Data Processing Agreement

November 2026 · v1.0 · VKT

This agreement applies when a workspace installs VKT and VKT processes personal data on that workspace's behalf. It sits alongside the Terms of Service and only covers the processing VKT performs as a processor. Nothing has to be signed in advance: the terms apply on install, and a signed copy is only needed if a customer's own procurement process asks for one.

1 Definitions

1.1 "Agreement" means this Data Processing Agreement together with its Annexes. The Annexes form an integral part of it.

1.2 "Terms" means the VKT Terms of Service published at vktapp.com/terms.

1.3 "Personal data", "processing", "controller", "processor", "data subject" and "personal data breach" carry the meaning given in Article 4 of the GDPR. Where the GDPR does not apply, they carry the meaning given by the comparable law of the customer's jurisdiction.

1.4 "Customer data" means personal data that the customer submits, imports or generates through VKT.

2 Roles and scope

2.1 For customer data, the customer is the controller and VKT is the processor. VKT does not process customer data for its own purposes.

2.2 The subject matter, nature, purpose, duration, categories of data and categories of data subjects are set out in Annex A.

2.3 This Agreement covers only the processing VKT performs as a processor. Where VKT acts as controller — the installer's account and billing details — the Privacy Policy applies.

2.4 This Agreement does not authorise monitoring of employees beyond what the customer's own law permits, and does not create any right for VKT to use customer data independently.

3 Instructions

3.1 VKT processes customer data only on the customer's documented instructions, including those given through in-app settings, the web console, and this Agreement.

3.2 If VKT considers an instruction to breach data protection law, it will tell the customer without undue delay and may suspend that instruction until the customer confirms it.

3.3 The Terms, the Privacy Policy and this Agreement together constitute the customer's documented instructions. Where they conflict on data protection matters, this Agreement prevails.

4 Confidentiality and personnel

4.1 Access to customer data is limited to persons who need it to provide the service, and who are bound by confidentiality obligations.

4.2 VKT is currently operated by a single developer, with no layered subcontracting. Any person engaged in future remains subject to this clause.

5 Security measures

5.1 VKT implements technical and organisational measures proportionate to the risk. The measures currently in place are those published on the security page at vktapp.com/security.

5.2 Those measures include: HTTPS in transit, workspace tokens encrypted at rest, tenant isolation enforced at the data layer, administrator rights derived from the org chart, and session cookies set HttpOnly, Secure and SameSite.

5.3 This Agreement is not a statement of SOC 2, ISO 27001 or any other certification. VKT does not currently hold such certifications, and nothing here should be read as claiming otherwise.

6 Assistance

6.1 Data subject requests: where the customer receives a request for access, correction, deletion, restriction or portability, VKT provides reasonable assistance, including the export functions built into the service.

6.2 Impact assessments and prior consultation: VKT provides the information the customer reasonably needs to carry out a data protection impact assessment or to consult a supervisory authority.

6.3 Assistance beyond the standard export functions is provided at the customer's cost, agreed in advance.

7 Personal data breaches

7.1 After confirming a personal data breach affecting customer data, VKT notifies the customer without undue delay, and typically within 72 hours.

7.2 The notification describes the nature of the breach, the categories and approximate volume of data involved, the likely consequences, and the measures taken or proposed.

7.3 If the investigation is incomplete, VKT gives preliminary information first and supplements it afterwards. An unfinished investigation is not a reason to delay telling the customer.

7.4 VKT provides reasonable assistance with the customer's own notifications to regulators or data subjects. Those notifications remain the customer's obligation.

8 Sub-processors

8.1 The customer gives general authorisation for the sub-processors listed in Annex B.

8.2 VKT gives 30 days' notice before adding or replacing a sub-processor, by updating Annex B on this page and notifying the customer.

8.3 The customer may object in writing on data protection grounds within 15 days of the notice. If no agreement is reached within 30 days, the customer may terminate the affected service; fees already paid are handled under the Terms.

8.4 VKT imposes data protection obligations on each sub-processor that are no less protective than this Agreement, and remains responsible for their performance.

8.5 The self-operated database listed in Annex B is not a third-party sub-processor. It is listed there for transparency only.

9 International transfers

9.1 Customer data is stored on servers in Osaka, Japan, operated by VKT.

9.2 Where customer data is transferred out of the EEA, the UK or Switzerland, the parties may sign the European Commission's Standard Contractual Clauses (2021/914) or the UK Addendum separately. This Agreement does not itself constitute those clauses.

9.3 VKT provides the information needed to sign those clauses within 10 business days of a request.

10 Deletion and return

10.1 When the service ends — the app is uninstalled, or the customer asks in writing — VKT deletes customer data within 30 days, except where law requires retention.

10.2 Before deletion the customer can export through the console, or by email. Export requests are accepted while a workspace is suspended as well.

10.3 Residual copies in backups are cleared in the normal rotation cycle; they are not retrieved individually.

10.4 Data that must be retained by law is isolated, and is not processed for any purpose other than meeting that legal obligation.

11 Audit and compliance questions

11.1 VKT answers security and compliance questions in writing, through documentation, and in remote calls where needed.

11.2 An on-site audit takes place only where the customer's law requires it, on 30 days' written notice, during business hours, without affecting other customers, and under a confidentiality agreement.

11.3 No audit, whether by the customer or a third party engaged by them, may access another tenant's data.

12 Liability

12.1 Liability under this Agreement is subject to the limitation of liability in the Terms. This Agreement does not expand it.

12.2 The customer is responsible for the consequences of instructions that are unlawful, or that exceed what the customer is authorised to give.

13 Term, termination and changes

13.1 This Agreement applies from the moment the app is installed in a workspace, and remains in force until the service ends and processing stops. No signature is required for it to apply.

13.2 Changes are made by updating this page. Material changes are announced in the app 30 days in advance. Processing already under way is completed under the terms in force when it began.

13.3 Sections 7, 10 and 12 survive termination of this Agreement.

14 Governing law and disputes

14.1 Governing law and dispute resolution follow the Terms.

14.2 This Agreement is made in Chinese and English. Both texts have equal effect; where they differ, the English text prevails.

15 Annex A — Processing details

Subject matter	Providing the seven core modules the customer installs — org chart, directory, weekly reports, time off, approvals, people calendar and lifecycle — inside Slack and in the web console.
Nature of processing	Storage, structuring, retrieval, calculation, display and export.
Categories of data	Name, job title, department, reporting line, work email, Slack user id, start and end dates, time-off records and balances, approval requests and attachments, report content, org chart change history.
Categories of data subjects	Members of the customer's workspace, including managers, HR staff and anyone participating in an approval chain.
Duration	While the app is installed; deletion afterwards follows Section 10.
Out of scope	Slack channel messages and direct messages, workspace files, Slack credentials or user tokens, salary and bank account details, identity document images, health or biometric data, background-check material.

If the customer chooses to type any of the above into a free-text field — a report body, an approval note — that is the customer's instruction. VKT does not request it, does not extract it separately, and does not use it for any other purpose.

16 Annex B — Sub-processors

PROVIDER	PURPOSE	LOCATION	NOTES
Cloudflare, Inc.	CDN, DNS, WAF, edge caching	Global edge network	Reverse proxy; request content is not used for any other purpose
VKT self-operated MySQL	Customer data storage	Osaka, Japan	Self-hosted, not a third-party processor; listed for transparency

No other sub-processors are engaged today. Changes follow Section 8.

17 Signature

Optional. If your procurement needs a signed copy, either print and sign, or reply to the email thread with “accepted, DPA v1.0” and the workspace name — both are sufficient. Nothing here needs to be signed to use VKT.

Customer (controller)

Workspace or legal name

Representative

Title

Date

Signature

VKT (processor)

ZHANG SHUXIA, independent developer

Cainiao Station, Fuxingyuan, Shangzhuang, Luquan District, Shijiazhuang, Hebei 050227, China

support@vktapp.com

Date

Signature