Capital Investment Club

Transfer Impact Assessment

CIC assessment of international personal-data transfers, destination-country risks, transfer mechanisms, safeguards, residual risks, and required approvals.

Status: Draft for external legal and privacy review
Version: 0.9
Supersedes: None - initial publication
Last reviewed: 12 August 2026
Next review: 12 November 2026
Owner: Privacy and compliance owner - confirmation required
Approver: Executive owner and privacy counsel - pending

Document control	Value
Document ID	CIC-PIA-TIA-001
Version	0.9
Superseded version	None - initial publication
Status	Draft for external legal and privacy review
Publication classification	Public
Owner	Privacy and compliance owner - confirmation required
Approver	Executive owner and privacy counsel - pending
Effective date	Pending approval
Last reviewed	12 August 2026
Next review	12 November 2026 or earlier after a material change

Executive determination

Capital Investment Club uses cloud, communications, identity, financial, support, and collaboration services that may make personal information available across national borders. CIC has implemented meaningful technical and organizational safeguards, including encryption for selected restricted identifiers, role-based access, audited sensitive-data reveal, correction and appeal workflows, notification preference separation, retention analysis, and compliance reporting.

This assessment does not approve every transfer. The codebase confirms integration capability, but code alone cannot prove which provider is active in production, the contracted legal entity, the selected storage region, remote-support locations, executed transfer clauses, or Data Privacy Framework participation. Transfers involving

restricted identity information, financial identifiers, recordings, or unknown storage and support locations remain High until those facts and mechanisms are confirmed by authorized owners.

CIC may publish this report as a transparent working assessment. It must remain labelled Draft for external legal and privacy review until the approval schedule is complete. AI-assisted preparation is not legal advice and is not a substitute for controller, privacy-owner, executive, or counsel approval.

Purpose

This Transfer Impact Assessment evaluates whether personal information retains an appropriate level of protection when CIC makes it available to a separate organization or operational team in another country. It supports:

- European Union GDPR transfer assessment and supplementary-measures analysis.
- United Kingdom transfer risk assessment and data protection test analysis.
- Nigeria Data Protection Act cross-border transfer accountability.
- Canadian accountability and comparable-protection expectations.
- CIC vendor, security, privacy, retention, incident, and governance controls.

The assessment considers both transmission and remote access. A provider or support team does not need to copy a dataset to create a transfer risk; access from another jurisdiction can be relevant.

Scope

Systems reviewed

- CIC member web application.
- CIC API and data services.
- CIC notification service.
- CIC public website, careers, and Governance Center.
- Cloud hosting and object storage configuration.
- Database connectivity and application data models.
- Authentication and social sign-in.
- Wallet, payment, bank-data, verification, and marketplace integrations.
- Video, support, and recording integrations.
- Source control, build, deployment, and operational evidence workflows.

Data subjects

- Guests, investors, pitchers, assessors, grant participants, and other CIC members.
- Organization members, directors, controllers, beneficial owners, and representatives where collected.
- Applicants, referees, support requesters, and public-profile visitors.
- Administrators, reviewers, approvers, support personnel, contractors, and vendor contacts.

Data categories

- Account, authentication, contact, role, profile, and organization data.

- Nationality, residence, tax residency, and eligibility information.
- Government identity documents, photographs, address evidence, and KYC/KYB records.
- Financial and national identifiers, bank-data responses, and verification outcomes.
- Wallet, ledger, payment, contribution, bid, grant, pitch, receipt, and reconciliation records.
- Messages, notifications, support records, attachments, consent records, calls, and recordings.
- IP address, device, browser, location, session, security, fraud, analytics, and audit signals.
- Careers application, resume, and employment-related information.

Exclusions

- Employee payroll and benefits systems not present in the reviewed repositories.
- Provider contract terms that were not available in the reviewed evidence.
- Provider account-console settings and current subprocessor subscriptions not independently exported.
- Legal conclusions about a specific CIC corporate entity until the controller identity is confirmed.
- Transfers initiated independently by users outside CIC-controlled workflows.

Assessment method

For each transfer family CIC applies the following sequence:

- Map the exporter, importer, roles, purpose, data, subjects, frequency, duration, and access method.
- Distinguish deployed configuration from optional integration capability.
- Identify source, storage, processing, remote-access, support, and onward-transfer locations.
- Identify adequacy, certification, contractual safeguard, or permitted exception relied upon.
- Evaluate destination-country government access, oversight, enforceability, and individual redress.
- Evaluate practical likelihood and severity using the actual transfer context.
- Evaluate contractual, technical, and organizational supplementary measures.
- Record inherent risk, residual risk, blockers, treatment, owner, and review trigger.

This method follows the EDPB Recommendations 01/2020 (https://www.edpb.europa.eu/documents/recommendation/recommendations-012020-on-measures-that-supplement-transfer-tools-to_en), the European Commission Standard Contractual Clauses decision (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en), and the ICO transfer risk assessment guidance (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/completing-a-transfer-risk-assessment/).

Evidence standard

Evidence state	Meaning	Permitted conclusion
Confirmed	Deployed configuration, authoritative owner record, executed agreement, provider console export, or other durable evidence confirms the fact.	The report may state the fact without qualification.
Integration evidenced	Source code, dependency, route, workflow, or environment-variable name proves CIC can use the service.	The report may identify transfer potential but must not claim current production use.

Evidence state	Meaning	Permitted conclusion
Confirmation required	Contract, provider account, storage region, support location, certification, or mechanism was unavailable.	The report must show an open owner action and cannot mark the transfer approved.

LIA and remediation reconciliation

This assessment reconciles the legitimate-interests assessment and remediation work recorded in the controlled CIC governance evidence for webapp issues 2140 and 2142 as of 12 August 2026. The public report does not reproduce private issue content, screenshots, personal data, or restricted implementation evidence.

The controlled evidence index identifies those records as:

- EVD-LIA-2140: revised CIC legitimate-interests assessment, balancing analysis, and identified open risks.
- EVD-LIA-2142: LIA remediation control matrix, implementation evidence, and verification record.

The LIA addresses whether identified processing can rely on legitimate interests; this TIA separately addresses whether international availability and onward access preserve required protection. Completion of one does not automatically approve the other. Where the LIA, production inventory, contract evidence, or transfer evidence is incomplete, this TIA retains Confirmation required status.

Current transfer architecture

The reviewed repositories confirm that CIC services are deployed using Google App Engine and use Google Cloud object storage capabilities. The public application endpoints indicate a United States Google Cloud deployment region, but the exact contractual customer entity, service-specific data-location commitments, backups, and support access locations require owner confirmation.

The services connect to MongoDB-compatible databases. The connection configuration does not by itself prove whether the database is MongoDB Atlas, another managed provider, or a self-managed deployment, nor does it prove the cluster region. Database provider and location are therefore confirmation requirements.

The API contains integrations or configuration paths for payment, banking, identity, video, email, notification, analytics, e-signature, and file-storage services. The Transfer Processing Inventory (/governance/documents/transfer-processing-inventory) identifies each family and the evidence boundary.

Transfer family determinations

Transfer family	Data sensitivity	Current conclusion	Residual risk
Cloud application hosting and object storage	Confidential and Restricted	Transfer occurs where global users submit data to the US-hosted CIC services. Provider terms and configured regions must be confirmed.	Medium-High
Primary application database	Confidential and Restricted	Database use is confirmed; provider, region, support access, DPA, and transfer mechanism are not confirmed.	High

Transfer family	Data sensitivity	Current conclusion	Residual risk
Authentication and Google OAuth	Account and authentication metadata	Integration is evidenced. Production activation and provider agreement require confirmation.	Medium
Payments, wallets, banking, and financial verification	Restricted financial and transaction data	Multiple provider integrations are evidenced. Activation, data fields, legal entity, location, and mechanism must be confirmed provider by provider.	High
Identity and KYC/KYB verification	Restricted identity and financial identifiers	CIC stores and reviews sensitive evidence. Any external verification transfer requires provider-specific confirmation and heightened safeguards.	High
Email, notification, and messaging delivery	Contact, message, security, and workflow data	Delivery services are confirmed as a processing class; the selected production provider and transfer terms require confirmation.	Medium-High
Video, calls, screen sharing, and recording	Audio, video, session, identity, and support data	Agora integration and cloud-recording configuration are evidenced. Production routing, recording region, and support access require confirmation.	High
Public-site careers applications	Contact, resume, and application data	Website uses cloud hosting, database, object storage, OAuth, and email delivery capabilities. Exact locations and agreements require confirmation.	Medium-High
Source control and deployment	Source, configuration, test data, logs, and governance evidence	GitHub Actions use is confirmed. End-user data should not be placed in source or build logs; evidence uploads require classification.	Medium
Personnel and contractor remote access	Potential access to all authorized categories	Role controls exist, but workforce locations and recurring access certification require confirmation.	High

European Union and EEA analysis

Personal information subject to EU GDPR may leave the EEA when a CIC user submits it to a service hosted outside the EEA or when a non-EEA provider or support team can access it. An adequacy decision can support an in-scope transfer. Canada adequacy is limited to covered commercial organizations, and United States adequacy is limited to organizations participating in the EU-US Data Privacy Framework. CIC must verify scope and current participation before relying on adequacy.

Where adequacy does not apply, the current EU Standard Contractual Clauses may provide an Article 46 safeguard. The clauses do not remove the need to assess destination-country laws and practices and apply effective supplementary measures. CIC must retain the executed module, annexes, subprocessor flow-down, security measures, and transfer assessment.

No provider is treated as DPF-certified or covered by Canadian adequacy solely because it is based in the United States or Canada.

United Kingdom analysis

For a restricted transfer subject to UK GDPR, CIC must identify whether adequacy regulations apply or use an appropriate safeguard such as the UK International Data Transfer Agreement or the UK Addendum to EU SCCs. When using an appropriate safeguard, CIC must complete a transfer risk assessment, now described in UK legislation as a data protection test, and decide reasonably and proportionately that protection is not materially lower after transfer.

The ICO international transfer guidance (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/) and ICO TRA tool (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/completing-a-transfer-risk-assessment/the-ico-s-tra-tool/) inform this report. Execution of an IDTA or Addendum has not been evidenced for the reviewed providers and remains pending confirmation.

Nigeria analysis

Sections 41 to 43 of the Nigeria Data Protection Act address transfers outside Nigeria. CIC must document an adequate level of protection or another lawful statutory basis and retain evidence of the transfer analysis. The Nigeria Data Protection Commission guidance (https://ndpc.gov.ng/faqs/) confirms that controllers and processors must ensure adequate protection for personal data transferred abroad.

Nigerian KYC, financial, nationality, tax, wallet, and identity information has high potential impact. Export to global infrastructure or non-Nigerian providers should not be approved until the recipient, destination, contract, access path, and safeguards are confirmed. Consent must not be used as a routine substitute for an available, sustainable transfer mechanism.

Canada analysis

PIPEDA uses an accountability model for transfers to third parties for processing. CIC remains responsible and should use contractual or other means to provide comparable protection, assess the provider, limit use, and explain that information may be processed abroad and accessible under foreign law. The Office of the Privacy Commissioner of Canada cross-border guidance (https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/) is the primary source used here.

Provincial laws may add requirements. Quebec, Alberta, and British Columbia applicability must be reviewed when CIC confirms Canadian establishment, targeting, user population, and processing operations.

United States analysis

The United States has sectoral federal and state privacy rules rather than one comprehensive federal private-sector data protection law. US service providers can be subject to lawful government demands. The US Department of Justice CLOUD Act resources (https://www.justice.gov/criminal/cloud-act-resources) explain that US-based providers may be compelled to produce data within their possession, custody, or control, including data held abroad in qualifying circumstances.

The EU-US Data Privacy Framework may provide adequacy only for an organization currently listed for the

relevant data and recipient. Otherwise CIC must use an appropriate transfer tool and supplementary measures. Encryption materially reduces exposure only when the recipient does not require intelligible access and keys remain under separate control; it is not a universal solution for SaaS providers that must process plaintext.

Necessity and proportionality

International infrastructure can be necessary to provide a reliable platform to users in several countries, support payments and verification, deliver security notices, and operate support. Necessity is not established merely because an integration exists or a provider is convenient.

Before approving each provider, CIC must demonstrate:

- The service purpose cannot reasonably be met with materially less data.
- Optional integrations are disabled until approved.
- Restricted fields are excluded when not required.
- Provider retention and onward use are bounded.
- Production and test environments do not use real restricted data unnecessarily.
- Support access is just-in-time, authorized, and audited where available.
- A transfer can be suspended without corrupting financial or compliance records.

Supplementary safeguards

Existing or required safeguards include:

- TLS for data in transit.
- Provider and service-specific encryption at rest.
- Application-level encryption for selected KYC and financial fields.
- Separation and rotation of encryption and authentication secrets.
- Masking by default and reason-gated, audited reveal for restricted identifiers.
- Role-based reviewer, approver, administrator, and support authorization.
- Restricted-document access and audit events.
- Data minimization in notification templates, logs, exports, and support artifacts.
- Contractual purpose limitation, confidentiality, incident notice, deletion, audit, onward-transfer, and government-request provisions.
- User correction, appeal, objection, and support paths.
- Retention schedules, legal holds, approved exceptions, and report-only deletion analysis.
- Transfer suspension, provider offboarding, and incident escalation procedures.

The Transfer Safeguards and Controls (/governance/documents/transfer-safeguards-and-controls) report records implementation and evidence status.

Government access and enforceability

Contractual clauses bind the recipient but do not bind a foreign public authority. CIC must consider both third-party access and whether CIC and affected individuals can enforce the transfer safeguard. The practical assessment must use the data, recipient, purpose, industry, request history where available, and technical architecture rather than a country label alone.

For providers that need intelligible access to perform the service, contractual and organizational measures carry more weight. For storage where CIC can retain exclusive key control, strong encryption and pseudonymization may materially reduce access risk. These architectural facts require service-by-service confirmation.

Data subject rights and transparency

CIC's Privacy Policy states that cloud, support, analytics, payment, notification, security, and infrastructure providers may process data in different jurisdictions. Before final approval CIC must verify that notices clearly describe:

- Relevant transfer purposes and provider categories.
- Countries or meaningful destination categories.
- The relied-upon safeguard or how a copy can be requested where required.
- Foreign government-access risk where meaningful notice requires it.
- Rights, complaint, correction, appeal, and privacy-contact routes.

Product restrictions must not prevent a user from reaching privacy, support, correction, or appeal channels.

Residual risk conclusion

Risk class	Determination
Low	No material transfer family is currently classified Low because provider account and contract evidence was not available for this assessment.
Medium	Source control and limited technical metadata may be acceptable with minimization, access control, and evidence-classification controls.
Medium-High	Cloud hosting, careers applications, authentication, and communications may be acceptable after contract, region, subprocessor, and mechanism confirmation.
High	Primary database, restricted KYC/financial transfers, recordings, unknown providers, and unconfirmed workforce access locations require confirmation and approval before being represented as closed.

Overall TIA posture: Medium-High, with High transfer-specific risks awaiting owner and counsel confirmation.

Decision rules

- Proceed: transfer facts, mechanism, destination analysis, safeguards, and approvals are complete; residual risk is accepted.
- Proceed with conditions: temporary use is approved with explicit compensating controls, owner, expiration, and remediation.
- Suspend new data: material facts or safeguards are missing for Restricted data; no new transfer should begin until resolved.
- Stop: destination conditions or recipient capabilities prevent an essentially equivalent or otherwise legally acceptable level of protection and no effective exception applies.

This draft does not issue a blanket Proceed decision. The Transfer Risk Register (/governance/documents/transfer-risk-register) and Transfer Remediation and Review Plan

(/governance/documents/transfer-remediation-and-review-plan) control the outstanding decisions.

Approval schedule

Before changing the status to Approved, CIC must record:

- Confirmed controller legal entity and establishment.
- Named privacy/compliance owner and executive risk owner.
- Complete processor, subprocessor, region, and remote-access inventory.
- Executed DPA and transfer mechanism for each active provider.
- DPF certification checks where relied upon.
- Privacy counsel approval of jurisdiction and mechanism conclusions.
- Executive acceptance of any remaining Medium-High or High residual risk.
- Confirmation that public and restricted evidence locations are appropriate.

Review triggers

Review at least quarterly while in Draft and at least annually after approval. Review immediately when:

- A provider, subprocessor, storage region, or support location changes.
- CIC introduces a new data category, KYC requirement, payment rail, recording mode, analytics capability, or AI service.
- A transfer mechanism, adequacy decision, certification, or material destination law changes.
- A government-access request, privacy incident, contract breach, or audit finding affects a transfer.
- CIC changes controller entity, establishment, user geography, or operating model.
- A provider cannot comply with its transfer obligations or supplementary safeguards.

Related reports

- Executive Summary (/governance/documents/transfer-impact-assessment-executive-summary)
- Transfer Processing Inventory (/governance/documents/transfer-processing-inventory)
- Transfer Jurisdiction Assessments (/governance/documents/transfer-jurisdiction-assessments)
- Transfer Vendor and Subprocessor Assessment (/governance/documents/transfer-vendor-and-subprocessor-assessment)
- Transfer Safeguards and Controls (/governance/documents/transfer-safeguards-and-controls)
- Transfer Risk Register (/governance/documents/transfer-risk-register)
- Transfer Remediation and Review Plan (/governance/documents/transfer-remediation-and-review-plan)
- Transfer Assessment Evidence Index (/governance/documents/transfer-assessment-evidence-index)

Limitation

This is an evidence-based governance assessment prepared with AI assistance. It is not legal advice, a certification, a warranty, or proof that every referenced contract or control is in force. Authorized CIC owners and qualified counsel must confirm factual and legal conclusions before approval.