Capital Investment Club

Data Processing Addendum Summary

Operational summary of DPA topics for processing roles, subprocessors, security measures, rights requests, and incident notice.

Last updated: 06/07/2026

Purpose

This summary describes the operational topics CIC should cover in a Data Processing Addendum or similar data protection terms with customers, organizations, vendors, and partners where applicable.

Scope

This summary applies when CIC exchanges personal information, organization information, platform content, support records, transaction records, or technical data with customers, organizations, vendors, subprocessors, API providers, support providers, infrastructure providers, analytics providers, security providers, or other partners. It is not a substitute for executed legal terms, but it defines the minimum operational topics CIC should be prepared to address.

Processing Roles

CIC may act as a controller, processor, service provider, business, or platform operator depending on the feature, jurisdiction, and relationship. The applicable agreement should define the role clearly.

Where roles differ by feature, the agreement or service description should identify the role for each relevant processing activity. For example, CIC may independently determine purposes for account security and platform administration while processing organization-provided records according to organization instructions in specific workflows.

Processing Subject Matter

CIC may process data to provide:

- Account management
- User and organization profiles
- Pitches and grants
- Marketplace workflows
- Assessments
- Messaging
- Wallet and transaction workflows
- Support

- Security, fraud prevention, monitoring, and compliance

Data Categories

Relevant data may include:

- Identity and contact data
- Profile data
- Organization data
- Platform content
- Transaction and wallet records
- Support files and messages
- Technical and log data
- Verification and KYC-adjacent data

Data Subject Categories

Relevant individuals may include CIC users, organization members, founders, pitchers, investors, grantors, assessors, marketplace participants, support requesters, administrators, vendors, applicants, reviewers, and individuals whose information is submitted inside platform content.

Subprocessors and Vendors

CIC should maintain records of vendors and subprocessors that process data on CIC's behalf. Critical vendors should be reviewed before onboarding and at least annually.

Subprocessor records should include provider name, service purpose, data categories, processing location where known, security review status, contract/DPA status, breach notice terms, deletion support, and review cadence. CIC should provide notice or approval mechanisms where required by contract or law.

Security Measures

Applicable measures may include:

- Access controls
- Encryption in transit
- Encryption at rest where supported
- Logging and monitoring
- Vulnerability management
- Incident response
- Vendor review
- Secure SDLC
- Backup and recovery controls

Security measures should be mapped to the sensitivity of the data and service. Restricted data, wallet-adjacent records, identity verification evidence, support files, and organization administration records require stronger access control, monitoring, and retention discipline than public website content.

Data Subject Requests

CIC should maintain a process to help respond to valid data access, correction, deletion, portability, objection, or restriction requests where legally applicable.

Deletion and Return

Agreements should define how data is returned or deleted at termination, subject to legal, financial, security, fraud prevention, audit, and operational retention requirements.

Incident Notification

Agreements should define notification obligations for security or privacy incidents affecting protected data.

Notification terms should define the trigger, timing, communication path, required content, follow-up updates, cooperation expectations, and any law enforcement or regulator considerations. CIC should avoid making unsupported guarantees that conflict with the Incident Response Policy or vendor contract terms.

Audit and Assurance

CIC should be prepared to provide reasonable evidence of its security and privacy controls, subject to confidentiality and operational constraints.

Evidence may include policy summaries, control registers, access review evidence, vendor review evidence, risk assessment summaries, incident response summaries, penetration test or assessment summaries, secure SDLC evidence, and business continuity evidence. Detailed logs, source code, sensitive architecture, customer data, and exploit details should be shared only under appropriate confidentiality and need-to-know controls.

Contractual Safeguards

Where CIC processes data for customers, organizations, vendors, or partners, data protection terms should address:

- Processing instructions.
- Confidentiality obligations.
- Security controls.
- Subprocessor approval or notice.
- Cross-border transfer safeguards where required.
- Assistance with data rights requests.
- Assistance with security incident investigation.
- Data return or deletion.
- Audit, assessment, or assurance support.
- Liability and limitation language aligned with the commercial agreement.

Cross-Border Transfers

Where data is transferred across jurisdictions, CIC should evaluate transfer requirements and document

appropriate safeguards. Safeguards may include contractual clauses, data processing terms, vendor transfer documentation, technical controls, data minimization, and risk-based review of destination countries and providers.

Processor Instructions and Change Control

Where CIC processes data on behalf of a customer or organization, processing instructions should be documented in the agreement, product configuration, support ticket, or approved workflow. Material processing changes should be reviewed for privacy, security, and contract impact before release.

Data Return, Deletion, and Retention Constraints

Data return and deletion commitments must account for legal, financial, security, fraud prevention, audit, dispute, operational, backup, and recordkeeping obligations. CIC should distinguish between active production deletion, backup expiration, anonymization, suppression, and retained audit records.

Assistance Obligations

Where required, CIC should be prepared to reasonably assist with:

- Data subject requests.
- Security incident investigation.
- Privacy impact or transfer assessments.
- Audit or assurance inquiries.
- Deletion or return requests.
- Subprocessor information requests.

Conflict Handling

If a customer instruction conflicts with law, security obligations, platform integrity, another user's rights, or CIC's financial/audit obligations, CIC should document the conflict, notify the appropriate party where allowed, and escalate to legal or leadership before acting.

Subprocessor Register

CIC should maintain a subprocessor register with provider name, service purpose, data categories, location, security review status, contract status, and review cadence.

DPA Evidence

CIC should retain executed DPAs, vendor data processing terms, subprocessor review records, security exhibits, and data deletion or return evidence.

Review

This summary must be reviewed at least annually and when CIC introduces a material new vendor, cross-border transfer, data category, customer contract model, or regulated integration.