
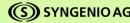


PSR in der Praxis
EU COM(2023)367 Art 43 & 88



We⁺ make IT work.



1

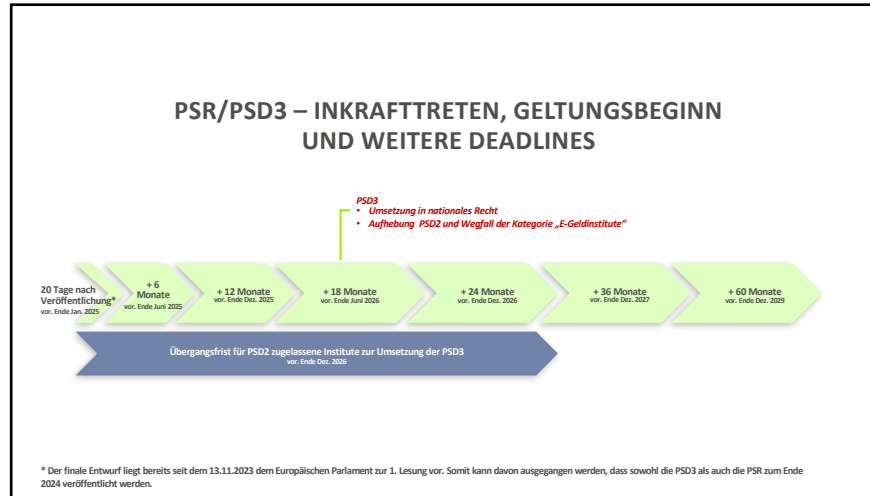


**NACH PSD & PSD2 KOMMEN
PSD3 und PSR**

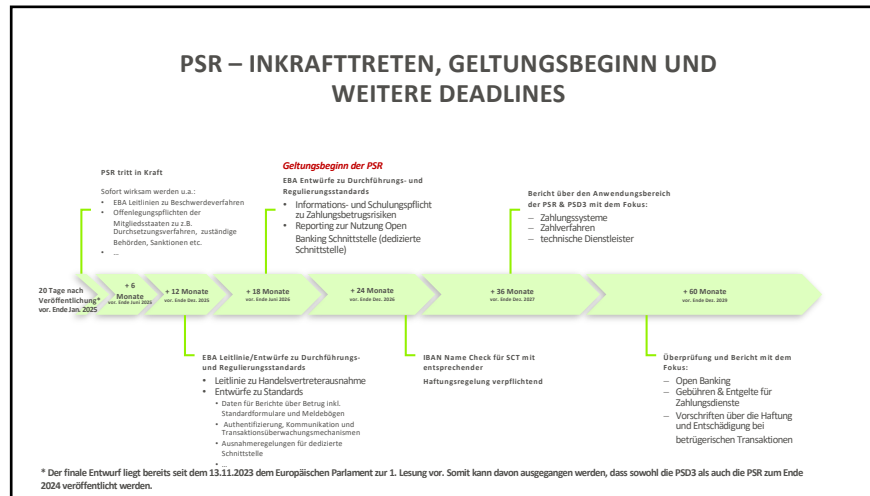
- **PSD3 liefert ...**
 - ... das Rahmenwerk für alle Themen zur Zulassung & Beaufsichtigung von Zahlungsinstituten
 - ... verprobt neue Geschäftsmodelle
- **PSR harmonisiert ...**
 - ... Zahlungsverkehr
 - ... Sanktionen
 - ... Zwangsgelder
- **Nationale Gesetzgeber & Behörden** verlieren an Einfluss, im Gegenzug erhält die **EBA** mehr Kompetenzen



2



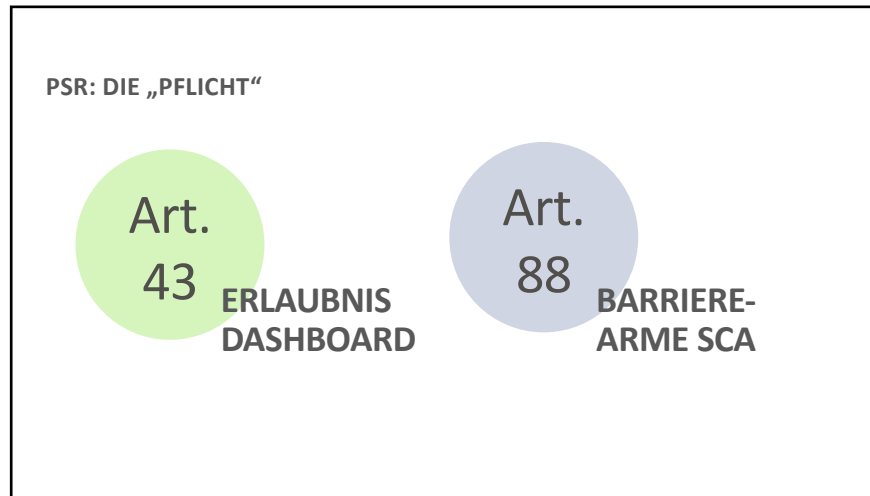
3



4

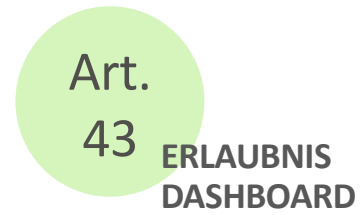


5



6

PSR: DIE „PFLICHT“



7

DASHBOARD: DIE „PFLICHT“

Banken müssen ein in ihre Benutzeroberfläche integriertes Dashboard bereitstellen. Dieses Dashboard dient den Zahlungsdienstnutzern zur Überwachung und Verwaltung von Erlaubnissen für Kontoinformationsdienste oder Zahlungsauslösedienste, insbesondere für Mehrfachzahlungen oder wiederkehrende Zahlungen:

Übersicht
über die
Erlaubnisse

Das Dashboard muss einen Überblick über jede laufende Berechtigung bieten, einschließlich Details wie den Namen des Anbieters, das Kundenkonto mit gewährtem Zugriff, den Zweck der Berechtigung, ihre Gültigkeitsdauer und die Kategorien der freigegebenen Daten.

Entzug oder
Wiedererteilung
von Erlaubnissen

Die Nutzer sollten in der Lage sein, den Datenzugang für bestimmte Dienste oder Anbieter zu entziehen und anschließend wiederherzustellen, wenn sie dies wünschen.

Datensatzpflege

Das Dashboard muss eine Aufzeichnung der entzogenen oder abgelaufenen Datenzugriffsberechtigungen für die Dauer von zwei Jahren enthalten.

8

DASHBOARD: DIE „PFLICHT“

Kontoführende Zahlungsdienstleister müssen dem Zahlungsdienstnutzer ein Dashboard zur Verfügung stellen zur Verwaltung und Überwachung seiner erteilten Open-Banking-Erlaubnisse.

Anforderungen an die Nutzerfreundlichkeit

- das Dashboard muss in der Nutzerschnittstelle leicht auffindbar sein
- die Informationen müssen klar, richtig und für den Nutzer verständlich sein

Kontoführende Zahlungsdienstleister und Kontoinformations- oder Zahlungsauslösedienstleister arbeiten zusammen und tauschen Informationen in **Echtzeit** aus

- über Änderungen, die der Nutzer über das Dashboard an der Erlaubnis vorgenommen hat
- über neue Zugangserlaubnisse mit Angabe von
 - Zweck
 - Geltungsdauer
 - betroffenen Datenkategorien

Sicht für den Zahlungsnutzer

Funktionen: einen neuen Dienstleister anlegen, Datenzugriff einem Dienstleister entziehen, nach Entzug auch wiederherstellen

aktive und alle entzogene oder abgelaufene Zugangserlaubnisse der letzten 2 Jahre

TPP	Kundenkonto	Zweck	Kategorien	gültig von	gültig bis	Status	Buttons
TPP1	Konto1	AIS		Jan 23	Dez 24	aktiv	deaktivieren
TPP1	Konto2	PIS		Dez 22	Okt 24	aktiv	deaktivieren
TPP2	Konto1	PIS / PIIS		Dez 22	Mai 23	abgelaufen	...
TPP3	Konto2	AIS		Jan 23	Sep 25	deaktiviert	reaktivieren

TPP hinzufügen

AIS = Account Information Service (nur Kontoinformationen), PIS = Payment Initiation Service (Zahlung initiieren), PIIS = Payment Instrument Issuing Service (w/heim Bestätigung des verfügbaren Betrags)

9

AGGREGATED DASHBOARD: DIE „KÜR“?

Können die Kunden über einem Dashboard alle Erlaubnisse steuern, so wird diese bevorzugt: UX entscheidet!

Weitere Konten (Drittbanken) registrieren

- Onboarding & Authentisierungsprozess (erstmalig)
- “shake hands“ Prozess im Hintergrund danach, bzw. zumindest für bestimmte Funktionen (z.B. einsehen, löschen, aber nicht neu einrichten?)

Art. 43: „Kontoführende Zahlungsdienstleister und Kontoinformations- oder Zahlungsauslösedienstleister arbeiten zusammen und tauschen Informationen in Echtzeit aus“

Art. 31

Zugang zu Zahlungssystemen

Art. 32

Zahlungskonten, die von Kreditinstituten für Zahlungsinstitute bereitgestellt werden

Art. 35

Bereitstellung dedizierter Zugangsschnittstellen

Art. 43

10

WELCHE VALUE ADDED SERVICES WÄREN
DANN MÖGLICH / DENKBAR?

BREAKOUT #1



11

PSR: DIE „PFLICHT“

Art.
88

BARRIERE-
ARME SCA

12

BARRIEREFREIHEIT & SCA: DIE „DOPPEL-PFLICHT“

Art. 88 PSR : Barrierefreiheitsanforderungen für die starke Kundenauthentifizierung

- (1) Unbeschadet der Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 stellen die Zahlungsdienstleister sicher, dass allen ihren Kunden, einschließlich Menschen mit Behinderungen, Älteren, Menschen mit geringen digitalen Kompetenzen und Menschen, die keinen Zugang zu digitalen Wegen oder Zahlungsinstrumenten haben, mindestens ein auf ihre besondere Situation abgestimmtes Mittel zur Verfügung steht, um eine starke Kundenauthentifizierung durchführen zu können.
- (2) Die Zahlungsdienstleister dürfen die Leistungsfähigkeit der starken Kundenauthentifizierung nicht von der ausschließlichen Verwendung eines einzigen Authentifizierungsverfahrens abhängig machen und dürfen die Leistungsfähigkeit der starken Kundenauthentifizierung weder explizit noch implizit vom Besitz eines Smartphones abhängig machen. Die Zahlungsdienstleister entwickeln eine Vielfalt an Verfahren für die Durchführung der starken Kundenauthentifizierung, um der besonderen Situation all ihrer Kunden gerecht zu werden.



13

ES GIBT GUTE NACHRICHTEN, JEDOCH ...

Bestehende Lösungen und Prozesse können weiter genutzt werden, es sind „nur“ ...

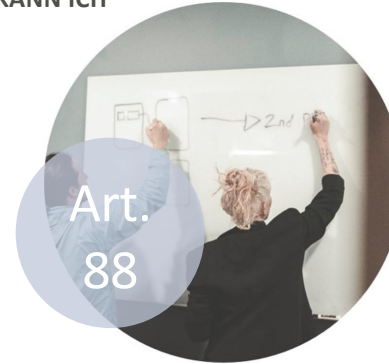
- ✓ aktuell bestehende SCA-Lösungen per Smartphone barrierearm zu gestalten
- ✓ weitere barrierearme Lösungen zur SCA ohne Smartphone zu etablieren



14

**WELCHE ANFORDERUNGEN HAT EINE
BARRIEREARME SCA UND WIE KANN ICH
DAS ERREICHEN?**

BREAKOUT #2



15

VIELEN DANK.



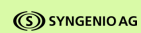
Sybille Schorn
+49 151 7304 2315
Sybille.Schorn@syngenio.de

Mark Spiessl
+49 160 9649 8611
Mark.Spiessl@syngenio.de



We⁺ make IT work.

HAMBURG DÜSSELDORF KÖLN BONN FRANKFURT STUTTGART MÜNCHEN
Sitz der Gesellschaft: München | Registergericht Amtsgericht München
Handelsregisternummer: HRB 138143
Vorstand: Jürgen Franke, Joachim Mühlrad
Aufsichtsratsvorsitzender: Thomas Balgheim



16