General Data Protection Regulation Compliance

Version 1.1

Document Code: KYK-FRM-0099-Kayako GDPR Whitepaper

January, 2021

Legal Notice

Contents

Overview

This document outlines how Kayako Limited ("Kayako") complies with the European Union General Data Protection Regulation ("GDPR").

Kayako's data protection program (the "Programme") is designed to safeguard Personal Data (defined below) according to the GDPR requirements. In particular, this document describes the Programme elements pursuant to which Kayako intends to (i) ensure the security and confidentiality of Personal Data, (ii) protect against any anticipated threats or hazards to the security of Personal Data, and (iii) protect against unauthorised access or use of Personal Data in ways that could result in substantial harm to Kayako's customers and their respective clients.

At Kayako, respecting and protecting privacy is of critical importance, and one of our key business principles. You can read our Privacy Policy at: https://www.kayako.com/about/privacy

Scope of the Programme

The Programme applies to personal data (as defined by the GDPR) that is accessed or received by Kayako acting as a data processor on behalf of its customers (data controllers) in connection with providing the contracted services ("Personal Data").

This document describes Kayako's data protection general practices, however, each product might follow specific methods.

Official GDPR Compliance Statement

Kayako currently processes Personal Data lawfully in accordance with the GDPR.

With respect to the GDPR, Kayako has identified its obligations as a data processor and established internal teams with specific obligations, responsibilities, and deadlines to meet these obligations.

Appointment of a Data Protection Officer

Kayako's Data DPO ("DPO") is responsible for coordinating and overseeing the Programme. The DPO may designate other representatives of Kayako to oversee and coordinate elements of the Programme.

Privacy Impact Assessment

Kayako identifies and assesses external and internal risks to the security, confidentiality, and integrity of the Personal Data that could result in the unauthorised disclosure, misuse, alteration, destruction or other compromise of such information.

Kayako ensures the organisation's risks are appropriately addressed in a manner which is cost effective and allows Kayako to balance the operational and economic costs of risk management measures. Kayako has a process for the selection and implementation of security safeguards to reduce the risks of Personal Data to reasonable and manageable levels.

The DPO will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Privacy by Design

At Kayako, a software product typically undergoes several development life cycles, from its creation and throughout subsequent upgrades. Each such development life cycle constitutes a project. Such projects continue until the underlying technology ages to the point where it is no longer economical to invest in upgrades and the application is considered for either continued as-is operation or retirement. Kayako's Product Development team utilises the Agile software development methodology for development, testing, verification, and validation.

Kayako understands that to be more effective, information security must be integrated into the Software Development Life Cycle ("SDLC") from system inception. Early

integration of security into the SDLC enables Kayako to strengthen its information security practices, through:

- Early identification and mitigation of security vulnerabilities and misconfigurations;
- Awareness of potential engineering challenges caused by mandatory security controls;
- Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques; and
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner.

Overseeing Sub-Processors of Personal Data

The DPO coordinates with those responsible for the sub-processors related activities to raise awareness of, and to institute methods for selecting sub-processors that are capable of maintaining appropriate safeguards for Personal Data. In addition, the DPO works with legal counsel to develop and incorporate standard, contractual protections applicable to sub-processors, which will require such providers to implement and maintain appropriate data protection safeguards. In addition, sub-processors may be subject to a risk assessment on a periodic basis.

Data Hosting Services

The Kayako solutions are primarily hosted by Customers on premise whilst some are using SaaS hosting services.

Generally, Kayako utilises hosting services provided by Amazon Web Services, Inc. (“AWS”) for development and other activities, and access is controlled by AWS according to its data protection policies and procedures. You can read further details on AWS’ GDPR compliance at https://aws.amazon.com/compliance/eu-data-protection/.

Note that some Kayako products may utilise services other than those provided by AWS.

Protecting Access to Data

Kayako has established consistency for controlled access to its computing resources and data owned or controlled by Kayako. Kayako enforces business process controls and data classification policies and authorisation mechanisms that specifies the level of access for a user, a process, or a system.

Kayako has also established the requirements for ensuring authorised use of its computing resources via proper user identification and password authentication.

Data Retention

Kayako reviews, retains, and disposes of records received or created in the transaction of its business in accordance with regulatory requirements and contractual agreements. Kayako works towards eliminating accidental destruction of records and at the same time, facilitates its operations by promoting efficiency and reducing unnecessary costs of storage of records. Customer data is retained according to legal and contractual requirements.

Encryption

Kayako's services are designed to provide data security and integrity. All services are accessed through encrypted connections using industry standard ssl/tls. Additionally, the architecture of some of the services provide further security of data by segregating the object data, the indices and the encryption keys on physically and logically separated systems.

- **Encryption in Transit.** Encryption via signed SSL certificates is enabled for data transmission through our hosted Kayako Product Server service. Transmissions to and from our Customer Support Portal are also encrypted. Our Customers who host the application on premise are responsible for ensuring appropriate levels of encryption in transit. Except as noted in this section, Kayako is not responsible for the security of any data transmitted to us via any other channels.
- **Encryption at Rest.** Our Customers who host the data on premise are

responsible for ensuring appropriate levels of Personal Data protection including any encryption at rest. The databases we host for our Customers are encrypted utilizing industry standard encryption approaches.

Data Breach Notification

Kayako has developed and implemented a data breach response plan designed to provide guidance to employees and contractors on how to report suspected data breaches. Upon becoming aware of a security issue involving Personal Data, employees and contractors must report the issue immediately to the DPO. This plan outlines steps to be taken by compliance management to investigate potential data security breaches. These steps include performing a risk analysis of each suspected data breach to determine whether the event requires notification per applicable laws. Kayako also addresses mitigation and remediation actions as part of the data breach response activities.

Training and Education

The Programme policies and procedures are communicated to relevant employees and contractors via new hire on-boarding and annually thereafter as part of the Information Security Programme Training. Notification of significant revisions to existing policies and procedures outside of the on-boarding and the Information Security Programme Training are communicated via email to relevant employees and contractors or via special training sessions. Such training includes material relevant to GDPR. In addition, employees and contractors are bound by confidentiality provisions.

Periodic Programme Evaluation

The DPO is responsible for evaluating and adjusting the Programme based on the risk identification and assessment activities undertaken pursuant to the Programme, as well as any material changes to Kayako’s operations or other circumstances that may have a material impact on the Programme.

Product Customisations

3rd party Professional Services team is also available to assist you with customisations or configurations needed for your GDPR compliance undertakings.

Customisation or configurations are not automatically covered by our GDPR product compliance program and maintenance services. You may require a separate Professional Services engagement to assist you with making the necessary product changes to facilitate your GDPR compliance needs.

Contacting Us

If you have any additional questions or need assistance, please contact your Account Manager.