04/2026

sopra steria

OPEN FINANCE

WAS PSR UND PSD3 IM PAYMENT VERÄNDERN (MIT FIDA-AUSBLICK)

PSR UND PSD3 IN BRIEF. **WAS JETZT ZÄHLT**

FÜNF AUSSAGEN, DIE BANKEN MITNEHMEN SOLLTEN

1. **PSR ist ein Betriebsprojekt.** Die Verordnung zielt auf messbare Standards. Stabilität, Transparenz und Fairness werden prüfbar.
2. **Consent wird auditierbar.** Ein Permission-Dashboard zwingt zu einem sauberen Einwilligungs- und Berechtigungsmodell. Das betrifft Frontend und Backend zugleich.
3. **APIs werden zur kritischen Infrastruktur.** Qualität, Verfügbarkeit und Datenumfang müssen zur Nutzerstrecke im Online-Banking passen.
4. **Fraud wird Pflichtprogramm.** Echtzeit-Monitoring, Informationsaustausch und standardisiertes Reporting werden konkreter. Haftung hängt stärker an nachweisbaren Kontrollen. Haftung und Beweislast verschieben sich zum Zahlungsdienstleister.
5. **FIDA ist die nächste Stufe.** Der politische Prozess ist offen, die Vorarbeiten sind klar. Dateninventar, Ownership, Use Cases, Consent-Logik, API-Industrialisierung.

30-TAGE-CHECK – WAS INSTITUTE SOFORT PRÜFEN KÖNNEN

- **Consent und Berechtigungen:** Wo liegt die Wahrheit? Gibt es Historie, Zweck und Datenkategorien pro Zugriff?
- **Permission-Dashboard:** Können Widerrufe und Wiederherstellungen ohne Medienbruch umgesetzt werden?
- **API-Betrieb:** Welche SLAs gelten wirklich? Welche Kennzahlen werden aktiv gemessen und gemanagt?
- **Fraud und Haftung:** Gibt es ein Echtzeit-Set-up? Welche Regeln sind dokumentiert? Wie wird die Nachweispflicht erfüllt?
- **Kundenschutz und Erstattung:** Sind Prozesse, Texte und Eskalationen klar?
- **FIDA-Vorarbeit:** Dateninventar, Use Cases, Data Governance. Gibt es ein gemeinsames Zielbild?

Einordnung: In vielen deutschen Häusern ist Open Banking technisch vorhanden, aber organisatorisch verteilt. Die schnellsten Fortschritte entstehen, wenn Consent, API-Betrieb und Fraud als zusammenhängender Prozess betrachtet werden.

MARKTSTAND. WARUM EUROPA BEI OPEN BANKING NACHSCHÄRFT

Open Banking ist in Europa angekommen, wird aber ungleich genutzt. In einigen Ländern ist es Alltag, in anderen bleibt die Nutzung punktuell. Die Gründe liegen vor allem in der Fragmentierung durch unterschiedliche Umsetzung, der technischen Qualität der APIs und dem Vertrauen der Nutzer.

ZWEI BAUSTEINE, ZWEI NUTZENLOGIKEN

AIS. Account Information Services: AIS bündelt Kontoinformationen mit Einwilligung. Ziele sind Übersicht, Aggregation, Analysen und persönliche Finanzübersicht.

PIS. Payment Initiation Services: PIS löst Zahlungen aus, oft als „Pay by Bank"-Alternative zu Karten. Vorteile sind potenziell geringere Kosten, schnelle Abwicklung und direkte Kontozahlung. Der Engpass liegt in Stabilität, Conversion und Vertrauen.

WARUM DIE NUTZUNG FRAGMENTIERT BLEIBT

- **API-Qualität ist nicht konstant.** Wenn Schnittstellen instabil sind, sinken Nutzung und Vertrauen.
- **Vertrauen in Datenteilung variiert.** Nutzer wollen Kontrolle und Transparenz, besonders bei sensiblen Finanzdaten.
- **Regulatorische Auslegung war unterschiedlich.** PSD2 als Richtlinie ließ nationale Spielräume. Das führte zu unterschiedlichen Standards.

	GERINGE STABILITÄT UND WENIG VERTRAUEN	HOHE STABILITÄT UND VIEL VERTRAUEN
STARKE NUTZUNG	Nutzer-Akzeptanz trotz Instabilität, z. B. bei innovativen Use Cases oder Early Adopters	Optimal: alltagstaugliche Nutzung, stabile Journeys, hohes Vertrauen – Zielbild für Open Banking
GERINGE NUTZUNG	Kaum Nutzung – fehlende Stabilität und mangelndes Vertrauen verhindern Akzeptanz	Potenzial vorhanden, aber Use Cases nicht ausgereift oder noch nicht bekannt

Nutzung hängt im Alltag weniger an Use Cases, sondern an stabilen Journeys und Vertrauen.

Einordnung: Für Deutschland ist die „Vertrauensfrage" besonders relevant. Viele Nutzer akzeptieren Datenteilung nur, wenn sie eine verständliche Kontrolle haben. Genau hier setzen Permission-Dashboard und Kundenschutz an. Für Banken heißt das: Transparenz ist nicht nur Kommunikation. Es ist Produkt und Prozess.

PSR UND PSD3. VON DER FRAGMENTIERUNG ZUR HARMONISIERUNG

WER WAS MACHT

- **PSD3** ist eine Richtlinie. Sie schafft den Rahmen für Zulassung und Aufsicht und wird national umgesetzt.
- **PSR** ist eine Verordnung. Sie gilt unmittelbar und zielt stärker auf einheitliche, durchsetzbare Standards im Betrieb.

PSR und PSD3 sind kein kleines Update, sie sind ein normativer Umbau.

WAS PSR KONKRET ADRESSIERT

- Mehr **Kundenschutz und Transparenz** in Payment Journeys
- Besserer Umgang mit **Fraud** und klare Verantwortung
- Fairer Zugang und **stabile Qualität** bei Open-Banking-APIs
- Weniger **Regulierungsarbitrage** durch einheitlichere Regeln

WARUM DER DRUCK HOCH IST

PSR koppelt Anforderungen an Durchsetzung. Zentrale Pflichtverstöße führen zu Sanktionen, die in der Größenordnung bis zu einem signifikanten Anteil des globalen Umsatzes liegen können. Nachweisbarkeit wird damit ein Projekttreiber für Banken.

VIER OPERATIVE HEBEL DER PSR

Die Wirkung der PSR lässt sich in vier Hebel übersetzen, die in der Umsetzung besonders relevant sind.

1. Permission-Dashboard
2. Regulatory APIs
3. Fraud-Framework
4. Customer Protection

Wichtig ist nicht das Datum, sondern die Vorarbeit. Consent, API-Betrieb und Fraud lassen sich nicht in vier Wochen aufbauen.

Einordnung: Bei deutschen Banken sind die betroffenen Verantwortlichkeiten oft getrennt. Regulatory Change sitzt anderswo als Betrieb. Fraud sitzt anderswo als Produkt. Wer zu spät integriert, baut doppelt oder übersieht Abhängigkeiten, zum Beispiel VoP plus Erstattung plus Fraud.

PSR. DIE 4 HEBEL

HEBEL 1: PERMISSION-DASHBOARD. CONSENT WIRD SICHTBAR UND PRÜFBAR

Ein Permission-Dashboard wird zur Pflicht im Banking-Interface. Nutzer sollen in Echtzeit sehen und verwalten können, welcher Drittanbieter Zugriff hat: auf welche Konten, für welche Datenkategorien, für welchen Zweck und welchen Zeitraum.

Zwei Anforderungen sind für die Umsetzung besonders wichtig:

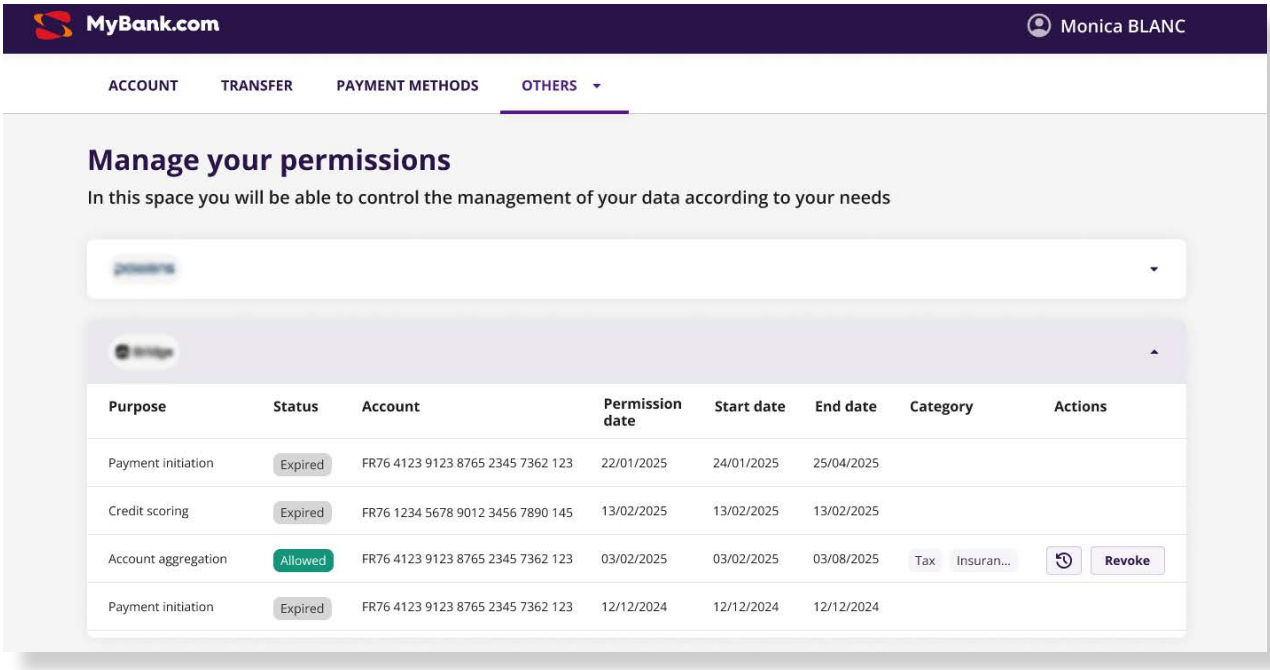
1. Beherrschbarkeit: Zugriff soll innerhalb kurzer Fristen entzogen oder wiederhergestellt werden können.
2. Historie: Nutzer sollen vergangene Berechtigungen nachvollziehen können, inklusive abgelaufener oder widerrufener Zugriffe.

Was das technisch bedeutet:

- granulares Berechtigungsmodell, nicht nur „ein Consent pro Anbieter"
- Nachvollziehbarkeit pro Datenkategorie und Zugriff
- Echtzeit-Statuswechsel: Widerruf, Ablauf, Wiederherstellung
- konsistente Benachrichtigung bei Statusänderungen

Was das für UX bedeutet:

- klare Darstellung und verständliche Begriffe
- keine manipulative Gestaltung, Transparenz statt Hürden



Beispiel für ein Permission-Dashboard. Ein Pflicht-Frontend, das nur funktioniert, wenn das Berechtigungsmodell im Backend stimmt.

Drei Fragen, die Banken im Haus sofort klären sollten:

1. Wo liegt der Consent heute? Kanal, IAM, API-Gateway, Consent Store oder verteilt?
2. Wie werden Daten kategorisiert? Welche Datenkategorien werden heute tatsächlich geteilt und ist das dokumentiert?
3. Wie läuft Widerruf – technisch, prozessual, kommunikativ? Und wie wird die Historie gespeichert?

HEBEL 2: REGULATORY APIS. VON DER SCHNITTSTELLE ZUR BETRIEBSQUALITÄT

PSR adressiert „Hindernisse" im Open-Banking-Alltag und verlangt eine faire, nicht diskriminierende Bereitstellung. Typische Problemfälle sind:

- unbegründete Aufruflimits oder wiederkehrende Nichtverfügbarkeit
- erzwungene Disconnects
- nicht begründete Session-Abläufe
- instabile Synchronisierung

Zwei Leitplanken sind entscheidend:

Performance-Parität: Die API soll so gut funktionieren wie die Standard-Nutzerstrecke im Online-Banking.

Daten-Parität: Über APIs soll derselbe Informationsumfang verfügbar sein wie im Endkunden-Frontend.

KENNZAHL	ZIELWERT	MESSPUNKT	OWNER
 VERFÜGBARKEIT PRO ENDPOINT	≥ 99,9 % (monatlich)	API-Monitoring	API-Operations
 LATENZ (P95)	≤ 500 ms (Read)	API-Gateway/ Response Time	API-Engineering
 FEHLERRATE (4XX/5XX)	≤ 0,5 % aller Requests	Error-Tracking	API-Engineering
 INCIDENT-DAUER (MTTR)	≤ 60 Minuten (P1)	Incident-Management-System	IT-Service-Management
 API-COMPLIANCE (PSD3/PSR)	100 %	Audits und Compliance-Prüfungen	Regulatory Compliance

API-Qualität wird steuerbar, wenn Messpunkte und Owner klar sind.

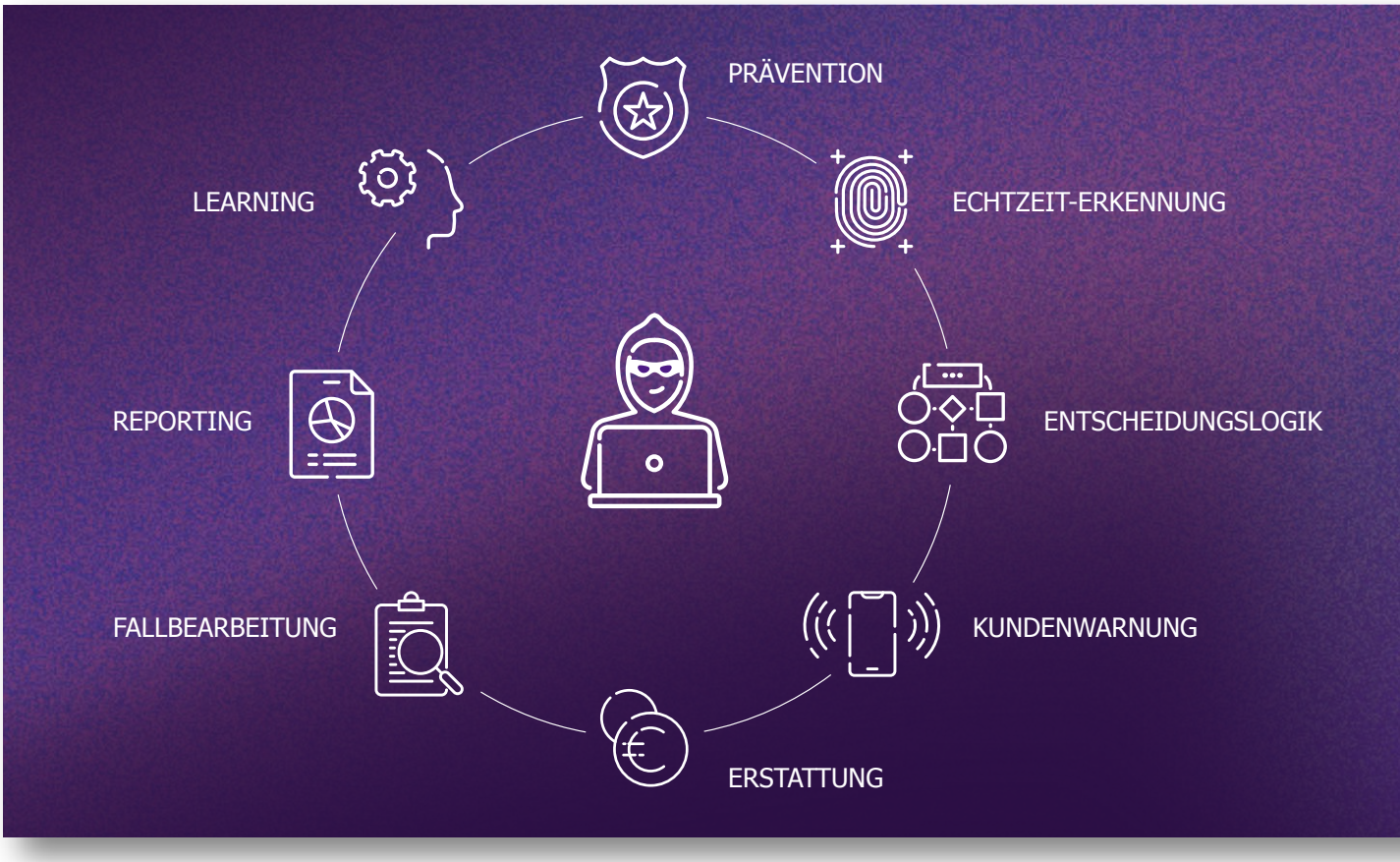
Minimal-Set, mit dem Banken starten können:

- Endpoint-Verfügbarkeit und Latenz. P95 und P99
- Fehlerraten und Timeouts. Pro Endpoint
- Abbruchquoten entlang der Journey
- Rate-Limit-Events plus Ursache
- Change-Fenster, Regressionen, Incident-Dauer

HEBEL 3: FRAUD-FRAMEWORK. ECHTZEIT, AUSTAUSCH, NACHWEISPFLICHT

PSR schafft ein stärker harmonisiertes Fraud-Framework mit konkreteren Pflichten:

- **standardisiertes Fraud-Reporting** an nationale Behörden nach einheitlichem Format
- **Informationsaustausch zwischen Zahlungsdienstleistern** bei begründetem Verdacht mit Schutzmechanismen wie Anonymisierung und begrenzter Aufbewahrung
- **EU-Plattform** für Trends, Best Practices und Empfehlungen
- **Prävention**: Kundenwarnungen, Sensibilisierung, Training, Fokus auf schutzbedürftigen Gruppen
- **Detektion**: Pflicht-zu-Echtzeit-Monitoring – auf Zahlerseite vor Ausführung, auf Empfängerseite bei Eingang ohne (unnötige) Verzögerung der Gutschrift
- **Haftung**: Wenn Kontrollen fehlen oder als unzureichend gelten, liegt die Verantwortung beim Zahlungsdienstleister, inklusive Nachweispflicht und Sanktionierung
- **Haftungsumkehr:** Ein Institut haftet, wenn sich Betrüger als Bankmitarbeiter ausgeben und die gleichen Kanäle nutzen wie die Bank.



Fraud-Management entwickelt sich vom Scoring zum geschlossenen Entscheidungs- und Lernsystem.

Wo Projekte typischerweise hängen bleiben:

- Echtzeit-Datenflüsse über Kanäle sind unvollständig.
- Regeln sind nicht versioniert und nicht belegbar.
- Erstattung, Kundendialog und Fraud-Entscheidungen sind nicht abgestimmt.

HEBEL 4: CUSTOMER PROTECTION – LIMITS, EMPFÄNGERPRÜFUNG, ERSTATTUNG

Kundenschutz wird zu einem konkreten Pflichtbündel.

Payment-Limits: Nutzer sollen Zahlungslimits selbst steuern können – nach Tag, pro Transaktion oder pro Instrument. Limit-Erhöhungen sollen zusätzliche Sicherheitsmechanismen auslösen, zum Beispiel eine Sicherheitsverzögerung und starke Kundenauthentifizierung.

Verification of Payee: Die Empfängerprüfung soll Warnungen in Echtzeit ermöglichen, typischerweise über einen Abgleich von Name und IBAN. Der Kunde entscheidet dann bewusst, ob er trotzdem ausführt.

Erstattung und Beweislast: Bei unautorisierten Zahlungen wird eine kurzfristige Erstattung erwartet. Ausnahmen greifen bei nachweisbarem Betrug oder grober Fahrlässigkeit. Die Beweislast liegt tendenziell beim Zahlungsdienstleister. Dadurch steigt das Risiko, dass finanzielle Schäden bei der jeweiligen Bank verbleiben.

Kundenschutz ist Prozessdesign. VoP, Fraud-Monitoring und Erstattung müssen zusammenpassen.

Was das für Produkte und Prozesse heißt:

- Limits sind Produktfeature und Fraud-Hebel zugleich. Es braucht klare Kommunikation und konsistente Logik.
- Verification of Payee (VoP) und Erstattung berühren Support, Reklamation, Rechtsbereich und Betrugsabwehr.
- Wer erst im Betrieb feststellt, dass Texte und Prozesse fehlen, verliert Wochen.

FIDA-AUSBLICK. WAS ABSEHBAR, WAS OFFEN IST

FIDA steht für einen Rahmen, der Datenzugang über Zahlungskonten hinaus ausdehnen soll. Typische Datenfelder sind Sparen, Investments, Kredite, Versicherungen, Altersvorsorge und weitere Finanzdaten. Der Kern sind nutzergesteuerte Freigabe, standardisierte Schnittstellen und Regeln für Teilnahme und Betrieb.

WIE ES ORGANISIERT WERDEN SOLL

Financial Data Sharing Schemes sind als Regelwerk gedacht. Sie definieren Standards, Governance, SLAs und Kompensation. Wichtig ist die Klarstellung. Ein Scheme ist in diesem Verständnis kein zentraler Datenspeicher, sondern ein Rahmen, dem Teilnehmer beitreten.

WAS POLITISCH NOCH OFFEN IST

In der Debatte sind mehrere Punkte strittig. Für Banken sind vier besonders relevant:

1. **Scope**: Welche Datenarten, welche Nutzergruppen, welcher Ausbaupfad? Diskussion über priorisierte Use Cases und mögliche Begrenzung, zum Beispiel auf Retail und kleine Unternehmen. Diskussion über Datenhistorie, zum Beispiel 2 bis 5 Jahre.
2. **Kompensation**: „Reasonable Compensation" ohne Marge versus Modelle mit möglicher Marge.
3. **Schemes**: Wer initiiert, wer betreibt und was passiert, wenn keine tragfähigen Schemes entstehen?
4. **Gatekeepers**: Frage, ob und wie große Plattformen teilnehmen und was das für Souveränität und Wettbewerb bedeutet.

FIDA ist weniger eine Technik- als eine Marktstrukturfrage. Banken sollten jetzt trotzdem mit der Vorarbeit beginnen.

Einordnung: Für Banken lohnt sich ein pragmatischer Ansatz. Nicht auf den finalen Text warten, sondern Grundlagen schaffen, die ohnehin gebraucht werden: Dateninventar, Ownership, Consent-Logik, API-Industrialisierung, Use-Cases-Priorisierung.

NEXT STEPS. KONKRETE ARBEITSAUFTRÄGE FÜR 2026

Ziel: Die Anforderungen aus PSR und PSD3 strukturiert in eine realisierbare Roadmap übersetzen. FIDA als Ausblick früh vorbereiten, ohne auf den finalen Text zu warten.

Guter Startpunkt: ein strukturierter Readiness-Check entlang von fünf Feldern:

1. DATEN UND CONSENT ZUR BILDUNG EINES FUNDAMENTS AUFRÄUMEN

Dateninventar erstellen: Welche Daten werden für AIS, PIS, Fraud und Kundenschutz benötigt? Wo liegen sie? Welche Qualität haben sie?
Ownership festlegen: Wer ist fachlich und technisch verantwortlich für Consent, Berechtigungen und Nachweise?
Berechtigungsmodell standardisieren: Datenkategorien, Zwecke, Laufzeiten, Statuswechsel, Historie. Einheitlich über Kanäle.

2. PERMISSION-DASHBOARD ALS PRODUKT UND KONTROLLPUNKT PLANEN

MVP definieren: Welche Ansichten und Funktionen müssen zum Start abgedeckt sein? Welche Fristen und Statusfälle?
Backend-Anschluss sichern: Consent Store, IAM, API-Layer und Benachrichtigungen müssen konsistent sein.
Texte und UX prüfen: Verständlichkeit, Transparenz, klare Handlungsoptionen. Ohne Hürden.

3. APIS INDUSTRIALISIEREN – BETRIEB, SLAS, MONITORING

Servicekatalog und SLAs: Endpoints, Zielwerte, Messpunkte, Owner. Verfügbarkeit, Latenz, Fehlerrate, Timeouts, Abbrüche.
Observability aufsetzen: Messung entlang kritischer Journeys, nicht nur Uptime.
Incident- und Change-Prozesse: Playbooks, Regression-Tests, planbare Kommunikationsfenster. Versionierung und Deprecation.

4. FRAUD, KUNDENSCHUTZ UND ERSTATTUNG VERZAHNEN

Echtzeit-Monitoring priorisieren: kritische Use Cases, Datenquellen, Schwellenwerte, Eskalationswege.
Nachweisfähigkeit herstellen: versionierte Regeln und Modelle, dokumentierte Entscheidungslogik, Audit-Trails.
Customer Protection integrieren: Limits, Empfängerprüfung, Warntexte und Erstattungsprozesse als zusammenhängende Kette.
Ist-Analyse der Betrugsprävention durchführen und strategische Roadmap erstellen, um die Lücken zu schließen.

5. FIDA PRAGMATISCH VORBEREITEN

Use Cases priorisieren: eine kurze Liste mit klarer Kosten-Nutzen-Logik statt „alles öffnen".
Data Governance erweitern: Ownership, Zugriffspfade, Datenqualität, Einwilligungslogik für weitere Finanzdaten.
Scheme Readiness denken: Welche Standards, SLAs und Betriebsmodelle wären erforderlich? Welche Kompensationslogik wäre realistisch?

WAS IN 90 TAGEN VORLIEGEN SOLLTE

Ein abgestimmtes **Zielbild** mit den wichtigsten Abhängigkeiten zwischen Consent, APIs, Fraud und Kundenschutz.
Ein priorisiertes **Backlog**, inklusive Verantwortlichkeiten und Risikopunkten.
Ein **Monitoring- und SLA-Set** für Open-Banking-APIs, das im Betrieb gelebt wird.
Ein **Umsetzungsplan** für das Permission-Dashboard und die wichtigsten Prozessanpassungen bei Erstattung.

ANSPRECHPARTNER

SEBASTIAN FEUSTER
Head of Payment
E. sebastian.feuster@soprasteria.com

ANTONIA GREIL
Senior Consultant Payment
E. antonia.greil@soprasteria.com

SARAH GOLDBERG
Senior Consultant Payment
E. sarah.goldberg@soprasteria.com

KONTAKT

Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg

T. 040 22703-0
E. banking.de@soprasteria.com
W. www.soprasteria.com

www.soprasteria.com