Crown

Privacy Notice

Crown

TECHNICAL SHEET

Last Updated: March 23, 2026

CONTROLLER: Crown Sociedade Prestadora de Ativos Virtuais Ltda. (CNPJ: 59.386.340/0001-45) **(“Crown”)**

REGISTERED ADDRESS: Av. Rebouças 2748, conj. 111, Pinheiros, CEP 05402-500

DPO: dpo@crown-brlv.com **| Compliance:** compliance@crown.finance

Crown

Your privacy is our responsibility.

Crown is a Virtual Asset Service Provider (VASP / PSAV / SPSAV) under Law No. 14,478/2022, regulated by Resolutions BCB No. 455/2023 and No. 519, 520 and 521/2025. Our platform enables you to buy, sell, custody and transfer virtual assets, and to conduct foreign exchange operations.

To deliver these services securely and in compliance with applicable law, we need to collect and process certain data about you. This Notice explains what data we collect, what we use it for, who we share it with, how long we are required to keep it, and what your rights are.

Important: some data we collect is required by law — as a regulated VASP, we have no choice but to process it. Other processing activities are optional and depend on your consent. This Notice clearly distinguishes between the two.

Minors: Crown does not provide services to persons under 18 years of age. If we identify that data of a minor has been collected without proper authorisation, it will be deleted immediately. Please contact dpo@crown-brlv.com.

A note for international clients — Understanding Brazil's regulatory framework

If you are based outside Brazil, some of the regulations referenced throughout this Notice may be unfamiliar. This section provides a plain-language overview of the key frameworks that govern how Crown handles your data, and why they apply to you as a Crown client regardless of where you are located

Brazilian data protection law — the LGPD

Brazil's General Data Protection Law — known as the LGPD (Lei Geral de Proteção de Dados Pessoais, Law No. 13,709/2018) — is Brazil's comprehensive data protection framework. It governs the processing of personal data of any individual whose data is collected or processed in Brazil, or whose data is processed by a Brazilian company, regardless of where the individual is located. If you are a Crown client, the LGPD applies to you.

The LGPD is broadly comparable to the European General Data Protection Regulation (GDPR) in its structure and principles. It requires that personal data be processed with a specific legal basis, for defined purposes, with transparency, and only for as long as necessary. It grants data

subjects a comprehensive set of rights — including access, correction, deletion and portability — and establishes the National Data Protection Authority (ANPD) as the supervisory body with power to investigate complaints and impose fines of up to 2% of annual revenue, capped at BRL 50 million per violation.

One important difference from the GDPR: the LGPD places greater emphasis on legitimate interests and legal obligation as bases for processing, and somewhat less emphasis on consent. This is relevant for Crown because most of the data we collect is processed on the basis of legal obligation — not consent — due to the regulated nature of our business.

Virtual asset regulation — the Brazilian VASP framework

Brazil enacted Law No. 14,478/2022 (the Virtual Assets Framework Law), which formally recognised virtual asset service providers as regulated entities subject to oversight by the Central Bank of Brazil (Banco Central do Brasil — BCB). This was followed by a series of regulations issued by the BCB, culminating in Resolutions BCB No. 519, 520 and 521, published in November 2025 and in force since 2 February 2026.

Under this framework, virtual asset service providers operating in Brazil are classified as SPSAVs (Sociedades Prestadoras de Serviços de Ativos Virtuais) and are subject to requirements equivalent to those applicable to traditional financial institutions — including governance standards, minimum capital requirements, internal controls, cybersecurity policies, and full AML/CFT compliance. Crown is in the process of obtaining formal authorisation under this framework.

The practical consequence for you as a client is that Crown operates under the same level of regulatory scrutiny as a bank or payment institution. This means we are legally required to verify your identity, monitor transactions, report to authorities, and retain records — often for periods far longer than you might expect from a technology company.

Anti-money laundering obligations — why we ask for so much information

Brazil's AML/CFT framework is based on Law No. 9,613/1998 and implemented for virtual asset providers through Circular BCB No. 3,978/2020 (as amended). These rules require Crown to identify every client, understand the origin of funds, monitor transaction patterns, and report suspicious activity to COAF — Brazil's Financial Intelligence Unit, equivalent to FinCEN in the United States or the NCA in the United Kingdom.

The FATF (Financial Action Task Force) — the international standard-setter for AML/CFT — has designated virtual asset service providers as obligated entities globally. Crown applies FATF

standards, including Recommendation 16 (the Travel Rule), which requires the exchange of originator and beneficiary information in virtual asset transfers above certain thresholds. This is why, when you send or receive virtual assets, we may collect and share information about you with the counterparty's service provider.

Data retention — why we keep your data for 10 years

The 10-year minimum retention period that appears throughout this Notice is not a business decision — it is a legal requirement imposed by multiple converging obligations: AML/CFT record-keeping rules (Circular BCB No. 3,978/2020), virtual asset regulation (Resolution BCB No. 455/2023), Federal Revenue Service reporting obligations (Tax Authority IN No. 1,888/2019) and Brazil's general limitation period for civil claims (Civil Code, art. 205). These rules exist because regulators and courts may need to reconstruct the history of transactions years after they occurred.

This 10-year period applies even after you close your account. It is not negotiable and cannot be waived by you or by Crown. Any request for deletion of data subject to these retention obligations will be declined until the applicable period has expired.

The Central Bank of Brazil and the ANPD

Crown is supervised by two principal authorities. The Central Bank of Brazil (BCB) supervises Crown's activities as a virtual asset service provider and foreign exchange operator, with powers to authorise, inspect and sanction. The National Data Protection Authority (ANPD) supervises Crown's compliance with the LGPD and handles data subject complaints. Both authorities have jurisdiction over Crown's activities involving your personal data, and both may receive reports, conduct investigations and impose penalties in their respective areas of competence.

As a data subject, you have the right to file a complaint with the ANPD at gov.br/anpd. The ANPD accepts complaints in Portuguese; if you require assistance, Crown's DPO at dpo@crown-brlv.com can help you understand the process.

1. What Data We Collect

1.1 Registration and identity verification (KYC / KYB / KYP)

To open and maintain your account, we collect:

- full name, CPF or CNPJ, date of birth, nationality and address;
- email address, telephone number and identity documents (national ID, driver's licence or equivalent);
- professional, corporate and financial information, as required by anti-money laundering regulations; and
- data relating to legal representatives, officers and ultimate beneficial owners (UBOs), where applicable.

Legal basis: legal obligation (LGPD art. 7, II) — required by Resolution BCB No. 455/2023, Resolution BCB No. 520/2025 and Circular BCB No. 3,978/2020.

1.2 Biometric data — Sensitive Personal Data

> **Note:** your selfie and facial recognition data are classified as Sensitive Personal Data under LGPD art. 5, II. They receive heightened legal protection and are processed under specific legal bases.

We collect selfie images and facial recognition data exclusively for identity verification and fraud prevention during account registration and authentication.

Legal basis: legal obligation (LGPD art. 11, II, 'a') and fraud prevention and data subject security (art. 11, II, 'g') — required by Resolution BCB No. 455/2023.

Retention: for the period required by the purpose; deleted upon termination of the contractual relationship, subject to applicable legal retention periods.

1.3 Operational data

To execute your orders and maintain your operation history, we collect:

- transaction data: type, value, date, asset involved and counterparties;
- digital wallet addresses (including self-custodied wallets) and on-chain identifiers;
- banking information required for BRL deposits and withdrawals; and
- source and destination of funds data, required for AML/CFT compliance and the Travel Rule.

Self-custodied wallet identification (Resolution BCB No. 521/2025): when a transaction involves a transfer to or from a wallet that is not held at a regulated VASP — known as a self-custodied or unhosted wallet — Resolution BCB No. 521/2025 requires Crown to identify the owner of that wallet and document the origin and destination of the assets involved. This means

we may ask you to provide evidence of ownership of the external wallet, including a signed message or declaration, before the transaction can proceed. This data is collected under legal obligation (LGPD art. 7, II).

Legal basis (general): performance of contract (LGPD art. 7, V) and legal obligation (art. 7, II) — including Tax Authority IN No. 1,888/2019, Resolution BCB No. 455/2023 and Resolution BCB No. 521/2025.

1.4 Sanctions screening

Crown is required to screen all clients, counterparties and transaction parties against international sanctions lists and watchlists, under Resolution BCB No. 44/2020 and Law No. 13,810/2019 (which implements UN Security Council resolutions in Brazil). This processing involves:

- name and identifier matching against OFAC, UN, EU and Brazilian government sanctions lists;
- adverse media and reputational screening; and
- ongoing monitoring throughout the client relationship.

Legal basis: legal obligation (LGPD art. 7, II) — Resolution BCB No. 44/2020; Law No. 13,810/2019.

Retention: minimum 10 years after the end of the relationship, consistent with general AML/CFT obligations.

1.5 Technical access data

We automatically collect technical browsing and access data:

- IP address, device identifiers and browser type;
- access date and time, pages visited and authentication records; and
- security events and audit trails.

Legal basis: legal obligation (LGPD art. 7, II) and legitimate interests (art. 7, IX) — required by cybersecurity regulations (Resolutions BCB No. 85/2021 and No. 538/2025) and the Marco Civil da Internet (Law No. 12,965/2014).

2. Who We Share Your Data With

We share your data only when strictly necessary and always on the basis of an adequate legal ground. The categories of recipients are:

- **Infrastructure and security providers:** cloud computing companies (such as AWS and GCP) and MPC custody specialists. These providers act as Processors with data protection agreements. Where servers are located outside Brazil, transfers are covered by the Standard Contractual Clauses (SCCs) approved by the ANPD under Resolution CD/ANPD No. 19/2024.
- **Financial and foreign exchange partners:** institutions involved in the settlement of your foreign exchange and transfer operations, as required by Resolution BCB No. 277/2022 and Resolution BCB No. 521/2025.
- **Regulated counterparties (Travel Rule; FATF R.16):** for virtual asset transfers at or above the equivalent of BRL 5,000 or USD/EUR 1,000 (or the threshold set by the applicable FATF Recommendation/applicable Regulation), Crown is required to collect and transmit originator and beneficiary information to the receiving VASP. Where the counterparty VASP is located in a jurisdiction that does not have data protection standards equivalent to Brazil's, Crown will apply additional contractual and technical safeguards, including SCCs under Resolution CD/ANPD No. 19/2024, to protect the data in transit.
- **Competent authorities:** Central Bank of Brazil, Federal Revenue Service, COAF, CVM and other regulatory, judicial or law enforcement bodies, whenever required by law or valid order.

3. Data Retention Schedule

As a Virtual Asset Service Provider regulated by the Central Bank of Brazil, Crown is subject to mandatory data retention obligations that are independent of your wishes or ours. This is not a choice: the law prohibits us from deleting these records before the applicable period has elapsed.

> **Legal obligation to retain data for 10 years**

Crown

Your registration, KYC/KYB, suitability and transaction records must be kept for a minimum of 10 (ten) years after the termination of the contractual relationship. This period is imposed by anti-money laundering regulations (Circular BCB No. 3,978/2020), virtual asset regulation (Resolution BCB No. 455/2023) and Federal Revenue Service reporting rules (Tax Authority IN No. 1,888/2019). Even if you close your account, these records will remain stored throughout this entire period.

Direct consequence: while this period is running, requests for deletion of these data categories cannot be fulfilled.

Data category	Minimum period	Regulatory basis (legal obligation)
Registration and KYC/KYB/KYP data	**10 years after termination**	Circular BCB No. 3,978/2020; Civil Code art. 205 (subsidiary)
Suitability and risk profile data	**10 years**	Circular BCB No. 3,978/2020
Virtual asset transaction records	**10 years**	Tax Authority IN No. 1,888/2019; Circular BCB No. 3,978/2020
Foreign exchange operation data	**10 years**	Res. BCB No. 277/2022; Res. BCB No. 521/2025; Circular BCB No. 3,978/2020
Sanctions screening records	**10 years**	Res. BCB No. 44/2020; Law No. 13,810/2019; Circular BCB No. 3,978/2020
Biometric data (Sensitive Personal Data)	Period necessary for the purpose; deleted after the end of the relationship.	LGPD art. 11 e 16
Authentication and security logs	5 years	Res. BCB No. 85/2021 and No. 538/2025; Marco Civil da Internet, arts. 13 and 15
Security incident records	5 years from date of record	Res. CD/ANPD No. 15/2024, art. 10
Marketing data (consent-based)	Until withdrawal or 24 months, whichever is earlier	LGPD art. 7, I and art. 8, §5

After the applicable periods expire and there is no remaining legal basis for retention, your data is deleted, anonymised or placed in blocked format according to the nature of the information.

4. Your Rights (LGPD)

Under the LGPD (arts. 17 to 22), you have the following rights. You also have the right to file a complaint directly with the National Data Protection Authority (ANPD) at www.gov.br/anpd under LGPD art. 18, §1 — this right exists independently of any request made to Crown. To exercise any right against Crown, contact dpo@crown-brlv.com — we will respond within 15 business days.

Right	What it means for you
Confirmation and access	Know whether Crown processes your data and receive a copy of it.
Correction	Request correction of incomplete, inaccurate or outdated data.
Deletion	Request deletion of unnecessary or unlawfully processed data. Data subject to mandatory legal retention periods cannot be deleted before those periods expire.
Portability	Receive your data in a structured format for transfer to another provider, in accordance with ANPD regulations.
Sharing information	Know which public and private entities have received your data.
Consent information	Be informed of the option not to provide consent for optional processing activities and of the consequences of refusal.
Consent withdrawal	Withdraw any consent at any time, at no cost. Withdrawal does not affect processing based on legal obligation.
Review of automated decisions	Crown uses automated tools for AML/CFT transaction monitoring, suitability scoring, risk profiling and fraud detection. Automated processing may result in decisions that materially affect your account — such as transaction holds, blocking or flagging. You have the right to request human review of any such decision under LGPD art. 20. Contact dpo@crown-brlv.com with

	the subject line 'Human Review Request — [your account number]'.
Petition to the ANPD	File a complaint directly with the ANPD at www.gov.br/anpd if you believe your rights have been violated (LGPD art. 18, §1). This right can be exercised at any time, regardless of whether you have previously contacted Crown.

How to submit a request: send an email to dpo@crown-brlv.com with the subject line 'Data Subject Request — [Right being exercised]'. Include a copy of a valid identity document (passport, national ID or equivalent) so we can verify your identity before processing the request. If we cannot verify your identity, we will contact you to request additional documentation. We will respond within 15 business days of receipt of a valid, verifiable request.

5. Security & Protection

We adopt technical and organisational measures to protect your data, including:

- digital asset custody using MPC (Multi-Party Computation) technology, splitting private keys so that no single agent has complete access to the assets;
- encryption of data in transit and at rest;
- multi-factor authentication (MFA) for platform and internal system access;
- role-based access controls with segregation of duties; and
- continuous real-time threat monitoring and security event detection.

If a security incident occurs: in the event of a breach capable of causing risk or material harm to you, we will notify the ANPD and affected data subjects within 3 business days of becoming aware of the incident, under Resolution CD/ANPD No. 15/2024. Where we do not have all information within that initial period, we will issue a preliminary notification and supplement it within 20 business days.

6. International data transfers

Some of our technology infrastructure providers (such as AWS and GCP) have servers located outside Brazil, which may involve international transfers of your personal data.

For all international transfers, we ensure compliance with the Standard Contractual Clauses (SCCs) approved by the ANPD under Resolution CD/ANPD No. 19/2024, as required since August 2025. Foreign exchange operations with overseas counterparties also observe the requirements of Resolution BCB No. 277/2022 and Resolution BCB No. 521/2025.

Crown maintains an updated record of international transfers, identifying destination countries, protection mechanisms and overseas processing parties. This record is available for inspection by the ANPD upon request. A public summary of Crown's international transfer arrangements is published at crown.finance/privacy.

7. Cookies and Tracking Technologies

Crown uses cookies and similar technologies to enhance your experience, ensure account security, and analyze platform traffic. The cookies we use are categorized as follows:

- **Strictly Necessary Cookies:** Essential for the platform to function (such as login, security, and authentication). These cannot be disabled as the service would not function correctly without them.
- **Performance and Analytics Cookies:** These allow us to count visits and traffic sources so we can measure and improve our website's performance. They help us understand which pages are the most popular.
- **Functionality Cookies:** These enable the platform to provide enhanced functionality and personalization (such as remembering your preferred language).
- **Marketing Cookies:** These may be set through our site by our advertising partners to build a profile of your interests and show you relevant ads on other sites.

8. Changes to this Notice

This Notice may be updated when there are material changes in law, regulation or our services. The date of the most recent update is always shown at the top of this document.

If changes affect processing based on consent, we will notify you in advance by email and display a notice on the platform before the changes take effect, so you may decide whether to maintain or withdraw your consent.

9. Contact

To exercise your rights, ask questions or report a privacy concern:

Compliance	compliance@crown.finance
Data Protection Officer (DPO)	dpo@crown-brlv.com
Supervisory authority (ANPD)	www.gov.br/anpd — you may petition the ANPD directly under LGPD art. 18, §1
Controller	Crown Sociedade Prestadora de Ativos Virtuais Ltda. | CNPJ: 59.386.340/0001-45 | Av. Rebouças 2748, conj. 111, Pinheiros, CEP 05402-500

***Full Policy:** The detailed *Privacy and Data Protection Policy* is available upon request at **dpo@crown-brlv.com**.