POLICY DOCUMENT

Privacy Policy

WEB3 Technology B.V. (trading as RGLTD)

Document Title	Privacy Policy
Document Owner	Chief Risk & Compliance Officer (CRCO) / Data Protection Officer (DPO)
Applies To	All Users of WEB3 Technology B.V. services and the Website / App
Regulatory Basis	GDPR (EU) 2016/679 · Dutch Telecommunications Act (Tw) · MiCA Reg. 2023/1114 · TFR Reg. 2023/1113 · DAC8 Dir. 2023/2226 · Wwft · DORA
Version	2.0
Effective Date	05.05.2026
Review Cycle	Annual, or upon material regulatory or operational change
Approved By	Management Body / CRCO
Classification	Public — Privacy Notice

At WEB3 Technology B.V., we are committed to protecting the security of the information you entrust to us and ensuring that the principles governing its processing are transparent and easy to understand. We want individuals using our services to know what personal data we collect, for what purposes we process it, and what rights they have under applicable data protection laws. We follow the principles set out in the GDPR and relevant national privacy regulations, and we organise our data-processing activities to ensure security, confidentiality, and compliance with the law.

Before you begin using our services, we encourage you to read this Privacy Policy, which sets out the key information regarding the processing of your personal data.

1. Definitions Used in This Privacy Policy

Controller / WEB3 Technology / "we"	"RGLTD" is the trading name of WEB3 Technology B.V., a Netherlands-registered company licensed by the AFM as a Crypto-Asset Service Provider, registration no 41000022, located at Prins Hendrikkade 21E, Amsterdam, 1012TL, Netherlands | LEI number 724500YJVIN0Q94ZZG58 | KVK: 95206604.
Personal Data	Any information relating to an identified or identifiable natural person, as defined in Article 4(1) of the GDPR.
Policy	This Privacy Policy.
Cookies Policy	The cookies policy applicable to the website rgltd.com

Terms of Service	The WEB3 Technology Terms of Service are available on the Website rgltd.com
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
Markets in Crypto-Assets (MiCA)	As a licensed CASP under MiCA, we are subject to record-keeping, client communication, complaints handling, and reporting obligations that require the processing of personal data. Where such processing is mandated by MiCA, the legal basis is Article 6(1)(c) GDPR (compliance with a legal obligation).
EEA	The European Economic Area.
Website	The online service operated by the Controller at rgltd.com
User	Any natural person visiting the Website or using one or more services available through the Website, including, where the services are used by or on behalf of a legal entity, any natural person acting as an authorised representative, beneficial owner, director, or other contact person of such legal entity whose personal data are processed in connection with the provision of the Controller's services.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller, as defined in Article 4(8) of the GDPR.

Third Party A natural or legal person, public authority, agency or body other than the data subject, the Controller, the Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process personal data, as defined in Article 4(10) of the GDPR.

Any other terms capitalised in this Policy shall have the meaning assigned to them in the Terms of Service of the Website rgltd.com

2. Who Processes Your Personal Data?

The controller of your personal data is **WEB3 Technology B.V.**, with its registered office at Prins Hendrikkade 21E, 1012 TL Amsterdam, the Netherlands, registered under number 95206604.

2.1 How to Contact Us

You can contact us, in our capacity as the Controller of your personal data, by sending correspondence to the Company's registered address (Prins Hendrikkade 21E, 1012 TL Amsterdam, the Netherlands) or by email at dpo@rgltd.com

To enhance the protection of your personal data, we have appointed an internal Data Protection Officer. This is the person you can contact if you have any questions about how we process your data, wish to exercise your rights, or need clarification regarding any other matters related to the processing of your personal data.

For this purpose, you can send an email to **dpo@rgltd.com** or send a letter addressed as follows: Data Protection Officer · WEB3 Technology B.V. · Prins Hendrikkade 21E · 1012 TL Amsterdam · The Netherlands.

3. Personal Data of Individuals Under 18 Years of Age

Our services are intended for individuals who are at least 18 years old. The Controller does not knowingly process personal data of minors. As part of the onboarding process, the age of each User is verified through

our mandatory identity verification (KYC) procedures, which include the collection and review of official

identity documents such as a passport or national identity card. Where the identity verification process reveals that an individual is under the age of 18, the registration will be declined and any personal data already collected will be deleted without undue delay.

If, despite these measures, we become aware that personal data of an individual under the age of 18 has been provided to us, such data will be deleted without undue delay. If you suspect that we may have received such data, please contact the Controller or the Data Protection Officer so that appropriate measures can be taken.

4. Source of Data

The Controller may obtain personal data from the following sources:

4.1 Directly from the Data Subjects

These data are provided voluntarily by Users in connection with their use of the Controller's services, in particular through:

- completing a contact form on the Website,
- subscribing to a newsletter,
- providing data for the purpose of preparing, concluding or performing a contract with the Controller, including the use of its services,
- submitting application documents (e.g., CV) as part of recruitment processes,
- submitting data as part of User verification procedures (KYC – Know Your Customer or KYB – Know Your Business) carried out in accordance with applicable anti-money laundering and counter-terrorist financing laws, including the Dutch Act on the Prevention of Money Laundering and Terrorist Financing (Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft), as well as applicable EU AML/CFT regulations and implementing measures.

4.2 From Third Parties

To the extent permitted by applicable law, the Controller may also obtain personal data from other sources, including:

- from entities with which the User is associated (e.g., employer, business partner, or an entity commissioning the service),
- from payment service providers, financial institutions, or other essential service providers, • from publicly available registers and databases, such as: chambers of commerce, beneficial ownership registers/transparency registers, business registers, official sanctions lists, and publicly accessible and reliable online sources (e.g., search engines) — including through external verification service providers,
- from publicly available blockchain networks, including transaction timestamps, transaction identifiers, digital signatures, transaction amounts and wallet addresses, where such data are processed to execute transactions, ensure security, prevent fraud and comply with applicable legal obligations,
- from technical and operational service providers who supply information relating to transactions or the status of operations.

The Controller obtains data from the above sources only when it is justified by the purpose of the processing, necessary for the provision of services, or required by law.

4.3 Automatically

When using the Controller's website, certain data may be collected automatically, including: information on how the services are used (such as IP address, date and time of the visit, pages viewed and links clicked), technical information about the device and software (e.g., browser type, operating system, language settings), as well as information collected through cookies and similar technologies (the detailed rules of which are described in the Cookies Policy).

We may also collect information about how Users interact with our Website and Services, including site usage data, interaction data and, where applicable, age group information.

In addition, in some cases, we may receive information directly from Users prior to account creation, for example, when a User participates in surveys or contacts us before entering into a contract.

5. Processes in Which We Process Your Personal Data

Use of the Website and the App (without creating an account)	IP address, other identifiers and information collected through cookies and similar technologies	We process the data to enable you to use the Website, based on the Controller's legitimate interest (Article 6(1)(f) GDPR), consisting in ensuring the proper functioning of the site.	We process the data for the duration of your use of the Website.
Marketing based on consent (cold leads/newsletters)	First name, last name, email address	We process the data for the purpose of sending marketing communications, newsletters and promotional content, on the basis of the User's consent (Article 6(1)(a) GDPR), Article 11.7 of the Dutch Telecommunications Act (Telecommunicatiewet), which implements the ePrivacy Directive (2002/58/EC) in the Netherlands and in accordance with applicable electronic communications laws.	You may withdraw your consent at any time, without affecting the lawfulness of processing carried out before its withdrawal.
Marketing communications to existing customers (similar products and services)	First name, last name, email address	We process the data for the purpose of marketing our own similar products or services to existing customers, on the basis of the Controller's legitimate interest (Article 6(1)(f) GDPR), in accordance with applicable electronic communications laws. Users may object to such processing at any time.	You may object to such processing at any time by using the unsubscribe mechanism in any marketing message or by contacting us directly.
Creation and management of a User Account on the Website	First name, last name, email address, phone number	We process the data for the purpose of providing services related to the creation, management and operation of User Accounts on the Website, on the basis of necessity for the performance of a contract (Article 6(1)(b) GDPR), and for the establishment, exercise or defence of legal claims, on the basis of the Controller's legitimate interest (Article 6(1)(f) GDPR), consisting in the protection of its rights.	Data processed for the performance of the contract are retained for the duration of the contract, and thereafter for up to 6 years, in accordance with applicable legal requirements and potential claims.
Contact form	Data necessary to initiate communication, including: first name, last name, email address, phone number	The data are processed for the purpose of identifying the sender and handling their enquiry; the legal basis for the processing is the necessity to perform a contract (Article 6(1)(b) GDPR). If the User provides additional data that are not required, the legal basis for processing such data is consent (Article 6(1)(a) GDPR).	Data processed for the purpose of identification and handling the enquiry are retained for the period necessary to perform the contract, and thereafter for the period required by applicable law and for up to 6 years for the purpose of securing potential claims.

			Data processed on the basis of consent are retained until the consent is withdrawn.

User identity verification (KYC/KYB), AML/CFT risk assessment	Identification data (first name, last name, national identification number, date of birth, citizenship, residential address), identity document data (document type, series and number, expiry date, issuing country), copies of identity documents (e.g. passport, national identity card, driving licence) submitted for verification purposes, image obtained from a photo or video submitted during verification, biometric information generated from such images, including facial geometry derived from the photo/video, processed solely for the purposes of unique identification and identity verification (electronic identity verification – EIDV), information on the sources of funds, source of wealth, financial situation, income and/or asset verification data, trading and investment experience, login and transaction data. For business Users: company details, tax identification number, business registry numbers, and details of directors and beneficial owners.	We process the data to comply with legal obligations under anti-money laundering and counter-terrorist financing regulations, to assess risk, and to ensure the security of our services. The legal basis is compliance with a legal obligation (Article 6(1)(c) GDPR). For fraud detection, the legal basis is our legitimate interest (Article 6(1)(f) GDPR), consisting in protecting against fraud and ensuring the security of transactions.	We process the data for the duration of the service relationship, and after its termination for an additional 5 years in accordance with AML legislation, as well as for the period necessary for the establishment, exercise or defence of legal claims — up to 6 years.

Execution of transactions, accounting and transfer of funds or crypto-assets	Identification data (first name, last name, email address, phone number), transactional data (including wallet addresses provided by the User and related transaction routing information), transaction identifiers, hashes, transaction history, sender and recipient details, transaction amount, currency preferences, payment method, date and/or timestamp), and payment data (e.g., information on payment methods, bank account number, payment card data (such as PAN), and settlement details)	We process the data for the purpose of executing transactions, correctly recording them, and handling financial settlements. The legal basis for the processing is the performance of a contract (Article 6(1)(b) GDPR). For the fulfilment of accounting, tax and AML obligations, the legal basis is compliance with a legal obligation to which the Controller is subject (Article 6(1)(c) GDPR). For the establishment, exercise or defence of legal claims, we process the data on the basis of our legitimate interest (Article 6(1)(f) GDPR), consisting in the protection of the Controller's rights and ensuring the security of transactions.	We retain the data for the period required under tax regulations — 5 years from the end of the tax year — and for an additional 5 years in accordance with AML obligations. For the purposes of legal claims, the data may be processed for an additional period of up to 6 years in line with applicable limitation periods.
Ensuring the safety, security and integrity of the Services (fraud prevention and abuse detection)	Identification data (such as first name, last name, email address, phone number and User account identifiers), transaction data, account activity data, communications data, and other data processed in connection with the use of the Services	We process the data to monitor transactions, detect, prevent and investigate fraud, abuse, unlawful behaviour, violations of our policies or Terms, and other security risks, as well as to ensure the integrity and security of our Services. The legal basis for the processing is the Controller's legitimate interest (Article 6(1)(f) GDPR), consisting in securing the platform, protecting Users and preventing misuse of the Services. Where applicable, the processing may also be carried out to comply with legal obligations (Article 6(1)(c) GDPR), in particular under AML/CFT regulations.	The data are processed for the duration of the service relationship and thereafter for the period necessary to fulfil legal obligations and to establish, exercise or defend legal claims, in accordance with applicable limitation periods.

Customer support and communications	Identification and contact data (such as first name, last name, email address, phone number and User account identifiers), communications data, including survey responses, information provided to customer support or user research teams, chatbot interactions and, where applicable, call recordings	We process the data to provide customer support, respond to enquiries, handle complaints, and improve the quality and functionality of our Services. The legal basis for the processing is the necessity for the performance of a contract (Article 6(1)(b) GDPR) and the Controller's legitimate interest (Article 6(1)(f) GDPR), consisting in ensuring effective customer support and service improvement.	The data are processed for the period necessary to handle the enquiry or support request and thereafter for the period required by applicable law or for the establishment, exercise or defence of legal claims.
Recruitment processes (job applicants)	Identification and contact data (first name, last name, email address, phone number), professional data (CV, work experience, education, qualifications), information provided during the recruitment process (including interview notes), and any other data voluntarily provided by the candidate	We process the data for the purpose of conducting recruitment processes and assessing candidates for employment or cooperation. The legal basis for processing is the necessity to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b) GDPR), compliance with legal obligations under applicable labour laws (Article 6(1)(c) GDPR), the Controller's legitimate interest (Article 6(1)(f) GDPR), consisting in conducting recruitment processes and selecting suitable candidates, consent (Article 6(1)(a) GDPR), where the candidate voluntarily provides additional data not required by law or applies for future recruitment processes.	Data are processed for the duration of the recruitment process, and thereafter for the period necessary to finalise the recruitment and address any related claims. If the candidate has consented to participate in future recruitment processes, the data may be processed for one year.
Compliance with mandatory tax reporting obligations under DAC8 (Council Directive 2023/2226/EU) and the OECD Crypto-Asset Reporting Framework (CARF)	Full name, date of birth, residential address, country(ies) of tax residency, Tax Identification Number(s) (TIN), aggregate transaction values per crypto-asset type per calendar year, wallet identifiers	Article 6(1)(c) GDPR — compliance with a legal obligation. The recipient would be the Dutch Tax and Customs Administration (Belastingdienst), and where applicable, competent tax authorities of EU Member States via automatic exchange of information.	7 years from the end of the reporting year in which the data was collected, in line with Dutch fiscal retention requirements.
Compliance with the Transfer of Funds Regulation (TFR) — mandatory exchange of originator and beneficiary data during crypto-asset transfers to detect and prevent money laundering and terrorist financing	Full name, crypto-asset account identifier (wallet address), transaction reference, and where required: residential address, national identity number, or date and place of birth of originator and/or beneficiary	Article 6(1)(c) GDPR — compliance with a legal obligation under Regulation (EU) 2023/1113. With recipients being counterparty CASPs and crypto-asset service providers involved in the transfer, as required by law.	5 years from the date of the transfer, in line with Article 21 of Regulation (EU) 2023/1113.

** Once the retention period has expired, the data are irreversibly deleted or anonymised.*

As a rule, we do not process special categories of personal data (such as data revealing racial or ethnic origin, political opinions, religious beliefs, health data or sexual orientation). However, for the purpose of identity verification (KYC), we process biometric data (facial geometry derived from photos or videos) solely to confirm the identity of the User and to prevent fraud. This processing is carried out to comply with legal obligations under applicable AML/CFT regulations (Article 6(1)(c) GDPR), in conjunction with Article 9(2)(g) GDPR (processing necessary for reasons of substantial public interest), as further specified under applicable EU and national AML/CFT legislation. Where required under applicable law, such processing may also rely on Article 9(2)(a) GDPR (explicit consent), obtained during the verification process.

Biometric data are processed only to the extent strictly necessary for identity verification, are not used for any other purposes and are not subject to further processing beyond identity verification and fraud prevention and are subject to enhanced security measures. Where special categories of personal data are included incidentally in transaction data or other information provided by Users, such data are not actively used or analysed by the Controller for any specific purpose.

Where processing is based on the Controller's legitimate interest, we have carried out a balancing test to ensure that such interests are not overridden by the rights and freedoms of the data subject.

Where more than one retention period applies to the same dataset (for example, AML records subject to a 5-year Wwft retention period and records also relevant to ongoing civil proceedings subject to a 6-year limitation period), we retain the data for the longer of the applicable periods. Retention periods begin from the end of the business relationship or the date of the relevant transaction, whichever is later, unless otherwise specified above.

6. Who Else Has Access to Your Data and for What Purposes?

6.1 Entities Processing Data on Our Behalf

In connection with the provision of our services, your personal data may be disclosed to third parties. Such disclosure takes place only when necessary for the achievement of a specific purpose, in accordance with the GDPR, on the basis of appropriate agreements, and with the application of adequate security measures.

We cooperate with trusted service providers who support us in the technical and operational delivery of our services. These may include, in particular: IT, hosting and cybersecurity providers; providers of software and tools used for User support; accounting firms; law firms; auditing companies; cloud, email, archiving and analytics providers; as well as entities supporting operational and administrative processes.

Each processor acts solely on our instructions and on the basis of a data processing agreement that sets out technical and organisational measures protecting the data.

6.2 Entities Processing Data for Their Own Purposes (Independent Controllers) In certain situations, personal data may be disclosed to entities that process such data as independent controllers. This applies to:

- entities within the Controller's corporate group, where such disclosure is necessary for internal administrative purposes, compliance with legal obligations (including AML/CFT), risk management, or the provision of services; such entities act as independent controllers or processors, depending on the context of the processing,
- entities providing key IT systems or infrastructure used in the delivery of our services (co-controllers with respect to a specific system),
- supervisory authorities and public institutions where disclosure is required by law (including, among others, the Dutch Authority for the Financial Markets – AFM, DNB and Financial Intelligence Unit – the Netherlands (FIU-NL) and other law enforcement authorities, tax authorities),

- Dutch Tax and Customs Administration (Belastingdienst) — certain personal and transaction data of our users will be reported to the Belastingdienst. This data may subsequently be shared with the tax authorities of other EU Member States via automatic exchange of information. We process this data solely to comply with our legal obligations and do not use it for any other purpose,
- Counterparty Crypto-Asset Service Providers (Travel Rule) — we are legally required to transmit originator and beneficiary personal data to the receiving CASP or crypto-asset service provider when processing crypto-asset transfers above applicable thresholds, and in certain cases, regardless of threshold. This data sharing is mandatory and cannot be opted out of,
- financial institutions and payment card operators (e.g., Mastercard, Visa) in connection with payment processing,
- entities involved in audit or inspection activities,
- law firms and professional advisers in the context of legal proceedings,
- entities involved in corporate processes (e.g., acquisition or restructuring transactions), where the disclosure is necessary for the conclusion or performance of an agreement.

In such cases, each of these entities is responsible for processing the data in accordance with its own privacy policy and the applicable legal framework.

6.3 Artificial Intelligence (AI)

As part of our operational processes, we use tools based on artificial intelligence to support specific functions, such as: …

- Identity verification and biometric comparison (e.g., liveness detection, document authentication) — provided by third-party certified KYC/IDV vendors operating under DPA and SCCs • Transaction monitoring and AML risk scoring — automated rules-based and machine-learning systems to detect unusual patterns and generate alerts for human review
- Sanctions and PEP screening — automated matching against sanctions lists (EU, UN, OFAC) and Politically Exposed Persons databases
- Customer support assistance — AI-assisted triage and response tooling, where queries involving personal data are escalated to human agents

No fully automated decision with legal or similarly significant effect is made without a human review step being available upon request. Where automated systems trigger an account restriction or transaction block, a human compliance officer reviews the case before any final determination is made.

Where AI tools process personal data, such processing is carried out in accordance with this Privacy Policy and applicable data protection laws.

The AI tools used in our operations are provided by third-party service providers acting on our behalf, on the basis of appropriate contractual arrangements.

6.4 Joint Controllership (Social Media)

When you contact the Controller via social media platforms (e.g., Instagram, LinkedIn), the personal data involved are jointly controlled by us and the owners of those platforms. We jointly determine the purposes and means of the processing, and the User has the right to exercise their GDPR rights with respect to both us and the platform operator. Further details can be found in the privacy policies of the respective social media services.

Although WEB3 Technology and the social media platforms (or key IT system providers) jointly determine the purposes and means of processing, we primarily handle the fulfilment of your data subject rights. You may, however, exercise your rights against either party.

A current list of our data processors and sub-processors, including their name, country of establishment, and processing purpose, is available upon request by emailing **dpo@rgltd.com** We will notify users of any material changes to our sub-processor list in advance where required under our DPA obligations.

7. Do We Transfer Your Data Outside the European Economic Area (EEA)?

We primarily process your personal data within the European Economic Area (EEA). However, for specific services (e.g., identity verification or technical infrastructure), we may transfer personal data to trusted partners outside the EEA (“Third Countries”).

We only transfer your data to a Third Country if one of the following safeguards is in place:

Adequacy Decision
The country has been recognised by the European Commission as ensuring an adequate level of data protection (e.g., the EU-U.S. Data Privacy Framework for certified U.S. entities).

Standard Contractual Clauses (SCCs) & Supplementary Measures
We use the Standard Contractual Clauses approved by the European Commission. In these cases, we conduct a Transfer Impact Assessment (TIA) to determine whether the destination country's laws and practices, including access by public authorities, may affect the level of protection of the transferred personal data.

Where necessary, we implement supplementary technical, organisational and contractual measures (such as encryption, access restrictions, and data minimisation) to ensure that personal data remain protected to a standard essentially equivalent to that guaranteed within the EEA.

We assess transfers on a case-by-case basis and, where an adequate level of protection cannot be ensured, we refrain from transferring personal data to the relevant third country.

You may request a copy of the specific safeguards used for your data by contacting us at **dpo@rgltd.com**

8. Is Providing Your Personal Data Voluntary?

Providing your personal data is voluntary; however, certain data are necessary for the provision of the services offered through our Website and the App, for e.g. data required for KYC/AML compliance and contract performance are mandatory. Failure to provide such data may prevent you from using specific features or from entering into or performing a contract with us.

Data marked as optional may be provided at your discretion, and choosing not to provide them does not affect your ability to use the core services. You always have the right to decide which data you wish to disclose.

If you voluntarily consent to the processing of your personal data for specific purposes (e.g., marketing), you may withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent before its withdrawal. It also does not result in the loss of access to services or other rights, unless their performance requires the continued processing of the data concerned.

Providing certain personal data may be a legal or contractual requirement, including in particular under AML/CFT regulations. Failure to provide such data may result in the inability to establish or continue the business relationship or to execute transactions.

9. Are Your Personal Data Subject to Profiling?

Users' personal data may be subject to profiling, understood as the automated processing of certain information about the User for the purpose of assessing selected factors relating to their activity, reliability, or the risk associated with the use of the services. Profiling is carried out in particular to fulfil obligations arising from anti-money laundering and counter-terrorist financing (AML) regulations, to ensure the security of the services, and to prevent fraud.

Where automated processing, including profiling, generates an output that may lead to a decision with legal or similarly significant effect (e.g. KYC rejection), such output is subject to mandatory human review before any final decision is made; the data subject has the right to request human review, contest the decision, and express their point of view.

The results of profiling processes are supportive and auxiliary in nature; their purpose is to enable risk assessment, ensure compliance with legal obligations, and enhance the security of both Users and the Controller.

If, in the course of using the services, a User meets certain criteria or obtains a result indicating a lower level of risk (e.g., in AML assessment), this may result in access to certain functionalities.

In particular, the results of automated checks performed during the video and biometric identity verification (KYC) process, including facial recognition and liveness detection mechanisms, are used solely as supporting information. Any refusal to onboard a User or any restriction of access to the Services based on such results (including results of automated biometric verification) is subject to meaningful human review and approval before it produces any legal or similarly significant effect, in accordance with Article 22 of the GDPR.

For transactions below a specified threshold, the Controller does not carry out profiling of Users' personal data within the meaning of Article 4(4) of the GDPR. In such cases, data are processed solely to the extent necessary to execute the transaction and to comply with legal requirements, without performing any automated assessment of factors relating to the User.

The profiling process may take into account high-level factors required under applicable AML/CFT regulations and standard fraud-prevention practices, including publicly available blockchain data (such as transaction timestamps, transaction identifiers, digital signatures, transaction amounts and wallet addresses). These may include, for example, whether a transaction exceeds legally defined thresholds, the frequency or nature of transactions, geographic or behavioural inconsistencies, or the status of the User's identity verification, as well as information relating to the User's interaction with the Website or Services (such as usage data, interaction data, or survey responses, including those collected prior to account creation). These indicators are used solely to assess risk and to ensure compliance with legal obligations; they do not involve the disclosure of proprietary risk models or detailed internal fraud-detection logic.

10. What Rights Do You Have in Connection with Our Processing of Your Personal Data?

Right of access	You have the right to know which of your personal data we process, for what purposes, and to obtain a copy of such data.
Right to data portability	You have the right to receive your personal data in a structured, commonly used and machine-readable format, enabling you to transmit those data to another controller.
Right to rectification	If your data are inaccurate or incomplete, you have the right to have them corrected or completed. If you have a User Account, you may update certain data yourself.
Right to restriction of processing / right to be forgotten	You have the right to request the restriction of processing or the deletion of your personal data, unless we are required to continue processing them due to applicable legal obligations or for the establishment, exercise or defence of legal claims.

Right to withdraw consent	You may withdraw your consent to the processing of your personal data at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.
Right to object	Where your personal data are processed on the basis of the Controller's legitimate interests or for direct marketing purposes, you also have the right to object to such processing.
Right to human review of automated decisions	Where we make decisions about you solely by automated means — including automated KYC rejection, risk scoring, or AML-triggered account restrictions — that produce legal or similarly significant effects, you have the right to: (i) request that the decision be reviewed by a human member of our team; (ii) express your point of view regarding the automated decision; and (iii) contest the decision.

To exercise any of the rights listed above, please submit your request in writing to: **dpo@rgltdcom**

We will respond to your request within one calendar month of receipt. In cases of complexity or high volume, we may extend this period by a further two months; if so, we will inform you within the first month and explain the reason for the extension (Article 12(3) GDPR).

Processing your request is free of charge. However, where requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may either charge a reasonable administrative fee or decline to act on the request (Article 12(5) GDPR).

To protect your data, we will verify your identity before processing any DSAR. We may request a copy of a government-issued identity document or use our existing KYC verification records for this purpose. Identity verification data submitted solely for DSAR purposes will not be retained beyond the period necessary to process your request.

If you believe that your personal data are being processed unlawfully, you have the right to lodge a complaint with the Dutch Data Protection Authority: Autoriteit Persoonsgegevens, Bezuidenhoutseweg 30, 2594 AV Den Haag, Netherlands. Website: www.autoriteitpersoonsgegevens.nl Telephone: +31 88 1805 250.

Important limitation — on-chain data: Please be aware that where your personal data has been incorporated into a public blockchain (for example, a wallet address or transaction hash that is linkable to you), it is technically impossible for us to delete or alter that data once confirmed on-chain. This is an inherent limitation of distributed ledger technology that falls outside of our control as a data controller. In such cases, we will erase or anonymise all associated off-chain records (such as your name, email address, and account data) within our systems in accordance with our retention schedule, and we will inform you of the on-chain limitation when handling your request.

11. How We Protect and Store Personal Information

We implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks associated with the processing of personal data, in accordance with Article 32 of the GDPR. These measures include, in particular:

- Restricting access to personal data to authorised personnel only
- Data minimisation and role-based access controls
- Encryption of data in transit and at rest
- Monitoring of systems and activities for security and fraud-prevention purposes • Regular security reviews, audits and testing of IT systems
- The use of secure, certified service providers that meet industry standards

Personal data are stored only for the periods indicated in this Privacy Policy and exclusively in secure environments that ensure confidentiality, integrity and availability of the data. Once the relevant retention

periods expire, the data are irreversibly deleted or anonymised.

11.1 Data Breach Notification

We maintain an internal process for identifying, assessing, and responding to personal data breaches in accordance with Articles 33 and 34 of the GDPR.

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, we will notify the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in such a risk.

Where a breach is likely to result in a high risk to your rights and freedoms — for example, where it involves sensitive financial data, identity documents, or biometric data — we will also notify you directly, without undue delay, using the contact details held on your account.

We maintain an internal breach register documenting all incidents, their impact, and remedial actions taken, in accordance with our accountability obligations under Article 5(2) GDPR.

11.2 Anonymised Data

In order to monitor and mitigate fraud and other risks, improve the performance of our services, and enhance security, we may process information in an anonymised form.

Anonymised data do not constitute personal data within the meaning of the GDPR, as they do not allow for the identification of an individual. Such data are processed exclusively for analytical, statistical and security-related purposes.

The anonymisation process is designed to ensure that individuals cannot be re-identified, directly or indirectly.

12. Cookies

The rules and types of cookies and similar technologies used are set out in the Cookies Policy. A detailed description of the cookies and similar technologies we use can be found at rgltd.com

13. Changes to Your Personal Data

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes or if you become aware that any personal data that we hold is not accurate.

14. Changes to the Policy

This Privacy Policy is effective as of 05.05.2026.

We may modify this Privacy Policy from time to time to reflect any changes in the ways in which we process personal data or any changes in data protection laws. To the extent that our policy changes in a material way (being a change in processing purposes, a change to the identity of the controller, or a change as to how you can exercise your rights in relation to our processing), we will communicate this to you and post a new version on our website (www.rdltd.com). Please check our Privacy Policy regularly so that you are aware of any changes. The date at the top of this notice shows when it was last updated.

15. DPIA Statement

In accordance with Article 35 GDPR, we conduct Data Protection Impact Assessments (DPIAs) prior to undertaking processing activities that are likely to result in a high risk to the rights and freedoms of individuals. This includes, but is not limited to: processing of biometric data for identity verification, systematic automated monitoring of transaction behaviour for AML/CFT purposes, and large-scale processing of special category data. The results of DPIAs inform our technical and organisational measures and are documented in our internal records of processing activities (RoPA) maintained under Article 30 GDPR.

16. Version History

1.0 120.10.2024	DPO / CRCO	Baseline document — initial publication. Approved by the Management Body
2.0 05.05.2026	DPO / CRCO	Updated to reflect DAC8 / CARF obligations, TFR Travel Rule, AI tool usage, joint controllership, DPIA statement, and on-chain data limitation. Approved by the Management Body.