



DATA PRIVACY AND PERSONAL INFORMATION MANAGEMENT AGREEMENT

Section 1.1: Scope and Applicability

This Data Privacy and Personal Information Management Agreement (the “**Data Privacy Agreement**”) forms part of the contractual documentation governing the Customer’s access to and use of the Company’s Services.

For the purpose of providing and administering the Services, **COURTIRO** (the “**Company**,” “**we**,” “**our**,” or “**us**”) may collect, process, store, use, and disclose personal data obtained through its websites, applications, electronic systems, trading platforms, and related digital environments (collectively, the “**Platform**”).

This Data Privacy Agreement establishes the principles governing the collection, use, storage, disclosure, protection, and retention of personal data in connection with the Services and shall be applied in accordance with Applicable Law and any mandatory data protection and privacy requirements applicable to the Company.

The Customer acknowledges that the provision of certain personal data may be necessary for account registration, identity verification, regulatory compliance, payment processing, and the provision and administration of the Services.

Section 1.2: Categories of Personal Data Collected

The Company may collect personal data directly from the Customer and through automated or third-party sources where reasonably necessary for lawful and legitimate business, contractual, security, operational, or regulatory purposes.

1.2.1 Customer-Provided Information



Information provided by the Customer during registration, account maintenance, verification, or use of the Services may include, without limitation:

- (a) full name;
- (b) contact information;
- (c) date of birth;
- (d) nationality;
- (e) country and status of residence;
- (f) employment information;
- (g) financial information;
- (h) investment or trading experience;
- (i) income information;
- (j) source of funds or source of wealth information; and
- (k) other information reasonably required for the administration of the Customer Account or provision of the Services.

1.2.2 Regulatory and Identity Verification Data

To satisfy Applicable Law and regulatory requirements, the Company may collect, verify, and retain identification and verification documents, including passports, national identity documents, proof of address, financial documents, source of funds documentation, and other legally acceptable records.

Such information may be processed for Know Your Customer (**KYC**), Anti-Money Laundering (**AML**), counter-terrorist financing, sanctions screening, fraud prevention, and other regulatory or compliance purposes.

Section 1.3: Information Security and Data Safeguards



The Company implements technical, administrative, organizational, and security measures designed to protect personal data against unauthorized access, misuse, alteration, loss, destruction, or other forms of unauthorized processing.

The Company may review and update its security measures from time to time in response to technological developments, identified risks, regulatory requirements, or operational needs.

1.3.1 Authentication and Access Controls

The Company may apply enhanced authentication and access-control measures, including two-factor authentication, multi-factor authentication, identity verification, security codes, or other verification procedures, to protect Customer Accounts and prevent unauthorized access.

1.3.2 Encryption and Secure Communications

Where appropriate, personal data transmitted through or in connection with the Platform may be protected using encryption technologies, secure communication protocols, access controls, and other technical safeguards designed to protect the confidentiality and integrity of such information.

1.3.3 Security Monitoring and Oversight

The Company may conduct ongoing monitoring, internal reviews, security assessments, system audits, and other control activities to identify security risks, detect unusual or unauthorized activity, and respond to actual or suspected security incidents.

1.3.4 Account Recovery and Identity Verification

Where access to a Customer Account is lost, compromised, or suspected to have been compromised, the Company may require additional identity verification or other security procedures before restoring access.



The Company may delay, restrict, or refuse account recovery where the information or documentation provided is insufficient to establish the identity or authority of the requesting person.

Section 1.4: Automated and Technical Data Collection

The Company may collect certain technical and usage information automatically when the Customer accesses or uses the Platform.

1.4.1 System-Generated Information

Automatically collected information may include IP addresses, device identifiers, browser type, operating system, session information, access times, usage logs, device information, and other technical data reasonably necessary for security, analytics, system administration, fraud prevention, and operational purposes.

1.4.2 Cookies and Similar Technologies

The Platform may use cookies and similar technologies to support functionality, maintain security, remember preferences, improve user experience, analyze Platform usage, and support other legitimate operational purposes.

Where consent is legally required for the use of particular cookies or tracking technologies, the Company shall obtain or manage such consent in accordance with Applicable Law.

The Customer may be able to manage certain cookie preferences through available browser or Platform settings, subject to the functionality and requirements of the relevant Services.

Section 1.5: Purposes of Data Processing



The Company may process personal data for lawful and legitimate purposes connected with the Customer relationship and the provision, administration, security, and improvement of the Services, including:

- (a) account creation, identity verification, and account administration;
- (b) compliance with legal, regulatory, KYC, AML, sanctions, and counter-terrorist financing requirements;
- (c) fraud detection, risk assessment, security monitoring, and prevention of misuse;
- (d) operation, maintenance, development, and improvement of the Platform and Services;
- (e) payment processing and administration of financial transactions;
- (f) customer support and communication;
- (g) dispute resolution, investigation, enforcement, and legal proceedings;
- (h) protection of the Company's rights, property, systems, and legitimate business interests; and
- (i) any other purpose permitted or required by Applicable Law.

Section 1.6: Disclosure and Sharing of Personal Data

The Company may disclose personal data where reasonably necessary for the purposes described in this Data Privacy Agreement, the Customer Terms of Use, or where otherwise permitted or required by Applicable Law.

1.6.1 Authorized Data Recipients

Personal data may be shared, where appropriate and necessary, with affiliates, service providers, payment providers, financial institutions, professional advisers, auditors, technology providers, compliance providers, and other third parties supporting the Company's operations.



Where appropriate, such disclosures shall be subject to confidentiality, security, contractual, or other safeguards required by Applicable Law.

1.6.2 Legal and Regulatory Disclosure

The Company may disclose personal data to courts, regulators, law enforcement authorities, governmental bodies, competent authorities, or other legally authorized recipients where required or permitted by Applicable Law, court order, regulatory requirement, or lawful request.

The Company may make such disclosure without prior notice to the Customer where notification is not legally required or where providing notice would be prohibited or would reasonably interfere with a legal, regulatory, security, or investigative process.

1.6.3 Requests Concerning Other Customers

The Company shall not disclose personal data relating to another Customer in response to a request unless such disclosure is legally permitted and the requester has demonstrated a valid legal basis or authority for obtaining the information.

The Company may reject any request where the applicable legal basis, authority, or supporting documentation is insufficient.

Section 1.7: Third-Party Websites and External Services

The Platform may contain links to, integrations with, or references to websites, applications, payment services, or other services operated by third parties.



The Company does not control third-party services and, unless expressly stated otherwise, is not responsible for their privacy practices, content, security measures, or data processing activities.

The Customer should review the applicable privacy notices and terms of any third-party service before providing personal data or using such service.

Section 1.8: Data Retention and Secure Disposal

The Company shall retain personal data for as long as reasonably necessary to fulfill the purposes for which it was collected and to satisfy applicable contractual, legal, regulatory, accounting, compliance, dispute resolution, security, and recordkeeping requirements.

Different categories of personal data may be retained for different periods depending on the applicable purpose and legal or regulatory requirements.

Once the applicable retention period has expired, personal data may be securely deleted, anonymized, destroyed, or otherwise disposed of in accordance with Applicable Law and the Company's applicable policies and procedures.

Section 1.9: Agreement Amendments

The Company may amend or update this Data Privacy Agreement from time to time to reflect changes in Applicable Law, regulatory requirements, technology, security practices, Services, or operational procedures.

The updated version may be published through the Official Website, Customer Portal, Platform, or another Official Communication Channel designated by the Company.



Unless otherwise required by Applicable Law, an updated Data Privacy Agreement shall become effective on the date specified by the Company or, where no date is specified, upon publication.

Section 1.10: Cross-Border Data Transfers

Personal data may be processed, stored, or accessed in jurisdictions outside the Customer's country of residence where reasonably necessary for the provision or administration of the Services or for other lawful purposes.

Where personal data is transferred across jurisdictions, the Company shall implement such safeguards as are required by Applicable Law and reasonably appropriate to the nature of the transfer and the personal data concerned.

The Customer acknowledges that the legal and regulatory framework governing personal data may differ between jurisdictions.

Section 1.11: Requests for Data Erasure

Subject to Applicable Law, the Customer may request the deletion or erasure of personal data held by the Company by submitting a request through the Company's designated communication channels.

The Company may require appropriate identity verification before processing such a request.

A request for deletion does not require the Company to delete personal data where retention is required or permitted by Applicable Law, regulatory obligations, contractual requirements, legal proceedings, dispute resolution, fraud prevention, security purposes, or other legitimate grounds.



Where deletion cannot lawfully be completed, the Company may retain the relevant information for the applicable retention period.

Section 1.12: Marketing Communications

The Company may send the Customer service-related, administrative, security, transactional, or other communications necessary for the operation and administration of the Customer Account and Services.

Where permitted by Applicable Law, the Company may also send promotional or marketing communications relating to the Company, its Services, or related products.

Where consent is required for promotional communications, the Customer may withdraw such consent in accordance with the applicable communication or preference-management procedures.

Withdrawal of consent to marketing communications shall not affect the Customer's receipt of communications that are necessary for the administration, security, or provision of the Services.

Section 1.13: Customer Responsibility and Indemnification

The Customer shall use the Platform and provide personal data in accordance with the Customer Terms of Use, this Data Privacy Agreement, Applicable Law, and any applicable instructions issued by the Company.

To the fullest extent permitted by Applicable Law, the Customer shall indemnify and hold harmless the Company, its affiliates, directors, officers, employees, agents, and service providers from claims, losses, liabilities, damages, costs, and reasonable expenses arising directly from:

- (a) the Customer's misuse of the Platform;
- (b) the Customer's breach of this Data Privacy Agreement or the Customer Terms of Use;
- (c) the Customer's provision of false, misleading, or unauthorized information; or
- (d) the Customer's violation of Applicable Law or the rights of another person.

The indemnification obligations under this Section shall apply only to the extent that the relevant loss or liability is attributable to the Customer's conduct and shall be subject to any limitations imposed by Applicable Law.

Section 1.14: Non-Waiver of Rights

A failure or delay by the Company in exercising or enforcing any right, power, or remedy under this Data Privacy Agreement shall not constitute a waiver of that right, power, or remedy.

Any waiver shall be effective only where expressly given by the Company in writing and shall apply only to the specific circumstance for which it was provided.