OKRs Tool

Data Processing Agreement

Processor	Kingspoint OÜ (trading as OKRs Tool), Tallinn, Estonia
Controller	The customer identified in the applicable Order or Terms of Service
Applies to	Personal data processed via the OKRs Tool service
Version	1.1 (18 November 2026)
Effective date	On acceptance / signature
Contact	dpo@okrstool.com

This Data Processing Agreement ("DPA") forms part of the agreement between the Customer ("Controller") and Kingspoint OÜ trading as OKRs Tool ("Processor") for the provision of the OKRs Tool service (the "Service"). It governs the Processor's processing of personal data on the Controller's behalf and reflects the parties' obligations under the EU General Data Protection Regulation ("GDPR").

Contents

1. Definitions

Terms such as "personal data", "processing", "controller", "processor", "data subject", and "personal data breach" have the meanings given in the GDPR. "Sub-processor" means any third party engaged by the Processor to process personal data on the Controller's behalf. "Standard Contractual Clauses" ("SCCs") means the clauses approved by the European Commission for transfers of personal data to third countries.

2. Roles of the Parties

The Controller is the controller of the personal data it submits to the Service. The Processor acts as a processor, processing that personal data only on the Controller's behalf. Where the Processor engages sub-processors, it does so as described in Section 6. The Controller remains the sole and exclusive owner of all personal data and other content that it and its users submit to the Service; the Processor acquires no rights in that data other than as needed to provide the Service.

3. Scope and Purpose of Processing

The Processor processes personal data only to provide, maintain, secure, and support the Service in accordance with the agreement and the Controller's documented instructions. The subject matter, duration, nature and purpose of processing, the types of personal data, and the categories of data subjects are set out in Annex A.

4. Processor Obligations

The Processor shall:

- process personal data only on the Controller's documented instructions, including as set out in the agreement and this DPA, unless required otherwise by law (in which case it will inform the Controller unless prohibited from doing so);

- ensure that persons authorised to process the personal data are bound by confidentiality obligations;
- implement appropriate technical and organisational security measures as described in Annex B;
- respect the conditions in Section 6 for engaging sub-processors;
- assist the Controller, taking into account the nature of the processing, in responding to data subject requests (Section 7) and in meeting its obligations relating to security, breach notification, and data protection impact assessments (Sections 8 and 9);
- at the Controller's choice, delete or return the personal data at the end of the provision of the Service, as set out in Section 10;
- make available information necessary to demonstrate compliance with Article 28 GDPR and allow for audits as set out in Section 11.

5. Controller Obligations

The Controller shall ensure that it has a lawful basis for the processing, that it has provided any required notices to data subjects, and that its instructions to the Processor comply with applicable data protection law. The Controller is responsible for the personal data it and its users choose to submit to the Service, and undertakes not to submit special categories of personal data except where the Service is expressly designated for such use.

6. Sub-processors

The Controller provides general authorisation for the Processor to engage the sub-processors listed in Annex C to process personal data in connection with the Service. The Processor shall:

- impose data protection obligations on each sub-processor that are no less protective than those in this DPA, by way of a written contract;
- remain liable to the Controller for the performance of each sub-processor's obligations;
- maintain an up-to-date list of sub-processors (published at okrstool.com/sub-processors) and give the Controller reasonable advance notice of the addition or replacement of a sub-processor, allowing the Controller to object on reasonable data-protection grounds.

7. Data Subject Rights

Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests to exercise data subject rights (access, rectification, erasure, restriction, portability, and objection). Where the Processor receives such a request directly from a data subject, it shall forward it to the Controller and shall not respond except on the Controller's instructions. Much of this can be actioned by the Controller directly within the Service, including data export and deletion.

8. Security

The Processor implements and maintains the technical and organisational measures set out in Annex B, designed to ensure a level of security appropriate to the risk, including encryption of personal data in transit and at rest, tenant isolation, access control, and monitoring.

9. Personal Data Breach

The Processor shall notify the Controller without undue delay, and in any event within 72 hours, after becoming aware of a personal data breach affecting the Controller's personal data. The notification shall describe, to the extent known, the nature of the breach, the likely consequences, and the measures taken or proposed. The Processor shall assist the Controller in meeting its own breach-notification obligations to supervisory authorities and data subjects.

10. Return and Deletion of Data

On termination or expiry of the Service, or on the Controller's earlier request, the Processor shall delete or return the personal data. On verified request, the Controller's data is hard-deleted, including audit logs, with no soft-delete retention window. The Controller may export its data prior to deletion via JSON export, organisation-level export, audit-log CSV, or the REST API. Backups containing personal data expire on the Processor's standard rolling cycle of about 14 days. The Processor may retain personal data to the extent required by law.

11. Audit

The Processor shall make available to the Controller information reasonably necessary to demonstrate compliance with this DPA and Article 28 GDPR. This includes the Processor's Information Security Policy and the independent audit reports (e.g. SOC 2 Type II) of its infrastructure sub-processors, available under NDA. Where the Controller reasonably requires further information, the parties shall discuss a proportionate audit, conducted on reasonable notice and without disrupting the Processor's operations or the confidentiality of other customers' data.

12. International Transfers

The Processor stores the Controller's core customer data within the EU (Ireland). Where a sub-processor processes personal data outside the European Economic Area (as indicated in Annex C), such transfers are made under an appropriate transfer mechanism, including the Standard Contractual Clauses or an adequacy decision, together with encryption in transit and at rest. The Processor shall not store or process the Controller's personal data in any country other than those disclosed in Annex C and at okrstool.com/sub-processors without first giving the Controller reasonable advance written notice and the opportunity to object, as set out in Section 6.

13. Liability and Term

This DPA is effective for as long as the Processor processes personal data on the Controller's behalf under the agreement. The liability of each party under this DPA is subject to the limitations and exclusions of liability set out in the agreement. In the event of conflict between this DPA and the agreement on the subject of data protection, this DPA prevails.

Signatures

For the Processor — Kingspoint OÜ / OKRs Tool	For the Controller — Customer
Name:	Name:
Title:	Title:
Signature:	Signature:
Date:	Date:

Annex A — Details of Processing

Item	Detail
Subject matter	Provision of the OKRs Tool goal-management service.
Duration	For the term of the agreement and until deletion/return of data.
Nature and purpose	Hosting, storage, and processing of OKR content and account data to deliver, secure, and support the Service.
Types of personal data	Name, work email, company, role; user-generated OKR content, comments, check-

Item	Detail
	ins; authentication and usage data.
Categories of data subjects	The Controller's personnel and authorised users of the Service.
Special categories	None processed by design.

Annex B — Technical and Organisational Measures

The Processor maintains the following measures (as further described in its Information Security Policy):

- Encryption of personal data in transit (TLS 1.2/1.3) and at rest (AES-256).
- Tenant isolation between customer organisations enforced at the database layer through row-level security (RLS).
- Role-based access control, and multi-factor authentication that organisations can require, enforced at the database level; least-privilege internal access.
- Passwordless authentication (magic link / OAuth) and privileged credentials confined to backend processes.
- Edge protection (WAF, DDoS mitigation) and 24/7 monitoring with automated alerting.
- Daily automated database backups, retained for about 14 days in the same EU region.
- Automated dependency and application security scanning with severity-based remediation.
- A documented incident response process with 72-hour breach notification.

Annex C — Authorised Sub-processors

The current list of sub-processors is maintained at okrstool.com/sub-processors. As at the effective date, the principal sub-processors are:

Sub-processor	Purpose	Location
Supabase (on AWS)	Primary database, authentication, file storage	EU (Ireland)
Cloudflare	CDN, WAF, DDoS mitigation, edge delivery	Global edge; no customer data at rest
Amazon Web Services	Underlying cloud infrastructure	EU (Ireland)
Stripe	Payment and billing processing	US (SCCs); PCI DSS Level 1
Anthropic	AI feature processing (on-demand)	US (SCCs); not used for training
Resend	Transactional email delivery	US (SCCs)
Scalekit	Single sign-on and SCIM provisioning	US (SCCs); support access from India
Lovable	Development platform; administrative access to the production database	US (SCCs)
Datadog	Performance monitoring and error tracking; system telemetry only	US (SCCs)