

Pushary Team Data Processing Agreement

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

Agreement copy for signature. This DPA takes effect when both parties sign it together with the completed schedules, or expressly incorporate this exact version into a signed service agreement. Viewing, downloading, account creation and checkout do not execute this agreement. An existing executed DPA remains controlling.

1. Parties and scope

RalphNex OÜ, Estonian registry code 16932562, trading as Pushary (Provider), and the customer legal entity identified in the execution schedule (Customer) enter into this Data Processing Agreement (DPA). The main agreement is the service agreement identified in that schedule. Privacy, security and data-rights correspondence may be sent to business@pushary.com.

This DPA applies to personal data Provider processes on Customer's behalf through the Pushary Team service (Customer Personal Data). Customer is the controller, or a processor acting under its controller's authority; Provider is its processor or subprocessor. Each party remains responsible for its own obligations under applicable data-protection law. Provider's independent billing, account administration and legal obligations are governed by the applicable privacy notice.

2. Documented instructions

Provider shall process Customer Personal Data only to provide the agreed service under Customer's documented instructions, including the service configuration and this DPA. Customer shall establish the legal basis, give required notices and ensure it has authority to provide the data and instructions. Customer may send additional written instructions to the contact above. The parties shall record any agreed change in scope.

Provider shall promptly inform Customer if it believes an instruction infringes applicable data-protection law and suspend the affected instruction until resolved. Where EU or Member State law requires other processing, Provider shall inform Customer before processing unless that law prohibits notification.

3. Confidentiality and access

Provider shall limit access to authorised personnel with a service need and ensure they are bound by confidentiality obligations or an appropriate statutory duty. Customer controls workspace membership and roles. Workspace members can see the shared sprint record; personal approval requests have separate recipient and permission checks. Removal of a member ends access but does not itself erase retained business records.

4. Security measures

Provider shall implement and maintain appropriate technical and organisational measures under Article 32 GDPR, taking account of the processing, risks, available technology and implementation costs. The measures described in Annex B form the baseline. Provider shall assess their effectiveness and shall not materially reduce protection during the service.

Customer shall use access controls, configure recipients carefully and avoid including unnecessary personal data or credentials in task titles, commands and approval context. No independent certification, managed SSO, SCIM, guaranteed hosting region or zero-knowledge architecture is included unless expressly agreed in writing.

5. Other processors

Customer specifically authorises the subprocessors identified in the completed Annex C. Provider shall impose written data-protection obligations providing the protection required by Article 28 GDPR and remains responsible to Customer for the performance of its subprocessors' obligations.

Before adding or replacing an authorised subprocessor, Provider shall give Customer written details of its identity, purpose, locations and safeguards and obtain Customer's written authorisation. Silence is not authorisation. If authorisation is withheld, the parties shall seek a suitable alternative; the affected processing shall not move to the proposed subprocessor without authorisation. This specific-authorisation procedure does not rely on an automated notification subscription.

6. International transfers

Provider shall not transfer Customer Personal Data outside the EEA without Customer's documented instructions and a valid transfer mechanism under Chapter V GDPR. Annex C shall identify relevant destinations and safeguards. Where required, the parties shall execute the applicable transfer clauses, complete their annexes and assess supplementary measures before the transfer.

This DPA is an Article 28 processing agreement, not a substitute for international-transfer clauses. A provider's European hosting option does not establish that all support or processing stays in the EEA.

7. Assistance to Customer

Provider shall assist Customer, through appropriate measures and taking account of the nature of processing, with data-subject requests. Provider shall refer requests received directly to Customer without undue delay and shall not respond substantively except on Customer's instructions or as required by law.

Taking account of the information available, Provider shall assist Customer with security obligations, breach notifications, impact assessments and prior consultation with a supervisory authority. Customer shall identify an authorised contact in the execution schedule. Provider shall verify the authority and workspace scope of instructions before disclosing, exporting or erasing data.

8. Personal data breaches

Provider shall notify Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. The notice shall describe the nature of the breach, affected data and people where known, likely consequences, measures taken or proposed, and a contact for follow-up. Information not yet available may be supplied in subsequent updates without undue delay.

Provider shall take appropriate steps to contain, investigate and remediate the breach and cooperate with Customer. Customer remains responsible for its regulatory and data-subject notifications unless law provides otherwise. Notification does not by itself constitute an admission of liability.

9. Return, deletion and retention

This DPA continues for as long as Provider processes Customer Personal Data. When the relevant services end, Customer may instruct Provider to return the data in an agreed commonly used electronic format or securely delete it, and delete remaining copies, unless EU or Member State law requires retention. Customer may change its choice before the return or deletion is completed.

The parties shall complete the retention and deletion schedule before execution, covering active records, encrypted transcripts, logs, processors, backups and restoration handling. Provider shall confirm completion against that schedule, identify any lawful retention exception, protect retained data and restrict its further use to the required purpose. A database deletion alone is not confirmation that every processor or backup copy has been erased.

10. Evidence and audits

Provider shall make available information necessary to demonstrate compliance with its processing obligations and allow and contribute to audits, including inspections, by Customer or an auditor it mandates. Requests should be sent to the contact above, identifying scope and relevant concerns. The parties shall coordinate reasonable notice, confidentiality and arrangements protecting other customers and service availability.

Those arrangements shall not prevent an urgent investigation, regulatory access or a mandatory audit right. Provider may supply relevant existing evidence first, but this does not remove Customer's inspection rights. Provider shall address substantiated deficiencies and report the corrective action.

11. Relationship to the service agreement

This DPA prevails over conflicting terms in the main agreement concerning processing of Customer Personal Data. Mandatory data-protection law and any applicable executed transfer clauses prevail over this DPA. The main agreement governs other commercial matters, liability and dispute resolution to the extent permitted by law; nothing limits statutory rights of data subjects or supervisory authorities.

Amendments require a written agreement identifying the new version. A website update does not replace an executed version. The parties shall retain the signed agreement, completed schedules, signatory authority and effective date. This agreement does not become binding merely through use of the website or checkout.

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 for enabled features. Processing lasts for the service and the agreed return/deletion period. The execution schedule shall record retention

periods and any additional restrictions. The service is not intended for special-category or criminal-offence data; Customer shall not intentionally submit it without a separate written assessment and agreement.

Annex B — Security measures

Access and isolation: authenticated accounts, workspace membership and role checks, recipient checks for decisions, and application queries scoped to the relevant workspace or site. Database row-level security is not represented as the enforced isolation boundary. Customer administrators manage membership and roles.

Credentials and communications: server API keys are stored as hashes; device credentials have scope and revocation paths; clients communicate with hosted endpoints over encrypted transport. Transcript capture uses local redaction and encryption with configured recovery access. Approval text, task titles and other metadata are separate data paths and must not be assumed to have transcript encryption.

Operational measures: before execution, the parties shall attach the applicable access-management, incident-handling, backup/recovery and deletion procedures, including responsible contacts and verification records. Customer-specific requirements beyond the implemented baseline require written agreement. No provider certification is represented as a certification of Pushary.

Annex C — Authorised subprocessors

The provider information page at <https://pushary.com/legal/sub-processors> identifies integrations and related services. It is a starting inventory, not evidence that a particular legal entity, region, transfer safeguard or contract has been verified for the Customer.

Attach the authorised processing schedule before signing: for each subprocessor, identify the contracting legal entity, service, data categories, storage and support countries, transfer mechanism and applicable agreement. Identify customer-selected integrations separately. Unverified entries must be resolved before they are included in the authorised schedule.

Execution schedule

Customer legal name, registration number and address: _____. Customer authorised contact and email: _____. Provider registered address and authorised contact: _____. Main agreement reference: _____. Covered workspace identifiers: _____.

Attach the completed processing/retention schedule, operational security procedures and authorised subprocessor/transfer schedule referenced above. Identify any customer-specific terms: _____. These schedules are required parts of the executed agreement.

For Customer — name, title and authority: _____; signature: _____; date: _____. For RalphNex OÜ — name, title and authority: _____; signature: _____; date: _____. Effective date: _____.
Document version: 2026-10-28-1.