Data Processing Agreement

This Data Processing Agreement (this “Agreement”) is incorporated into and made a part of the most recent Terms & Conditions in effect between Akamai and a legal entity that has purchased Services from Akamai (“Customer”). "Terms & Conditions" shall mean the terms and conditions, network services agreement, master services agreement and/or other similar agreement or terms (including, as applicable, the Akamai Terms & Conditions set forth at www.akamai.com/terms) governing the purchase of Akamai offerings signed by and between Customer, or its Affiliate(s) (as defined in the Terms & Conditions), and Akamai, or its applicable Affiliate(s), as the same may be or have been amended by the parties from time to time. If the provisions of this Agreement and the Terms & Conditions conflict, including any previously executed or incorporated data protection agreement or privacy terms and conditions, then the provisions of this Agreement shall control. Except for any changes made by this Agreement, the Terms & Conditions remain unchanged and in full force and effect.

1. **Definitions**. Unless otherwise defined herein, all capitalized terms used in this Agreement shall have the meanings assigned to such terms in the Terms & Conditions.

“Agreement Personal Data”	means all Personal Data that Akamai processes on behalf of Customer as a Data Processor as specified in Schedule 1.
“Authorized Sub-Processor”	means any third party appointed by Akamai in accordance with this Agreement to process Agreement Personal Data on behalf of and as instructed by the Customer. For the avoidance of doubt, suppliers to Akamai that provide bandwidth connectivity and/or colocation services for Akamai owned and controlled servers globally, where such providers have no access to communications or any data located on Akamai servers (i.e., such suppliers acting as “mere conduits”), shall not be considered Authorized Sub-Processors.
“Cross-Border Transfer Mechanism”	means applicable legal mechanisms required for the transfer of Personal Data from a Data Controller or Data Processor in a given jurisdiction to another Data Controller or Data Processor operating in a separate jurisdiction where applicable Data Protection Laws require a legal mechanism for cross-border transfer. Such mechanisms include, by way of example and without limitation, adequacy decisions, binding corporate rules, the EU standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council pursuant to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as may be updated or replaced from time to time.
“Data Protection Laws”	means all applicable laws (including decisions and guidance by relevant Supervisory Authorities) relating to data protection, the processing of personal data, and privacy applicable to Akamai and the Customer in respect of the processing of Agreement Personal Data to provide the Services, including such laws, by way of example and without limitation, the General Data Protection Regulation, the California Consumer Privacy Act, and the Personal Information Protection and Electronic Documents Act.
“Data Controller, **“Data Exporter”, “Data Importer”, “Data Processor” “Data Subject”, “Personal Data”, and “Personal Data Breach”**	shall each have the definitions and meanings ascribed to them by the applicable Data Protection Laws, and shall include any equivalent or corresponding terms applied by such applicable Data Protection Laws (e.g., “Business” instead of “Data Controller” and “Service Provider” instead of “Data Processor” under the California Consumer Privacy Act, or “organization” or “agency” under the Australian Privacy Principles).
“Supervisory Authority”	means the government agency, department or other competent organization given authority over the processing of Personal Data relevant to this Agreement.

2. Data Processing

2.1 **Compliance with Law.** Customer and Akamai each shall comply with their respective obligations as Data Controller and Data Processor, as applicable, under the Data Protection Laws.

2.2 **Data Processor Terms.** The parties agree and acknowledge that (i) Akamai, (and any relevant Affiliates, if applicable), when providing the Services to Customer, will be acting as a Data Processor in respect of the processing by or for it of Agreement Personal Data and, (ii) Customer hereby authorizes Akamai to process Agreement Personal Data as a Data Processor (on its and its Affiliates' behalf, if applicable) for the purposes of providing the Services only.

2.2.1 Akamai is authorised to engage, use or permit an Authorized Sub-Processor for the Processing of Agreement Personal Data provided that:

(a) Akamai undertakes reasonable due diligence on them in advance to ensure appropriate safeguards for Agreement Personal Data and respective individual rights in accordance with applicable Data Protection Laws;

(b) Akamai shall provide Customer with advance written notice of any intended changes to any Authorized Sub-Processor, allowing Customer sufficient opportunity to object; and

(c) The Authorized Sub-Processor's activities must be specified in accordance with the obligations set out in this Section 2.2.

Without prejudice to this Section 2.2.1, Akamai shall remain responsible for all acts or omissions of the Authorized Sub-Processor as if they were its own. Customer hereby approves the Authorized Sub-Processors that Akamai uses to provide the Services, listed at https://www.akamai.com/legal/compliance/privacy-trust-center/list-of-sub-processors. Further, to the extent that any Data Protection Laws would deem an Akamai Affiliate, by sole virtue of its ownership of Akamai servers used to provide the Services, to be a sub-processor for purposes of this Agreement, Customer hereby authorizes Akamai's use of such Akamai Affiliates as Authorized Sub-Processors.

2.2.2 Akamai shall (and procure that any Authorized Sub-Processor shall):

(a) process Agreement Personal Data only on documented instructions from Customer, including those set forth in the Terms & Conditions, this Agreement, technical specifications provided for administration of the Services, and configuration settings set in any of Akamai's customer portals provided for administration of the Services;

(b) without prejudice to Section 2.2.2(a), ensure that Agreement Personal Data will only be used by Akamai as set forth in this Agreement or the Terms & Conditions;

(c) ensure that any persons authorized to process Agreement Personal Data:

(i) have committed themselves to appropriate confidentiality obligations in relation to Agreement Personal Data or are under an appropriate statutory obligation of confidentiality;

(ii) access and process Agreement Personal Data solely on written documented instructions from Customer; and

(iii) are appropriately reliable, qualified and trained in relation to their processing of Agreement Personal Data;

(d) implement technical and organizational measures at a minimum to the standard set out in Schedule 2 to ensure a level of security appropriate to the risk presented by processing Agreement Personal Data, including as appropriate:

(i) the pseudonymisation and encryption of Personal Data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

(e) notify Customer without undue delay (and in any event no later than 48 hours) after becoming aware of a Personal Data Breach as set forth in Section 4;

(f) assist Customer in:

(i) responding to requests for exercising the Data Subject's rights under the Data Protection Laws, by appropriate technical and organizational measures, insofar as this is reasonably possible, provided that Akamai shall not be required to store or process any data for the purpose of re-identifying an individual when such information is not normally processed or stored by Akamai;

(ii) responding to any requests or other communications from the Customer as Data Controller relating to the processing of Agreement Personal Data under this Agreement;

(iii) reporting any Personal Data Breach to any Supervisory Authority or Data Subjects and documenting any Personal Data Breach;

(iv) taking measures to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and

(v) conducting mandatory privacy impact assessments of any processing operations and consulting with any applicable Supervisory Authority or appropriate persons accordingly;

(g) at the choice of Customer and where appropriate, to the extent that Agreement Personal Data is stored by Akamai, securely delete or return all Agreement Personal Data to Customer after the end of the provision of relevant Services relating to processing, and securely delete any remaining copies and certify when this exercise has been completed;

(h) make available to Customer all information necessary to comply with its obligations to do so under Data Protection Laws;

(i) immediately inform Customer if Akamai is of the opinion that an instruction of Customer regarding the processing of Agreement Personal Data violates applicable Data Protection Laws; and

(j) not sell, rent, disclose, release, transfer, make available or otherwise communicate, Agreement Personal Data to a third party for monetary or other valuable consideration.

2.3 **Cross-Border Transfers.**

2.3.1 The Customer hereby acknowledges and accepts that Akamai transfers Agreement Personal Data for service operation purposes to countries outside the jurisdiction the Customer operates in to Authorized Sub-Processors. Where Agreement Personal Data is transferred to a country that is not considered to have an adequate data protection level under Data Protection Laws, Akamai ensures that the data transfers comply with Data Protection Laws, e.g., by having in place at least one effective Cross-Border Transfer Mechanism(s) and having performed data transfer risk assessments. Details of Akamai's data transfers, the data transfer mechanism(s) in place and assessments performed are available in Akamai's Privacy Trust Center in the Cross-Border Data Transfer section, at: https://www.akamai.com/legal/compliance/privacy-trust-center and to the extent applicable respective Cross-Border Transfer Mechanism(s) available in Akamai Privacy Trust Center shall be incorporated herein and form part of this Agreement.

2.3.2 Where Customer is acting on behalf of an affiliate located outside the jurisdiction the Customer operates in and that affiliate acts as data exporter and Akamai Technologies, Inc. and its Authorized Sub-Processors act as data importers for any Personal Data transferred by Akamai as part of its service operation, Akamai offers to agree on EU Standard Contractual Clauses with the Customer on behalf of the data exporting affiliate. The respective EU Standard Contractual Clauses are available for Customer to download in the Cross-Border Data Transfer Section in Akamai's Privacy Trust Center: https://www.akamai.com/legal/compliance/privacy-trust-center.

3. Audits

Akamai shall conduct periodic audits of its processing of Agreement Personal Data to ensure compliance with Data Protection Law. Upon request, Akamai shall deliver to Customer relevant compliance documentation from such audit(s) (e.g., Akamai's then-current SOC 2 Type 2 (or its successor) report) and certain, selected policies, procedures and evidence that have been approved for distribution to customers.

In addition, in the event that Customer reasonably believes that the relevant documentation provided by Akamai warrants further examination to demonstrate compliance with Data Protection Laws and this Agreement, upon Customer's request not less than thirty (30) days in advance, one (1) on-site audit per annual period during the Term may be conducted at a representative Akamai facility involved in the delivery of Services, at reasonable times during business hours and at Akamai's then-current rates. The scope of such audit, including conditions of confidentiality, shall be mutually agreed prior to initiation of the audit.

4. Personal Data Breach

4.1 Akamai shall notify Customer without undue delay (and in any event within 48 hours), after becoming aware of a Personal Data Breach via e-mail to the 24/7 security contacts provided by Customer from time to time in the respective customer portal (e.g. Akamai Control Center). Such notice shall include a description of the nature of the Personal Data Breach and, where possible, other information as is required by applicable Data Protection Law(s); provided, that, where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

4.2 Akamai shall take all commercially reasonable measures and actions as are appropriate to remedy or mitigate the effects of the Personal Data Breach and shall keep Customer (and where applicable the Supervisory Authority) up to date about developments in connection with the Personal Data Breach.

5. Akamai's Processing of Service Logs

During its service operation, Akamai logs accesses made to one of its servers or to its cloud computing environment ("**Service Logs**"). The logging ensures the application of security rules, the ability to block non-legitimate access attempts, creation, and improvement of Akamai's knowledge about cyberthreats and attacks and its knowledge about the state of its server network, as well as improvement of Akamai Services. Further it enables Akamai to collect the data required to bill customers in accordance with their traffic usage, plan future capacity and deployment needs and create reports on the traffic on its server network.

Depending on the Akamai Services the Service Logs created consist of Cloud Computing Log Personal Data, Traffic Log Personal Data, Enterprise Security Personal Data, Application Security Personal Data or API Personal Data (as defined in Schedule 1).

The Service Logs are created locally on an Akamai server or in the cloud computing environment and transferred to Akamai's backend systems deployed in the USA and/or (remotely) accessed by Akamai's global employee base based on the least privilege principle. Related data transfers are governed by data transfer mechanism(s) in place between the relevant Akamai entities and made available to Customer upon request. Details of the processing of Service Logs is described in Akamai's Privacy Statement, available at: https://www.akamai.com/legal/privacy-and-policies/privacy-statement, and in the "Overview of Processing Activities and Roles", available in Akamai's Privacy Trust Center at: https://www.akamai.com/content/dam/site/en/documents/akamai/overview-of-akamai-personal-data-processing-activities-and-role.pdf.

Where the processing of Service Logs is considered under Data Protection Laws as processing for Akamai's own (service operation) purposes, Akamai ensures Personal Data included in the Service Logs is processed only as describe above and in compliance with Data Protection Laws, and Customer hereby acknowledges and agrees to the processing of Personal Data in Service Logs by Akamai as Data Controller.

Schedule 1 of the Data Processing Agreement:
Details of Akamai's Processing Activities

1. Data Processor

Akamai is a provider of cloud computing, delivery and security services.

2. Data Subjects

Akamai processes Personal Data of individuals:

a) accessing Customer Content or whose personal data is embedded in the Customer Content, or

b) accessing Customer's corporate systems

when performing the Akamai Services for the Customer.

"Customer Content" means:
all content, applications, services or API traffic packet, including any third-party content, applications or services, provided to Akamai in connection with Customer's and/or individual's access to or use of the Akamai Services.

3. Categories of data processed

Akamai processes the following categories of Personal Data when performing the Akamai Services:

a) <u>Cloud Computing Services</u>

Akamai processes Personal Data embedded in Customer Content ("**Customer Content Personal Data**") when providing Cloud Computing Services to Customer. Upon the Customer's or individual's choice, Customer Content Personal Data may include data such as:

a. Login credentials
b. Subscriber name and contact information
c. Financial or other transaction information
d. Other Personal Data relating to the individual embedded in Customer Content

Special categories of personal data or sensitive data as defined under Data Protection Laws or any other applicable law or regulation, may be part of Customer Content Personal Data, as determined by the Customer or individual.

Akamai processes Personal Data embedded in cloud computing environment and servers used to host virtual machines logs which may include access logs relating to individual's access made to the Akamai cloud computing environment ("**Cloud Computing Log Personal Data**") when providing Cloud Computing Services to Customer. The Cloud Computing Log Personal Data may include such data as:

a. Individual's IP address
b. URLs of sites visited with time stamps (with an associated IP address)
c. Geographic location based upon IP address and location of Akamai server
d. Browser data (type, version, language, OS version)

b) <u>Delivery Services</u>

Akamai processes **Customer Content Personal Data** as defined above when providing Delivery Services to Customer.

Akamai processes Personal Data embedded in server access logs relating to individual's access made to the Akamai servers ("**Traffic Log Personal Data**") when providing Delivery Services to Customer. The Traffic Log Personal Data may include such data as:

a. Individual's IP address
b. URLs of sites visited with time stamps (with an associated IP address)
c. Geographic location based upon IP address and location of Akamai server

d. Browser data (type, version, language, OS version)

For the Service **mPulse** Akamai solely processes Personal Data associated with individual's activity and interaction with web and internet protocol sessions transiting Akamai's servers as part of an individual's 's session with the Customer's Content i.e. **Traffic Log Personal Data** as defined above.
For the Service Global Traffic Management (**GTM**) Akamai processes solely **Traffic Log Personal Data** which includes individual's IP address only.
Customer Content Personal Data is not processed for the Service mPulse and GTM.

c) Security Services

(i) Enterprise Security Services

Akamai processes Personal Data as provided by Customer or collected during the provision of Akamai's Enterprise Security Services in order to protect users of the Customer's enterprise network and the network itself from Internet security and policy abuse risks ("**Enterprise Security Personal Data**"). The Enterprise Security Personal Data includes such data as:

a. Login and user authentication data
b. Contents of communications, including attachments
c. Individual's IP address
d. Browser and device information, including location information, browser type, version, OS version, chosen language, device name, MSIN, device type, other information shared by the device as chosen by the individual)
e. URLs visited

For the Services **Prolexic** and **EdgeDNS** Akamai processes **Enterprise Security Personal Data** which includes individual's IP address only.

(ii) Application Security Services

Akamai processes Personal Data to determine whether access to Customer Content in form of applications or via API is made in a legitimate manner or not and to then apply rules set by Customer to allow or block the access request ("**Application Security Personal Data"**). The Application Security Personal Data includes such data as:

a. Individual's IP address
b. URLs of sites visited with time stamps (with an associated IP address)
c. Geographic location based upon IP address and location of Akamai server
d. Browser data (type, version, language, OS version)
e. For the Service **Account Protector** also login and user authentication data

(iii) API Security Services

Akamai processes Personal Data to determine whether there is any anomalous API traffic behavior. Personal Data processed within API Security Services includes any Personal Data embedded in Customer Content (e.g. IP address, name, email, credit card number, SSN) ("**API Personal Data**").

d) Support Services

Akamai processes **Cloud Computing Log Personal Data** to troubleshoot Cloud Computing Services and **Traffic Log Personal Data** to troubleshoot Delivery Services.
Akamai processes **Enterprise Security Personal Data** to troubleshoot Enterprise Security Services, **Application Security Personal Data** to troubleshoot Application Security Services and **API Personal Data** to troubleshoot API Security Services.

4. Description of Akamai's Personal Data processing activities

The below listed processing activities are performed when providing the following Akamai Services:

a) Cloud Computing Services

For Cloud Computing Services, Customer Content Personal Data is uploaded by Customer and/or individual, stored on Akamai servers, and deleted in accordance with the retention period set by the Customer.
The storage location is chosen by the Customer.
Where the location of data center(s) chosen includes countries that are not recognized to have an adequate data protection level under Data Protection Laws, data transfers may take place (e.g., where the Customer Content Personal Data relates to an EU individual and the storage location chosen is the USA).

Akamai collects and conducts analysis of Cloud Computing Log Personal Data to perform Cloud Computing Services and support for the Customer and to conduct security analytics and reports.

b) Delivery Services

For Delivery Services, Customer Content Personal Data is transmitted via Akamai's server network (without being stored) to ensure Customer Content can be accessed by individuals in a fast reliable and secure manner.
Depending on the location of the individual and the Customer origin server, Customer Content Personal Data may be transferred to a country recognized to have a non-adequate data protection level under Data Protection Laws (e.g., where an EU individual is accessing Customer Content on a Customer origin server located in the USA).

Akamai collects and conducts analysis of Traffic Log Personal Data to perform Delivery Services for the Customer and to provide Customer with copies of traffic logs and data analytic reports.

For mPulse, Traffic Log Personal Data is collected, transferred, analyzed, stored and deleted, to enable Customer to understand the nature of individual's traffic to their Customer Content, as well as to monitor the performance of Customer Content. Akamai offers a service configuration, where, if chosen, the individual's IP address embedded in the mPulse Traffic Log Personal Data is anonymized within in an instance after having been collected at the Akamai server and the data further processed for website performance purposes, does not consist of Personal Data anymore. For this configuration mPulse Traffic Log Personal Data is only collected and anonymized.

c) Security Services

(i) Enterprise Security Services

For Enterprise Security Services, Enterprise Security Personal Data is collected, transferred, analyzed, stored and deleted, to monitor Customer network activity, provide secure access to Customer's enterprise applications, and establish and enforce access policies.

For certain Enterprise Security Services (like Akamai Guardicore Platform) Akamai offers an on-Customer-prem version that does not require any Personal Data processing by Akamai except for Support Services. Where Customer has chosen to use the Services on its own premises, Akamai will not be processing any Personal Data as the processing takes place by Customer in the Customer environment only, unless Customer shares such data with Akamai for support purposes.

(ii) Application Security Services

For Application Security Services, Application Security Personal Data is collected, transferred, analyzed, stored and deleted to protect application and APIs that are part of Customer Content from malicious activities. Where malicious activities are recognized, access to Customer Content is blocked and further analyzed in accordance with Customer's instructions.

(iii) API Security Services

For API Security Services, API Personal Data is collected, transferred, analyzed, stored and deleted to protect APIs that are part of Customer Content from malicious activities. Where anomalous API traffic patterns are recognized, depending on the functionality chosen by the Customer, access to Customer Content is blocked and further analyzed in accordance with Customer's instructions or suspicious API traffic packets are stored after it has passed through the Customer API for Customer's analysis.

For certain API Security services Akamai offers an on-Customer-prem version that does not require any Personal Data processing by Akamai except for Support Services. Where Customer has chosen to use the Services on its own premises, Akamai will not be processing any Personal Data as the processing takes place by Customer in the Customer environment only, unless Customer shares such data with Akamai for support purposes.

For certain API Security services Akamai offers data anonymization of the API Personal Data, so that after the anonymization no Personal Data is processed anymore.

d) **Support Services**

For Support Services, depending on the Akamai services, Cloud Computing Log Personal Data, Traffic Log Personal Data, Enterprise Security Personal Data, Application Security Personal Data and API Personal Data, as applicable, is collected, transferred, analyzed, stored, shared with Customer to resolve incidents and deleted.

5. List of Countries for Akamai Server Deployment

A list of countries in which Akamai operates its servers is available in Akamai's Privacy Trust Center: https://www.akamai.com/legal/compliance/privacy-trust-center.

6. Cookies used for Akamai Services

Customer acknowledges that in connection with the performance of certain Akamai Services Personal Data is collected and processed using cookie technology as outlined in Akamai's Cookie List, available in the Akamai Control Center at https://control.akamai.com/apps/download-center/#/products/14;name=Control-Center.
It is the responsibility of the Customer to ensure its cookie notices, and individuals' consent management tools and practices govern the cookies placed by the Akamai Services in accordance with applicable laws.

Schedule 2 to the Data Processing Agreement
Akamai’s Technical and Organizational Measures

Akamai’s Technical and Organisational Measures to secure Agreement Personal Data processed are publicly available in Akamai’s Privacy Trust Center at: https://www.akamai.com/legal/compliance/privacy-trust-center.