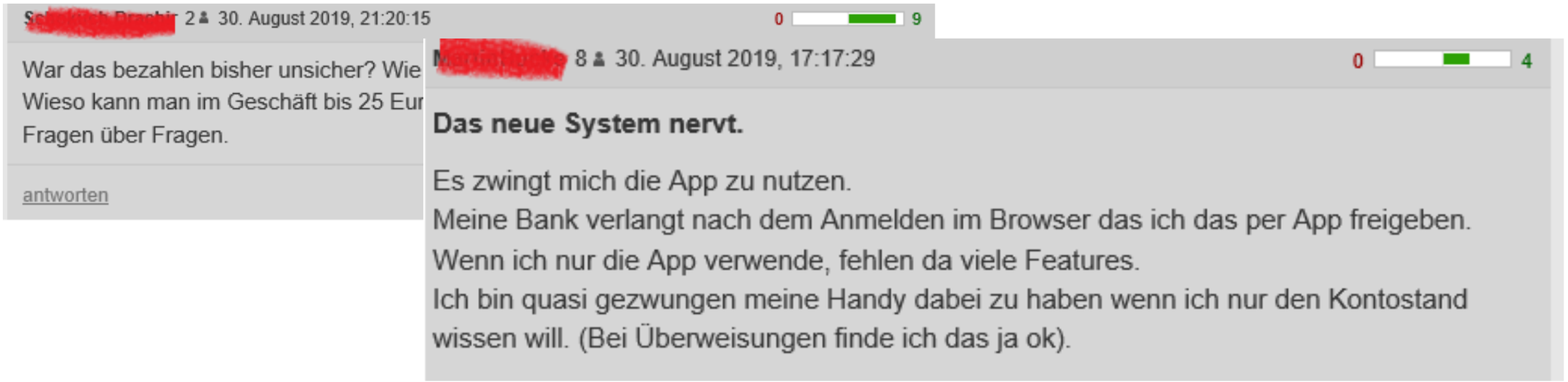
- Vorgabe, starke Kundenauthentifizierung durchzuführen plus Sanktion (§§ 87 und 100 ZaDiG 2018)
- Konzessionierung bzw Registrierung der TPP (§§ 1 Abs 2 Z 7 und 8; 7 und 15 ZaDiG 2018)
- Begrenzung des Zugangs zu Zahlungskonten (§ 62 ZaDiG 2018)

STARKE KUNDENAUTHENTIFIZIERUNG

STARKE KUNDENAUTHENTIFIZIERUNG



STARKE KUNDENAUTHENTIFIZIERUNG



[redacted] 2 30. August 2019, 21:20:15 0 9

War das bezahlen bisher unsicher? Wie
Wieso kann man im Geschäft bis 25 Eur
Fragen über Fragen.

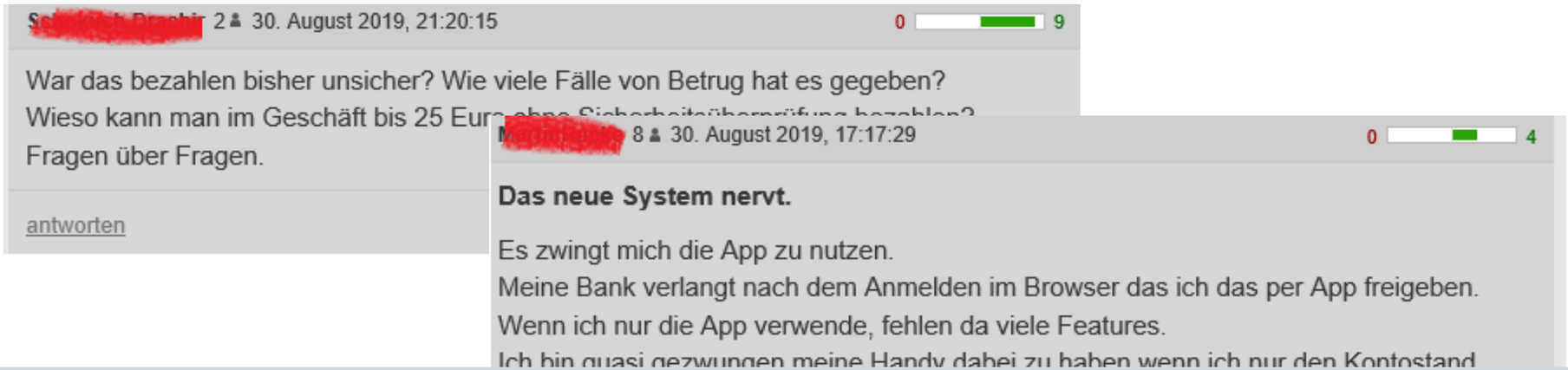
antworten

[redacted] 8 30. August 2019, 17:17:29 0 4

Das neue System nervt.

Es zwingt mich die App zu nutzen.
Meine Bank verlangt nach dem Anmelden im Browser das ich das per App freigeben.
Wenn ich nur die App verwende, fehlen da viele Features.
Ich bin quasi gezwungen meine Handy dabei zu haben wenn ich nur den Kontostand wissen will. (Bei Überweisungen finde ich das ja ok).

STARKE KUNDENAUTHENTIFIZIERUNG



[redacted] 2 30. August 2019, 21:20:15 0 9

War das bezahlen bisher unsicher? Wie viele Fälle von Betrug hat es gegeben?
Wieso kann man im Geschäft bis 25 Eur[redacted]
Fragen über Fragen.

antworten

[redacted] 8 30. August 2019, 17:17:29 0 4

Das neue System nervt.

Es zwingt mich die App zu nutzen.
Meine Bank verlangt nach dem Anmelden im Browser das ich das per App freigeben.
Wenn ich nur die App verwende, fehlen da viele Features.
Ich bin quasi gezwungen meine Handy dabei zu haben wenn ich nur den Kontostand

[redacted]**5. Juni 2019 um 14:06**

ANTWORTEN

Mit anderen Worten, man wird GEZWUNGEN Telebanking künftig nur mehr übers Handy abzuwickeln, was mir persönlich zutiefst zuwider ist! Bei mir lief es immer zweigeteilt über den PC und TAC SMS übers Handy ab. Das erschien mir ziemlich sicher! Immer wieder werden Handys geklaut, passiert mir das, kann ich künftig nicht mal mehr überweisen!

STARKE KUNDENAUTHENTIFIZIERUNG

ZWEI VON DREI ELEMENTEN AUS DER KATEGORIE WISSEN, BESITZ UND INHÄRENZ MÜSSEN ZUR AUTHENTIFIZIERUNG DES KUNDEN/DER KUNDIN HERANGEZOGEN WERDEN:

- Wissen: zB Passwort, PIN, bestimmte Wischbewegungen
- Besitz: zB mittels Kartenlesegerät eingelesene Kreditkarte/Debitkarte, App (device-binding!), Handy (SIM-Karte)
- Inhärenz: zB: Fingerabdruck, Gesichtserkennung, Spracherkennung

WANN HAT EINE STARKE KUNDENAUTHENTIFIZIERUNG ZU ERFOLGEN (§ 87 ZADIG)?

- Wenn der Zahler/die Zahlerin online auf sein/ihr Zahlungskonto zugreift
- Einen elektronischen Zahlungsvorgang auslöst (über einen Fernzugang)

STARKE KUNDENAUTHENTIFIZIERUNG

AUSNAHMEN:

- Zugriff auf Zahlungskontoinformationen (Art 10)
- Kontaktlose Zahlungen (Art 11)
- Unbeaufsichtigte Terminals für Verkehrsnutzungsentgelte und Parkgebühren (Art 12)
- Vom Zahler als vertrauenswürdig eingestufte Empfänger (Art 13)
- Wiederkehrende Zahlungsvorgänge (Art 14)
- Zahlungen an die eigene Person (beim selben Zahlungsdienstleister) (Art 15)
- Kleinbetragszahlungen (Art 16)
- Zahlungsmethoden mit hohem Sicherheitsniveau, zu denen nur Unternehmen zugelassen sind (Art 17)
- eine durchgeführte Transaktionsrisikoanalyse hat ein niedriges Risiko der Zahlung ergeben (Art 18)

STARKE KUNDENAUTHENTIFIZIERUNG

„SUPERVISORY FLEXIBILITY“ IM HINBLICK AUF E-COMMERCE-ZAHLUNGEN:

- Hintergrund: europäischer Markt nicht ausreichend auf Umstellung vorbereitet
- Vor allem kleinere und mittlere Handelsunternehmen haben aufwändigen Implementierungsbedarf
- Mit EBA-Opinion vom 16.10.2019 wurde Ende der aufsichtlichen Nachsicht mit 31.12.2020 festgelegt

NOCH FRAGEN?

ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

OPEN BANKING – DEDIZIERTE SCHNITTSTELLEN AUS DER SICHT DER FMA

FMA, 21.11.2019

Mag. Philipp Großfurtner, MiM

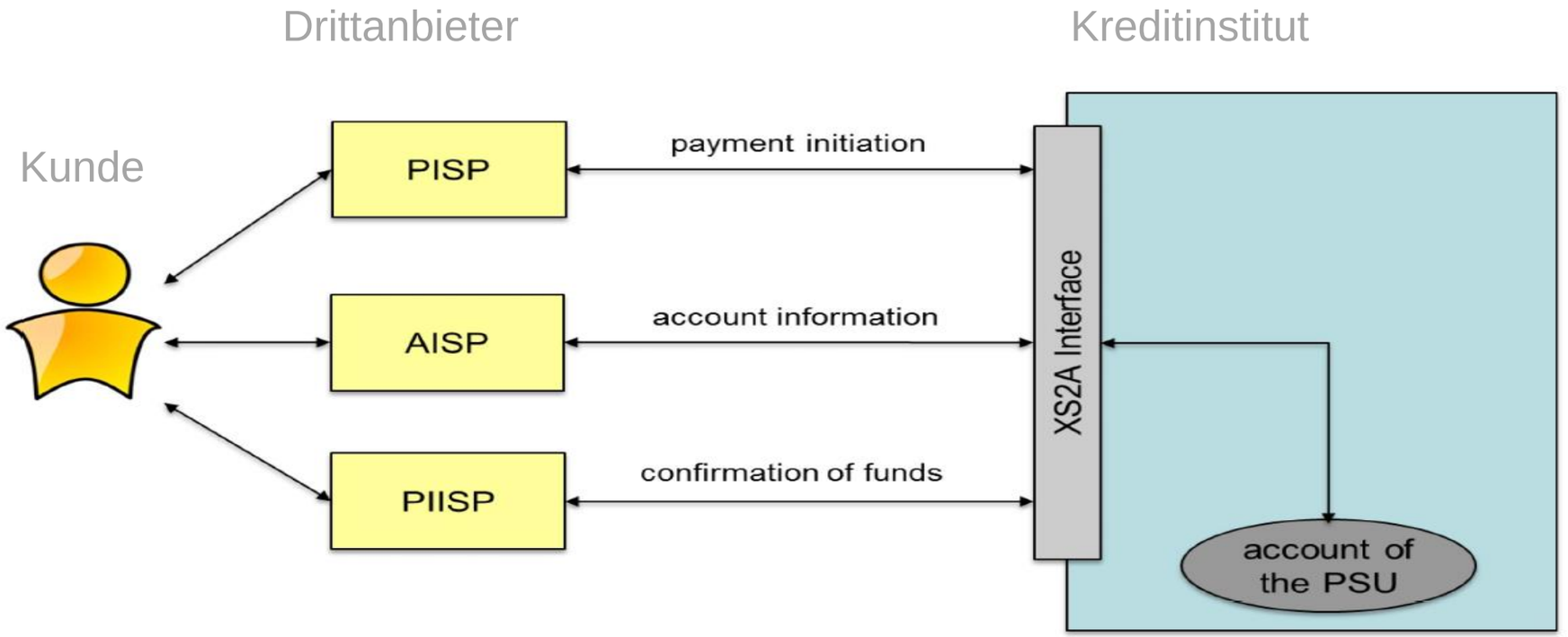
INHALTSVERZEICHNIS

EBA, NCA und RTS
SCA, AIS und TPP
PIS, API, PIISP, AIS, ASPSP und PSU?

API – APPLICATION PROGRAMMING INTERFACE

- API ist die Kurzform von "Application-Programming-Interface“. In den einschlägigen Gesetzestexten wird dafür der Begriff „dedizierte Schnittstelle“ verwendet.

- Mithilfe dieser Schnittstelle wird Programmen ein Tool zur Verfügung gestellt, über welches sie sich an das jeweilige Softwaresystem anbinden können.



ZUGANGSSCHNITTSTELLEN – OPTIONEN

Das kontoführende Institut muss einen PSD2-konformen Zugang zu den Online-Konten seiner Kunden bereitstellen:

Option A: Dediziertes Schnittstelle (API) incl. Notfallmechanismus

Option B: Dedizierte Schnittstelle ohne Notfallmechanismus (von der FMA zu bewilligen)

Option C: Gewöhnliche Kundenschnittstelle (Online-Banking-Website) plus

DEDIZIERTE SCHNITTSTELLE VS. KUNDENSCHNITTSTELLE

Dedizierte Schnittstelle

- Eigener Zugang für Third Party Provider
- Nur jene Daten ersichtlich, die der Third Party Provider für Erbringung seiner Dienstleistung benötigt
- Identifikation der Third Party Provider über eIDAS-Zertifikate beim Einstieg

Gewöhnliche Kundenschnittstelle

- Zugang für Kunden und Third Party Provider gleichermaßen
- Third Party Provider sieht mehr als er benötigt und zwar alles, das der Kunde selbst auch sieht (zB.: Sparkonten, Wertpapierkonten, Verfügerlimits)
- **Erst ab 14.9.2019** Identifikationspflicht der Third Party Provider über eIDAS-Zertifikate beim Einstieg

WAS VERSTEHT MAN UNTER „THIRD PARTY PROVIDER“?

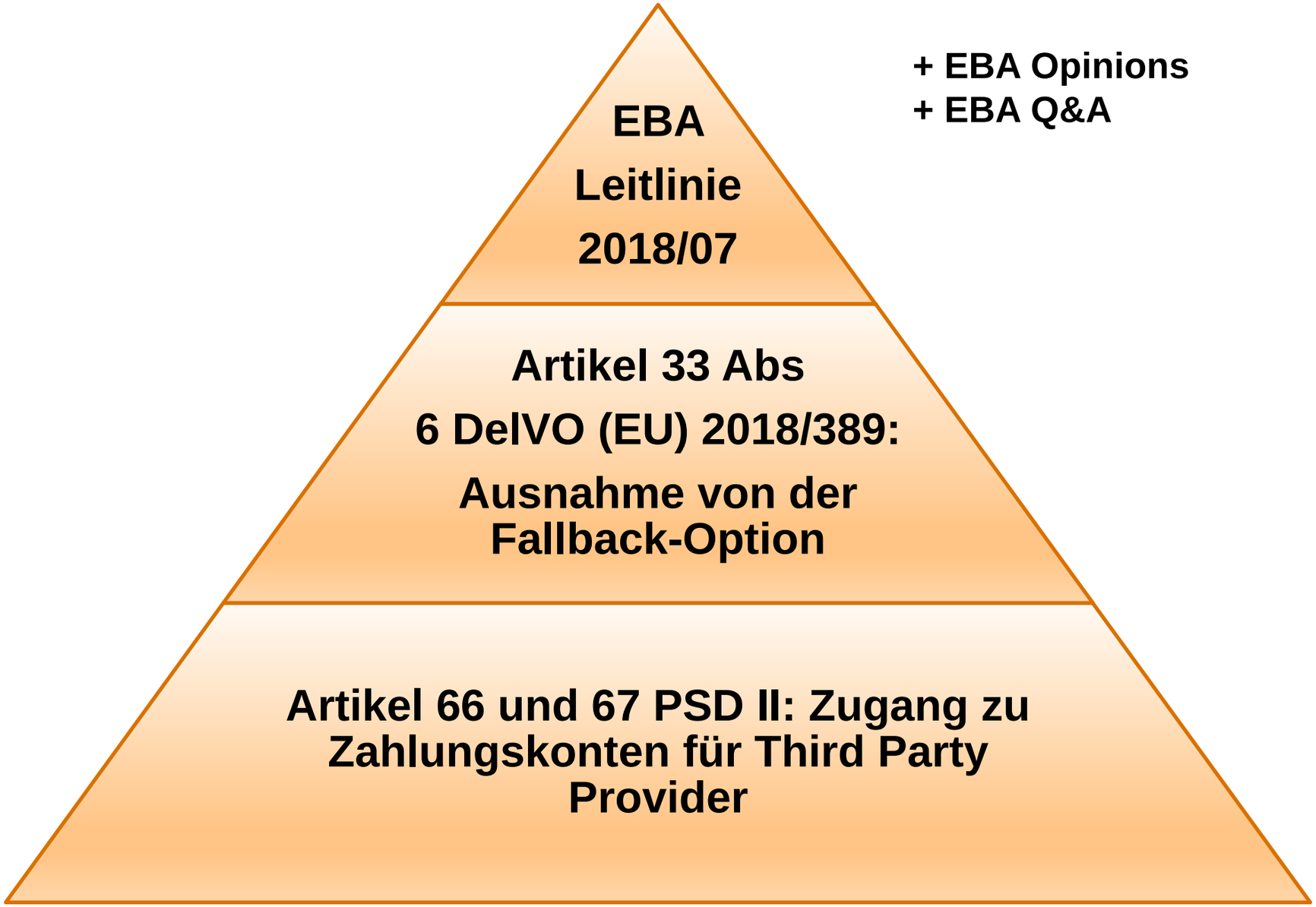
Zahlungsauslösedienstleister

- Ein Dienst, der einen Zahlungsauftrag auslöst, der sich auf ein bei einem anderen Zahlungsdienstleister geführtes Zahlungskonto (z.B.: Hausbank des Kunden) bezieht und die Initiierung auf Antrag des Zahlungsdienstnutzers erfolgt.
- Interessant für jene Personengruppe, die bspw. über keine Zahlungskarten (Kreditkarten) verfügen oder diese nicht einsetzen wollen.
- Zahlungsauslösedienstleister kommt aber selbst nie in Besitz des zu transferierenden Geldbetrages.

Kontoinformationsdienstleister

- Kontoinformationsdienste sind als *„Onlinedienste zur Mitteilung konsolidierter Informationen über ein Zahlungskonto oder mehrere Zahlungskonten des Zahlungsdienstnutzers bei einem oder mehreren anderen Zahlungsdienstleistern“* definiert.
- Benutzerfreundlich aufbereiteten Gesamtüberblick über seine finanzielle Situation zu einem bestimmten Zeitpunkt auf elektronischem Wege erhalten.
- Anwendungsfall: Das automatische Erkennen von Einsparpotenzialen, z. B.: direkt in Ihrer Buchhaltungsanwendung.

RECHTLICHE GRUNDLAGEN



+ EBA Opinions
+ EBA Q&A

FORMULAR

- Alle Artikel ohne Normenbezeichnung entstammen DelVO 2018/389/EU
- Alle Verweise auf Leitlinien beziehen sich auf die EBA Leitlinie GL 2018/07
- Alle Fragen sind vollständig und wahrheitsgemäß zu beantworten
- Ausdrücklich vorbehalten ist das Recht der FMA, zu allen getätigten Angaben zusätzliche Dokumente anzufordern

AUSNAHMEBEWILLIGUNGEN - STATUS QUO

- **Bis dato 19 Anträge eingelangt ➔ keine Ausnahmebewilligungen erteilt**
- **Verbesserungsaufträge**
- **Defizite des Berlin Group Standards**
  - Derzeit keine Möglichkeit Daueraufträge über die API abzurufen
- **Aktuell Verstoß gg. Artikel 36 Abs 1 DelVO (EU) 2018/389:**

„….stellen den Kontoinformationsdienstleistern dieselben Informationen von bezeichneten Zahlungskonten und damit in Zusammenhang stehenden Zahlungsvorgängen bereit, die auch dem Zahlungsdienstnutzer bereitgestellt werden, wenn er den Zugang zu Kontoinformationen direkt anfordert, sofern diese Informationen keine sensiblen Zahlungsdaten enthalten.“

Q&A

FINANZMARKTAUFSICHT ÖSTERREICH

Kompetenz Kontrolle Konsequenz