DATA PROCESSING AGREEMENT

Date: 01/10/24

Document: AK-ISMS-054

Classification: Public

This Akixi (“us””we” “our”) Data Processing Agreement (“DPA”) reflects the parties' agreement with respect to the Processing of Personal Data by us on behalf of you (“Customer”) in connection with the Akixi Subscription Services under the Akixi terms of services between you and us.

This DPA is supplemental to and forms an integral part of the agreements with you. It is effective upon its incorporation into the agreements, which may be specified in the agreement, as an order form or an executed amendment to an agreement. In case of any conflict or inconsistency with the terms of any agreement with you, your contractual terms will take precedence to the extent of such conflict or inconsistency.

We update these terms from time to time.

1. Definitions

1.1. **"Data Protection Laws"**: Any applicable data protection laws, including but not limited to the General Data Protection Regulation (GDPR), the UK Data Protection Act, and any other laws related to data privacy and protection.

1.2. **"Personal Data"**: Any information relating to an identified or identifiable natural person that is processed under this DPA.

1.3. **"Processing"**: Any operation or set of operations performed on personal data, such as collection, storage, use, access, transmission, or deletion.

1.4. **"Sub-Processor"**: Any third party appointed by the Processor to process personal data on behalf of Akixi.

1.5. **"Data Controller"**: The party that determines the purposes and means of processing personal data, i.e., this could be you, your reseller or your resellers customer, the relationship will be defined by you.

1.6. **"Data Processor"**: The party that processes personal data on behalf of the Data Controller, i.e., Akixi as the Service Provider, you may wish to declare yourself as a processor and define your relationship with the controller.

2. Subject Matter

Akixi agrees to process personal data on behalf of the customer in accordance with this DPA and the applicable Data Protection Laws.

3. Scope and Purpose of Processing

3.1. Akixi shall process personal data only to provide the services to you set forth in agreements or contracts and according to the customer's instructions. The services include Call Metrics and/or CRM solutions depending on the services you request.

3.2. Depending on the services provided by Akixi or interaction with Akixi, the categories of personal data processed may include, but are not limited to, the following: Contact details, gender, title, company name , telephone numbers, extension numbers, usernames, e-mail address, work address, online identifiers such as IP address, cookies, browser details, images, usage data, meta data, transcriptions, video or call recordings and personal data provided by you via communication with us which may be recorded.

3.3. The processing of personal data by Akixi is limited to the following purposes:

- To provide access to the solutions and platforms we provide
- To fulfil the contractual obligations
- To provide you with technical support
- To provide you with training material and repository of information
- To improve our services to you
- To accurately transcribe and/or record content of calls to enhance our service, training and for dispute resolution
- To provide you with communication methods and to engage with you
- To market news and information specific to our products and services
- To comply with legal obligations and to respond to legal requests

4. Obligations of Akixi (Processor)

4.1. Akixi shall process personal data only on documented instructions from the customer, unless required to do so by law.

4.2. Akixi will implement appropriate technical and organisational measures to protect your personal information from unauthorised access, disclosure, alteration, or destruction, these security measures are detailed in Annex 2 of this DPA. We have also obtained assurances from our Sub-Processors that they also implement sufficient security measures to protect your personal information. However, no method of transmission over the internet or electronic storage is completely secure, therefore we cannot guarantee absolute security.

4.3. Akixi shall ensure that all personnel authorised to process personal data are bound by confidentiality obligations.

4.4. Akixi shall promptly inform the customer if it believes that an instruction from the customer violates applicable law or Data Protection Laws.

4.5. Akixi shall notify the customer without undue delay upon becoming aware of any personal data breach.

5. Obligations of the Customer (Controller)

5.1. The customer shall ensure that all personal data provided to Akixi is processed in accordance with applicable Data Protection Laws and that it has obtained the necessary consents or other legal bases for processing.

5.2. The customer shall provide clear and lawful instructions to Akixi regarding the processing of personal data.

5.3. The customer acknowledges that they are responsible for responding to requests from data subjects to exercise their rights and shall seek assistance from Akixi only when necessary.

6. Sub-Processing

6.1. You agree that Akixi can engage Sub-Processors to process personal data on your behalf, and we do so in three ways. First, we may engage with Sub-Processors to assist us with hosting and infrastructure. Second, we may engage with Sub-Processors to support product features and integrations. Third, we may engage with Akixi Sub-Processors for services and support to fulfil our contractual obligations. Some Sub-Processors will apply to you as default, and some Sub-Processors will apply only if you opt in.

We have currently appointed Sub-Processors, the third parties are listed in the appendix Annex 1 to this DPA.

We will provide you with the opportunity to object to the engagement of a new Sub-Processor on reasonable grounds relating to the protection of Personal Data within 30 days of notifying you. If you do notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected service in accordance with termination agreements we have with you.

6.2. Akixi shall ensure that any Sub-Processor it engages is bound by data protection obligation and are suitably vetted and aligned with Data Protection principles and legislation.

7. International Data Transfers

7.1. Akixi shall not transfer personal data outside the UK or European Economic Area (EEA) without ensuring appropriate safeguards, such as standard contractual clauses or other legally recognised mechanisms are in place as set out under Art 45 of the GDPR. When transferring personal information to the United States, we shall ensure that, by

default, the Sub-processor is compliant with the EU-US Data Privacy Framework and the UK extension to the EU-US Data Privacy Framework.

7.2 For Canadian data subjects, and to comply with Canadian data protection laws, Personal data will be collected and stored on servers located in the United States which regionally may have different privacy laws compared to Canada, access to personal data may be subject to United States Laws, including access by United States Law enforcement agencies under specific circumstances, such as the Patriot Act.

Akixi will ensure suitable security safeguards are in place regarding the transfer and processing of data in the United States consistent with the obligations set out in this DPA.

7.3 For South-African data subjects: We will ensure your customers personal data is stored regionally in a tenant in South Africa. However, South African data subjects' personal information may be transferred to the UK or EU, Under South African data protection laws it is lawful to transfer personal data to the UK or EU as the GDPR is recognised as adequate data protection under the Protection of Personal Information Act (POPIA).

7.4 For Australian data subjects: We will ensure your customers personal data is stored regionally in a tenant in Australia. However, Australian data subjects' personal information may be transferred to the UK or EU, Under Australian data protection laws it is lawful to transfer personal data to the UK or EU as the GDPR is recognised as adequate data protection under the Australian Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs).

7.5 For United States data subjects: We will ensure your customers personal data is stored regionally in a tenant in the United States. However, United States data subjects' personal information may be transferred to the UK or EU. Under United States data protection laws, it is lawful to transfer personal data to the UK or EU as Akixi will ensure that specific frameworks and security measures are in place to ensure the lawful transfer of data, this may include the EU-US Data Privacy Framework and the UK extension to the EU-US Data Privacy Framework.

California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA): The CCPA and its successor, CPRA, regulate data transfers out of California, which may include international transfers. To comply with Californian data protection, Akixi will not sell Californian data subject personal information, additionally data subjects can execute their rights to delete, opt-out or restrict processing their data as set out in section 8 of this DPA

7.6 By default, Akixi shall with best efforts, build tenants and process personal data regionally to the data subjects and comply with regional legislation regarding the transfer of personal data internationally.

8. Data Subject Rights

8.1. Akixi shall, to the extent possible, assist the customer in fulfilling their obligation to respond to data subject requests, such as requests for access, correction, deletion, or restriction of processing. To exercise these rights, please contact us detailed in section 14 of this DPA.

8.2. Akixi shall promptly inform the customer if they receive a request directly from a data subject, without responding to the request, unless authorised to do so by the customer.

9. Data Breach Notification

9.1. In the event of a personal data breach, Akixi shall notify the customer without undue delay after becoming aware of the breach mandated by the GDPR.

9.2. The notification shall include details regarding the nature of the breach, the categories of data affected, the number of affected data subjects, and any steps taken to mitigate the effects of the breach.

10. Data Retention and Deletion

10.1. Upon termination of the Agreement, Akixi shall, at the choice of the customer, either delete or return all personal data to the customer unless deletion is prohibited by law.

10.2 Within the production server tenants we will retain a backup of data for 3yrs after deletion of data after which the data will be permanently deleted.

10.3. We will retain the information we hold about you until the termination of any agreement we have with you. Data that you or your customers upload onto the services that Akixi provide to you are retained by you or your customers respective data retention policies.

10.4. Personal data that is deleted will be removed from all systems, backups, and storage media, unless such deletion is prohibited by law.

10.5. We will delete data upon a data subject access request, providing it is permittable by law. Should the deletion of data potentially impact the service we provide to you, we will discuss the impact with you in good faith to find a reasonable solution.

11. Demonstration of Compliance, Audits and Inspections

11.1. Akixi, upon reasonable request and subject to confidentiality, make available to the customer all information necessary to demonstrate compliance with this DPA.

11.2. The customer may, at its own expense and upon reasonable notice, conduct audits of Akixi's processing of personal data to verify compliance with this DPA and applicable laws.

11.3. You acknowledge that the subscription services that are hosted by our hosting Sub-Processors maintain independent validation security programs

(including SOC2 and/or ISO27001) and that our own systems are audited periodically internally and annually externally to comply with our ISO27001 accreditation and upon request will provide certifications and evidence of compliance. Additionally, we conduct regular penetration testing and vulnerability scans of our infrastructure and systems. The business has a Business Impact Assessment (BIA) and Business Continuity Plan (BCP) which is tested annually.

12. Limitation of Liability

12.1. Akixi liability under this DPA shall be subject to the limitations and exclusions set forth in the agreements we have with you, except to the extent such limitations are prohibited under applicable Data Protection Laws.

12.2. Akixi shall be liable only for damages caused by processing where it has not complied with its obligations under this DPA or applicable laws.

13. Governing Law

13.1. This DPA shall be governed by and construed in accordance with the laws of England, without regard to its conflicts of law principles.

13.2. Any disputes arising from this DPA shall be subject to the exclusive jurisdiction of the courts of England.

14. Contact us

Akixi Limited, Churchill Court, 3 Manor Royal, Crawley RH10 9LU

Email: DPO@akixi.com

Telephone number: +44(0)1293 853060

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). You can contact the ICO as follows:

By phone: 0303 123 1113

By post: Information Commissioner's Office, Wycliffe House Water Lane, Wilmslow, Cheshire,SK9 5AF, United Kingdom.

We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

15. Signatures

We can provide a signed copy to execute this DPA should you so wish, please contact us using the details provided in section 14 of this DPA.

IN WITNESS WHEREOF, the parties have executed this Data Processing Agreement as of the date of the last signature below.

[Customer Name]

By: _____
Name: _____
Title: _____
Date: _____

[Your Company Name]

By: _____
Name: _____
Title: _____
Date: _____

Annex 1: List of Sub-Processors

Sub-Processor Name	Purpose of Processing	Location of Processing
AWS	Main service platform for call metrics processing.	Regional to the customers data subjects
AZURE	Service to supplement the AWS environment for Teams integration. Services and repository for information	Regional to the customers data subjects
HubSpot	CRM contact platform for engagement with the customer	USA
AccountsIQ	Finance/Billing/ Accountancy	UK

Sub-Processor Name	Purpose of Processing	Location of Processing
FreshService / Freshdesk	Technical Support services and logging	USA
MindMatrix	Training facilities – documentation and videos	USA
Microsoft	Email, Teams, communication	EU
Jiminny	Transcribing and recording sales calls for training and dispute resolution	UK
Entergrade	Support services for Teams integration	Canada
Monday.com	Project management and Proof of concept delivery	EU
DataXchange	Billing process	UK
Dubber	Recording incoming support calls for training and dispute resolution	UK
TeamViewer	Remote support at desktop level	EU
Oak Innovate	Providing call recording features for customers	UK
Zapier	Integration tool to pass data between platforms	USA

Annex 2: Security measures

We currently observe the security measures described in this Annex 2. For more information on these security measures, please refer to Akixi Statement of Applicability and Security Policy available on request.

- ✓ **Information Security Policy**

  We maintain and adhere to an internal, written Information Security Policy, aligned with the ISO27001:2013 standard. We can provide you with a copy of the security policy on request and/or a copy of our ISO27001:2013 certification.

- ✓ **Access Controls**
  - **Preventing unauthorised product access**

    Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs to protect data processed or stored by these vendors.

    Physical and environmental security: We host our product infrastructure with multi-tenant, segregated, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centres. Production servers and client-facing applications are logically and physically secured and segregated from each other and from our internal corporate information systems. The infrastructure providers' physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

    Authentication: We implement a uniform password policy for our customer products and information systems ensuring strong passwords, including suitable complexity requirements and lockout features. Customers who interact with the products via the user interface must authenticate before accessing customer personal data on their Axixi provided services. Security features such as MFA are provided to you and your customers and would encourage you to use this feature to further secure your access controls to your data sets.

    Authorisation: Customer data is stored on multi-tenant storage systems accessible to customers via application user interfaces.

Customers are not allowed direct access to the underlying application infrastructure, only authorised Akixi staff are allowed privileged access, access is restricted to appropriately assigned individuals who will have unique secure access to the infrastructure gained through layers of security protocols.

- **Preventing unauthorised product use**
  We implement industry standard access controls and detection capabilities for the internal networks that support its products.

  Network access control mechanisms are designed to prevent network traffic using unauthorised protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include: Virtual Private Network (VPN) implementation, security group restrictions, access lists, traditional firewall rules and service restrictions.

  We provide monitoring for intrusion detection and prevention through controls that may include Web application Firewalls (WAF) and/or through suspicious activity monitoring tools including capacity and service management and suspicious login activity.

  Static code analysis: Code stored in our source code repositories is checked for best practices and identifiable software flaws using automated tooling.

  Dynamic code analysis: we use various penetration and vulnerability scanning techniques to identify security flaws and for the implementation of best practice.

  Endpoint Harding: Endpoints are hardened in accordance with industry standard practice. Laptops and systems are protected using anti-malware and endpoint detection plus response tools, receiving regular definition and signature updates.

✓ **Transmission Control**

In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces on every customer site hosted on the Akixi products. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We take a layered approach of at-rest encryption

technologies to ensure customer data and customer-identified Permitted Sensitive Data are appropriately encrypted.

- ✓ **Incident Management, Logging and Monitoring**

  Incident Response Plan: We maintain a written Incident Response Plan and other necessary processes and procedures to fulfil the standards and obligations reflected therein.

  Detection: we implement various systems and tools to monitor and alert about system behaviour, traffic activity, system authentication, anomalous activities, malicious activity. We also implement various threat intelligence tools to detect threats or potential threats to our assets and estates. Akixi internal support, Development and DevOps are accountable for responding to incidents or concerns raised.

  Response & tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, actions taken, closing out description and lessons learned. Suspected and confirmed security incidents are investigated by internal support, DevOps or development and reported to the compliance manager who will assemble a response team. Appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimise product and customer damage or unauthorised disclosure. Notification to you will be in accordance with the terms of the Agreement we have with you and complaint with legislation.

- ✓ **Availability Control**

  Infrastructure availability: the infrastructure providers use commercially reasonable efforts to ensure a minimum uptime consistent with the agreements we have with you on Service Level Agreements and system uptime.

  Fault tolerance: We use replication and backup strategies that are designed to ensure redundancy and fail-over protection during a significant failure. Customer data is backed up to separate regions with replication across multiple zones. Backups are taken every 24 hours, with additional “off-site” cold storage facilities. Backups are encrypted to ensure additional security.

  Business Continuity Planning (BCP): We maintain and test BCP, identifying key business assets and systems aligned with a business impact assessment. Identifying and planning help ensure availability of information following interruption to or failure of critical business processes.

Our products and services are designed to ensure redundancy and minimal disruption as possible and limiting downtime.

- ✓ **Vulnerability Management Program**

Vulnerability Remediation: We take a risk-based approach to determining a vulnerability applicability, likelihood and impact on our environment and retain a register of security risks. These risks are reviewed at least annually by management to ensure relevance, accuracy and mitigation.

Vulnerability scanning: We utilise technology, detection tools and industry standards to monitor our information assets for vulnerability. Scans are performed at regular intervals during the day or from threat intelligence sources daily. Potential vulnerabilities are internally assessed for relevance and impact with mitigation measures deployed.

Penetration testing: We maintain relationships with industry-recognised penetration testing service providers for penetration testing of both the Akixi production server environments and applications at least annually. The intent of these penetration tests is to identify security vulnerabilities and mitigate the risk and business impact they pose to the in-scope systems.

- ✓ **Personnel Management**

We employ qualified personnel to develop, maintain, and enhance our security program. We train all employees on security policy, processes, and standards relevant to their role and in accordance with industry practice.

Background checks: Where permitted by applicable law, Akixi employees undergo a background or reference check. All Akixi employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.