

---

APPENDIX 6

# Data Processing Agreement

Version 08.09.2026 · <https://akirolabs.com/assets/>

---

This Appendix "Data Processing Agreement" together with the main body of the Service Agreement and its other integral components constitutes the "Agreement". Capitalized terms used herein that are not otherwise defined herein shall have the meaning assigned to them in the Agreement.

## Introduction

With the Agreement, the Parties entered into a data processing relationship pursuant to the EU General Data Protection Regulation (hereinafter the "GDPR") and the Swiss Federal Act on Data Protection (hereinafter the "FADP"). In order to regulate the rights and obligations arising from their data processing relationship in the context of the provisions of the GDPR and FADP, the Parties enter into this Data Processing Agreement (hereinafter the "DPA").

The FADP article numbers stated in this DPA refer to the revised FADP (Swiss Federal Gazette 2020 7639).

## 1 Scope

This DPA applies to all activities that form the subject matter of the Agreement and during the performance of which akirolabs or sub-processors of akirolabs under this DPA process personal data relating to the Customer. This DPA is only valid insofar as (i) the Customer is either the controller or processor within the scope of the GDPR and/or FADP and (ii) in the Agreement, the Customer commissions akirolabs as processor or sub-processor of personal data that fall within the scope of the GDPR and/or FADP (hereinafter "personal data").

If the Customer acts as processor for its own customers and akirolabs acts as sub-processor, akirolabs hereby grants the Customer's own customers the same rights as are due to the Customer under this DPA.

## 2 Specification of contractual obligations

The data processing agreed upon by the Parties comprises activities described in the Agreement. The detailed scope of the individual activities follows from the Agreement. This DPA supplements the contractual arrangements in the Agreement. The subject matter and duration of the processing, its nature and purpose, the types of personal data and the categories of data subjects, as required by Art. 28(3) GDPR, are set out in Annex 3 to this DPA.

## 3 Responsibility and authority

akirolabs processes the personal data solely for purposes of contract fulfilment and/or for the purposes identified in the Agreement. akirolabs will not process the personal data for any other purposes and is, in particular, not entitled to disclose it to third parties (with the exception of sub-processors).

The Customer is responsible for complying with the provisions of data protection laws, particularly for the legality of the data transfer to akirolabs and for the lawfulness of the instructions it issues. akirolabs remains responsible for the lawfulness of its own processing and for its obligations under Art. 28 and Art. 32 GDPR.

akirolabs may only process personal data within the limits of the Customer's instructions. An instruction is a written order from the Customer regarding how akirolabs is to handle personal data. The Customer's instructions are set down in this DPA and in the Agreement. The Customer has the right to issue written instructions to akirolabs at any time that supplement, amend or replace the existing instructions. akirolabs must follow these instructions, provided that this is feasible and it is objectively reasonable to expect akirolabs to do so in the context of the contractually stipulated akirolabs Services. akirolabs's requirement to follow instructions only ceases to apply if akirolabs is subject to a legal duty to process. This must be communicated to the Customer immediately and documented accordingly.

The Customer instructions should be directed to the data protection department ([privacy@akirolabs.com](mailto:privacy@akirolabs.com)). The Customer will inform akirolabs of the employees that have the authority to issue instructions and will do so by suitable means (e.g. by e-mail). Any change in the designated recipient of instructions (akirolabs) or the employees authorised to issue instructions (Customer) must be reported to the respective other Party.

akirolabs must inform the Customer without delay if akirolabs believes that an instruction violates the requirements of data protection laws. akirolabs is entitled to suspend the execution of such an instruction until the Customer confirms or changes it.

## 4 Obligations of akirolabs

akirolabs will only process the personal data in a manner that is compliant with the provisions of this DPA and the Agreement, subject to the fulfilment of statutory, regulatory or governmental provisions and obligations. The Customer will inform akirolabs without delay if the Customer discovers a violation of the requirements of data protection laws in the course of service provision by akirolabs.

akirolabs will ensure that the employees involved in processing the personal data are prohibited from processing the personal data for purposes other than those stated in the Agreement or in a way that deviates from this DPA. akirolabs will further ensure that employees involved in data processing are obligated to maintain confidentiality and are familiar with those provisions of data protection law that are relevant for them. This includes familiarising them with the obligation to follow instructions.

akirolabs will make the contact information of the contact person responsible for data protection issues (who is also the data protection officer pursuant to Art. 37 GDPR) available to the Customer on the website.

akirolabs will inform the Customer without delay of audits, measures or investigations by supervisory authorities, to the extent they relate to the processing of the Customer's personal data and disclosure is legally permitted.

On request, akirolabs will provide the Customer with all relevant information the Customer needs, for example, to carry out a data protection impact assessment or in connection with consultation of or a report to a supervisory authority.

akirolabs will maintain a record of processing activities and disclose the most recent applicable version to the Customer on request. At the Customer's request, akirolabs will provide the Customer with information for inclusion in the Customer's record.

Other mandatory legal obligations of akirolabs remain unaffected by this DPA.

## 5 Technical and organisational measures (TOM)

akirolabs will implement the technical and organisational measures listed in Annex 1 to protect the processed personal data and to guarantee a level of data security proportionate to the risk. The security concept described in Annex 1 presents state-of-the-art technical and organisational measures appropriate for the identified risk, taking into account the security objectives and, in particular, the IT systems and processing procedures used by akirolabs.

Technical and organisational measures change as technology evolves. For this reason, akirolabs may adjust the agreed technical and organisational measures or implement appropriate alternative measures at any time. However, the agreed level of security must always be maintained. Major changes must be documented and communicated to the Customer on request.

## 6 Queries by data subjects

If a data subject contacts akirolabs directly to exercise its rights (e.g. right to information, deletion, rectification or data portability), akirolabs will immediately forward this request to the Customer or refer the data subject to the Customer if the information provided by the data subject makes it possible to associate the data subject with the Customer. akirolabs may only make direct disclosures to the data subject or to third parties with the prior written consent of the Customer. However, akirolabs will provide reasonable assistance to the Customer in responding to requests and enforcing data subjects' rights.

## 7 Evidence and audits

On request, akirolabs will provide the Customer with all relevant information needed to document compliance with the obligations established under the GDPR/FADP and this DPA.

akirolabs may satisfy a request under this section 7 in the first instance by providing its current ISO/IEC 27001 certificate and scope statement, its Statement of Applicability, and a summary of its most recent penetration test. Where those documents do not reasonably answer the Customer's question, the following paragraph applies.

For auditing purposes, the Customer or an auditor appointed by the Customer (who shall not be a competitor of akirolabs and shall be bound by confidentiality obligations) may verify compliance with the obligations established under this DPA, especially the compliance with the agreed technical and organisational measures, on akirolabs's business premises during usual business hours without interrupting the course of business. The principle of proportionality must be observed during such an audit and akirolabs's legitimate interests (especially relating to confidentiality) must be appropriately safeguarded. The audit must be announced at least 2 weeks in advance and may take place not more than once in any twelve (12) month period, unless a personal data breach has occurred or a supervisory authority requires otherwise. akirolabs is under no obligation to tolerate or cooperate with the audit if it is carried out without such advance notice, unless the Customer proves good cause for not complying with the obligation to provide advance notice or the obligation to comply with the lead time. The Customer will bear all costs of such audits, save that akirolabs shall bear its own costs and reimburse the Customer's reasonable audit costs where the audit establishes a material failure by akirolabs to comply with this DPA.

Any compulsory statutory auditing rights of the Customer or the Customer's supervisory authorities are unaffected.

If the presentation of evidence or reports or the performance of an audit shows that akirolabs has failed to comply with obligations under this DPA or to the required standard, akirolabs must take suitable measures to remedy the defects without delay and at own cost.

## 8 Notification in case of data breach

akirolabs will notify the Customer without undue delay after becoming aware of a personal data breach affecting personal data processed on behalf of the Customer, including where the breach involves one of its sub-processors. Any notification will be made in accordance with applicable legal, regulatory and contractual requirements. akirolabs will provide the Customer with the information reasonably necessary to support the Customer in meeting its obligations under Articles 33 and 34 GDPR, with further information provided as it becomes available.

The notification shall, to the extent known at the time and supplemented as further information becomes available, describe: the nature of the personal data breach, including where possible the categories and approximate number of data subjects and of personal data records concerned; the name and contact details of akirolabs' data protection officer or other contact point from which further information can be obtained; the likely consequences of the personal data breach; and the measures taken or proposed to address the breach and to mitigate its possible adverse effects.

akirolabs shall not notify any supervisory authority or data subject on the Customer's behalf without the Customer's prior written instruction, unless required to do so by law. In such a case, the Parties will take the necessary steps to ensure the protection of the affected personal data and to reduce any negative consequences for the data subjects and for the Parties.

## 9 Place of processing, disclosure abroad, remote work

akirolabs will preferably process the personal data in the EU/EEA. akirolabs may disclose personal data to recipients outside the EU/EEA only if akirolabs complies with the provisions of Chapter V EU-GDPR.

Where personal data is processed by akirolabs or a sub-processor in a country outside the EU/EEA that is not the subject of an adequacy decision, the Standard Contractual Clauses adopted by the European Commission by Implementing Decision (EU) 2021/914 (the "SCC") are hereby incorporated into this DPA by reference and form an integral part of it, on the following basis: Module Two (controller to processor) applies where the Customer acts as controller; Module Three (processor to sub-processor) applies where the Customer acts as processor for its own customers; the optional docking clause in Clause 7 applies; in Clause 9, Option 2 (general written authorisation) applies, with the notice period set out in section 11 of this DPA; in Clause 11, the optional independent dispute resolution paragraph does not apply; in Clause 17, the SCC are governed by the law of the Federal Republic of Germany, and in Clause 18(b) the courts of the Federal Republic of Germany are the competent courts; Annex I.A of the SCC is completed by the details of the Parties set out in the Agreement; Annex I.B by Annex 3 to this DPA; Annex I.C designates the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen as competent supervisory authority; Annex II by Annex 1 to this DPA; and Annex III by Annex 2 to this DPA.

For transfers subject to the FADP, the SCC apply with the amendments recognised by the Swiss Federal Data Protection and Information Commissioner, namely that references to the GDPR are read as references to the FADP, the competent supervisory authority is the FDPIC, the term "member state" does not restrict data subjects from bringing proceedings in Switzerland, and the SCC also protect the data of legal entities until such protection is repealed.

akirolabs has carried out an assessment of the laws and practices of the destination countries in accordance with Clause 14 of the SCC and will make the assessment available to the Customer on request. akirolabs will inform the Customer without undue delay if it becomes unable to comply with the SCC.

akirolabs may permit its employees which are entrusted with processing personal data for the Customer to process personal data in coworking facilities, private residences or other suitable locations. akirolabs must ensure that compliance with the contractually agreed technical and organisational measures is also guaranteed during remote working. In particular, akirolabs must ensure that when personal data is processed outside the office premises, the storage locations are configured in such a way that local storage of data on the IT systems used is excluded. If this is not possible, akirolabs shall ensure that local storage is encrypted and that other persons do not have access to the data concerned.

## 10 Return and deletion of data

Upon a request made by the Customer, within 60 days after the effective date of termination or expiration of the Agreement between the Customer and akirolabs, akirolabs will make the customer specific data available to the Customer for export or download in a mutually agreed format. After that 60-day period, akirolabs will be under no obligation to maintain or provide the Customer data and will thereafter delete or destroy all copies of the Customer data residing in the SaaS Solution or otherwise in akirolabs' possession or control, unless legally prohibited (e.g. in case of statutory retention obligations). Further, akirolabs can retain documentation intended to prove that data has been processed properly and in accordance with the Agreement for a suitable period of time after the termination or expiration of the Agreement.

Additionally, upon completion of the 60-day period, akirolabs deletes the Customer data from its cloud hosting environments (see Annex 2). Decommissioning of the underlying storage media is carried out by the cloud hosting providers in accordance with their documented media sanitisation practices, which are aligned with NIST SP 800-88 ("Guidelines for Media Sanitization"). akirolabs will confirm completion of deletion in writing on the Customer's request.

## 11 Sub-processors

akirolabs is entitled to use sub-processors. The list of sub-processors at the time of entry into force of this DPA is contained in Annex 2. akirolabs shall notify the Controller of any intended addition or replacement of subprocessors before the relevant subprocessor processes personal data on behalf of the Controller, thereby giving the Controller an opportunity to object on reasonable data protection grounds. Where a change is required urgently for security, availability, continuity, legal compliance, or other material operational reasons, akirolabs may provide shorter prior notice or, where prior notice is not reasonably practicable, notify the Controller without undue delay after the change. If an important data protection reason is given and the Parties cannot come to an amicable agreement, the Customer may terminate the Agreement without notice and shall receive a pro-rata refund of Subscription Fees pre-paid for the unused portion of the Subscription Term.

akirolabs agrees to set up its contractual agreements with its sub-processors in such a way as to guarantee the obligations established under this DPA, especially including adequate guarantees for a sufficient level of data security.

The Customer has the right to request in writing that akirolabs discloses information about the essential content of the contractual agreements with its sub-processors, the implementation of data protection obligations by the sub-processors, and the guarantees for a sufficient level of data security.

For the purpose of this provision, services are not considered to be rendered by sub-processors if akirolabs obtains them as incidental services from third parties to help with contract performance pursuant to the Agreement, such as telecommunications services and maintenance of data processing facilities during which access to personal data cannot be excluded. akirolabs is obliged, however, to take appropriate technical and/or organisational measures as well as control measures in order to ensure the security of the Customer's personal data.

## 12 Term

The term of this DPA is the same as the term of the Agreement. This DPA will end when the Agreement ends or the Customer stops using the akirolabs Services, except where the provisions of this DPA establish obligations of longer duration.

## 13 Liability

akirolabs's liability to the Customer for culpable breaches of this DPA is regulated by the Agreement, or secondarily by statutory regulations. For the avoidance of doubt, the limitations and exclusions of liability set out in the Agreement, including the General Terms and Conditions, apply to claims arising under or in connection with this DPA, save where mandatory law provides otherwise. The precedence of this DPA under section 14 concerns the substantive data protection obligations of the Parties and does not displace those limitations.

akirolabs is liable for damage culpably caused by its sub-processors as for damage caused by itself.

akirolabs bears the burden of proof that any damage is not the consequence of a circumstance for which it is responsible. akirolabs satisfies its burden of proof if it can demonstrate that it observed the provisions of this DPA when processing personal data and, in particular, that it implemented the agreed technical and organisational measures.

## 14 Final provisions

Changes and supplements to this DPA require a written agreement and an express notice that the document is a change or supplement to this DPA. The same applies to any waiver of this form requirement.

"Written" for the purpose of this DPA means (i) written (paper and original signatures) or (ii) e-mail.

Should individual provisions or parts of this DPA prove to be invalid or incomplete, this shall not affect the validity of the legal relationship established by this DPA in other respects. The invalidity and/or incompleteness of a provision shall not affect the validity of the other provisions. The invalid and/or incomplete provision shall be replaced by a legally valid substitute provision of the Parties which comes as close as possible to the invalid or incomplete provision.

This DPA replaces all earlier agreements, accords or declarations regarding data processing. With respect to the processing of personal data, this DPA shall take precedence over akirolabs's GTC or other agreements between the Parties to the contrary, subject to section 13. Where the SCC apply under section 9 and conflict with this DPA, the SCC prevail. With respect to applicable law and jurisdiction, the provisions in the Agreement between akirolabs and the Customer shall apply.

## ANNEX 1

# Technical and organisational measures (TOM)

Version 08.09.2026

This Annex 1 to the Data Processing Agreement (DPA) describes the technical and organisational measures implemented by akirolabs for the protection of the processed personal data and to guarantee a degree of data security proportionate to the risk. The measures described below apply to cases in which akirolabs processes personal data itself. If personal data is processed by sub-processors, akirolabs will enter into suitable contractual agreements to ensure that these sub-processors take appropriate and suitable technical and organisational measures. This Annex 1 also serves as Annex II to the Standard Contractual Clauses where these apply under section 9 of the DPA.

## 1 General principles

The following sections are applicable to the akirolabs Services provided to the Customer:

- Information security policies & procedures
- Physical security controls
- Data encryption
- Network security
- Data leakage prevention controls
- Access controls
- Application security
- Adherence to privacy regulations
- Security & privacy awareness
- Incident response
- Business continuity and backup

## 2 Information security policies & procedures

akirolabs is an ISO/IEC 27001:2022 certified organisation and maintains a documented Information Security Management System (ISMS). The ISMS includes policies, procedures, and technical and organisational measures covering information security governance, risk management, access control, data protection, secure development, compliance, and other relevant areas. akirolabs designs, develops, operates and supports the SaaS Solution itself; the certification is held by akirolabs GmbH and covers the design, development, operation and support of the SaaS Solution. The certificate, the name and accreditation of the certification body, and the scope statement are available to the Customer on request. akirolabs will maintain the certification for the duration of the Agreement and will inform the Customer without undue delay of any suspension, withdrawal, lapse or material reduction in its scope.

akirolabs maintains well-defined policies and security controls designed to protect personal data and customer data processed within the platform. Relevant policies, procedures, and controls are reviewed at least annually and updated where required in line with the ISO/IEC 27001-certified ISMS.

akirolabs is committed to protect the confidentiality, integrity and availability of its information assets and provide the same commitment to the information assets entrusted to it by its customers and business partners and has implemented security controls at all layers (application, network, database etc.) to ensure confidentiality, integrity, and availability of the Customer's Personal Information.

To meet this commitment, akirolabs shall:

- Maintain an effective information security management system ("ISMS")
- Deploy the most appropriate technology and infrastructure
- Create and maintain a security conscious culture within information services
- Continually monitor and improve the effectiveness of the ISMS.

### 3 Physical security controls

akirolabs' cloud hosting providers (Amazon Web Services and Google Cloud, see Annex 2) provide the physical security of the data centres as a managed service. The cloud hosting providers are compliant with requirements like ISO 27001, SOC 1, SOC 2 and SOC 3, which are the basis for akirolabs to rely on the security controls offered by them. akirolabs uses the cloud hosting providers' assurance reports to draw assurance over their controls and for evaluating any risks from the cloud hosting providers to the akirolabs Services. Additionally, akirolabs has appropriate physical security controls in its offices.

### 4 Data encryption

All Customer data is stored in encrypted format. Data at rest – encryption is achieved by encrypting storage in all systems hosting the SaaS Solution with AES-256 or equivalent encryption. Data in transit – data is transferred over HTTPS (TLS 1.2 or higher) for user-to-service and service-to-service communications.

### 5 Network security

Production workloads follow a private-by-default network posture. Internet-facing components are separated from internal services and data layers. Network access is restricted using cloud-native controls (VPC configuration, security groups, route tables, private subnets, NAT gateways and controlled ingress/egress rules). Security groups are configured to allow only required traffic between approved components, in a default deny-all mode, and are reviewed as part of infrastructure and security management. Production, staging and development environments are logically separated. akirolabs uses AWS WAF (Web Application Firewall) to protect against common web exploits that may affect availability and/or compromise security. Denial of Service (DoS) protection is provided at the infrastructure level through AWS Shield, and Amazon GuardDuty provides continuous threat detection across the cloud environment, including runtime monitoring of workloads.

### 6 Data leakage prevention controls

Customer data is logically segregated in the multi-tenant SaaS Solution using tenant-aware access controls and application-level authorisation. Each Customer tenant is identified by a unique tenant ID, and every transaction is performable only with reference to that tenant ID. Unique accounts are used to access a specific Customer tenant. Secrets and credentials are securely managed; hardcoding of secrets is prohibited and access to them is restricted.

### 7 Access controls

All Customer data resides in the SaaS Solution. Access to the SaaS Solution is controlled through role-based and user level access controls. Each Authorised User is provided access based on 'need-to-know' and 'need-to-do' principles. The access matrix is agreed with the Customer at the time of design & implementation and rights are provided as per agreed rules. akirolabs' support team assists with user access management (creation, deletion, modification, and maintenance).

Administrative access to the SaaS Solution and its infrastructure follows least-privilege and role-based access control. Privileged access is restricted to authorised personnel, approved, logged, reviewed periodically and removed when no longer required. Joiner, mover and leaver processes are used to grant, modify and revoke access based on business need.

The SaaS Solution includes a user authentication module that allows users to be authenticated via login / password. Multi-factor authentication is supported and can be enforced upon the Customer's request. The SaaS Solution also supports the use of the Customer's Single sign-on (SSO), which can be provided upon the Customer's request: the SaaS Solution can integrate with the Customer's identity provider system which may be based on different types of protocols, e.g. SAML 2.0, to allow login into the SaaS Solution.

## 8 Application security

akirolabs follows a secure software development lifecycle to ensure that security is embedded in each phase of development. Code changes follow a controlled workflow including review, approval, testing and CI/CD deployment practices. Security testing is integrated into the development lifecycle, including dependency and vulnerability scanning and code review. Production changes are traceable through change and release management tooling, and security-relevant changes are assessed for impact before release. Vulnerabilities are identified, tracked, prioritised by severity and risk, and remediated according to defined timelines. Critical security updates are expedited based on risk and exploitability. Vulnerability management covers application, dependency, container and cloud infrastructure risks. akirolabs also performs annual security testing through an external partner.

## 9 Adherence to privacy regulations

akirolabs is committed to data protection and ensures compliance with privacy regulations like GDPR. akirolabs conducts annual privacy impact assessments for high impact processes that involve personal data and ensures remediation of gaps, if any.

## 10 Security & privacy awareness

akirolabs conducts ongoing security and privacy awareness trainings that assure that the individuals (both employees and contractors) are trained on their information security responsibilities in handling the Customer data. Additionally, regular security awareness mailers are sent to all individuals. Annual online training and assessment is done to ensure that all employees are aware and adhere to security and privacy policies and procedures.

## 11 Incident response

A documented incident response process defines roles, responsibilities, escalation paths, investigation steps and communication procedures. Security incidents are triaged, investigated, contained, remediated and documented. Lessons learned and corrective actions are recorded following relevant incidents. Customer notification is performed in line with Section 8 of the DPA and applicable legal and regulatory obligations.

## 12 Business continuity and backup

Production is designed for high availability using a Multi-AZ architecture within an EU cloud region. Backup and recovery measures support restoration of service and data following disruption. Recovery procedures are maintained and tested periodically. Disaster recovery and business continuity measures are reviewed based on operational and Customer requirements.

## ANNEX 2

# Sub-processors

Version 08.09.2026

This Annex 2 to the Data Processing Agreement (DPA) lists the sub-processors used by akirolabs. Any addition of new sub-processors or replacement of existing sub-processors will comply with the provisions of the DPA. This Annex 2 also serves as Annex III to the Standard Contractual Clauses where these apply under section 9 of the DPA.

| Sub-processor                                                                                                                                   | Activity                                                                              | Personal data processed                                                              | Data storage location                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Amazon Web Services EMEA SARL</b><br>38 Avenue John F. Kennedy,<br>L-1855 Luxembourg                                                         | Cloud hosting, data storage and infrastructure management for the akirolabs platform  | Account data, usage logs, customer content                                           | EU                                                                                                                       |
| <b>Google Cloud EMEA Limited</b><br>70 Sir John Rogerson's Quay,<br>Dublin 2, Ireland                                                           | Cloud hosting, storage, logging and monitoring                                        | Account identifiers, usage logs, support artifacts                                   | EU                                                                                                                       |
| <b>Microsoft Ireland Operations Ltd</b><br>One Microsoft Place, South<br>County Business Park,<br>Leopardstown, Dublin 18, D18<br>P521, Ireland | Email, collaboration and productivity services (incl. user/stakeholder notifications) | Email content, contact details, shared files                                         | EU (EU Data Boundary regions)                                                                                            |
| <b>PostHog, Inc.</b><br>2261 Market Street #4008, San<br>Francisco, CA 94114, USA                                                               | Product analytics for the akirolabs platform                                          | User IDs, usage/event data, session metadata                                         | EU (AWS eu-central-1, Frankfurt)                                                                                         |
| <b>Whatfix GmbH</b><br>Große Gallusstraße 16-18, 60312<br>Frankfurt am Main, Germany                                                            | In-app guidance and digital adoption platform                                         | User identifiers, in-app interaction data                                            | EU                                                                                                                       |
| <b>Functional Software, Inc. dba Sentry</b><br>45 Fremont Street, San<br>Francisco, CA 94105, USA                                               | Application error and performance monitoring                                          | Error payloads which may contain user identifiers, IP addresses and request metadata | EU (de.sentry.io)                                                                                                        |
| <b>OpenAI OpCo, LLC</b><br>1455 3rd Street, San Francisco,<br>CA 94158, USA                                                                     | Large language model API for the in-app chat feature                                  | Prompts and text entered by users in the chat                                        | Transient – not stored by akirolabs; retained by OpenAI per its policy (currently 30 days); no training on Customer data |
| <b>Perplexity AI, Inc.</b><br>2261 Market Street STE 14441,<br>San Francisco, CA 94114, USA                                                     | AI-based research/response API                                                        | User queries submitted through the integration                                       | Transient – not stored by akirolabs; no training on Customer data                                                        |

akirolabs maintains written agreements with each sub-processor imposing data protection obligations no less protective than those in this DPA. Where a sub-processor is established outside the EU/EEA, the Standard Contractual Clauses apply as set out in section 9.

## ANNEX 3

# Description of the processing (Art. 28(3) GDPR)

Version 08.09.2026

This Annex 3 sets out the details of the processing required by Art. 28(3) GDPR. It also serves as Annex I.B to the Standard Contractual Clauses where these apply under section 9 of the DPA.

## 1 Subject matter of the processing

The provision of the akirolabs SaaS Solution, a platform for strategic procurement and category strategy development, together with the related maintenance, support and hosting services described in the Agreement.

## 2 Duration of the processing

For the term of the Agreement, followed by the retrieval and deletion periods set out in section 10 of the DPA and any statutory retention obligations.

## 3 Nature and purpose of the processing

Collection, recording, organisation, structuring, storage, hosting, retrieval, display, use, transmission within the SaaS Solution, backup, restriction, erasure and destruction of personal data, in each case for the purpose of providing the SaaS Solution and the associated support, maintenance, availability monitoring, error diagnosis and in-app assistance functionality to the Customer.

## 4 Categories of data subjects

- employees, officers, contractors and temporary staff of the Customer and its Affiliates who are Authorised Users of the SaaS Solution;
- employees and other personnel of the Customer and its Affiliates who are named or referenced within the SaaS Solution, for example as stakeholders, approvers, budget holders or team members in a category strategy;
- contact persons at the Customer's suppliers and other business partners whose details are entered into the SaaS Solution by the Customer; and
- personnel of an Authorized Partner designated by the Customer as Authorised Users.

## 5 Types of personal data

- identification and contact data: first and last name, business e-mail address, business telephone number, employer, business unit or department, job title and role;
- account and authentication data: user ID, credentials, single sign-on identifiers, assigned roles and permissions, account status;
- usage and event data: log-in records, IP address, device and browser metadata, activity and audit logs, session metadata, in-app interaction data;

- content data entered by Authorised Users: comments, assessments, stakeholder assignments, task allocations, free-text entries within category strategies and other content that may incidentally contain personal data;
- prompts and text submitted by Authorised Users to in-app artificial intelligence functionality; and
- support and incident data: correspondence with akirolabs support, error payloads and diagnostic information.

## 6 Special categories of personal data

None. The SaaS Solution is not intended for the processing of special categories of personal data within the meaning of Art. 9 GDPR or of personal data relating to criminal convictions and offences within the meaning of Art. 10 GDPR. The Customer shall not enter such data into the SaaS Solution.

## 7 Frequency of the processing

Continuous, for the duration of the Agreement.

## 8 Processing by sub-processors

The sub-processors listed in Annex 2 process the categories of personal data identified in that Annex, for the activities and for the duration stated there, and in each case only as necessary to enable akirolabs to provide the SaaS Solution.

## 9 Retention and deletion

Personal data is retained for the term of the Agreement and deleted in accordance with section 10 of the DPA, subject to statutory retention obligations.