

# Transfer Vendor and Subprocessor Assessment

Public-safe assessment of provider integrations evidenced in CIC repositories and the contractual or location facts that authorized owners must confirm.

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 vendor-risk owners - confirmation required  
Approver: Executive owner and privacy counsel - pending

| Document control           | Value                                                  |
|----------------------------|--------------------------------------------------------|
| Document ID                | CIC-PIA-TIA-005                                        |
| Version                    | 0.9                                                    |
| Superseded version         | None - initial publication                             |
| Status                     | Draft for external legal and privacy review            |
| Publication classification | Public                                                 |
| Owner                      | Privacy and vendor-risk owners - 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    |

## Purpose

This report assesses vendor families evidenced in CIC repositories and states what must be confirmed before a transfer can be approved. It intentionally does not publish account identifiers, credentials, private endpoints, detailed security topology, contracts, or restricted provider evidence.

An integration in source code proves capability, not production activation. A named provider must remain Confirmation required until an authorized owner reconciles source evidence with contracts, invoices, production consoles, data-flow logs, and the vendor register.

# Required vendor evidence set

Every active provider must have a controlled record containing:

- provider and contracting legal entities;
- product, account owner, business purpose, and controller/processor role;
- categories of data and data subjects;
- production activation and feature configuration;
- storage, processing, backup, support, and remote-access locations;
- current subprocessor list and change-notification subscription;
- executed contract, DPA, security exhibit, and deletion/return terms;
- transfer mechanism, completed annexes, certification scope, and effective date;
- encryption, key management, access, logging, incident, continuity, and deletion controls;
- government-request policy and relevant transparency information;
- inherent risk, residual risk, exceptions, approvals, and next review.

## Provider-family assessment

| Provider family                  | Repository evidence                                                      | Primary transfer concern                                                                      | Required closure evidence                                                                                                 | Current risk                           |
|----------------------------------|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| Google Cloud hosting and storage | Deployment and storage integrations confirmed                            | Global submission to US-hosted services; storage, backup, support, and subprocessor locations | Contracting entity, DPA, service regions, transfer terms, subprocessor record, security settings, retention               | Medium-High; High for Restricted files |
| MongoDB-compatible database      | Database connectivity confirmed                                          | Broad data concentration and unknown provider, cluster, backup, and support locations         | Provider identity, cluster topology, region, DPA, clauses, encryption/key evidence, access and backup controls            | High                                   |
| Google identity and APIs         | OAuth and API capabilities evidenced                                     | Account, authorization, profile, media, and metadata exposure across global service locations | Active APIs, configured scopes, entity, terms, retention, transfer mechanism, revocation and deletion controls            | Medium to Medium-High                  |
| Email and notifications          | Resend, SendGrid, and AWS SES/SNS capabilities evidenced across services | Message content, addresses, delivery metadata, and subprocessor routing                       | Active provider per message type, entity, location, DPA, minimization, template review, suppression and deletion evidence | Medium-High                            |
| Paystack                         | Payment capability evidenced                                             | Identity, payment, reference, bank-partner, and transaction data                              | Production status, provider entity, DPA, banking recipients, location, retention, mechanism, incident terms               | High                                   |
| Stripe                           | Payment and connected-account capability evidenced                       | Identity, business, bank, payment, compliance, and global subprocessor data                   | Enabled products, account country, entity, DPA, DPF or clauses, connected-account roles, retention and deletion           | High                                   |

| Provider family                                | Repository evidence                                                                             | Primary transfer concern                                                                                      | Required closure evidence                                                                                              | Current risk        |
|------------------------------------------------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|---------------------|
| Embedly                                        | Wallet and bank-transfer capability evidenced                                                   | Identity, wallet, bank-transfer, inflow, and webhook data                                                     | Provider identity, production status, data map, contract, DPA, location, banking partners, security and transfer basis | High                |
| Mono                                           | Financial-data capability evidenced                                                             | Linked bank account, transactions, verification, and connected-institution roles                              | Enabled products, provider and bank roles, consent, retention, deletion, DPA, location, transfer mechanism             | High                |
| Plaid                                          | Financial-data capability evidenced                                                             | Bank, account, balance, transaction, identity, and token processing                                           | Enabled products/countries, entity, DPA, certification or clauses, bank roles, retention, deletion and user controls   | High                |
| Agora                                          | Real-time video and cloud recording capability evidenced                                        | Voice, video, screen, identity, routing, recording, and storage locations                                     | Production use, routing region, recording configuration, consent, contract, DPA, subprocessors, retention, deletion    | High                |
| Electronic signature                           | Generic capability evidenced; provider identity not confirmed                                   | Agreement content, signatures, identity, and audit trail                                                      | Name provider, entity, service, contract, DPA, location, authentication, retention, export and deletion                | High                |
| GitHub and Actions                             | Use confirmed                                                                                   | Contributor data, source/configuration, workflow logs, fixtures, issue evidence, and accidental personal data | Organization terms, DPA, region options, retention, access review, secret scanning, evidence classification            | Medium              |
| Analytics, observability, and error monitoring | Monitoring and analytics capability evidenced; active provider and payload require confirmation | Telemetry can unintentionally capture identifiers, content, URLs, tokens, or errors and route them globally   | Provider, payload schema, redaction, sampling, location, DPA, mechanism, retention, access, and deletion               | Medium-High         |
| External counsel, auditors, and responders     | Controlled disclosure is contemplated by governance policies                                    | Case-specific disclosure of governance, incident, user, transaction, or security records                      | Recipient, necessity, minimization, confidentiality, location, mechanism, access duration, return/deletion record      | Medium-High to High |

## Google Cloud-specific assessment

CIC's repository evidence confirms Google App Engine deployment and Google Cloud storage capability. The public deployment endpoint supports an inference that the hosted application is in a United States region. The exact billing entity, contractual customer, storage bucket regions, backup locations, support settings, and enabled services are not established by source code.

Owner evidence must include the service inventory, project and resource regions in a controlled export, current Google Cloud Data Processing and Security Terms (<https://cloud.google.com/terms/data-processing-addendum>), applicable Google Cloud subprocessors (<https://cloud.google.com/terms/subprocessors>), transfer terms,

encryption settings, privileged access controls, logging, deletion, backups, and support configuration. The public report records conclusions, while the controlled evidence repository retains sensitive exports.

## Financial and identity providers

Financial and identity integrations receive enhanced scrutiny because they can combine identity, national identifier, bank, wallet, payment, transaction, and compliance information. CIC must not approve all configured rails as a group. Each enabled product and country combination requires its own recipient, purpose, data-field, retention, security, incident, onward-transfer, and mechanism decision.

Minimum conditions are:

- production activation is explicitly approved;
- data fields are limited to the selected product requirement;
- user notice and consent or other legal basis are documented;
- webhook payloads are authenticated and replay-safe;
- provider data is not duplicated into application logs;
- credentials and secrets remain outside source control;
- sandbox and production data are segregated;
- deletion, account closure, reconciliation, dispute, and incident workflows are defined;
- provider support access is time limited and recorded where available.

## Communications and recordings

Email, push, SMS, voice, video, and recording providers can expose message content and metadata to global infrastructure. CIC must maintain a channel-to-provider map. Restricted identifiers, credentials, full bank data, and identity documents must not appear in notification content. Recording must default off unless a documented workflow requires it, and consent, access, storage location, retention, and deletion must be configured before use.

## Subprocessor governance

For each active provider CIC must:

- retain the approved subprocessor list and retrieval date;
- subscribe to change notifications where available;
- identify each subprocessor's service and country;
- assess material additions before the objection period expires;
- document the decision to accept, mitigate, replace, or object;
- ensure onward-transfer obligations are no less protective than the primary contract;
- update notices and this assessment where the change is material.

## Provider change decision

| Change                      | Required response                                                  |
|-----------------------------|--------------------------------------------------------------------|
| New provider or new product | Complete diligence and transfer assessment before production data. |

| Change                                  | Required response                                                                     |
|-----------------------------------------|---------------------------------------------------------------------------------------|
| New country or remote-support location  | Complete jurisdiction assessment before new Restricted-data access.                   |
| New material subprocessor               | Assess, approve, mitigate, or object within the contractual window.                   |
| New Restricted data or expanded purpose | Reassess necessity, mechanism, security, retention, and user notice.                  |
| Contract or certification expiry        | Suspend reliance on the affected mechanism until renewed or replaced.                 |
| Material incident or government request | Reassess practical risk, safeguards, and continuation decision immediately.           |
| Provider termination                    | Revoke access and credentials; verify export, return, deletion, and residual backups. |

## Current conclusion

Repository review provides a credible starting inventory but not enough evidence for blanket provider approval. The most material gaps are the active-provider list, database identity and location, executed transfer terms, subprocessor reconciliation, workforce access countries, and recording configuration. These are tracked in the Transfer Remediation and Review Plan (/governance/documents/transfer-remediation-and-review-plan).

## Limitation

This report was prepared with AI assistance from repository and governance evidence. Authorized vendor, privacy, security, finance, and legal owners must validate it against production and contractual evidence.