

Data Processing Agreement

Template · version 21 June 2026

Template. Have a lawyer review before signing. The Customer fields shown like **[this]** are completed by the customer. Replio acts as the **Processor**; the customer is the **Controller**.

This Data Processing Agreement ("**DPA**") forms part of the agreement between:

- **Neodevz Software Services and Website Design W.L.L.** (Commercial Registration No. 241112), Doha, State of Qatar, operating the **Replio** service ("**Replio**", "**Processor**"); and
- **[Customer legal entity name]**, **[registered address]** ("**Customer**", "**Controller**").

It governs Replio's processing of Personal Data on the Customer's behalf in connection with the Replio services (the "**Services**") and is effective on the date of last signature (the "**Effective Date**").

1. Definitions

Terms such as "**Personal Data**", "**Processing**", "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data Breach**", and "**Sub-processor**" have the meanings given in applicable data-protection law (including the EU/UK GDPR where it applies). "**Applicable Data Protection Law**" means all privacy and data-protection laws applicable to the processing under this DPA.

2. Roles and scope

2.1 The Customer is the Controller and Replio is the Processor of the Personal Data described in Annex I.

2.2 Replio processes Personal Data only to provide the Services and only on the Customer's documented instructions (including those given through the Replio dashboard and configuration), unless required to act otherwise by law (in which case Replio will inform the Customer where legally permitted).

2.3 Replio will inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law.

3. Processor obligations

Replio will:

- **(a) Confidentiality** — ensure that personnel authorized to process Personal Data are bound by appropriate confidentiality obligations.
- **(b) Security** — implement and maintain the technical and organizational measures set out in Annex III, appropriate to the risk.
- **(c) Sub-processors** — engage Sub-processors only under Section 4.

- **(d) Data Subject requests** — taking into account the nature of processing, assist the Customer, insofar as possible, to respond to Data Subject requests. The Customer can also access, export, correct, and delete data directly through the dashboard.
- **(e) Assistance** — assist the Customer, taking into account the nature of processing and information available to Replio, with its obligations regarding security, breach notification, and (where applicable) data-protection impact assessments.
- **(f) Breach notification** — notify the Customer without undue delay, and in any event within **72 hours**, after becoming aware of a Personal Data Breach affecting the Customer's Personal Data.
- **(g) Deletion / return** — at the Customer's choice, delete or return the Personal Data at the end of the Services, and delete existing copies unless storage is required by law. Default operational timelines: deletion requests honored within **30 days**; on account closure, data deleted within **90 days**.
- **(h) Audits** — make available information necessary to demonstrate compliance and, on reasonable prior notice and no more than once per year (or following a Personal Data Breach), allow for and contribute to audits, including by responding to a reasonable security questionnaire in lieu of an on-site audit.

4. Sub-processors

4.1 The Customer provides general authorization for Replio to engage the Sub-processors listed in Annex II.

4.2 Replio will impose data-protection obligations on each Sub-processor no less protective than those in this DPA, and remains responsible for its Sub-processors' performance.

4.3 Replio will give the Customer notice of any intended addition or replacement of a Sub-processor, with the opportunity to object on reasonable data-protection grounds within **[14]** days.

5. International transfers

Where processing involves a cross-border transfer of Personal Data, the parties will ensure an appropriate transfer mechanism recognized under Applicable Data Protection Law (e.g. Standard Contractual Clauses) is in place. Replio's hosting region is available on request.

6. Liability and term

6.1 Each party's liability under this DPA is subject to the limitations and exclusions of liability in the main agreement between the parties.

6.2 This DPA remains in effect for as long as Replio processes Personal Data on the Customer's behalf.

7. General

This DPA is governed by the laws of the **State of Qatar**, and the parties submit to the jurisdiction of the courts of Qatar. If there is a conflict between this DPA and the main agreement on data-protection matters, this DPA prevails. If any provision is found invalid, the remainder stays in effect.

Replio (Processor)	Customer (Controller)
Name:	Name:
Title:	Title:
Signature & Date:	Signature & Date:

Annex I — Details of processing

- **Subject matter:** provision of AI customer-support Services connected to the Customer's messaging channels.
- **Duration:** for the term of the Services and until deletion per Section 3(g).
- **Nature and purpose:** receiving end-user messages, generating and delivering AI replies, logging enquiries/complaints, routing conversations to the Customer's team, and related support operations.
- **Categories of Data Subjects:** the Customer's end-users who contact the Customer through connected channels; the Customer's authorized dashboard users (team members).
- **Types of Personal Data:** identifiers and contact details provided by end-users (e.g. name/handle, email, phone/account references), the content of messages (including images) exchanged with the assistant, and dashboard-user account data (name, email, hashed password). Replio does not store full payment-card numbers.
- **Special category data:** not intended to be processed; end-users should not submit it.

Annex II — Sub-processors

Sub-processor	Purpose
Anthropic	AI reply generation (Claude)
Voyage AI	Knowledge retrieval (embeddings)
Railway	Cloud hosting / managed database
Stripe	Payments (no full card numbers stored by Replio)
Resend	Transactional email
Privy	Crypto wallet features (only if the Customer enables them)
Telegram, Meta (WhatsApp / Messenger / Instagram)	Message delivery on the channels the Customer connects

A current list is available on request; Replio will notify the Customer of additions/replacements per Section 4.3.

Annex III — Technical and organizational security measures

- **Encryption in transit:** all dashboard, API, webhook, and chat-widget traffic over TLS/HTTPS.
- **Encryption at rest:** data stored on managed, encrypted infrastructure; account passwords hashed (never plaintext).
- **Access control:** logical tenant isolation so each Customer's data is accessible only to that Customer's authenticated team; optional two-factor authentication (TOTP); role-based access (owner / admin / agent).
- **Least privilege:** access to production data limited to personnel who require it.
- **AI processing:** Customer conversations are not used to train the AI providers' models.
- **Sub-processor diligence:** reputable providers under their own data-protection terms (Annex II).
- **Deletion:** self-serve and on-request deletion; operational timelines per Section 3(g).
- **Breach response:** notification to the Customer within 72 hours of becoming aware.

Replio · replio.live · hello@replio.live · see also the Privacy Policy (replio.live/privacy.html) and Security & Data Handling (replio.live/security.html).