

Pushary Team Data Processing Agreement

English review copy | Version 2026-10-28-review-1 | 2026-10-28

Draft for review — not effective. Downloading, viewing or using this document does not accept an agreement. The proposed obligations below require legal approval and agreement by the parties. Any separately executed agreement remains controlling.

1. Parties and scope

This review copy is prepared for RalphNex OÜ, registry code 16932562, trading as Pushary (Provider), and the customer legal entity to be identified in the service agreement (Customer). The registered address, customer details, authorised signatories and effective date must be confirmed before execution.

The proposed DPA covers personal data processed on Customer's behalf to provide the Pushary Team service. Customer acts as controller, or as a processor authorised by its controller. Provider acts as processor or subprocessor for that processing. Processing for Provider's own account administration and legal obligations must be identified separately in the applicable privacy notice.

2. Documented instructions

Provider would process covered personal data only on Customer's documented instructions, including the agreed service configuration. Customer remains responsible for the lawfulness of its instructions, notices and disclosure of personal data. An instruction believed to breach applicable data protection law would be raised with Customer before it is acted on.

Where law requires processing outside those instructions, Provider would inform Customer before processing unless that law prohibits notification. Additional instructions, including export and deletion requests, would be recorded through the agreed support contact.

3. Confidentiality and access

Provider would limit access to people who need it to deliver or support the service and who are bound by confidentiality obligations. Customer manages its workspace membership and roles. A shared sprint record is visible to workspace members; a personal approval request has its own recipient and permission checks. Removing access does not itself erase retained records.

4. Security measures

The parties would agree appropriate technical and organisational measures for the data and risks involved. Annex B identifies the implementation topics to verify. Provider would maintain the agreed measures and assess material changes. This draft does not represent a certification, independent audit or guarantee of a particular hosting region.

5. Other processors

Provider would engage other processors only under the agreed authorisation procedure and written obligations protecting the covered data. Provider would remain responsible to Customer for those processors' performance of their applicable obligations.

The initial approved list, legal entities, locations, advance change notice, objection period and resolution procedure must be agreed before execution. The linked provider register is a review inventory, not a completed authorisation schedule. No automated change-notice subscription is offered by this draft.

6. International transfers

Before a transfer requiring safeguards takes place, the parties would identify the countries, recipients and applicable transfer mechanism. Where standard contractual clauses are needed, the correct modules, annexes and supplementary measures must be completed. This draft does not itself incorporate or execute transfer clauses, or promise EU-only processing.

7. Assistance to Customer

Provider would assist Customer with requests relating to the covered data and with security, impact-assessment and regulatory obligations, taking account of the service and information available. Requests received directly from an individual would be referred to Customer unless law requires otherwise. The parties must agree the contact, identity checks, export format and operational procedure before execution.

8. Personal data breaches

Provider would notify Customer without undue delay after becoming aware of a personal data breach affecting covered data, provide available information about its nature and impact, and cooperate on containment and remediation. Information could be supplied in stages as the investigation develops. The incident contact and escalation procedure must be confirmed; no fixed-hour notification commitment is made in this review copy.

9. Return, deletion and retention

At the end of the service, Provider would return or delete covered data at Customer's choice, subject to applicable legal retention requirements. The agreed schedule must address active records, transcripts, logs, downstream processors and backups, including how retained copies are protected and eventually removed. No deletion deadline or backup expiry is agreed in this review copy.

10. Evidence and audits

Provider would make information needed to demonstrate compliance with the agreed processing obligations available and allow appropriate audits, including inspections, by Customer or its mandated auditor. The parties must agree practical arrangements protecting other customers, credentials and service availability without removing applicable audit rights.

11. Relationship to the service agreement

The final DPA would specify its relationship to the service agreement, including precedence for data protection obligations, duration and the treatment of liability. Governing law, dispute terms and signature or incorporation method remain for legal review. This version has no effective date and is not incorporated by checkout or continued use.

Annex A — Processing description

Service: receive and deliver agent notifications and approval requests; record responses and action receipts; maintain sessions and shared sprint evidence; synchronise supported clients; provide configured history, support and account access.

People: Customer's employees, contractors and invited workspace members, and other people whose information Customer includes in submitted content.

Data: user and workspace identifiers; names and email addresses; device and push identifiers; notification text, task titles, commands and responses; session and repository metadata; commit evidence; and encrypted transcript records when history is enabled. Free text may contain customer or employee information. Payment and independent account-administration processing require separate role analysis.

Operations: receipt, routing, storage, retrieval, display, export and deletion as applicable to the enabled features. The processing duration and retention schedule must be completed. This draft does not authorise special-category or criminal-offence data; any such requirement needs a separate assessment.

Annex B — Security review

Topics for the final schedule: authenticated access and key lifecycle; workspace and recipient authorisation; role enforcement; encrypted transport; database and backup protection; transcript encryption and recovery access; operational access logging; incident response; restoration tests; and deletion verification.

The Team implementation uses application authorisation and workspace-scoped queries. Database row-level security is not relied on as an enforced isolation boundary. Transcript recovery capability means the service must not be described as zero knowledge. Managed SSO, SCIM and enterprise certifications are not included in the self-serve Team offer. These statements are not a substitute for an agreed, evidenced security schedule.

Annex C — Provider review and open terms

Review the accompanying subprocessor inventory at <https://pushary.com/legal/sub-processors>. It describes service integrations, related account providers and platform dependencies. Provider legal entities, contractual roles, locations, transfer safeguards and completeness still require verification before the approved schedule can be attached.

Before execution, resolve: party details and contacts; the final provider schedule and change procedure; transfer safeguards; security measures; retention and backup periods; rights and incident operations; audit arrangements; governing terms; and the approved version and effective date. Send review questions to business@pushary.com. Do not send passwords, API keys or sensitive customer content.