Data Processing Addendum

Voxly — customer DPA template · Version 0.1 (2026-07-16) · Generated 2026-07-18

DRAFT TEMPLATE — NOT FOR EXECUTION. This document has not been reviewed by licensed counsel and is not legally binding. It is published for customer security-review convenience only. Before executing, both parties must obtain legal review in their respective jurisdictions. The authoritative sub-processor list is always voxly.io/legal/sub-processors.

How to use this template

Complete the Parties section and Schedule 1 particulars, then sign. This DPA is also deemed incorporated into the Voxly Customer Agreement by reference (see voxly.io/legal/dpa); a countersigned copy is only necessary where Customer's procurement process requires a standalone executed document.

Parties

	CUSTOMER ("CONTROLLER" / DATA EXPORTER)	VOXLY ("PROCESSOR" / DATA IMPORTER)
Legal entity name	_____	Daya Corp d/b/a Voxly
Registered address	_____	_____
Contact for privacy notices	_____	privacy@voxly.io
Agreement this DPA forms part of	The Voxly Customer Agreement (or other written agreement between the parties governing Customer's use of the Voxly platform) — the "**Agreement**".	

1. Scope and Roles

1.1 Roles of the parties

For the purposes of this DPA: (a) Customer is the **Controller** (or, where Customer acts on behalf of another controller, the processor passing instructions to Voxly); and (b) Voxly is the **Processor** of Customer Personal Data. A description of the processing is in Schedule 1.

1.2 Term

This DPA takes effect on the commencement date of the Agreement and terminates when Voxly ceases all processing of Customer Personal Data (or, if later, the date the Agreement terminates).

1.3 Order of precedence

In the event of conflict among (a) the region-specific terms in Schedule 2 (including the Standard Contractual Clauses), (b) Schedule 1, (c) this DPA body, and (d) the Agreement, the order of precedence is highest to lowest as listed.

2. Processing of Personal Data

2.1 Customer's instructions

The Agreement, this DPA, applicable Orders, and Customer's use of the Voxly platform (including configuration choices) constitute Customer's documented instructions regarding processing. Voxly will process Customer Personal Data only in accordance with those instructions, except where required to comply with applicable law (in which case Voxly will inform Customer first, where lawful).

2.2 Customer responsibilities

Customer is responsible for ensuring its instructions comply with applicable data protection law and for determining whether the Voxly platform is appropriate for Customer's intended processing. Voxly is not responsible for monitoring Customer's compliance.

2.3 Confidentiality

Voxly will treat Customer Personal Data as Customer's Confidential Information. Voxly personnel authorised to process Customer Personal Data are bound by written or statutory obligations of confidentiality.

3. Security

3.1 Security measures

Voxly implements and maintains appropriate technical and organisational measures to protect the confidentiality, integrity, and availability of Customer Personal Data, as described in Schedule 4 (Technical and Organisational Measures).

3.2 Security incidents

Voxly will notify Customer without undue delay, and where feasible no later than seventy-two (72) hours, after becoming aware of a Security Incident affecting Customer Personal Data. Voxly will make reasonable efforts to identify the cause, mitigate the effects, and remediate to the extent within Voxly's reasonable control. Notification is not an admission of fault.

4. Sub-processors

4.1 General authorisation

Customer grants Voxly general authorisation to engage the sub-processors listed in Schedule 3 (as updated per Section 4.3) to process Customer Personal Data. Voxly enters into written agreements with each sub-processor imposing data protection obligations no less protective than those in this DPA, and remains liable to Customer for sub-processor performance.

4.2 Current sub-processors

The current list is published, and maintained in human-readable form, at voxly.io/legal/sub-processors. Schedule 3 contains a snapshot of that list as of the date this document was generated; **the published list is authoritative**.

4.3 Notice of new sub-processors

Voxly will notify Customer at least thirty (30) days before any new sub-processor begins processing Customer Personal Data. Notices are sent automatically by email to Customer's billing contact on file. To change the contact that receives these notices, or to add additional recipients, email privacy@voxly.io.

4.4 Objection

Customer may object to a new sub-processor during the 30-day notice window for legitimate data protection reasons. Customer's sole and exclusive remedy in that case is to terminate the affected subscription in accordance with the Agreement's termination provisions.

5. Assistance and Cooperation

5.1 Data subject rights

Taking into account the nature of the processing, Voxly will provide reasonable and timely assistance to enable Customer to respond to requests from data subjects exercising their rights of access, rectification, erasure, restriction, objection, and portability. Voxly's self-serve admin tools and export capabilities are designed so most requests can be fulfilled by Customer directly.

5.2 Regulatory cooperation

On Customer's reasonable request, Voxly will provide reasonable assistance with data protection impact assessments and consultations with regulatory authorities, where Customer cannot reasonably fulfil such obligations independently using available documentation.

5.3 Third-party requests

Unless prohibited by law, Voxly will promptly notify Customer of any valid, enforceable legal process or governmental request compelling disclosure of Customer Personal Data. Voxly will redirect inquiries from data subjects or regulators to Customer and will not respond itself unless required by law.

6. Deletion and Return

6.1 During the term

During the term of the Agreement, Customer can access, retrieve, and delete Customer Personal Data through the Voxly platform's admin tools and export functionality.

6.2 Post-termination

Within ninety (90) days of termination of the Agreement, Voxly will delete all Customer Personal Data, except as required by applicable law or as retained in Voxly's standard backup or record retention systems. Retained data remains subject to this DPA's confidentiality and security obligations and will not be further processed.

7. Audit

7.1 Audit reports

Voxly is regularly assessed against industry standards including SOC 2 Type II (in progress; ETA Q4 2026) and provides summary audit reports to Customer under NDA on request, no more than once every twelve

(12) months.

7.2 On-site audits

Where Customer cannot reasonably verify compliance through Section 7.1, or where required by applicable data protection law, Customer (or its authorised representative) may conduct an audit at Customer's expense, no more than once every twelve (12) months, on at least sixty (60) days' written notice, subject to reasonable confidentiality obligations.

8. International Transfers

Where Voxly transfers Personal Data protected by EU GDPR, UK GDPR, or Swiss FADP from those regions to a country that does not benefit from an adequacy decision, the transfer mechanisms elected in Schedule 2 — the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914, the "**EU SCCs**"), the UK International Data Transfer Addendum to the EU SCCs (Version B1.0, the "**UK Addendum**"), and the Swiss adaptations — are incorporated into this DPA and deemed signed by both parties as of the Agreement commencement date. Customer is the data exporter; Voxly is the data importer.

Where Voxly processes data subject to US state privacy laws (including the CCPA/CPRA and VCDPA), Voxly acts as a Service Provider / Processor and will not sell or share Customer Personal Data, and will not retain, use, or disclose it outside the direct business relationship except as permitted by law.

9. Liability

Each party's liability under or in connection with this DPA is subject to the limitations and exclusions of liability set out in the Agreement.

10. Definitions

- **Customer Personal Data** means Personal Data contained in customer content that Voxly processes solely on Customer's behalf.
- **Personal Data**, **Controller**, **Processor**, and **Processing** have the meanings given in applicable data protection law.
- **Security Incident** means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data processed by Voxly or its sub-processors.
- **Sub-processor** means any third party engaged by Voxly to process Customer Personal Data, as listed per Section 4.2.

Execution

Signature is required only where Customer's procurement process needs a standalone executed DPA (see "How to use this template").

Customer	**Daya Corp d/b/a Voxly**
Signature	Signature
Name, title	Name, title
Date	Date

Schedule 1 — Description of Processing (EU SCCs Annex I.B)

- **Categories of data subjects:** Customer's employees and contractors (workspace members) and end users of Customer's feedback portals (portal users).
- **Categories of Personal Data:** name, email address, workspace role, feedback content authored by data subjects, votes and comments, IP-derived rate-limit metadata. Customer controls what additional content data subjects submit.
- **Sensitive data:** Voxly does not solicit special category data. Customer is responsible for not directing data subjects to submit it.
- **Frequency of the transfer:** continuous, for the duration of the Agreement.
- **Nature and purpose of the processing:** hosting, storage, transmission, search, aggregation, AI-assisted summarisation, and ancillary operations needed to provide the Voxly platform.
- **Duration:** the term of the Agreement plus the deletion window in Section 6.2.
- **Onward transfers to sub-processors:** as listed per Section 4.2 / Schedule 3, for the same purposes and duration.

Schedule 2 — Cross-Border Transfer Terms

2.1 EU Standard Contractual Clauses (2021/914)

The EU SCCs apply to transfers described in Section 8 with the following elections (to be confirmed by counsel):

- **Modules:** Module Two (controller → processor) where Customer is a Controller; Module Three (processor → processor) where Customer is itself a Processor.
- **Clause 7 (docking):** included.
- **Clause 9(a):** Option 2 (general written authorisation), with the thirty (30) day notice period in Section 4.3.
- **Clause 11(a) (independent redress body):** the optional language is not used.
- **Clause 13 / Annex I.C (competent supervisory authority):** determined by the data exporter's establishment or, where Article 3(2) GDPR applies, the data subjects' habitual residence.
- **Clauses 17 and 18 (governing law / forum):** Option 1 — the law and courts of Ireland, unless the exporter's Member State law is required.
- **Annex I:** parties per the Parties table; description of the transfer per Schedule 1. **Annex II:** Schedule 4. **Annex III:** Schedule 3.

2.2 UK Addendum (Version B1.0)

For transfers subject to UK GDPR, the UK International Data Transfer Addendum applies: Table 1 is populated from the Parties table; Table 2 refers to the EU SCCs as elected above; Table 3 refers to Schedules 1, 3 and 4; for Table 4, neither party may end the Addendum as set out in Section 19 of the Addendum.

2.3 Swiss FADP

For transfers subject to the Swiss FADP, the EU SCCs apply with the standard Swiss adaptations: references to the GDPR are read as references to the FADP; the competent supervisory authority is the Swiss FDPIC; the term "Member State" is interpreted to allow Swiss data subjects to sue in Switzerland; and data of legal entities is protected to the extent the FADP so provides.

2.4 Other regions

Where Customer is established in, or its data subjects reside in, other regions with applicable transfer requirements (e.g. Brazil's LGPD), the equivalent standard mechanism for that region is deemed incorporated and signed on the Agreement commencement date.

Schedule 3 — Sub-processors (EU SCCs Annex III)

Snapshot generated **2026-07-18** from Voxly's canonical sub-processor registry. The live list at voxly.io/legal/sub-processors is **authoritative** and updates with thirty (30) days' advance notice per Section 4.3. "Opt-in" vendors process data only for workspaces that explicitly install the corresponding connector.

SUB-PROCESSOR	CATEGORY	PURPOSE	LOCATION	OPT-IN?
Vercel Inc.	Infrastructure	Application hosting, edge network, CDN, and serverless function execution.	United States (multi-region)	No
Supabase Inc.	Infrastructure	Managed PostgreSQL database, authentication, storage, and Vault for encrypted secrets.	United States (AWS, multi-region)	No
Functional Software, Inc. (Sentry)	Observability	Server- and client-side error tracking. PII is scrubbed before transmission via Sentry beforeSend hook.	United States (AWS, GCP)	No
Stripe, Inc.	Payments	Subscription billing. Voxly never sees raw card data — Stripe Checkout/Elements tokenises payment instruments before they reach our servers.	United States; EU subsidiaries for EU customers	No
Resend, Inc.	Communications	Transactional email delivery (workspace invites, notifications, GDPR Art.17 erasure-verification emails).	United States (AWS)	No
Anthropic, PBC	AI services	LLM-powered feedback summarisation and categorisation (Claude API). Voxly does not allow Anthropic to retain prompts for training (zero-retention enrolment).	United States (AWS)	No
OpenAI, L.L.C.	AI services	Embedding generation for semantic feedback search. API access only; prompts not retained for training under our zero-retention agreement.	United States	No
Atlassian Pty Ltd / Atlassian, Inc.	Customer-opt-in connectors	Customer-opt-in connector. When a workspace admin connects Jira, Voxly relays feedback content the admin chooses to push, plus OAuth tokens stored in Voxly Vault, to Atlassian. Voxly never accesses the customer's Jira data outside the explicit push action.	United States (AWS), Europe	Yes
Slack Technologies, LLC	Customer-opt-in connectors	Customer-opt-in connector. When a workspace admin connects Slack, Voxly posts notifications to the channels the admin selects. OAuth tokens stored in Voxly Vault.	United States (AWS)	Yes
Zapier, Inc.	Customer-opt-in connectors	Customer-opt-in connector. When a workspace admin enables Zapier, Voxly delivers trigger payloads (feedback events) to Zaps the admin configures. Authentication is via a Voxly-issued API key.	United States (AWS)	Yes
Linear Orbit, Inc.	Customer-opt-in connectors	Customer-opt-in connector. When a workspace admin connects Linear, Voxly creates Linear issues from feedback the admin chooses to promote. OAuth tokens stored in	United States (GCP)	Yes

SUB-PROCESSOR	CATEGORY	PURPOSE	LOCATION	OPT-IN?
		Voxly Vault; Voxly never reads Linear data outside the connected organization.		
GitHub, Inc.	Customer-opt-in connectors	Customer-opt-in connector. When a workspace admin connects GitHub, Voxly creates GitHub issues from feedback the admin chooses to promote. OAuth tokens stored in Voxly Vault; access is limited to repositories the authorizing account can reach.	United States (multi-region)	Yes
Zendesk, Inc.	Customer-opt-in connectors	Customer-opt-in connector. When a workspace admin connects Zendesk (subdomain + agent API token, stored in Voxly Vault), tagged support tickets can be converted into Voxly feedback. Voxly only reads tickets surfaced by the admin-configured trigger.	United States (AWS), EU pods available	Yes
Intercom, Inc.	Customer-opt-in connectors	Customer-opt-in connector. When a workspace admin connects Intercom, qualified support conversations can be converted into Voxly feedback. OAuth tokens stored in Voxly Vault; app permissions are configured read-only for conversations.	United States (AWS), EU/AU hosting available	Yes
HubSpot, Inc.	Customer-opt-in connectors	Customer-opt-in connector. When a workspace admin connects HubSpot, Voxly logs feedback activity on matching HubSpot contacts (contacts read/write scopes only). OAuth tokens stored in Voxly Vault.	United States (AWS), EU data residency available	Yes
Discord Inc.	Customer-opt-in connectors	Customer-opt-in connector. When a workspace admin attaches a Discord webhook to an AlertConfig rule, Voxly POSTs notification payloads to the channel the webhook addresses. The webhook URL itself (which is the credential) is stored in Voxly Vault; Discord never receives Voxly credentials. No PortalUser PII is sent unless the workspace admin includes it in the alert template. For the webhook-outbound model, the workspace admin's acceptance of the Discord Developer Terms of Service is the operative agreement governing data handling.	United States (GCP, multi-region)	Yes

Schedule 4 — Technical and Organisational Measures (EU SCCs Annex II)

- **Tenant isolation:** workspace-level data segregation enforced in the database via PostgreSQL row-level security policies on all customer-data tables.
- **Encryption in transit:** TLS 1.2+ for all external connections; HSTS enforced on production domains.
- **Encryption at rest:** AES-256 for the primary datastore (managed PostgreSQL) and backups.
- **Secrets handling:** third-party OAuth tokens and connector credentials stored encrypted in a dedicated vault (Supabase Vault); payment instruments are tokenised by the payment processor and never touch Voxly servers.
- **Access control:** role-based access control across platform, workspace-admin, and portal-user tiers; least-privilege service credentials; MFA for production administrative access.
- **Audit logging:** append-only audit log of administrative and data-affecting actions, with sensitive-access flagging; outbound customer email is recorded in a notification log.
- **Availability and resilience:** managed multi-AZ infrastructure, automated backups, and point-in-time recovery for the primary datastore.
- **Data minimisation in telemetry:** error tracking scrubs personally identifiable information before transmission.
- **Incident response:** documented incident-response runbook; customer notification per Section 3.2 (without undue delay, 72-hour target).
- **Deletion:** self-serve deletion and export tooling in-product; verified erasure workflow for data-subject requests; post-termination deletion per Section 6.2.
- **Personnel:** confidentiality obligations for all personnel with access to Customer Personal Data; access reviewed on role change and revoked on departure.
- **Secure development:** mandatory code review, CI checks (type safety, tests, RLS policy tests), and dependency vulnerability monitoring before production deploys.

Voxly DPA template v0.1 — DRAFT, pending counsel review. Generated 2026-07-18. Questions: privacy@voxly.io.