Data Processing Agreement

Version 2026-11-08 · Last updated November 8, 2026 · Draft for legal review, not legal advice

Version 2026-11-08. This agreement (GDPR Article 28, and the UK GDPR where it applies) is between the customer (controller) and Inboxed (demo company details: registration in progress), 1 Demo Street, Dhaka, Bangladesh (processor). An admin accepts it for a workspace in Settings > Compliance; that acceptance is recorded with their name, the time and the version.

1. Subject matter and duration

Inboxed processes personal data to provide the cold email service described in the Terms of service, for as long as the customer's workspace exists, and afterwards only for deletion as described in section 10.

2. Nature and purpose

Storing and verifying lead lists; sending campaign emails from mailboxes the customer connects; receiving and classifying replies; tracking opens and clicks when the customer turns tracking on; AI drafting and summaries when the customer turns those features on; reporting.

3. Personal data and data subjects

Data subjects: the customer's leads and prospects, people who reply to campaigns, and the customer's own team members. Data: names, business email addresses, job titles, company, location, any custom fields the customer uploads, email content, and engagement data (opens, clicks, approximate device type). The customer must not upload special categories of data (GDPR Art. 9) or data about children.

4. Instructions

Inboxed processes the personal data only on the customer's documented instructions, which are these terms and the settings the customer chooses in the product, including for transfers to third countries, unless EU or member state law requires otherwise; in that case Inboxed tells the customer first unless the law forbids it. Inboxed tells the customer if it believes an instruction infringes data protection law.

4a. Shared bounce list

The customer instructs Inboxed, when a campaign email sent through Gmail, Microsoft or another major provider is rejected with an enhanced status code meaning the address doesn't exist (5.1.1, 5.1.2 or 5.1.10; never spam, policy or other rejections), to add to a list shared by all customers a keyed hash (HMAC-SHA256, secret held by Inboxed) of that address, a bounce count, the last-seen date and a keyed hash of the sending workspace (at most five per address). The list holds no address, customer name or campaign. An address counts only after hard bounces from at least two different workspaces within 180 days; it is checked only when a campaign is about to send to it (limited per workspace per day), never at import or in previews, and a skipped email shows only "Skipped to protect deliverability". Entries expire 12 months after the last bounce. Inboxed may turn the list off; changing its secret resets it. (Draft for legal review.)

5. Confidentiality

Everyone at Inboxed who can access the personal data is bound by confidentiality, and access is limited to people who need it to run, support or secure the service.

6. Security (Art. 32)

Inboxed keeps appropriate technical and organisational measures, including: encryption in transit (TLS) and of credentials and secrets at rest (AES-256-GCM); hashed passwords (Argon2id) and optional or required two-factor

sign-in; workspace isolation of every query; role-based access; audit logs of settings changes; rate limits; and daily encrypted backups kept in the same region as the database.

7. Sub-processors

The customer gives general authorisation for the sub-processors listed at /legal/subprocessors. Inboxed gives at least 30 days' notice of any addition or replacement by email to subscribers of that page, and the customer may object on reasonable data protection grounds; if no solution is found the customer may close the affected workspace. Inboxed imposes data protection obligations on each sub-processor equivalent to these and remains responsible for them. Services the customer connects themselves (their own mailbox provider, CRM, AI provider key, verification or enrichment provider) are the customer's own processors, not Inboxed sub-processors.

8. Data subject requests

The product lets the customer export, correct and erase a person's data (Settings > Compliance > Erase a person) and keeps unsubscribes. Inboxed forwards any request it receives directly to the customer and helps with requests the customer can't handle in the product.

9. Breaches and assistance

Inboxed notifies the customer without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting the customer's data, with the information the customer needs for its own notifications. Inboxed helps the customer with security, breach notification, data protection impact assessments and prior consultation, taking into account the nature of the processing.

10. Deletion at the end

When a workspace is deleted, its personal data is deleted from the live database at once and from backups within 30 days, except where the law requires Inboxed to keep it (for example billing records).

11. Audits

Inboxed makes available the information needed to show compliance with Article 28 and allows for and contributes to audits, including inspections, by the customer or an auditor it mandates, with reasonable notice, no more than once a year unless required by a supervisory authority or after a breach.

12. International transfers

Where personal data is transferred outside the EEA, UK or Switzerland to a country without an adequacy decision, the transfer is covered by the EU Standard Contractual Clauses (Commission Decision 2021/914, module 2 or 3 as applicable) and, for the UK, the International Data Transfer Addendum, or by the EU–US Data Privacy Framework where the recipient is certified.

13. Liability and order of precedence

Liability under this agreement follows the Terms of service. If this agreement and the Terms conflict on personal data, this agreement wins.

Signature

Accepted electronically in Inboxed (Settings > Compliance). The acceptance record shows who accepted, when, and which version.