Appendix 6 – Data Processing Agreement

https://akirolabs.com/assets/

Version: 01.09.2023

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). The provisions set forth herein apply mutatis mutandis before the revised FADP comes into force.

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.

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-

akirolabs GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com

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 the legality of the data processing by akirolabs.

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). 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.

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 GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com

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.

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.

For auditing purposes, the Customer or an auditor appointed by the Customer 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. 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.

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

akirolabs GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com

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 delay if akirolabs becomes aware of breaches in personal data protection by akirolabs or one of its sub-processors and will provide the Customer with all relevant information in text form (nature and extent of the breach, possible remedial actions, etc.). 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.

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 30 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 30-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 30-day period, akirolabs wipes the data on the akirolabs instance on Amazon AWS or Oracle ("Cloud Provider") using technology compliant with U.S. Department of Defense (DoD 5520.22-M) standard. The Cloud Provider will decommission the hardware using techniques outlined in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization"), and in certain cases, degauss or physically destroy the hardware in accordance with industry-standard practices.

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. The Customer must be notified in advance if akirolabs

akirolabs GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com

commissions new sub-processors or replaces existing sub-processors after this DPA has come into force. The Customer may object to a new sub-processor or the replacement of an existing sub-processor for important data protection reasons within 30 days (calculated from receipt of notice). 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.

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.

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

akirolabs GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com

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.

With respect to applicable law and jurisdiction, the provisions in the Agreement between akirolabs and the Customer shall apply.

akirolabs GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com

Annex 1 – Technical and organisational measures (TOM)

Version: 01.09.2023

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.

1. General principles

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

a) Information security polices & procedures

b) Physical security controls

c) Data encryption

d) Network security

e) Data leakage prevention controls

f) Access controls

g) Application security

h) Adherence to privacy regulations

i) Security & privacy awareness

2. Information security policies & procedures

akirolabs' platform and development partner is an ISO 27001 certified organization and has a comprehensive information security policy in place that covers all aspects of information security strategy including framework, protocols, and procedures. akirolabs and its platform and development partner have well-defined policies and security controls implemented for data protection. All policies and procedures are updated on an annual basis and controlled periodically as per ISO 27001 standard.

akirolabs is committed to protect the confidentiality, integrity and availability of its information assets and provide the same commitment to the in-formation assets entrusted to it by its customers and business partners and have implemented a gamut of 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

akirolabs GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com

- Continually monitor and improve the effectiveness of the ISMS.

3. Physical security controls

The Cloud Provider provides the physical security of Data Centres as a managed service. The Cloud Provider is compliant with requirements like ISO 27001, SOC 1, SOC 2, which are the basis for akirolabs to rely on the security controls offered by the Cloud Provider. akirolabs uses the Cloud Provider reports to draw assurance over Cloud Provider controls and for evaluating any risks from the Cloud Provider to akirolabs Services to its customers. 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 the servers hosting SaaS Solution with AES-256 encryption. Data in transit – data is transferred over HTTPS (TLS 1.2).

5. Network security

akirolabs uses a Web Application Firewall (WAF) to protect against common web exploits that may affect availability and/or compromise security. Cloud Provider Security Groups (firewall), Network Intrusion Detection Systems (NIDS), Denial of Service (DoS) Protection, are also implemented to control all inbound and outbound traffic while ensuring network security. The Security Groups restrict traffic by protocol, service port and IP address, in addition to these only specific ports have been allowed and configured in a default deny-all mode.

6. Data leakage prevention controls

The Cloud Provider, being a multi-tenant cloud, has implemented strong controls to prevent data leakage to its other customers. Customer data is logically segregated and controlled by data access layer. Data access layer abstracts the data store and provides an API object which business services leverages for data request. This is the 1st layer from which access control and data separations comes into play because of which business services do not see any data leakage. Each customer tenant is identified by a unique tenant ID in the akiro application, and every transaction is performable only with reference to the unique tenant ID. Unique accounts are used to access specific customer tenant.

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. Access matrix is agreed with the Customer at the time of design & implementation and rights are provided as per agreed rules. akiro’s application support team assists with user access management (creation, deletion, modification, and maintenance).

The SaaS Solution includes a form-based user authentication module that allows users to be authenticated via a login / password. Two-factor authentication is supported. SaaS Solution also

akirolabs GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com

supports the use of Customer's Single sign-on (SSO) and hence 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 SaaS Solution.

8. Application security

akirolabs follows secure software lifecycle development process to ensure that security is embedded in each phase of development. Pre-release application security testing validates that appropriate security controls are in place and that they cannot be circumvented. akirolabs also performs annual security testing through 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 assures 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.

akirolabs GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com

Annex 2 – Sub-processors

Version: 01.09.2023

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.

Sub-processor	Activity	Personal data processed
Amazon Web Services (Primary Hosting Location) 410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.	Primary hosting site for the customer's akirolabs instance and where the contract repository with contracts and all contract related data is housed	Name, Email
Amazon Web Services (Secondary Hosting Location) 410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.	Amazon Web Services (Back-up hosting site for the customer's akirolabs instance and where the contract repository with contracts and all contract related data is housed)	Name, Email
Microsoft Office 365 Services Microsoft Deutschland GmbH. Walter-Gropius-Straße 5 80807 München	The email services component of akirolabs utilizes these services for user/stakeholder notifications (e.g., obligation reminders, actions, etc.).	Name, Email
SurveySparrow Inc. 2345 Yale St FL 1, Palo Alto, CA 94306, U.S.A.	Survey capability	Name, Email
SirionLabs Pte Ltd. and its affiliates 10900 NE 4th St, Unit 2300, Bellevue, WA 98004, U.S.A.	Development, hosting and maintenance provider for the akirolabs Application	Name, Email

akirolabs GmbH
Am Holtwicker Bach 50, 46397 Bocholt, Deutschland
Amtsgericht Coesfeld HRB 19567 | USt.-ID: DE342195973 | Geschäftsführer: Detlef Schultz, Michael Pleuger
www.akirolabs.com