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.

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Agreement Personal Data&quot;</td>
<td>means all Personal Data that Akamai processes on behalf of Customer as a Data Processor as specified in Schedule 1.</td>
</tr>
<tr>
<td>&quot;Authorized Sub-Processor&quot;</td>
<td>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 &quot;mere conduits&quot;), shall not be considered Authorized Sub-Processors.</td>
</tr>
<tr>
<td>&quot;Cross-Border Transfer Mechanism&quot;</td>
<td>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, the EU-U.S. Privacy Shield Framework, Swiss-U.S. Privacy Shield Framework, and the EU standard contractual clauses for Data Processors established in third countries pursuant to European Commission Decision (2010/87/EC) under the EU Directive (95/46/EC), as may be updated or replaced from time to time.</td>
</tr>
<tr>
<td>&quot;Data Protection Laws&quot;</td>
<td>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.</td>
</tr>
<tr>
<td>&quot;Data Controller, Data Exporter, Data Importer, Data Processor, Data Subject, Personal Data, and Personal Data Breach&quot;</td>
<td>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., &quot;Business&quot; instead of &quot;Data Controller&quot; and &quot;Service Provider&quot; instead of &quot;Data Processor&quot; under the California Consumer Privacy Act, or &quot;organization&quot; or &quot;agency&quot; under the Australian Privacy Principles).</td>
</tr>
<tr>
<td>&quot;Supervisory Authority&quot;</td>
<td>means the government agency, department or other competent organization given authority over the processing of Personal Data relevant to this Agreement.</td>
</tr>
</tbody>
</table>
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/us/en/multimedia/documents/akamai/akamai-processors.pdf. 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 the Akamai platform is made up of servers owned and operated by Akamai and/or its Affiliates globally and that Akamai processes Agreement Personal Data not only in the applicable jurisdiction(s) where the Customer operates as a Data Controller, but also transfers Agreement Personal Data outside of such jurisdictions, dependent upon the location of the Customer's end user and the Akamai servers serving those connections. Such cross-border transfers shall take place in accordance with applicable Data Protection Laws, including, without limitation, completing any required prior assessments. A list of all countries in which Akamai operates servers, a list of all Akamai Affiliates that own such servers, as may be updated from time to time, is available at https://www.akamai.com/us/en/multimedia/documents/akamai/points-of-presence-countries.pdf.

2.3.2 To the extent that Agreement Personal Data is subject to a cross-border transfer to a non-EU member country that does not have an EU adequacy determination, at least one of the Cross-Border Transfer Mechanism(s) listed below shall apply in the order of preference listed in the event that more than one mechanism applies:

(a) Binding Corporate Rules -- To the extent Akamai has adopted Binding Corporate Rules, it shall maintain such Binding Corporate Rules and promptly notify Customer in the event that the Binding Corporate Rules are no longer a valid transfer mechanism between the Parties.
(b) EU-U.S. Privacy Shield/Swiss-U.S. Privacy Shield -- Akamai shall remain certified and shall promptly notify Customer if it does not renew or loses the certifications or amends the certifications so that Agreement Personal Data is no longer within the scope of the certification.

(c) EU Standard Contractual Clauses (processors) -- To the extent applicable, the EU standard contractual clauses for Data Processors established in third countries pursuant to European Commission Decision (2010/87/EC) under the EU Directive (95/46/EC), and as may be updated or replaced from time to time, are available at www.akamai.com/compliance/privacy (“Standard Clauses”), are hereby agreed and incorporated herein by Customer (as Data Exporter) and the relevant Akamai Authorized Sub-Processor (as Data Importer, as specified in the Standard Clauses), whereby Appendix 1 shall be deemed to be prepopulated with the relevant sections of Schedule 1 of this Agreement and Appendix 2 shall be deemed to be prepopulated with Schedule 2 of this Agreement. For the avoidance of doubt, the Customer hereby authorizes Akamai to agree on these Standard Clauses on its behalf as Data Exporter with the relevant Akamai Authorized Sub-Processor (as Data Importer).

2.3.3 In addition to the foregoing Section 2.3.2, any similarly applicable standard contractual clauses adopted by a Supervisory Authority or other body of competent jurisdiction to govern the cross-border transfer of Personal Data subject to applicable Data Protection Laws shall be incorporated herein by the parties hereto in accordance with their respective roles pursuant to such clauses as analogous to those set out herein. Such clauses shall be supplemented and/or prepopulated (as applicable) with the relevant sections of this Agreement and its appended Schedules.

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

1. Data Processor

Akamai is a provider of content delivery, media acceleration, web performance and Internet security services.

2. Data Subjects

Akamai processes data on behalf of its Customers that may contain the Personal Data of the end users accessing Customer Content and/or using Customer services when performing Services for the Customer under the Terms & Conditions. “Customer Content” means all content and applications, including any third-party content or applications, provided to Akamai in connection with Customer’s access to or use of the Services.

Categories of data processed

a) End User Personal Data

Akamai processes Personal Data included within Customer Content (“End User Personal Data”) when providing the Services to Customer. Upon the Customer’s choice, End User 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 data subject as set by Customer.

b) Logged Personal Data

Akamai processes Personal Data that is included in log files when performing the Services for Customer (Logged Personal Data”). Logged Personal Data is Personal Data logged by Akamai servers, relating to the access to Customer Content over the Akamai platform by Customer’s end users, as well as logged personal data associated with user activity and interaction with web and internet protocol sessions transiting Akamai’s servers as part of a data subject’s session with the Customer’s web property. Logged Personal Data include such data as:

   a. End user IP addresses;
   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. Telemetry data (e.g., mouse clicks, movement rates, and related browser data).

c) Site Personal Data

Akamai processes Personal Data associated with user activity and interaction with web and internet protocol sessions transiting Akamai’s servers as part of a data subject’s session with the Customer’s web property (“Site Personal Data”). The Site Personal Data consists of user telemetry data (e.g., mouse clicks, movement rates, and user agent and related browser data) designed to measure website performance.

d) Enterprise Security Personal Data
Akamai processes Personal Data on behalf of Customers of Akamai Enterprise Security Services that are provided by Customer or collected during the provision of 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. Browser and device information, including location information
d. URLs visited
e) **Special categories of data**
Customer as the Data Controller decides which categories of data are included in the End User Personal Data. Where Customer chooses to include special categories of data in the Customer Content, Akamai will process this data as End User Personal Data, as instructed by the Customer.

f) **Categories of data processed by particular Akamai Services**
Akamai maintains a list of service categories that provide further information regarding the processing of Personal Data conducted in providing Services in each category. This list is available at www.akamai.com/compliance/privacy/.

3. **Description of Akamai's Personal Data processing activities:**
The following processing activities are performed when providing the Services:

a) **End User Personal Data**
Akamai processes End User Personal Data on behalf of Customers, including instructions given through the Terms & Conditions, or via configuration of the Services via the relevant customer portals or support processes.

b) **Logged Personal Data**
Akamai collects Logged Personal Data and conducts analysis of Logged Personal Data to provide Customer with copies of traffic logs and data analytic reports related to the performance of its Services and the Customer’ web properties.

Logged Personal Data is also be processed for purposes of Service issue resolution.

c) **Site Personal Data**
Akamai processes Site Personal Data to provide website monitoring and analytics services to Customers to enable them to understand the nature of end user traffic to their web properties, as well as to monitor the performance of such properties.

d) **Enterprise Security Personal Data**
Akamai’s Enterprise Security Services provides customers with tools and services to protect their employees and guests, as well as their network infrastructure from Internet threats. In addition, these same tools may be used to monitor network activity, provide secure access to applications, and establish and enforce access policies. To provide these Services, Akamai processes Enterprise Security Personal Data as needed to access and monitor network traffic, process and store access credentials and related network data as part of the network infrastructure services ordered by Customer.
Schedule 2 to the Data Processing Agreement
Akamai’s Technical and Organizational Measures

1. Confidentiality
   a) Entry control:
   The Data Processor monitors its servers and the rooms in which the servers are deployed with perimeter cameras. It requires its co-location facility partners to restrict physical access to its servers to persons that have been authorized in advance to access the servers, inter alia by picture identification. Such persons are checked in and escorted to the servers by the personnel of the Data Processor’s co-location facility partner. The Data Processor also requires its co-location facility partners to enforce verification of the requester prior to answer any service request. The co-location facility partner may not attempt to gain any sort of access to the Data Processor’s data systems without written instructions from the Data Processor. Physical access to the servers by field technicians for purposes of first instalment or maintenance is limited to the technical functions of the servers. Field technicians do not have control over the ability of such servers to process the customer’s (“Data Controller’s”) content.

   b) Access control:
   The Data Processor limits the access to its data systems according to its business requirements and the least privilege principle. For example, field technicians are not granted administrative access to servers processing Data Controller’s content. Field technicians performing system diagnostics and analysis are provided with read-only logins. Administrative access is restricted to trained and authorized employees of the Data Processor. Field technicians are not granted administrative access to the servers processing the Data Controller’s content. Remote administrative access is only available via cryptographically secure connections, systems authenticate administrative connections using asymmetric key cryptography. User administrative access is provided through an access control gateway, which enforces a need-have access grant authorization model. All connections through the authorization gateway are logged. User SSH system are routinely rotated and access is immediately removed in case of reports of theft of devices or the termination of a person’s employment.

   A system of grants is used to track and permit access to all data processing systems of the Data Processor.

   Access to the Data Processor’s systems used to process the Data Controller’s content is gained via the Data Processor’s authorization gateway. Access to the authorization gateway itself requires possession of a grant authorized by one or more second parties, as well as a deployed SSH key. Issuance of a deployed SSH key requires access to the corporate network environment using a device with a corporate PKI issued Network Access Control (NAC) certificate, valid corporate authentication credentials for the Data Processor’s corporate web services, and either confirmation of possession of a usable, unexpired prior key or the confirmation by the Data Processor’s Network Operations Command Center (NOCC) of the user’s identity.

   Access to the Data Processor’s corporate network requires using a device with a corporate PKI issued NAC certificate. Access to data processing systems within the corporate network requires the NAC certificate as well as user authentication via either the Duo Security, Inc. Trusted Access System or the corporate active directory username and password management system.

   In case of password authentication, the complexity of the password is ensured by the Data Processor’s password policy (e.g. multiple character types, length of min. 8 characters, change requirements after 120 days, inability to reuse a password within the following 12 month).

   The Data Processor does not provide user accounts to servers transmitting content. Administrative access to such servers is limited to a number of authorized employees of the Data Processor. Access to these servers by authorized employees on a user level is logged by an authentication gateway. Remote access via the authentication gateway utilizes SSH keys and asymmetric cryptography. Introduction of a new SSH key requires either direct confirmation of identity with the Data Processor’s NOCC or possession of the prior SSH key, the prior SSH key password, a machine’s NAC for the Data Processor’s corporate network and a corporate Active Directory username and password.
c) Segregation control:
The Data Processor separates the environment for development, software, engineering, from the environment for testing and the environment for operations and has put in place several controls to ensure the code development, testing and production data handling environments are separated. E.g. employees within the development team do not have access to the same systems as the employees within the test or operation team. Separate cryptographic credentials are used to access development, test, operations and production environments, critical network operations systems are further isolated from the corporate, development and test network environments. The separation is supervised by granular logging of access to the production and operations servers, change control processes and by the responsible management.

2. Pseudonymization
In most cases Data Processor does not pseudonymize the personal data it processes. For End User Personal Data this would require modifications of the End User Personal Data which would mean a violation of the integrity of the End User Personal Data.

For Logged Personal Data this data is required in raw and clean for the purpose of the processing activities. E.g. Data Processor could not deliver the End User Personal Data in case the IP addresses in the log files would not be clear to determine the best way to route the traffic via the Akamai Platform. Neither could security analytics be performed in case the IP addresses would be encrypted.

3. Integrity
   a) Transmission control
The Data Processor has put in place a robust alert management system that provides for extensive monitoring of all servers. Fine grained monitoring of running processes allows the definition of predefined alerts to catch unexpected and suspicious behavior, including the execution of rogue processes.

In addition, the Data Controller can control access to the personal data in its content while having the Data Processor transmitting traffic to its server over encrypted and authenticated connections by its configuration of the services in the Data Processor’s Akamai Control Center. The Data Controller can control storage of personal data in its content by configuring property specific content caching rules. By it configuration the Data Controller can also limit the storage of personal data in its content to servers with enhanced physical security controls only. The integrity of the log data is ensured by various storage controls (e.g., log retention control) that are subject to several regular third-party assessments.

   b) Input control
Access to the Data Processor’s server is logged and monitored via audit systems and processes. Log data gathered by web-servers is digitally signed by “Edge Servers” and is audited by the distributed data processing facilities, to ensure that it is not modified or corrupted. Respective access logs consisting of aggregated and anonymized log data are provided to the Data Controller as part of the Data Processor’s “Log Delivery Service” offering.

4. Availability and resilience
The Data Processor’s web server networks have been created matching the principles of availability. The server network is self-curing and ensures that the content of the Data Controller is transmitted via the server network, even in case of an outage of single servers. This prevents an outage of the services which would require a fast recovery of the services.

5. Evaluation of effectiveness
The Data Processor has data protection management and incident response management policies and procedures in place, which are evaluated in the course of annual third-party audits, including Data Processor’s annual SOC 2 Type 2 and other assessments and certifications. Further the Data Processor ensures by its privacy by design processes that personal data is protected in all processing activities and that relevant data protection principles are applied. In addition, the Data Processor is offering, where
reasonably possible tools for the de-identification of personal data to assist in complying with the data minimization principle.

6. **Role Control**  
The Parties ensure that personal data is processed by the Data Processor only in accordance with the instructions of the Data Controller by agreeing on the data processing agreement. In addition, the Data Processor's robust alert system ensures that it transmits the Data Controller's web content only in accordance with the instructions of the Data Controller (which he has provided by way of its configuration how to process the content within the Data Processor's Akamai Control Center).