Celeris, by Apeyron

Privacy Policy

Effective date: 11 July 2026

Contents

Introduction

Apeyron (**“Apeyron”**, **“we”**, **“us”**, or **“our”**) operates a business-to-business platform for the settlement of international trade transactions. Our platform lets importers and exporters transact using blockchain-backed escrow and tokenised trade documents, with payment and document transfer settled atomically (**Delivery-versus-Payment**). Fiat currency conversion is always carried out by **licensed third-party partners** — Apeyron itself never holds, receives, or transmits fiat currency, and never controls or holds the private keys to your wallet.

This policy explains what personal data we collect, why we collect it, who we share it with, how long we keep it, and the rights you have. It applies to your use of our website, applications, and services (together, the **“Services”**).

Because our Services are offered across many jurisdictions, this policy is organised into a general section followed by **regional schedules**. Please read the general section together with the schedule that applies to where you are:

- **Schedule 1 —** European Economic Area (EEA) and United Kingdom (UK)
- **Schedule 2 —** United States
- **Schedule 3 —** South Africa
- **Schedule 4 —** Rest of the World

Where a regional schedule conflicts with the general section, the schedule prevails for residents of that region.

1. A note on our architecture (why we hold less than you might expect)

Two design choices shape everything in this policy:

1. **We are non-custodial.** Your funds sit in a user-owned wallet secured by a third-party wallet provider. **Apeyron never holds your private keys and can never move your funds on its own.** When you authorise an on-chain action, you sign it yourself; we only relay that signed instruction. We are never an owner, co-signer, or session-signer on your wallet.
2. **We never touch fiat.** Converting money to or from stablecoins (funding your wallet or cashing out) is performed entirely by **licensed on-ramp and off-ramp partners** — Apeyron never holds, receives, or transmits your fiat funds. As part of identity and business verification (KYC/KYB), we and our verification providers may collect and process certain **banking information you provide** (for example, a bank account or a bank statement used to confirm your address or source of funds). For the actual funding and payout, your bank details are used by the licensed partner; we hold a reference linking your account to that partner.

A consequence of using blockchain is that some information is **public and permanent** — see Section 5.

2. The personal data we collect

The data we collect depends on how you use the Services. Categories may include:

- **Identity data** — first name, surname, username, date of birth, and government identifiers you provide during identity verification.

- **Contact data** — email address and, where provided, postal address and telephone number.
- **Account and credential data** — your username and a securely hashed password.
- **KYC / verification data** — proof of identity and address, and the outcome/status of identity and sanctions checks. Verification documents are typically collected and processed **by our identity-verification provider** on our behalf.
- **Financial / banking data** — bank account or payment details you provide, and banking information contained in documents you submit for verification (such as a bank statement). Collected for verification and compliance; the movement of fiat is performed by our licensed partners, not by Apeyron.
- **Wallet data** — the public blockchain address(es) you register and any labels you assign them. (We do **not** hold your private keys.)
- **Transaction and trade data** — deals you create, your role (importer or exporter), your trade counterparty, escrow and settlement records, and on-chain references to tokenised documents.
- **Trade document data** — Bills of Lading, invoices, and related documents you upload, and their metadata (file name, storage reference). These may contain personal and commercial information about you and third parties.
- **Partner-reference data** — an identifier that maps your account to a licensed on/off-ramp partner so funding and redemption can be orchestrated.
- **Technical and usage data** — IP address, browser and device information, time-zone and language settings, and how you interact with the Services.
- **Communications data** — messages you send us, including via contact or support forms.

We may also receive data about you from **third parties**, including identity-verification and sanctions-screening providers, our licensed fiat on/off-ramp partners, our wallet and blockchain infrastructure providers, and analytics providers.

We do not seek to collect special-category / sensitive data beyond what is strictly necessary for identity verification and legal compliance; where we do, we apply additional safeguards and rely on an appropriate legal basis.

3. How and why we use your data

We use your personal data to:

- **Provide the Services** — create and secure your account, register wallets, create and settle deals, and store and tokenise trade documents.
- **Verify your identity and prevent financial crime** — perform KYC, sanctions, and fraud checks, and meet anti-money-laundering (AML) and counter-terrorist-financing obligations.
- **Orchestrate funding and redemption** — pass the necessary references to licensed on/off-ramp partners so you can move between fiat and stablecoins (a service the partners perform).
- **Meet trade, customs, and exchange-control obligations** — where required, make trade and settlement documentation available so that regulated partners can fulfil their reporting duties (for example, export-proceeds and balance-of-payments reporting).
- **Assess creditworthiness and offer financing — from day one** we collect and retain your trade, transaction, and settlement history. We intend to analyse this history to build a **credit profile or credit score** for your business, in order to offer **trade financing and related credit products.** This involves **profiling.** We collect this data now, but we are not yet making automated credit decisions or offering financing; before we launch any such product we will update this policy,

confirm the legal basis we rely on (see Section 4), and give you the information and choices the law requires — including, where applicable, the right to object and safeguards around any automated decision-making.

- **Secure and improve the platform** — monitor for abuse, debug, and develop our Services.
- **Communicate with you** — respond to enquiries, send service messages, and (where permitted) send marketing you can opt out of at any time.
- **Comply with law** — respond to lawful requests from regulators, courts, and authorities.

Where a deal involves a counterparty, please note that **some of your data is necessarily shared with that counterparty** — for example your identity, wallet address, and the trade documents relevant to the deal. This is inherent to completing a trade settlement.

4. Legal bases for processing (where applicable)

Where data-protection law requires a legal basis (e.g. in the EEA, UK, and South Africa), we rely on:

- **Performance of a contract** — to deliver the Services you request.
- **Compliance with legal obligations** — including AML/KYC, sanctions, tax, and trade/exchange-control requirements.
- **Legitimate interests** — to secure the platform, prevent fraud, and improve our Services, balanced against your rights.
- **Consent** — for optional processing such as marketing; you may withdraw consent at any time without affecting prior processing.

For the **planned credit-scoring and financing** use described in Section 3, we expect to rely on our **legitimate interests** and/or your **consent**, and — where credit or financing products are regulated — on **compliance with legal obligations.** We will confirm the precise basis, and any additional safeguards for profiling or automated decisions, before this processing begins.

5. Blockchain data is public and permanent

Certain information is recorded on a **public blockchain** to make settlement work. This can include wallet addresses, token identifiers for tokenised documents, and escrow and settlement transaction records. By design, blockchain records are **immutable and publicly visible**, and they are **not controlled by Apeyron.**

This means that, for on-chain data, we **cannot** edit, delete, or restrict processing on your request, because no single party can alter the blockchain. Your rights (Section 8) still apply to the off-chain data we hold, but they are **technically limited for on-chain data.** Please keep this in mind before recording information on-chain.

Uploaded document **files** themselves are stored **off-chain** (in encrypted cloud storage); only references/metadata are tokenised on-chain.

6. Who we share your data with

We share personal data only as needed to run the Services and meet our obligations, including with:

- **Wallet and blockchain infrastructure providers** — to enable non-custodial wallets and relay your signed transactions.
- **Identity-verification and sanctions-screening providers** — to perform KYC/AML checks.
- **Licensed fiat on-ramp and off-ramp partners** — to enable funding and redemption; these partners are independent controllers of the data you provide to them.
- **Cloud hosting and storage providers** — to host the platform and store documents securely.
- **Your trade counterparty** — as described in Section 3.
- **Analytics and communications providers** — to operate and improve our website and communications.
- **Professional advisers, auditors, and insurers.**
- **Regulators, authorities, and law enforcement** — where legally required, or to protect our rights, users, or the public.
- **A successor entity** — in connection with a merger, acquisition, or asset sale.

We require third parties that process data on our behalf to protect it and use it only as instructed.

7. International data transfers

Because we and our partners operate globally, your data may be transferred to and processed in countries other than your own, whose laws may differ. Where required, we put appropriate safeguards in place — such as **Standard Contractual Clauses**, the **UK International Data Transfer Agreement/Addendum**, or reliance on an **adequacy decision** — before transferring personal data internationally. You may request more information using the contact details below.

8. Data retention

We keep personal data only as long as necessary for the purposes it was collected for, or as required by law. In general:

- **KYC / AML records** — retained for at least the minimum statutory period after the end of our relationship (commonly **five years**, or longer where the law requires).
- **Account and transaction records** — retained for the life of your account and for any legally required period thereafter.
- **On-chain records** — permanent and immutable, as explained in Section 5.
- **Other data** — retained per business need and legal obligation, then deleted, anonymised, or pseudonymised.

9. How we protect your data

We apply security measures appropriate to the risk, including:

- **Non-custodial design** — we never hold your private keys, so we cannot move your funds.
- **Encryption** — data in transit is protected with TLS; documents at rest are held in encrypted storage.
- **Access controls** — access to personal data is restricted, logged, and monitored.
- **Screening and monitoring** — automated checks help us detect fraud and suspicious activity.

No method of transmission or storage is completely secure, and we cannot guarantee absolute security. You are responsible for keeping your login credentials and wallet recovery information confidential.

10. Cookies

We use cookies and similar technologies that are **strictly necessary** for the Services (for example, to keep you securely signed in). Where required by law, we ask for your consent before using non-essential cookies, such as analytics. You can control cookies through your browser settings; disabling some cookies may affect how the Services work.

11. Children

Our Services are intended for businesses and are **not directed to anyone under 18.** We do not knowingly collect data from children.

12. Your rights

Subject to the law where you live, you may have rights to: access your data; correct inaccurate data; request erasure; restrict or object to processing; request portability; and withdraw consent. You also have the right to complain to your data-protection authority.

To exercise any right, contact us using the details below. We will respond within the period required by applicable law. **Note:** as explained in Section 5, these rights are technically limited for data recorded on a public blockchain.

13. Changes to this policy

We may update this policy from time to time to reflect changes in our Services, our practices, or the law. We will post any changes on this page and, where appropriate, notify you. The “Effective date” at the top shows when the current version took effect.

14. Contact us

For any privacy question or to exercise your rights, email us at privacy@apeyron.io.

If you are not satisfied with our response, you may contact the relevant supervisory authority for your region (see the applicable schedule below).

Schedule 1 — European Economic Area (EEA) & United Kingdom (UK)

This schedule applies if you are in the EEA or the UK and supplements the general policy.

- **Controller & legal bases:** we act as controller and rely on the legal bases in Section 4.
- **Your GDPR rights:** access, rectification, erasure, restriction, objection, portability, and withdrawal of consent, as set out in the EU GDPR and UK GDPR — subject to the on-chain limitation in Section 5.
- **Response time:** we aim to respond within **one month**, extendable by two further months for complex or numerous requests, and will tell you if an extension applies.
- **International transfers:** safeguarded as described in Section 7 (SCCs / UK IDTA / adequacy).
- **Complaints:** you may complain to your local supervisory authority — for example, your national Data Protection Authority in the EEA, or the **Information Commissioner's Office (ICO)** in the UK.

Schedule 2 — United States

This schedule applies if you are a US resident and supplements the general policy.

California (CCPA/CPRA). California residents have the right to know what personal information we collect and why; to access, correct, and delete it (subject to exceptions); to opt out of any "sale" or "sharing" of personal information and of cross-context behavioural advertising; to limit the use of sensitive personal information; and not to be discriminated against for exercising these rights. We do not sell personal information for money.

Other states (e.g. Colorado, Connecticut, Utah, Virginia, and others as applicable). Residents of these states have comparable rights to access, correct, delete, and obtain a copy of their personal data, and to opt out of targeted advertising, sale, and certain profiling.

"Do Not Track." Because there is no common industry standard for browser Do-Not-Track signals, our Services do not currently respond to them.

Exercising rights. Use the contact details in Section 14. We will verify your identity before responding and will respond within the timeframe the law requires.

Schedule 3 — South Africa

This schedule applies if you are in South Africa and supplements the general policy. It reflects the **Protection of Personal Information Act, 2013 (POPIA).**

- **Responsible party:** Apeyron (or its local partner, where applicable) acts as the "responsible party" for your personal information.
- **Your rights under POPIA:** to be notified that your information is collected; to access the information we hold; to request correction or deletion; to object to processing; and to complain to the Regulator.
- **Trade-settlement context:** if you are an exporter, trade and settlement documentation may be processed and shared with licensed partners and their **Authorised Dealer** banks so that the fiat inflow can be reported to the authorities as required (for example, export-proceeds and balance-of-payments reporting under South African exchange-control rules). This is done to comply with legal obligations.

- **Complaints:** you may complain to the **Information Regulator (South Africa).**

Schedule 4 — Rest of the World

This schedule applies if you are in a jurisdiction not covered by Schedules 1–3 — including the other markets in which we operate at launch.

Regardless of where you are, we apply a **baseline standard of protection**, giving you the ability to:

- request **access** to the personal data we hold about you;
- request **correction** of inaccurate data and, where appropriate, **deletion**;
- **object to** or ask us to **restrict** certain processing; and
- request a **portable copy** of your data.

We handle your data in line with the laws applicable to your jurisdiction and the general policy above. Where your country imposes specific requirements (for example, export-proceeds repatriation or foreign-exchange reporting), we and our licensed partners process the necessary trade and settlement data to help meet those obligations. To exercise any right, or to find out which local authority you may complain to, contact us using the details in Section 14.