

01 / SCOPE & OVERVIEW

Security, Data Handling & Integration Reliability

Public security and compliance whitepaper

CompanyConnect.Tech | Version 1.0 | 19 October 2026

Connected systems need explicit decisions about data, access, consequential actions and recovery. This paper explains questions to resolve before go-live and the evidence to retain afterwards. It supports a scoped project conversation; it does not replace the governing agreement.

Three kinds of evidence

Website observations describe the mapper behaviour visible in the current implementation. Project design guidance describes controls and acceptance checks to agree and verify in selected accounts. Vendor statements are attributed documentation, not an audit of CompanyConnect configurations.

Operating standard

Scope the data: Identify records, sensitivity, ownership and storage locations. Providers do not necessarily share hosting or retention terms.

Choose access deliberately: Agree who grants, reviews and revokes role-appropriate access. Keep credentials out of ordinary project messages.

Control consequential actions: Define approvals and reconcile repeated events, failures and uncertain writes before taking the next action.

Test and hand over: Agree acceptance checks, recovery instructions and exception owners. A design principle alone does not prove installation.

Boundaries

This paper is not GDPR/POPIA certification, an ISO/SOC attestation, a data-processing agreement or a service-level agreement. Hosting location, subprocessors, retention, backup, incident response and service commitments must be confirmed for the selected platforms and governing agreement. No universal encryption, purge or uptime guarantee is implied.

[Read the public Trust Center](#)

Know what is shared, and why

Observed mapper behaviour

The tech stack mapper generates a preliminary roadmap locally in your browser. Work email, selected apps and bottleneck are shared with Ray only after the explicit consent checkbox and share action. Generating a roadmap or copying it is not a CRM save or marketing opt-in; the copy omits email. Sharing a mapper brief does not itself submit a CRM record. Follow the contact review and explicit submission steps shown by Ray before an enquiry is saved.

This description is mapper-specific. It is not a claim that the whole website has no analytics or network activity. Read the existing website privacy policy for the wider website. For access, correction or deletion enquiries, contact letsconnect@companyconnect.tech. Do not put passwords or confidential client records into an initial enquiry.

[Existing website privacy policy](#)

[Access, correction and deletion contact](#)

Responsibilities to resolve

For GDPR or POPIA questions, document purposes and lawful basis, responsible party/controller and operator/processor roles, the relevant agreements, security responsibilities and data rights. Check cross-border transfers, provider regions and the people who can access each selected account.

Use the official POPIA Act, including retention, security, operator, incident and cross-border provisions, and regulator guidance on GDPR retention as starting points for formal review. GDPR does not prescribe one universal retention period. This public guide is not legal advice or a blanket compliance claim. Formal review and the governing agreement determine project obligations.

Write down the decision

A useful data map names each system, account owner, purpose, permitted field set, destination region and access role. It should distinguish the website enquiry from later project records and identify external processors. Ask who can answer a rights request and who supplies configuration evidence; do not infer these responsibilities from a software logo.

Before sharing a sample

Use a sanitised process description for an initial discussion. Agree the approved route and scope before supplying private exports, sensitive inputs or credentials. Permissions for an enquiry and for marketing are separate decisions. A lawful-basis or contract question needs formal review in the context of the actual processing.

[POPIA: official Act](#)

[GDPR retention: Data Protection Commission](#)

03 / RETENTION

Track each distinct copy

Retention is set by data class and the governing agreement; this page does not promise a universal purge period for all client systems.

The existing website privacy policy does not publish a fixed CRM-enquiry retention period. For a project, request the retention schedule and verify the settings in each selected account. For every row below, record the owner, purpose, period or trigger, provider feature and plan, legal hold, access/deletion method and evidence.

Data class	Record before go-live	Deletion verification
Website enquiries / CRM	Owner, response purpose, CRM plan, period or trigger; correspondence.	Check enquiry and linked copies; record removal, restriction or exceptions.
Webhook queues / execution logs / incomplete bundles	Owner, diagnostic purpose, queue/log feature, plan and expiry settings.	Inspect pending payloads, logs and incomplete executions separately.
Source / destination records	Owner, purpose, authoritative record and linked identifiers.	Read back each permitted action. CRM deletion is not middleware deletion.
AI input / output / stored objects	Owner, purpose, endpoint state, files and control eligibility.	Check objects separately from abuse monitoring; record limits.
Exports / test data / backups	Owner, purpose, expiry/review trigger, rotation and restore protection.	Confirm copy disposal, backup expiry and restore safeguards.

For every row, record legal holds, access/deletion method and evidence as well as the owner, purpose, period or trigger and provider feature/plan. No numeric default is supplied here.

A proposed request workflow is to verify the requester and scope; locate distinct copies; check legal retention and holds; perform permitted deletion or restriction; obtain subprocessor confirmation where needed; check backup expiry and restore protection; then close with evidence and exceptions. This is a design workflow, not a claim that an automated global purge is deployed today. A CRM deletion alone does not remove middleware, log or backup copies.

04 / SECURE CONNECTIONS

Check the complete data path

Use HTTPS with certificate validation. Authenticate the sender using a provider-supported signature, OAuth or an authenticated gateway; a secret URL alone is not sufficient authentication. Define permitted payload fields, validate schema and size, limit account permissions and use approved secret storage. Redact logs and keep personal information and long-lived tokens out of URLs.

Check storage encryption, key custody and hosting for every destination and backup, rather than inferring end-to-end protection from one encrypted connection. Verify configuration and acceptance evidence in the actual accounts before go-live.

Provider documentation, not a CompanyConnect configuration audit: Make describes TLS 1.2/1.3 and AES-256 full-disk encryption, while some connectors allow security configuration. Salesforce requires TLS 1.2 or higher for secure communications. Confirm the actual connection, data store, key management and account settings for each project; provider documentation is not a configuration audit.

OpenAI distinguishes abuse-monitoring logs from endpoint application state. Zero Data Retention requires eligibility and approval and has limitations; endpoints, stored objects and capabilities are not all identical. Check the selected endpoint and enabled controls before sending data.

Evidence before go-live

Inspect an approved sample webhook and record the authentication method without exposing the secret. Confirm certificate checking, rejected invalid payloads, permitted fields and the least-privilege account. Review a redacted execution record and verify how operators find and resolve failed jobs.

Follow the payload beyond transport

Document where execution logs, incomplete bundles, exported samples and destination records persist. Check storage location, encryption settings and key custody independently for each service and backup. Provider capabilities can depend on account features and plans; a feature being available does not mean it is configured.

Provider sources reviewed 19 October 2026

[Make security](#)

[Make webhooks](#)

[Make error handling](#)

[Salesforce secure communications](#)

[Salesforce sensitive data](#)

[OpenAI data controls](#)

Fail visibly and recover deliberately

Proposed acceptance checks, not a claim that these runtime controls are installed for every client. Provider-specific error bodies and headers determine the recovery route.

Signal	Expected recovery and evidence
429 or limit code	Separate temporary limits from billing/quota exhaustion. Salesforce may use 403 for a limit; inspect the provider code. Respect valid Retry-After, otherwise exponential backoff with jitter.
Retry budget	Cap attempt count and elapsed time; include SDK retries in that budget. Retain the attempt history and demonstrated stop condition.
401 / 403 access failure	A genuine permission or access failure needs owner action. Stop denied attempts; do not retry indefinitely.
5xx / outage	Pause the affected route. Apply bounded queues or backpressure, expiry and an exception owner; dead-letter or human resolution when required.
Possible write, then timeout	Treat the result as unknown. Read back the destination before retrying. Hold an unresolved result rather than creating a repeated invoice.
Repeated event	Use a stable event key, persisted result and payload conflict check. Idempotency reduces duplicates; it is not an exactly-once guarantee.
AI unavailable	Leave the draft pending or use an authorised manual route. Never silently switch to an unapproved vendor, region or data flow.

Test recovery with a sanitised workload and approved destinations. Record the reconciled target identifier, exception decision and operator responsible for resuming the route. Clear the backlog under the agreed budget so recovery itself does not overload the provider.

[Integration outage recovery guide](#)

[OpenAI rate limits](#)

[Salesforce REST API error codes](#)

06 / EVIDENCE & SOURCES

Measure what actually completed

The work page links 20 published Upwork reviews about individual engagements. Our own 13 October 2026 controlled CRM test checked the form and typed Ray: each saved one consented record. That bounded internal test did not establish client ROI, a full voice journey or continuous uptime.

CompanyConnect is led by Lloyd Lew, a monday.com Authorized Partner. That relationship does not establish other platform certifications or an independent security audit. Provider documentation and review links are evidence with specific scope, not CompanyConnect security attestations.

Copy this measurement template into your project brief: baseline window []; comparison window []; eligible workload and exclusions []; unique completed exchanges []; attempts []; failures and replays []; manual handling time and measurement method []; operating cost and currency []; source records and responsible owner []; publication consent []. Keep the definitions and sample comparable, reconcile duplicates and report exceptions. Until supported by source, period, method and consent, an outcome remains unverified.

[20 published reviews and original links](#)

[Company Connect Upwork profile](#)

[Controlled enquiry test: scope and limits](#)

Primary reference index

Reviewed 19 October 2026. The linked documents support the specific provider or regulatory statements in this paper; they are not certifications of CompanyConnect. Account capabilities and terms may change.

[POPIA: official Act](#)

[GDPR retention: Data Protection Commission](#)

[Make security](#)

[Make webhooks](#)

[Make error handling](#)

[Salesforce secure communications](#)

[Salesforce sensitive data](#)

[OpenAI data controls](#)

[OpenAI rate limits](#)

[Salesforce REST API error codes](#)

For a project, request the agreed data map, retention schedule, access design, acceptance results and recovery instructions. Assess the selected configuration and governing agreement rather than treating this public paper as contractual evidence.