

Corstrate Email Tool — Security Overview

Document version: 0.4 — 2026-07-21 **Owner:** Imen Jelassi, Corstrate Founder **Contact:** ijelassi@corstrate.com **Status:** Operational reference. The Privacy Policy and Terms of Service are published at <https://oauth.corstrate.com/privacy> and <https://oauth.corstrate.com/terms>. For the processing described here, **Corstrate is the data controller** and is responsible for GDPR compliance, as set out in its client contracts.

1. Purpose of this document

This document gives IT administrators, security teams and Data Protection Officers (DPOs) the technical and organisational details needed to review the **Corstrate Email Tool** Microsoft 365 integration before granting OAuth admin consent.

If you have received an admin consent request in your Microsoft Entra portal for the application "Corstrate Email Tool" (App ID `905c5adb-20b1-4e7f-9d9b-3608e7639721`), this document explains:

- What the application does
- What data it accesses
- Where data is processed and stored
- How you stay in control

For any question not covered here, please contact ijelassi@corstrate.com .

2. Application identity

Attribute	Value
Application name	Corstrate Email Tool
Application (client) ID	905c5adb-20b1-4e7f-9d9b-3608e7639721
Publisher	Corstrate
Publisher verification status	Verified by Microsoft (cf. Microsoft Publisher Verification)
Microsoft Entra tenant (issuer)	Corstrate tenant — multi-tenant application
Application type	Public client application (PKCE flow), no client secret
Supported account types	Accounts in any organisational directory (multi-tenant)

You can independently verify the application identity by visiting:

- **Your Azure Portal** → Microsoft Entra ID → Enterprise Applications → search "Corstrate Email Tool"

3. Microsoft Graph permissions

The application requests the following **delegated permissions** (Microsoft Graph). All permissions are scoped to the consenting user's mailbox only — there is no tenant-wide or cross-mailbox access.

Scope	Purpose	Why it is needed
Mail.Send	Send emails on behalf of the signed-in user	Send outreach emails from the operator's mailbox (one mailbox per engagement)
Mail.ReadWrite	Read and write the signed-in user's mailbox	Read inbound replies to classify them (reply / out-of-office / bounce); move bounce notifications and out-of-office responses into dedicated sub-folders (/Inbox/Bounces , /Inbox/00F) to keep the operator's inbox clean. No email is deleted or forwarded outside the mailbox.
User.Read	Sign-in and basic profile of the signed-in user	Identify the user during authentication (read display name and email)
offline_access	Maintain access after the user signs out	Refresh the access token silently for 90 days so the operator does not need to re-authenticate every hour

What this application does NOT do:

- ✗ It does **not** access any mailbox other than the user who consented
- ✗ It does **not** access calendar, contacts, OneDrive, SharePoint, Teams or any other Microsoft 365 service
- ✗ It does **not** delete emails
- ✗ It does **not** forward emails to external addresses
- ✗ It does **not** impersonate other users
- ✗ It does **not** require any tenant-level administrative permission

3.1 Sending practices — no bulk mail, rate-limited

The Corstrate Email Tool is a **targeted B2B outreach** tool, not a mass-mailing or newsletter platform. The Mail.Send permission is used in a deliberately constrained way:

- **One recipient per message** — each email is individually addressed and personalised to a single identified business prospect; never a bulk send to a recipient list or distribution group.
- **Rate-limited and paced** — sending is throttled by design (a configurable delay between messages and pauses between small batches). Typical volume is in the **low hundreds per**

day per mailbox, well within Exchange Online service limits (10,000 recipients/day, 30 messages/minute, 500 recipients/message).

- **Operator-controlled** — campaigns are launched and supervised by a human operator from the Corstrate cockpit; there is no autonomous, unsupervised mass sending.
- **Suppression respected** — the tool automatically stops contacting any address that opts out or hard-bounces, and excludes leads whose company has already responded.
- **One mailbox per engagement** — no cross-mailbox or tenant-wide sending.

This keeps sending volume and pattern modest and well within your tenant's service limits.

4. Data flow

4.1 What data leaves the mailbox

The application reads and processes the following data:

Data	Direction	Purpose	Stored where
Outbound email content (body, subject, recipient)	Mailbox → Microsoft Graph	Sending outreach	Sent Items folder (your tenant)
Inbound reply metadata (sender, subject, internet message ID, headers)	Mailbox → Corstrate platform	Match reply to outreach campaign	Corstrate Teable database (OVH France, see §5)
Inbound reply content (first ~1 000 characters of the reply body, stripped HTML)	Mailbox → Corstrate platform	Display reply summary to the operator in the Corstrate UI	Corstrate Teable database
Bounce notification details (recipient address, error code)	Mailbox → Corstrate platform	Mark the lead as undeliverable, prevent re-sending	Corstrate Teable database
Out-of-office notifications	Mailbox → Corstrate platform	Suspend outreach to the lead until a configurable date	Corstrate Teable database

The application never accesses, processes or stores:

- Attachments of inbound replies
- Emails unrelated to ongoing outreach campaigns (the application matches replies via the **In-Reply-To** header against tracked outbound message IDs)

- Personal emails of the mailbox user

4.2 What stays in the mailbox

- Email content remains in your tenant's Microsoft 365 storage at all times for sent items, drafts and inbound replies
 - The Corstrate platform stores **derived data** (sender address, message ID, classification, reply excerpt) — not a full copy of the mailbox
-

5. Sub-processors and data residency

Corstrate stores all persistent personal data within the **European Union (France)**. A limited set of sub-processors used to build and verify prospect contact lists process business contact data in the United States, under Data Processing Agreements incorporating EU Standard Contractual Clauses (SCCs).

Sub-processor	Role	Region	Data processed
OVH SAS (France)	Primary hosting (VPS for Teable database and application backend)	Roubaix, France 	All persistent Corstrate operational data
Scaleway (France)	Encrypted backup storage (S3-compatible object storage)	Paris, France 	Daily database backups (age-encrypted, see §6)
Teable Community Edition (self-hosted by Corstrate on OVH)	Operational database (Postgres)	Roubaix, France 	Outreach campaigns, leads, tracker records
Cloudflare, Inc. (US-headquartered, GDPR-compliant, SCCs)	CDN, Edge Workers (API gateway), Pages (web hosting)	Global edge with EU routing preference	TLS termination, request routing (no personal data stored at edge)
Microsoft Corporation (US-headquartered, GDPR-compliant, Microsoft EU Data Boundary applicable)	Microsoft Graph API (mailbox access)	Your tenant's data residency (typically EU for EU customers)	Mailbox content stays in your tenant
FullEnrich (US-headquartered, GDPR-compliant, DPA + SCCs)	B2B email enrichment (finding and completing professional email addresses)	United States 	Business contact data submitted for enrichment (name, company, professional email)
NeverBounce (US-headquartered, GDPR-compliant, DPA + SCCs)	Email deliverability verification	United States 	Professional email addresses submitted for verification

Data residency summary:

- Persistent personal data (leads, tracker records, campaign data and backups) is stored exclusively in the EU (France: OVH Roubaix, Scaleway Paris).
- Mailbox content remains in your Microsoft 365 tenant under its own residency settings.
- Traffic transiting the Cloudflare edge is limited to TLS termination and routing, with no persistent storage.

- Business contact data sent to our enrichment and verification sub-processors (FullEnrich, NeverBounce) may be processed in the United States. These transfers are governed by Data Processing Agreements incorporating EU Standard Contractual Clauses, complemented by the UK International Data Transfer Addendum where applicable.
-

6. Security controls

6.1 Authentication

- **OAuth 2.0 Authorization Code with PKCE** — no client secret, no service account
- Permissions are granted via **user delegated consent** (or admin consent at your discretion)
- Refresh tokens are stored exclusively on the operator's local macOS Keychain — never on a server, never in environment variables, never in logs
- The application implements `prompt=select_account` to ensure the consenting account is explicitly chosen by the operator, preventing accidental cross-tenant token issuance

6.2 Encryption

Layer	Algorithm
Transport (all API and web traffic)	TLS 1.2+ (TLS 1.3 preferred) — HTTPS only
Database (Teable Postgres)	Standard TLS for client connections; disk-level encryption depends on OVH VPS configuration (encrypted volumes supported)
Backups at rest (Scaleway)	<u>age</u> asymmetric encryption (X25519 + ChaCha20-Poly1305) — Corstrate holds the private key on a separate offline storage
OAuth refresh tokens on operator's Mac	macOS Keychain encryption (AES-256, protected by Secure Enclave on M-series Macs)

6.3 Audit logging

All authentication and API events are visible to **your tenant** through Microsoft's standard audit infrastructure:

- **Microsoft Entra ID → Sign-in logs** : every silent token refresh and interactive sign-in by the application
- **Microsoft Entra ID → Audit logs** : `Consent to application` event when admin or user grants consent

- **Microsoft 365 Defender** (if licensed): "OAuth apps" dashboard shows the application's risk score and activity

You can revoke access at any time from Azure Portal — the application will lose access immediately on the next token refresh attempt.

6.4 Application security practices

- Source code reviewed for OWASP Top 10 vulnerabilities
- No third-party JavaScript in mailbox-facing components
- HTTP Content Security Policy enforced on web interfaces
- Dependencies tracked and updated on a regular cadence

6.5 Application development and use of AI

The Corstrate Email Tool is developed and maintained by Corstrate. Like most modern software teams, our development workflow uses AI-assisted coding tools to help write source code. This is a **development aid only** and does not change the security posture of the running application:

- **No AI/LLM in the runtime.** The running application contains **no AI component**. Its behaviour is deterministic Node.js code that communicates only with the Microsoft Graph API and a self-hosted database (EU). There is no AI in the request path.
- **No customer or mailbox data is ever sent to any AI/LLM service** (OpenAI, Anthropic, or any other). AI tooling operates on source code at design time — never on your data at run time.
- **Human-reviewed and tested.** All code is reviewed by a Corstrate engineer, version-controlled (git), and covered by an automated test suite (1,000+ tests) executed on every change.
- **Security is enforced by controls, not by authorship.** The guarantees in this document — minimal delegated permissions, mailbox-only scope, EU data residency, encryption, instant revocation, full Microsoft Entra audit visibility — hold regardless of which tools were used to write the code.

Source code review under NDA is available to your security team on request.

7. Data retention

Data	Retention	Rationale
Outreach campaign data (sent emails metadata, reply summaries, tracker history)	Retained for the duration of the engagement; client may request deletion at any time	Operational use
Daily database backups (Scaleway, age-encrypted)	1 year , then automatic deletion via S3 lifecycle policy	Disaster recovery and audit
Operational logs (application server, mailing agent)	30 days , then automatic rotation	Debugging and security incident response
OAuth refresh tokens (operator's Keychain)	Until explicit revocation (by user, admin or Corstrate)	Required for unattended re-authentication

Retention policies can be tightened on a per-engagement basis — contact ijelassi@corstrate.com to discuss specific contractual requirements (e.g. 30-day backup retention, immediate deletion clauses).

8. How to revoke access

Access can be revoked instantly at any time:

8.1 By the mailbox user (Imen Jelassi or the user who consented)

1. Visit <https://myapps.microsoft.com>
2. Click **Manage your apps**
3. Find **Corstrate Email Tool** in the list
4. Click **Remove**

8.2 By a tenant administrator

1. Open Azure Portal → **Microsoft Entra ID** → **Enterprise Applications**
2. Search for **Corstrate Email Tool**
3. Open the application → **Properties** → click **Delete**

After revocation, all existing access and refresh tokens become invalid on the next refresh attempt (typically within one hour). Any new sign-in attempt would require a fresh admin or

user consent.

9. Incident response and communication

In the event of a security incident affecting your data:

- Corstrate will notify the designated contact at your organisation **within 72 hours** of becoming aware
 - A written incident report will follow within 7 days, including timeline, scope, root cause and remediation
 - Contact for security incidents: ijelassi@corstrate.com
-

10. Additional documentation available on request

The following documents are available to your security team on request:

- **Sub-processor data-processing agreements (GDPR Article 28)** — summary available on request
- **Privacy Policy** — available on request (public web page in preparation)
- **Terms of Service** — available on request (public web page in preparation)
- Security questionnaire responses (SIG, CAIQ, custom)
- Architecture diagrams (high-level data flow)

Please email ijelassi@corstrate.com with your specific requirements.

11. Document changelog

Version	Date	Changes
0.1	2026-05-29	Initial publication
0.2	2026-06-02	Added §3.1 Sending practices (no bulk mail, rate-limited, operator-controlled)
0.3	2026-06-02	Added §6.5 Development & AI (no AI in runtime, no data sent to AI). Removed dead Privacy/Terms URLs (now "available on request")
0.4	2026-07-21	Updated §5 to list email enrichment and verification sub-processors (FullEnrich, NeverBounce, United States). Replaced the "all processing in the EU" wording with an accurate residency summary (persistent storage EU-only; enrichment/verification transfers to the US under SCCs + UK IDTA Addendum)

This document is provided for informational purposes to facilitate your security review. It does not constitute a contractual commitment. Contractual terms are set out separately in the agreement signed between Corstrate and the client; for the processing described here, Corstrate acts as the data controller.