Whitepaper

Was technisch passiert,

wenn Du Dein Konto bei nobank verbindest.

Drei Sorgen, drei Antworten — in 8 Minuten Lesezeit.

Wer dieses Whitepaper schreibt

Dirk Biering — verantwortlich für Risikomanagement, Compliance und Datenschutz bei nobank seit dem ersten Tag. 25+ Jahre vorher bei Banken, Zahlungsdienstleistern und Asset Managern. Details auf LinkedIn.

Externer Datenschutzbeauftragter: Rechtsanwalt Andreas Riehn, München.

Datenschutz-Aufsicht: Bayerisches Landesamt für Datenschutzaufsicht (BayLDA).

Version 1.5 • 12.05.2026 • nobank Finanzoptimierung GmbH, München

Inhalt

Vorwort

Hi, ich bin **Dirk**. Bei nobank verantworte ich seit dem ersten Tag Risikomanagement, Compliance und Datenschutz. Davor 25 Jahre in Banken, Zahlungsdienstleistern und Asset Managern. Meinen Werdegang findest Du auf LinkedIn.

Dieses Whitepaper existiert, weil wir in Gesprächen mit Testern drei Sorgen immer wieder hören, berechtigterweise:

- Können die mir was abbuchen?
- Was macht ihr mit meinen Daten?
- Schauen die Gründer in mein Konto?

Ich beantworte diese drei Fragen hier so, wie ich sie auch jemandem persönlich beantworten würde, direkt, mit Belegen, ohne Marketing-Sprech. Das Whitepaper richtet sich an alle, die es genau wissen wollen, und an alle, die uns gegenüber Freunden und Familie verteidigen müssen. Schick es ihnen einfach weiter.

Was dieses Whitepaper nicht ist

Es ist kein 100-Prozent-Versprechen. Niemand sollte Dir das geben, auch wir nicht. Stattdessen erklären wir, welche Schutzmechanismen wir haben, wo deren Grenzen liegen, und was passieren würde, wenn jemand die Grenzen überschreitet.

Es ist kein juristisches Dokument. Datenschutzerklärung, AGB und Impressum sind separate Dokumente und auf der Website verlinkt.

Es ist nicht statisch. Wenn sich etwas ändert, aktualisieren wir das Whitepaper. Versionsnummer und Datum stehen auf der Cover-Seite.

Kapitel 1: Können die mir was abbuchen?

Kurze Antwort: **Nein.** Wir können weder buchen noch ändern. Hier ist die lange Antwort.

nobank ist keine Bank

Das ist die wichtigste Klarstellung vorab: nobank selbst hat keine Banklizenz und braucht keine. Wir sind kein Zahlungsinstitut, kein Kreditinstitut. Du gibst uns kein Geld, wir verwalten kein Konto für Dich. Was Du auf nobank siehst, sind die Daten Deiner bestehenden Banken, eingelesen über eine offizielle, lizenzierte EU-Schnittstelle.

Wie die Verbindung technisch funktioniert

Den Lese-Zugriff auf Deine Bank stellt ein lizenzierter Dienstleister namens finAPI her. finAPI ist von der BaFin als Kontoinformationsdienst nach § 1 Abs. 33 ZAG registriert und arbeitet im Rahmen der EU-Richtlinie PSD2 (Payment Services Directive 2). PSD2 hat lizenzierungspflichtige Drittanbieter-Dienste auf Bankkonten geschaffen. Darunter den Kontoinformationsdienst (AIS, Art. 67 PSD2), den Zahlungsauslösedienst (PIS, Art. 66 PSD2) und den Bestätigungsdienst über die Verfügbarkeit eines Geldbetrags (CBPII, Art. 65 PSD2). finAPI nutzt für nobank ausschließlich den Kontoinformationsdienst (AIS). AISPs dürfen nach PSD2 nur Lese-Zugriff auf Deine Kontodaten, keine Buchungen, keine Änderungen.

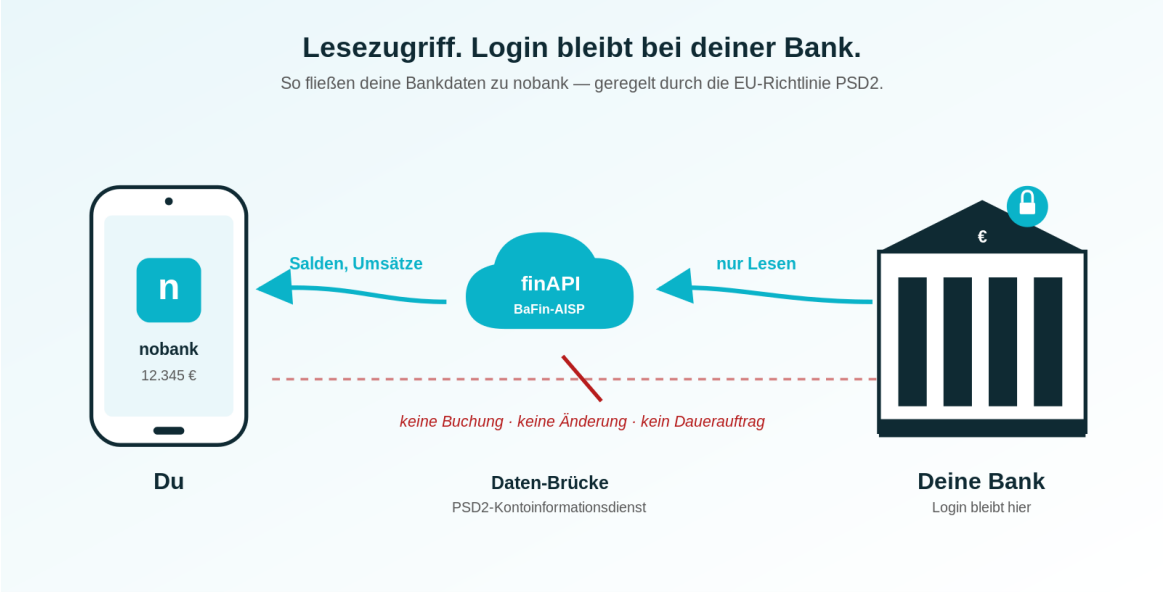

Schaubild 1: Lesezugriff. Login bleibt bei Deiner Bank.

Was wir sehen

- Saldo Deiner Konten.
- Umsatzhistorie (Datum, Betrag, Verwendungszweck).

- IBAN, BIC, Kontoinhaber-Name (so wie er bei der Bank hinterlegt ist).
- Bei Wertpapierdepots: ISIN, WKN, aktuelle Bestände.

Was wir nicht können

- Buchen, keine Überweisung, kein Lastschrift-Mandat.
- Daueraufträge anlegen oder ändern.
- Etwas an Deinen Bankdaten ändern (Adresse, Kontoinhaber, Limits).
- Auf andere Konten zugreifen, die Du nicht mit nobank verbunden hast.

Wo Dein Bank-Login eingegeben wird

Wichtig: Dein Bank-Login (PIN, TAN, Passwort) erreicht nobank **nie**. Wo Du ihn eingibst, hängt vom Verfahren ab, das Deine Bank unterstützt:

- XS2A (moderner EU-Standard nach PSD2): Du gibst PIN, TAN und Passwort direkt auf der Seite Deiner Bank ein. finAPI bekommt anschließend nur einen Lese-Token. Deine Logindaten verlassen die Bank-Seite nicht.
- finTS (älteres deutsches Verfahren, manche Banken nutzen es noch): Du gibst PIN und TAN bei finAPI ein. finAPI verwahrt sie verschlüsselt und authentifiziert sich damit gegenüber Deiner Bank.

In beiden Verfahren gilt: **nobank selbst sieht Deine Bank-Logindaten in keinem Fall.** Wir erhalten ausschließlich die über PSD2 freigegebenen Lese-Daten (Saldo, Umsätze), keine Zugangsdaten.

Wie Du den Zugang widerrufst

Du kannst die Verbindung jederzeit beenden, auf zwei Wegen:

- In der nobank-App unter Einstellungen das Konto entfernen.
- Bei Deiner Bank den finAPI-Zugang im Online-Banking widerrufen.

Ab diesem Zeitpunkt kann nobank keine neuen Daten mehr von Deiner Bank lesen. Bereits in der App angezeigte Daten bleiben in Deinem Account, bis Du den Account löschst (siehe FAQ „Wie lösche ich meine Daten?“.

Kapitel 2: Was macht ihr mit meinen Daten?

Kurze Antwort: **Wir werden nicht an Deinen Daten verdienen.** Heute verdienen wir gar nichts. Wir sind in der Beta. Später werden wir an Anbietern verdienen, nie an Dir.

Unser Geschäftsmodell: Phase 1 und Phase 2

nobank entwickelt sich in zwei Phasen. Heute (Phase 1, Beta) bekommst Du eine Uebersicht über Deine Konten, Verträge und Cashflows. Klarheit. Mehr nicht. In Phase 1 verdient nobank kein Geld. Wir bauen das Produkt mit Dir gemeinsam aus.

Später (Phase 2) kommt die Optimierungs-Komponente: Wir analysieren Deine Verträge und schlagen Dir bessere Konditionen vor: beim Strom, bei Versicherungen, beim Konto. Wenn Du Dich entscheidest zu wechseln, zahlt der neue Anbieter uns eine Vermittlungs-Provision. Du zahlst weiterhin nichts.

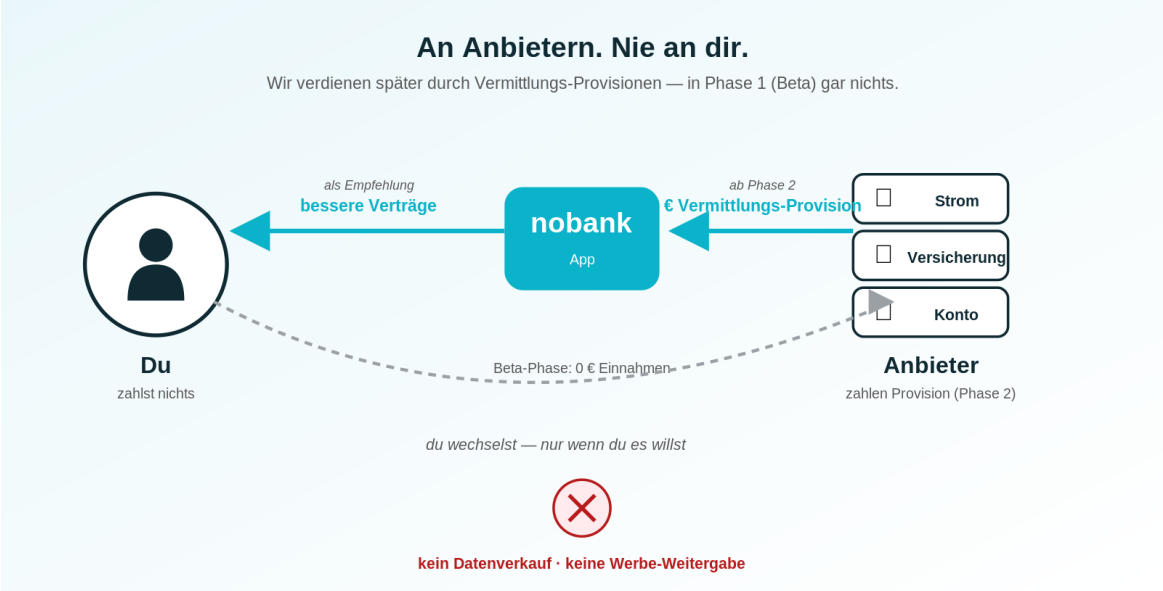

Schaubild 2: An Anbietern. Nie an Dir.

Was wir nicht tun und nicht tun werden

- Wir verkaufen Deine Daten nicht.
- Wir geben Deine Daten nicht an Werbe-Netzwerke weiter.
- Wir nutzen Deine Daten nicht für Profiling Dritter.
- Wir zeigen Dir keine Werbung in der App, die auf Deinen Bankdaten beruht.

Wer welche Daten sieht

Wir arbeiten mit einigen technischen Dienstleistern, weil wir nicht jede Komponente selbst bauen. Jeder davon hat eine spezifische Rolle und einen Auftragsverarbeitungsvertrag (AVV) mit uns:

- finAPI (Deutschland) — liest Deine Bankdaten über PSD2.
- Hetzner Online (Deutschland) — betreibt unsere Server.
- Supabase (EU-Region) — stellt unsere Datenbank- und Authentifizierungsplattform.
- Trigger.dev (selbstgehostet bei nobank): führt Hintergrund-Jobs aus (z.B. Sync-Vorgänge). Wird von uns selbst betrieben; keine Auftragsverarbeitung mit Drittlandbezug.
- PostHog (EU) — Produkt-Analytik, cookieless konfiguriert.
- Sentry (USA) — Fehler-Telemetrie, konfiguriert ohne standardmäßige Personenbezüge.
- Mailchimp (USA): Newsletter-Versand. Resend (USA): technische E-Mails (z.B. Registrierungs-Bestätigungen).

Wo Deine Daten liegen

Die Hauptdaten, also Dein Account, Deine Banktransaktionen, Deine Verträge) liegen in Rechenzentren in Deutschland (Hetzner) und der EU-Region von Supabase. Nicht in den USA.

Kapitel 3: Schauen die Gründer in mein Konto?

Kurze Antwort: **Niemand schaut mal eben rein.** Aber das ist eine Antwort in zwei Ebenen. Ich erkläre Dir beide, weil es nur so ehrlich ist.

> **Warum die Antwort zwei Ebenen hat**
>
> Eine pauschale Antwort wie "das geht technisch nicht" wäre bequem, aber nicht ehrlich. Es gibt zwei Ebenen, in denen überhaupt jemand auf eine Datenbank schauen könnte: den normalen App-Betrieb und den Wartungs-Betrieb. In beiden Ebenen haben wir Schutz, aber er funktioniert unterschiedlich.

Ebene 1: Im Alltag, technisch isoliert

Wenn Du Dich in der nobank-App einloggst und Deine Konten anschaust, dann sieht die App nur Deine eigenen Datensätze. Das wird technisch erzwungen durch einen Mechanismus namens Row-Level Security (RLS), den unsere Datenbank PostgreSQL beherrscht.

Konkret heißt das: Jeder Datensatz in der Datenbank ist mit Deiner Nutzer-Identität verknüpft. Die Datenbank-Rolle, mit der die App spricht, kann diesen Filter nicht umgehen. Sie hat weder Superuser- noch BYPASSRLS-Rechte. Selbst wenn ein Mitarbeiter wollte: Über die App kommt er nicht an fremde Daten.

Diese Ebene gilt für alle Lese- und Schreibzugriffe, die über die App oder die Schnittstelle laufen. Im Alltagsbetrieb sieht also wirklich nur Du Deine Konten.

Schaubild 3: Niemand schaut mal eben rein.

Ebene 2: Bei Wartung, organisatorisch gesichert

Es gibt einen zweiten Zugang zur Datenbank, der RLS umgehen kann: einen administrativen Service-Role-Key, beziehungsweise das Supabase-Dashboard. Den brauchen wir für drei Dinge:

- Wartungsarbeiten: Migrationen der Datenbankstruktur, Bug-Fixes, Datenrettung nach Störungen, Schnittstellen-Probleme.
- Erfüllung rechtlicher Verpflichtungen — etwa wenn ein Nutzer eine Auskunftsanfrage nach Art. 15 DSGVO stellt und wir alle gespeicherten Daten zusammenstellen müssen.
- Sicherheitsereignisse — etwa wenn wir einem Verdacht nachgehen müssen.

Dieser Zugang könnte technisch in alle Datensätze schauen. Genau deshalb haben wir vier Schutzmechanismen, die garantieren, dass das nicht routinemäßig oder aus Neugier passiert:

1. Berechtigungs-Konzept

Nicht jeder Mitarbeiter hat den administrativen Zugang. Es gibt eine kurze, schriftlich dokumentierte Liste mit klar definierten Rollen und Anlassbedingungen.

2. Genehmigungsprozess über Compliance/Datenschutz

Bevor jemand auf den administrativen Zugang zugreift, muss der Anlass dokumentiert werden, und je nach Sensitivität vom Compliance- oder Datenschutzverantwortlichen genehmigt werden. Vier-Augen-Prinzip.

3. Audit-Log: jeder Zugriff wird protokolliert

Jeder administrative Zugriff hinterlässt einen Eintrag, der nicht gelöscht werden kann. Mindest-Inhalt jedes Eintrags: Wer und wann. Im Berechtigungs-Konzept regeln wir zusätzlich, welche Daten betroffen waren und mit welchem Anlass der Zugriff erfolgte, sodass jeder Eintrag sich einem dokumentierten Vorgang zuordnen lässt.

4. Just-in-Time-Access (in Vorbereitung)

Der administrative Zugang soll perspektivisch nur für das aktuelle Anliegen erteilt und automatisch wieder entzogen werden, als Just-in-Time-Access. Aktuell ist dieser Mechanismus in Vorbereitung; die organisatorische Absicherung erfolgt heute über die Punkte 1 bis 3 (Berechtigungs-Konzept, Genehmigungsprozess, Audit-Log).

Was passiert, wenn jemand böswillig zugreift

Wenn ein Mitarbeiter trotz der Schutzmechanismen unrechtmäßig auf Daten zugreift, ist das eine Datenpanne im Sinne von Art. 33 DSGVO. Wir haben dann die Pflicht, das innerhalb von 72 Stunden an die Datenschutz-Aufsicht (BayLDA) zu melden und gegebenenfalls auch Dich als Betroffenen zu informieren. Strafrechtlich greift § 42 BDSG (unbefugte Datenübermittlung). Aufsichtsrechtlich kommen Bußgelder nach Art. 83 DSGVO und Schadensersatzansprüche nach Art. 82 DSGVO hinzu. Das ist kein theoretischer Hinweis. Die Audit-Logs machen solche Zugriffe nachweisbar.

Wer überprüft das

- Externer Datenschutzbeauftragter: Rechtsanwalt Andreas Riehn, München, unabhängig von der Geschäftsführung.
- Datenschutz-Aufsicht: Bayerisches Landesamt für Datenschutzaufsicht (BayLDA).
- Compliance intern: Dirk Biering. Schreib mir direkt, wenn Du Fragen hast.

Die Linie

> **Niemand schaut mal eben rein.**
>
> Im Alltag isoliert die Datenbank Deine Daten technisch. Für Wartung gibt es einen separaten Zugang. Der ist berechtigt, genehmigt, protokolliert und zeitlich begrenzt. Jeder Zugriff hat einen dokumentierten Anlass und hinterlässt eine Spur.

Kapitel 4: FAQ

Was, wenn ihr gehackt werdet?

Wir verschlüsseln Daten in der Datenbank, trennen sie technisch nach Nutzern (RLS) und betreiben unsere Server in der EU. Vor allem: Deine Bank-Login-Daten haben wir nie. Bei einem Vorfall würden wir die Datenpannen-Meldepflicht nach Art. 33 DSGVO erfüllen (72-Stunden-Frist) und betroffene Nutzer informieren. Den Bank-Token kannst Du jederzeit bei Deiner Bank widerrufen; dann ist der Zugriff weg, unabhängig von uns.

Was, wenn ihr pleitegeht?

Dein Lese-Zugriff über finAPI ist nicht an unsere Existenz gebunden, er liegt zwischen finAPI und Deiner Bank. Wenn nobank ausfällt, erlischt der Zugang automatisch, spätestens nach Ablauf der gesetzlich geregelten Token-Gültigkeit (max. 180 Tage Inaktivität nach PSD2). Du kannst den Zugang aber jederzeit selbst bei Deiner Bank widerrufen. Ab diesem Moment kann nobank keine neuen Daten mehr lesen. Deine Bank ist davon nicht betroffen. Solltest Du in der App ein Konto löschen wollen, ist die Account-Löschung implementiert; in seltenen Fällen kann eine technische Nachsynchronisation mit unserem Bankdaten-Dienstleister nötig sein. Der DSB ist direkt erreichbar.

Wie lösche ich meine Daten?

In der nobank-App findest Du in den Einstellungen die Option "Account löschen". Damit werden alle personenbezogenen Daten zu Deinem Account gelöscht. Wir behalten ausschließlich, was wir aus rechtlichen Gründen behalten müssen, etwa handelsrechtliche Aufbewahrung von Rechnungen, soweit zutreffend. In der Beta-Phase fallen für Dich als Tester typischerweise keine solchen Aufbewahrungspflichten an. Falls doch, wird das nach Ablauf der gesetzlichen Frist automatisch gelöscht. Du kannst zusätzlich jederzeit eine Löschung per Mail an den DSB anfordern.

Welche Daten teilt ihr mit Sentry, PostHog, Mailchimp, Resend?

Sentry erhält Fehler-Telemetrie. Wir konfigurieren Sentry so, dass keine personenbezogenen Daten standardmäßig übertragen werden. Restbestände in Stack-Traces aus dem Frontend können wir nicht vollständig ausschließen, deshalb prüfen wir die Sentry-Daten regelmäßig. PostHog erhält aggregierte, cookieless Nutzungsdaten, keine individuellen Profile. Mailchimp erhält Deine E-Mail-Adresse für Newsletter-Versand, sofern Du abonniert hast. Resend versendet technische E-Mails (z.B. Registrierungs-Bestätigungen). Bei US-Anbietern sind Drittland-Transfers mit Standardvertragsklauseln und dem EU-US Data Privacy Framework abgesichert. Details in der Datenschutzerklärung auf der Website.

Wie lange werden meine Daten gespeichert?

Solange Du Nutzer bist und solange wir die Daten zur Bereitstellung der App brauchen. Nach einer Löschung gelten gesetzliche Aufbewahrungsfristen, soweit anwendbar (z.B. GwG/HGB).

Eine detaillierte Speicherdauer-Tabelle pro Datenkategorie findest Du in der Datenschutzerklärung.

Was, wenn ich nur ausprobieren will?

Klar. Du kannst Dein Konto in drei Minuten verbinden, alles ansehen, und in der App genauso schnell wieder löschen. Es gibt keinen Vertrag, der Dich bindet, und keine Probezeit, die abläuft.

Wer haftet, wenn etwas passiert?

Die nobank Finanzoptimierung GmbH (Sitz München, Amtsgericht München HRB 306852) als Anbieter. finAPI ist von der BaFin als Kontoinformationsdienstleister nach § 1 Abs. 33 ZAG registriert, damit gelten ZAG- und PSD2-Pflichten zu Sicherheit, Transparenz und Aufsicht. Bei grober Fahrlässigkeit oder Vorsatz greifen über DSGVO und BDSG Schadensersatzansprüche. Ausgewogene Haftungsregeln stehen in den AGB.

Wie kontaktiere ich den Datenschutzbeauftragten direkt?

Per E-Mail an die Adresse, die im Impressum unter "Datenschutzbeauftragter" hinterlegt ist. Der DSB ist nicht weisungsgebunden gegenüber der Geschäftsführung.

Was hat die BaFin damit zu tun?

Die BaFin hat finAPI (unseren Bankdaten-Dienstleister) als Kontoinformationsdienstleister nach § 1 Abs. 33 ZAG registriert. Damit greifen Sicherheits-, Transparenz- und Aufsichtspflichten nach ZAG und PSD2. nobank selbst ist kein BaFin-reguliertes Institut. Wir nutzen lediglich die regulierten Schnittstellen von finAPI.

Schluss: Was hier nicht steht

Ein Whitepaper kann nicht alles abdecken. Drei Hinweise zum Schluss:

Was wir noch verbessern werden

Sicherheit ist ein laufender Prozess. Wir arbeiten kontinuierlich an Verbesserungen: bei der Verschlüsselung, den Zugriffsmechanismen, der Belastbarkeit unserer Backups. Wenn Du dazu konkrete Fragen hast, schreib mir.

Wo dieses Whitepaper aktualisiert wird

Aktuelle Version: 1.5 vom 12.05.2026. Bei Änderungen versionieren wir nach oben. Die jeweils aktuelle Version steht auf der Website unter Datenschutz / Whitepaper.

Direktkontakt

- Allgemeine Fragen: support@nobank.app
- Datenschutz / DSB: datenschutz@nobank.app
- Compliance / Dirk: compliance@nobank.app

Hinweis: Mail-Adressen oben sind Platzhalter. Die finalen Adressen findest Du im Impressum.

Glossar

PSD2
EU-Richtlinie 2015/2366 (Payment Services Directive 2). Schafft den rechtlichen Rahmen für den Drittparteien-Zugriff auf Bankdaten, unter anderem Lese-Zugriff durch lizenzierte Kontoinformationsdienste.

AISP
Account Information Service Provider, Kontoinformationsdienst im Sinne von Art. 67 PSD2. finAPI ist von der BaFin als AISP zugelassen.

PISP
Payment Initiation Service Provider, Zahlungsauslösedienst nach Art. 66 PSD2. Diese Lizenz erlaubt, Zahlungen im Namen des Kontoinhabers auszulösen. finAPI nutzt für nobank diesen Dienst nicht.

CBPII
Card-Based Payment Instrument Issuer, Bestätigungsdienst über die Verfügbarkeit eines Geldbetrags nach Art. 65 PSD2. Für Kartenherausgeber relevant. Bei nobank nicht im Einsatz.

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht. Zuständige Aufsicht u.a. für Banken, Zahlungsinstitute, Wertpapierdienstleister und Kontoinformationsdienstleister in Deutschland. Reguliert finAPI (als AISP), nicht nobank.

BayLDA
Bayerisches Landesamt für Datenschutzaufsicht. Zuständige Datenschutzaufsicht für Unternehmen mit Sitz in Bayern (also auch nobank).

Row-Level Security (RLS)
Mechanismus in PostgreSQL, der pro Datensatz einen Filter erzwingt, sodass die App nur Datensätze des eingeloggten Nutzers ausliefern. Auch privilegierte App-Rollen können RLS nicht umgehen, wenn sie keine Bypass-Rechte haben.

Service-Role-Key
Administrativer Datenbank-Zugriff, der RLS umgehen kann. Wird für Wartung gebraucht. Bei nobank durch Berechtigungs-Konzept, Genehmigungsprozess und Audit-Log organisatorisch gesichert. Ein Just-in-Time-Access-Mechanismus ist in Vorbereitung.

Just-in-Time-Access
Zugriffsmodell, bei dem privilegierter Zugang nur für das aktuelle Anliegen erteilt und nach Erledigung automatisch entzogen wird (kein Dauer-Zugang). Bei nobank in Vorbereitung.

DPF / Data Privacy Framework

Rechtsrahmen für Datenübertragungen zwischen EU und USA. Löst das früher genutzte Privacy Shield ab. Ergänzt durch Standardvertragsklauseln (SCCs).

SCA / Strong Customer Authentication

Starke Kundenauthentifizierung nach PSD2, typischerweise Zwei-Faktor-Bestätigung beim Bank-Login. Bei XS2A direkt auf der Seite Deiner Bank, bei finTS über den lizenzierten Kontoinformationsdienst finAPI. In keinem Fall bei nobank.

XS2A

EU-weit standardisierte Schnittstelle nach PSD2 für den Drittparteien-Zugriff auf Konten. Login findet direkt bei der Bank statt; der Kontoinformationsdienst (z.B. finAPI) erhält nur einen Lese-Token.

finTS

Aelteres deutsches Verfahren für den Bankdaten-Austausch (Financial Transaction Services). PIN/TAN werden beim lizenzierten Kontoinformationsdienst (z.B. finAPI) eingegeben und dort verschlüsselt verwahrt — nicht bei nobank.

Quellen

- EU-Richtlinie 2015/2366 (PSD2).
- DSGVO (EU-Verordnung 2016/679) — insbesondere Art. 13, 15, 30, 32, 33, 35.
- Bundesdatenschutzgesetz (BDSG) — insbesondere § 42 BDSG.
- Zahlungsdiensteaufsichtsgesetz (ZAG).
- BaFin-Lizenzregister (Eintrag finAPI als Kontoinformationsdienst).
- nobank Datenschutzerklärung (auf der Website).
- nobank AGB (auf der Website).
- nobank Impressum (auf der Website).