BRD CAPITAL PRIVACY POLICY

version 1.0
last updated: March 25, 2026

SKATT SOCIEDADE PRESTADORA DE SERVIÇOS DE ATIVOS VIRTUAIS LTDA., a limited liability company, enrolled with the Brazilian National Register of Legal Entities (CNPJ/MF) under No. **62.920.001/0001-01**, with registered offices at **Avenida Engenheiro Luiz Carlos Berrini, No. 1748, suite 1710, Cidade Monções, City and State of São Paulo, ZIP Code 04571-000**, hereinafter referred to as **"BRD Capital," "BRD," "SKATT," "we," "us,"** or **"Controller,"** hereby presents this Privacy Policy to explain how it processes personal data in the context of its products, services, website, applications, dashboards, integrations, and other environments operated by BRD.

This Policy describes how we collect, use, store, share, and protect personal data of users, clients, legal representatives, managers, ultimate beneficial owners, visitors, and other data subjects who interact with BRD.

By accessing or using BRD's services, the data subject declares that they have read and acknowledged this Policy. Where necessary, BRD may request specific consents for certain processing activities.

1. Who we are and how to contact us

BRD acts as the controller of the personal data processed in the context of its activities.

For matters related to this Policy, exercise of rights, questions, or requests, the data subject may contact us through the following channels:

support: support@brd.capital
privacy and data protection officer: dpo@brd.capital

2. What personal data we process

BRD may process personal data provided directly by the data subject, received from third parties, obtained from partners, or collected during the use of the platform and its services.

2.1. Personal data of individuals

In the case of individuals, BRD may process, as applicable:

a) full name
b) date of birth
c) CPF number
d) government-issued photo identification
e) full address
f) telephone number
g) email address
h) bank account or payment account details held by the user
i) login, password, access credentials, and authentication records
j) digital wallet address, public keys, hashes, transaction IDs, and transactional history related to the use of the platform
k) browsing data, IP address, logs, device identifiers, cookies, SDKs, telemetry, and technical usage information
l) data related to identity verification and security, including facial verification, biometric authentication, security questionnaires, and equivalent mechanisms, where applicable
m) information obtained in fraud prevention procedures, anti-money laundering procedures, regulatory compliance, on-chain monitoring, restrictive lists, and travel rule compliance

2.2. Personal data of legal entities

In the case of legal entities, BRD may process, as applicable:

a) CNPJ registration certificate
b) articles of association, bylaws, corporate amendments, and other constitutional documents
c) data of legal representatives, managers, attorneys-in-fact, and contact persons
d) information and documents related to the corporate structure

e) identification of ultimate beneficial owners or UBOs
f) bank account or payment account details held by the company
g) registration, operational, financial, and compliance information related to the legal entity

2.3. Automatically collected data

When accessing or using BRD's digital channels, we may process automatically collected data, such as access records, browsing events, security logs, cookies, SDKs, telemetry, preferences, page interactions, technical failures, and usage metrics.

3. How we collect data

BRD may collect personal data:

a) directly from the data subject during registration, onboarding, customer service, support, contracting, and use of the services
b) during navigation and use of the platform, website, dashboard, and APIs
c) through identity verification, security, and fraud prevention mechanisms
d) through specialized providers, including **Sumsub** for registration verification, KYC, and KYB, and **Chainalysis** for on-chain monitoring, risk analysis, and blockchain security
e) through partners necessary for operations, settlement, transactional accounts, custody, processing, or regulatory compliance
f) through cookies, SDKs, logs, pixels, and equivalent technological tools

4. The purposes for which we use data

BRD uses personal data for purposes related to its activities, including:

a) registration, identification, authentication, and account management
b) identity verification, customer due diligence, KYC, KYB, and identification of ultimate beneficial owners
c) fraud prevention, anti-money laundering, counter-terrorist financing, on-chain monitoring, travel rule compliance, and other compliance routines
d) risk analysis, operational security, platform protection, and incident

investigation
e) opening, maintaining, and using digital wallets and transactional accounts
f) enabling deposits, withdrawals, transfers, settlements, storage, custody, and other operations related to BRD's services
g) issuance, purchase, sale, transfer, and order processing related to virtual assets and BRD
h) recording, traceability, reconciliation, and maintenance of the user's movement instructions
i) provision of services such as staking, where contracted, and execution of related operational routines
j) compliance with legal, regulatory, administrative, judicial, or arbitral obligations
k) user support, operational communications, security notices, and responses to requests
l) sending institutional, promotional, and marketing communications, in accordance with applicable law
m) product improvement, technological development, statistical analysis, auditing, governance, and internal controls
n) regular exercise of rights in judicial, administrative, or arbitral proceedings

5. Legal bases for processing

BRD may process personal data, as applicable, based on the following legal grounds:

a) performance of a contract and preliminary procedures related to contracting
b) compliance with a legal or regulatory obligation
c) regular exercise of rights in judicial, administrative, or arbitral proceedings
d) BRD's or third parties' legitimate interest, always observing the data subject's fundamental rights and freedoms
e) fraud prevention and the protection of the data subject, the platform, and operations
f) consent, where legally required or where BRD chooses to request it specifically

The data subject acknowledges that a relevant part of the processing carried out by BRD arises from legal, regulatory, contractual, and operational obligations, which is why certain processing activities do not depend on consent.

6. With whom we share data

BRD may share personal data, to the extent necessary and subject to the applicable legal bases, with:

a) **Sumsub**, for identity verification, registration verification, KYC, KYB, document analysis, and related routines
b) **Chainalysis**, for on-chain monitoring, wallet analysis, blockchain security, fraud prevention, AML, and transaction investigation support
c) operational, financial, banking, settlement, transactional account, custody, infrastructure, cloud, hosting, support, and security partners
d) legal advisors, auditors, consultants, accountants, and specialized service providers
e) regulatory, judicial, administrative, police, or arbitral authorities, whenever there is a legal or regulatory obligation, valid order, or need for the regular exercise of rights
f) companies involved in corporate reorganization, corporate transactions, assignment, or succession, subject to applicable legal limits

By using BRD's services, the data subject acknowledges that their data may be shared for the purposes described in this Policy, including with third parties necessary for the performance of the services, operational security, and compliance with legal and regulatory requirements.

7. International transfer of data

BRD may carry out international transfers of personal data when necessary for the performance of its activities, use of global providers and partners, or for security, compliance, monitoring, storage, support, processing, or governance routines.

This may occur, including, due to the use of providers such as **Sumsub** and **Chainalysis**, as well as other operational or technological partners located outside Brazil.

In such cases, BRD will seek to adopt appropriate measures so that the international transfer takes place in compliance with applicable law.

8. On-chain data and blockchain particularities

Some BRD operations may involve blockchain networks and distributed ledger technologies. In such cases, certain technical identifiers and transactional data, such as wallet addresses, public keys, hashes, timestamps, and transaction IDs, may be recorded in a public, traceable, permanent, or difficult-to-modify manner, depending on the characteristics of the network used.

BRD may use tools to analyze the wallets sending and receiving virtual assets, as well as monitor transactions that present signs of elevated risk, including for the purposes of blocking, reversal, movement restriction, or termination of the user's account, where there is suspicion of unlawful origin or unlawful destination. This is already reflected in the Terms of Use themselves.

Whenever possible, BRD will seek to adopt an architecture that prioritizes the off-chain processing of personal data and uses on the blockchain only technical references, identifiers, or minimized records.

9. Cookies, SDKs, telemetry, and similar technologies

BRD uses cookies, SDKs, pixels, logs, and similar technologies to:

a) enable the technical operation of the website, applications, and systems
b) authenticate sessions and reinforce security
c) understand performance, failures, and stability
d) measure usage, navigation, engagement, and preferences
e) personalize content and communications
f) support marketing, analytics, fraud prevention, and protection against abuse

The data subject may manage part of these technologies through browser settings, device settings, or the tools made available by BRD, where applicable.

10. Retention and storage

BRD will store personal data for as long as necessary to fulfill the purposes set out in this Policy, provide the services, maintain operational records, comply with legal

and regulatory obligations, carry out compliance routines, prevent fraud, preserve audit trails, and regularly exercise its rights.

Even after account deletion, BRD may retain part of the information and personal data where there is a legal, regulatory, contractual, security, audit, fraud prevention, or other legitimate reason justifying retention. This logic is already set forth in the Terms of Use.

11. Information security

BRD adopts reasonable technical, administrative, and organizational measures to protect personal data against unauthorized access, loss, alteration, leakage, misuse, or unlawful processing.

These measures may include access control, profile segregation, monitoring, logs, credential management, encryption, access reviews, vendor due diligence, identity validation mechanisms, and internal governance procedures.

No environment is entirely immune to incidents. In the event of a relevant security incident, BRD will adopt the appropriate measures and, when required by applicable law, will make the required notifications.

12. Automated decisions, risk analysis, and blocks

BRD may use automated tools, security rules, on-chain monitoring, wallet analysis, AML screening, and risk models to support registration validations, transaction investigation, fraud prevention, preventive blocks, transaction reviews, and risk mitigation.

Whenever appropriate and subject to legal limits, the data subject may request additional information through the channels indicated in this Policy.

13. Data subject rights

Under applicable law, the data subject may request, subject to legal and regulatory limits:

a) confirmation of the existence of processing
b) access to personal data
c) correction of incomplete, inaccurate, or outdated data
d) anonymization, blocking, or deletion of unnecessary, excessive, or unlawfully processed data
e) portability, where applicable
f) information about sharing
g) information about the possibility of not providing consent, where consent is the legal basis used
h) withdrawal of consent, where applicable
i) objection to processing, in the cases provided by law
j) review of decisions made based on automated processing, where applicable

Requests may be sent to **dpo@brd.capital** or **support@brd.capital**.

BRD may request additional information to confirm the requester's identity and may limit compliance where there is a legal, regulatory, contractual, technical, or security basis for doing so.

14. Marketing and communications

BRD may send operational, institutional, informational, and promotional communications related to its services, products, content, campaigns, events, and updates.

Where required by applicable law, BRD will collect specific consent for promotional communications. In other cases, such communications may be sent based on legitimate interest, with opt-out rights ensured where applicable.

15. Third-party links

BRD environments may contain links, integrations, and references to third-party websites, applications, wallets, and services. This Policy does not apply to external environments, which may have their own privacy rules.

16. Children and adolescents

BRD's services are not intended for children. If BRD identifies improper processing of a child's or adolescent's data in violation of applicable law, it may adopt appropriate measures to restrict account use, request additional documentation, or remove the registration.

17. Changes to this policy

BRD may amend this Policy at any time to reflect legal, regulatory, operational, technological, or security changes.

The current version will always be available through BRD's channels, together with the relevant update date. If there are material changes, BRD may adopt additional communication measures.

18. Final provisions

This Policy must be interpreted together with BRD's Terms of Use, specific notices, cookie banners, onboarding flows, agreements, and other documents applicable to the relationship between BRD and the data subject.

In the event of a conflict between this Policy and a specific notice issued for a given operation or product, the specific notice shall prevail with respect to that activity.