Capital Investment Club

# Data Subject Rights Policy

Request intake, identity verification, review, response, and evidence for user data rights requests.

Last updated: 06/07/2026

## Purpose

This policy defines how CIC receives, validates, processes, and responds to user data rights requests where applicable.

## Scope

This applies to requests involving personal information processed through CIC websites, applications, support workflows, user accounts, organization accounts, pitches, grants, marketplace features, assessments, messaging, wallet-related records, and logs.

## Supported Request Types

Depending on applicable law and operational context, users may request:

- Access to personal information.
- Correction of inaccurate information.
- Deletion of personal information.
- Restriction or objection to processing.
- Portability of personal information.
- Information about processing.
- Support with privacy settings or public profile visibility.

## Request Intake

Requests should capture:

- Requester identity
- Account or organization context
- Request type
- Data scope
- Date received
- Verification status
- Response deadline
- Assigned owner

- Final disposition

## Intake Channels

CIC should accept privacy and data rights requests through authenticated account settings where available, support channels, published privacy contact channels, and legally required written channels. Requests received by sales, support, engineering, or leadership must be routed to the privacy owner or governance administrator and logged in the data rights request register.

If a request is made through an unauthenticated channel, CIC should avoid disclosing account existence or sensitive information until identity and authority have been verified.

## Verification

CIC must verify the requester before disclosing, changing, deleting, or exporting account-related information. Verification may use authenticated session context, email verification, phone verification, support codes, or other appropriate methods.

Verification must be proportionate to the sensitivity of the requested action:

- Low sensitivity: authenticated session plus confirmation of request intent.
- Medium sensitivity: authenticated session plus email or phone verification.
- High sensitivity: stronger verification, support code, recent login confirmation, or manual review.
- Organization data: confirmation that the requester has authority for the organization context.

CIC must not rely only on possession of an email address for requests involving wallet records, transaction records, organization administration, uploaded documents, support files, or other restricted data.

## Authorized Agents and Representatives

If a request is submitted by an authorized agent, CIC should require proof of authority and may require the user or organization owner to verify the request directly. CIC should record the agent's identity, authorization evidence, scope, and expiration.

## Review

CIC should review whether the requested data can be changed, deleted, exported, or disclosed. Some records may need to be retained for legal, financial, fraud prevention, security, audit, dispute, or operational reasons.

## Response Time Objectives

CIC should acknowledge data rights requests promptly and assign an owner within five business days. CIC should target completion within thirty calendar days unless a shorter or longer period is required or allowed by applicable law. If additional time is needed because the request is complex, broad, or requires third-party coordination, CIC should notify the requester where required and document the reason.

## Response

Responses should be accurate, understandable, and provided within applicable timelines. If CIC denies or limits a request, the reason should be documented.

Responses must avoid disclosing another user's personal information, confidential organization information, security-sensitive logs, fraud detection logic, proprietary scoring logic, or information that would compromise platform security.

# Request Workflow

1. Log request and requester. 2. Verify identity and account context. 3. Determine request type and legal applicability. 4. Search relevant systems and records. 5. Identify retention, legal, security, fraud, financial, and operational constraints. 6. Prepare response or action plan. 7. Complete approved correction, deletion, export, or restriction. 8. Send response. 9. Retain request evidence.

# Denial or Limitation Reasons

CIC may deny, limit, or defer a request where legally permissible because:

- Identity cannot be verified.
- The requester lacks authority for the account or organization.
- The record must be retained for legal, financial, accounting, security, fraud prevention, audit, or dispute reasons.
- The request is excessive, abusive, or technically infeasible.
- The request would disclose another user's information or confidential business information.

# Systems to Search

Depending on scope, CIC should consider user profile records, organization records, support tickets, public profile data, pitches, grants, marketplace records, assessments, messages, wallet/transaction records, logs, uploaded files, and vendor systems.

# Request Type Procedures

## Access and Portability

CIC should provide a reasonably complete export of personal information in a secure format. Exports should include profile metadata, account settings, organization relationships, submitted content, public profile data, support records, and wallet or transaction records that are legally and operationally appropriate to disclose.

## Correction

CIC should allow users to correct routine profile and contact information directly where possible. Corrections to financial, legal, KYC-adjacent, audit, transaction, grant, investment, or historical records may require review, annotation, or retention of the original record.

## Deletion

Deletion requests must be evaluated against retention requirements. CIC may anonymize, suppress, restrict, or delete data depending on record type. Financial, audit, security, fraud, tax, dispute, and legal records may be

retained where required or justified.

### Restriction, Objection, and Visibility

CIC should support reasonable restriction requests, including public profile visibility controls, communication preferences, and non-essential processing choices. Some processing may continue where necessary to provide the service, comply with legal obligations, prevent fraud, maintain security, or preserve transaction integrity.

## Vendor and Subprocessor Coordination

If responsive data is held by a vendor or subprocessor, CIC should coordinate the request according to vendor contracts and data processing terms. Vendor actions should be logged with date requested, date completed, evidence received, and unresolved limitations.

## Secure Delivery

Data exports should be delivered through authenticated download, encrypted file transfer, or another secure channel. CIC should avoid sending sensitive exports through plain email attachments unless encrypted or otherwise protected.

## Metrics and Monitoring

CIC should monitor:

- Number of requests received.
- Request types.
- Average completion time.
- Requests completed within deadline.
- Denials or limitations.
- Open overdue requests.
- Vendor-dependent requests.
- Repeat or complaint-driven requests.

## Evidence

Required evidence:

- Request record
- Verification result
- Systems searched
- Data provided or action taken
- Denial or limitation reason
- Response date
- Reviewer
- Approval for high-risk disclosure, deletion, or denial decisions
- Vendor/subprocessor actions where applicable

- Secure delivery evidence for exports

## Review

This policy must be reviewed at least annually.