Overview of Akamai's Personal Data Processing Activities and Roles in connection with Services Provisioning

Last Updated: November 19, 2024

This document is maintained by the Akamai Global Data Protection Office

Table of Contents

Introduction

Akamai Technologies, Inc. and its operated global affiliates ("Akamai") is a provider of cloud computing, delivery and security services designed to make the Internet fast, reliable and secure for its customers. Akamai operates over 350,000 servers, in over 1,600 networks within more than 130 countries (the "Akamai Connected Cloud"). Akamai follows a data protection and privacy framework designed to comply with data protection obligations around the globe and takes its obligations under applicable data protection laws very seriously.

This document provides an overview of Akamai's personal data processing activities associated with the Services it provides to customers.

Some Useful Terms

"**Akamai Services**", "**Services"** means services or products as described in the Akamai services page which may be ordered by the Customer.

"Customer" means an entity purchasing Akamai Services directly or indirectly via an Akamai partner.

"**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 or individual's access to or use of the Akamai Services.

"**Data Protection Laws**" means all applicable laws (including decisions and guidance by relevant supervisory authorities) relating to data protection, the processing of personal data or personal information, and privacy applicable to Akamai and the Customer with respect to the processing of Personal Data to provide the Akamai Services, including such laws, by way of example and without limitation, the General Data Protection Regulation ("GDPR"), the California Consumer Privacy Act ("CCPA"), the Brazilian General Data Protection Law ("LGPD") and the Personal Information Protection and Electronic Documents Act ("PIPEDA").

"**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data**", "**Processing**" 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 CCPA, or "organization" or "agency" under the Australian Privacy Principles, "Data Operator" instead of "Data Processor" under LGPD).

"**Session**" or "**Web Session**" means a single visit by an individual or automated client to particular Customer Content or other location on the Internet.

"**Web Property**" means a point of presence (e.g., a website, social media site or account, blog, etc.) on the Internet that is an asset of an entity (e.g., an individual or corporation) used for the purpose of representing a brand, person or other identity.

Personal Data Processing related to Akamai Services Provisioning at a glance

Figure 1: Akamai's Role depending on services and data category.

Akamai Services	Data Subject	Category of Personal Data	Akamai's Role
All Services	Customer/ prospective Customer or their representative	Contact Information Account Data *(in case of Cloud Computing Service only)* Telephone Chat Data	Controller
All Services	Partner/ prospective partner or their representative	Contact Information Account Data *(in case of Cloud Computing Service only)* Telephone Chat Data	Controller
Cloud Computing Services	Individuals accessing Customer Content or whose personal data is embedded in the Customer Content	Customer Content Personal Data Cloud Computing Log Personal Data Service Logs	Processor Processor Controller
Delivery Services	Individuals accessing Customer Content or whose personal data is embedded in the Customer Content	Customer Content Personal Data Traffic Log Personal Data Service Logs	Processor Processor Controller
Security Services (Enterprise, Application and API Security Services)	Individuals accessing Customer Content or whose personal data is embedded in the Customer Content, or accessing Customer's corporate systems	Enterprise Security Personal Data Application Security Personal Data API Personal Data Service Logs	Processor Processor Processor Controller
Support Services	Individuals accessing Customer Content or whose personal data is embedded in the Customer Content, or accessing Customer's corporate systems	Cloud Computing Log Personal Data Traffic Log Personal Data Enterprise Security Personal Data Application Security Personal Data API Personal Data	Processor

General Principles in Data Processing

Akamai processes Personal Data in compliance with the principles set forth in the applicable Data Protection Laws. Akamai processes only the Personal Data necessary and proportionate to meet the purposes outlined herein and does so in a fair and lawful manner taking into consideration not only our obligations to our Customers but the potential impacts and risks to individual Data Subjects posed by our data processing activities. Akamai takes steps to mitigate such impacts and risks and to secure the data in our possession. Except for Contact Information, Account Data and Telephone Chat Data, the processing of Personal Data conducted by Akamai is not used by Akamai to identify any individuals, but rather to identify events and activities between computers and agents (e.g., browsers) on the Internet, such as determining whether an action on a website is being performed by a human or a bot.

Categories of Personal Data

In providing the various Services to its Customers, Akamai processes the following categories of data:

1) With respect to Customers and partners and their representatives purchasing Akamai Services:

   (i) **Contact Information**: Personal Data of Customer's or partner's employees and representatives collected and maintained by Akamai to support the customer relationship ("Contact Information"). Contact Information may include, by way of example only, such data as:

   a. Contact names
   b. Title
   c. Business addresses
   d. Email addresses
   e. Telephone numbers
   f. Akamai's customer portals or API credentials

   (ii) **Account Data** (in case of Cloud Computing Services): This data includes Contact Information (as defined above) and any other data provided by the Customer or partner or their representatives during account creation, financial information, and payment information e.g., credit card numbers.

   (iii) **Telephone Chat Data**: This data includes content of the conversation and Contact Information (as defined above) provided by the Customer or partner or their representatives during the chat with Akamai representatives.

2) With respect to individuals accessing Customer Content or whose personal data is embedded in the Customer Content in connection with **Cloud Computing Services**:

(i) **Customer Content Personal Data**: 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.

(ii) **Cloud Computing Log Personal Data:** 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)

3) With respect to individuals accessing Customer Content or whose personal data is embedded in the Customer Content in connection with **Delivery Services**:

(i) **Customer Content Personal Data**: Akamai processes Personal Data included within Customer Content ("Customer Content Personal Data" as defined above) when providing Delivery Services to its Customers.

(ii) **Traffic Log Personal Data:** 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 on the 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 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.

4) With respect to individuals accessing Customer Content or whose personal data is embedded in the Customer Content, or accessing Customer's corporate systems in connection with **Security Services** covering **Enterprise Security Services**, **Application Security Services** and **API Security Services**:

(i) **Enterprise Security Personal Data:** 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 Personal Data**: 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 Personal Data**: 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").

5) With respect to individuals accessing Customer Content or whose personal data is embedded in the Customer Content, or accessing Customer's corporate systems, when performing the **Support Services** in connection with **Cloud Computing**, **Delivery** and **Security 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.

6) With respect to individuals accessing Customer Content or whose personal data is embedded in the Customer Content, or accessing Customer's corporate systems when performing the **Cloud Computing, Delivery** or **Security Services:**

Service Logs: 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 above).

Akamai's Policy Towards IP Addresses

Akamai treats IP addresses generally as Personal Data under the Data Protection Laws because, when processed for the purpose of identification of an individual, IP addresses can be combined with other data and used to identify an individual that was assigned that particular IP address during one or more Sessions.

In a large number of cases the IP addresses processed by Akamai will not be assigned to any individual, but rather will identify only the latest server from which a given IP data packet was sent. Only if the processing party can demonstrate that a given IP address is not associated with an individual (such as IP addresses associated with a corporate firewall), however, should such IP addresses be treated as non-personal data.

In many cases, the primary piece of Personal Data that Akamai processes and collects will be the IP address associated with a given web or IP Session. Indeed, many data elements identified by Akamai as Personal Data, such as Universal Resource Locators or URLs (e.g., http://www.akamai.com), are only Personal Data when combined with an associated individual's IP address. Akamai systems are not designed, however, to differentiate between an IP address that may be an individual's IP address and one that is not (i.e., an IP address of a server or router in the delivery chain of the session) and, therefore, as a matter of internal policy, all IP addresses at Akamai are treated as Personal Data.

The above policy notwithstanding, it is important to note that while Akamai collects and processes IP addresses as described above, it does not do so in a manner that gives Akamai the ability to identify any given individual associated with a web transaction. As an essential part of making sure individuals can securely access the websites and applications pages and content they request, Akamai must handle certain data, including individual's IP addresses, but Akamai does not identify the individual using an IP address when doing so. Rather, Akamai's processing of IP addresses is conducted to provide the contracted services and identify events and activities between computers and agents (such as browsers) on the Internet (e.g., determining whether an action on a website is being performed by a human or a bot) or other identify patterns that may indicate malicious or fraudulent activity.

Description of Processing Activities

Contact Information

Akamai collects and processes Contact Information to provide access to and use of tools to support the Services, communications with customers, and to manage customer relations. This data is stored by Akamai in its portal(s) (such as Akamai Control Center), customer community and developer sites, and in internal business process tools.

Retention period: Data will be retained as long as required for the customer relationship.

Account Data

Akamai uses Account Data for account creation, business relationship and account management, to handle service requests, orders, and process payments.

Retention period: Data will be retained as long as required for the business operation, security and compliance purposes.

Telephone Chat Data

Akamai processes Telephone Chat Data to provide Customers with technical support and assist with other queries as requested. In some cases, we may use the telephone chat recording for staff training and quality assurance purposes and in certain cases to retain evidence of a particular transaction or interaction.

Retention period: Data will be retained until the purpose of the processing is met.

Customer Content Personal Data

Cloud Computing Services

Akamai operates as hosting provider for Customer Content Personal Data which is uploaded by the Customer and/or individual and stored on Akamai servers within Akamai Connected Cloud. The Customer and/or individual determines what Customer Content Personal Data is stored on Akamai servers, including the storage location.

Retention period: Data is deleted in accordance with the retention period set by the Customer.

Delivery Services

Akamai operates largely as a conduit for Customer Content Personal Data transmitted by its Customers via the Akamai Connected Cloud. The Customer determines: what Customer Content Personal Data is processed by its Web Property, whether to use secure services offered by Akamai for encrypted delivery of Customer Content and whether or not any Customer Content is cached by Akamai's servers. Akamai determines how to optimally route and secure such Customer Content Personal Data via the Akamai Connected Cloud based upon numerous factors including customer configurations, applied security rules, Internet congestion, and best available routes.

As described above, Customer determines through design and configuration of its Web Properties and Customer Content and instructions entered via Akamai's service portals (e.g., Akamai Control Center), what Customer Content Personal Data will flow across the Akamai Connected Cloud. The Customer, therefore, will be responsible for compliance with applicable laws for such processing (e.g., appropriate end user notices or a legal basis for processing Customer Content Personal Data, and having chosen services appropriate for the type of Customer Content Personal Data transiting Akamai's servers (e.g., PCI compliant services and encryption settings)).

Absent Customer instructions, Akamai does not process Customer Content Personal Data other than as required to provide the Delivery Services purchased by the Customer.

Retention period: Akamai recommends configuring the services to have Customer Content Personal Data transmit the Akamai edge servers and to not store/cache such data. Such data will be stored/cached only if instructed so by Akamai's Customer and retained in accordance with the Customer's instructions.

Cloud Computing Log Personal Data

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.

Retention period: Data will be retained in accordance with Akamai data retention policies as long as necessary for security purposes.

Traffic Log Personal Data

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.

Retention period: Data will be retained on Akamai's backend systems for 14 days.

For mPulse, Akamai processes Traffic Log Personal Data to provide website monitoring and analytics services to Customers to enable them to understand the nature of traffic to their Customer Content, as well as to monitor the performance of such properties. Akamai offers a service configuration for mPulse, where, if chosen, the individual's IP address embedded in the 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 Traffic Log Personal Data is only collected and anonymized.

Retention period for mPulse: Data will be retained on the local edge server in accordance with the load of the edge server, usually a couple of hours. If the IP anonymization option was not chosen by the Customer the data will be retained for 18 months or is deleted earlier upon Customer's request.

Enterprise Security Personal Data

Akamai's Enterprise Security Services provide 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 network resources, and establish and enforce access policies. To provide these Services, Akamai processes Enterprise Security Personal Data as needed to control

access and monitor network traffic, processes and may store access credentials and related network data.

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.

Retention period: Subject to the below, data will be retained for 90 days except for data necessary for operation of the Services, which will be retained only as long as needed for the service relationship.

In case of Secure Internet Access Mobile services data is retained for 6 months.

In case of Guardicore Platform data is kept for audit reasons and deleted upon data controller's request.

Application Security Personal Data

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.

Retention period: Data will be retained for 90 days except for data necessary for operation of the Services, which will be retained only as long as needed for the service relationship.

API Personal Data

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.

Retention period: Depending on the API Security services, data will be retained for 90 days or for the contract duration or deleted upon Customer request.

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, are processed in connection with Support Services. The above data is collected, transferred, analyzed, stored, shared with Customer to resolve incidents and deleted.

Retention period: Subject to the below, data will be deleted after 120 days after ticket closure.

In case of Guardicore Platform (except for security incidents) data is removed automatically after 60 days unless longer retention period was requested by the data controller. In case of security incidents data is kept for audit reasons and deleted upon data controller's request.

In case of Cloud Computing and certain API Security services data is kept for audit reasons and deleted upon data controller's request.

Service Logs

The Service Logs are created locally on an Akamai server or in the cloud computing environment, collected from the individual's interaction with the Customer Content or access of Customer's corporate systems.

Akamai conducts analysis of traffic traversing its network both from system logs and data collected from the Web Session or an individual's browser, which sometimes includes Personal Data, in order to deliver and improve its Services, and provide Customers with data analytics products related to performance of the Services and the Customer Content, as well as provide fraud and bot management capabilities. Akamai also conducts traffic analysis to derive and compile information relating to the type, nature, content, identity, behavior, signature, source, frequency, reputation and other characteristics of malicious Internet traffic and activity. The resulting threat data is integrated into Akamai's tools, products (including data products that contain a subset of the threat data, which are sold to the Akamai's customers as part of its security service offerings), and services to protect itself and its customers from cyber-attacks, hacking, malware, viruses, fraud, exploits and other malicious activity.

Service Logs may also be processed for purposes of billing, service issue resolution, service improvement (e.g., mapping decisions), future capacity planning and aggregate reporting (aggregate reports do not identify any Customer or the data subjects visiting their Web Properties) such as Akamai's "State of the Internet" report.

Retention period: Data will be retained for up to 90 days in most of the cases. Where specific security events require updates of the existing algorithm, such data is retained for up to 180 days. For traffic analytics and for forensic aggregated data will be retained for up to 3 years.

Akamai Operates Both as a Data Controller and a Data Processor

In reviewing any processing of Personal Data under Data Protection Laws and similar laws, it is critical to understand the relative processing roles and which role each player assumes. In any given data processing scenario between multiple parties, parties may each be Data Processors or Data Controllers or both in their own rights. In order to understand the differing obligations of the parties and particularly to recognize when the more strict obligations of the Data Controller must be applied, we must properly designate these roles based upon the factual analysis of the various data processing activities.[1]

Traditionally, parties to a commercial agreement have simply designated any service provider as a Data Processor, the ordering entity as the Data Controller and taken the analysis no further. According to the EU Advocate General, however, "[a]ny interpretation that is based solely on the terms and conditions of the contract concluded by the [parties should] be rejected."[2] The division of tasks in a contract can only suggest the actual roles of the parties, for "[i]f it were otherwise, the parties would be able artificially to assign responsibility for the data processing to one or other of themselves."[3] Ever more frequently data processing is complex, comprising many distinct processes which involve numerous parties with differing degrees of control. Thus the traditional role is no longer automatically valid.

A Data Controller "alone or jointly with others, determines the **purposes** and **means** of the processing of personal data." This role is in contrast to the Data Processor role where the person or entity merely "processes personal data **on behalf of** the controller", subject to the authorization and explicit instruction of the Data Controller.

Akamai's activities as described above make it:

(i) **Data Processor** with respect to Customer Content Personal Data, Cloud Computing Log Personal Data, Traffic Log Personal Data, Enterprise Security Personal Data, Application Security Personal Data and API Personal Data processed in the course of performing the Services.

> Akamai does not collect these data elements for its own purposes but processes these data elements as a "Data Processor" or in any other equivalent role or corresponding terms applied by applicable Data Protection Laws (i.e., on behalf of our Customers, subject to their instruction) providing the Customer with storage capacity, assisting the Customer by making the Customer Content available to the Customer's website visitors in a fast, reliable and secure manner or securing Customer's corporate systems.

[1] "The concept of controller is a functional concept, it is therefore based on a factual rather than a formal analysis'. See the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 21.
[2] Opinion of Advocate General BOT delivered 24 October 2017, Case C-210/16, p. 60.
[3] *Id.*

For the Customer Content Personal Data Akamai's Customer determines the data elements processed. In case of Cloud Computing Services, the Customer determines the data elements to be stored and the storage location as well as the security settings. In case of Delivery Services, Customer determines the Service configuration (e.g., the data elements to be cached and the time to cache, the data elements not to be cached) made available by Akamai via its service portal(s) and finally it makes choices regarding security and encryption options offered by Akamai. By controlling the Service configuration, the Customer is providing the data processing instructions to Akamai[4].

In the above scenarios, Akamai has no control over or visibility into the specific data elements of the Customer Content Personal Data that is stored on or transit its servers. Such control and visibility is maintained by the Customer. Akamai's role is restricted to offer the above listed configuration choices as non-essential means to best accommodate the Customer's interest to process the Customer Content Personal Data[5]. In addition, with respect to Delivery Services Akamai operates largely as a conduit for Customer Content Personal Data collected, processed, and transmitted by its Customers via Akamai services. The Customer determines what Customer Content Personal Data is collected or otherwise used and how it will be processed by Akamai.

For the Cloud Computing Log Personal Data, Traffic Log Personal Data, Enterprise Security Personal Data, Application Security Personal Data or API Personal Data, Akamai is determining the technical aspects of the processing, however in the course of performing the Services the Customer remains responsible for determination of the processing purposes and provides processing instructions via its service configuration in Akamai customer portal (like e.g., defining security rules).

The Customer, therefore, is responsible for compliance with applicable laws for such processing (e.g., appropriate end-user notices or consents and having chosen services appropriate for the type of Customer Content Personal Data transiting Akamai's servers).

In connection with Support Services Cloud Computing Log Personal Data, Traffic Log Personal Data, Enterprise Security Personal Data, Application Security Personal Data or API Personal Data, as applicable, are collected, stored and analyzed by Akamai to resolve any service incidents if requested by the Customer via support ticket. Customer initiates and determines the purpose of the processing.

Akamai and Customer agree on a data processing and/or data transfer agreement to contractually ensure that Customer is responsible for the data processing activities, while Akamai follows the instructions provided by the Customer and has in place appropriate technical and organisational measures to secure the data processed by Akamai. In addition, Akamai assists the Customer to understand the data flows and

[4] See the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 40.

[5] "When one entity clearly determines purposes and means, entrusting another entity with processing activities that amount to the execution of its detailed instructions, the situation is straightforward, and there is no doubt that the second entity should be regarded as a processor, whereas the first entity is the controller." see the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 28.

privacy risks related to the Akamai Services via workshops and documentation. This enables the Customer as Data Controller to assess the risks and actively approve the way the processing is carried out [6].

In case of questions about Akamai's processing of Personal Data as Data Processor and execution of related data subject access rights, data subjects should contact Akamai Customers directly.

(ii) **Data Controller** with respect to Service Logs as well as Contact Information, Account Data and Telephone Chat Data.

Akamai processes Service Logs outside of the direct performance of the Services for purposes of traffic analytics, monitoring and management of the Akamai systems, security analytics, service development, billing and internal reporting. Contact Information, Account Data and Telephone Chat Data is processed by Akamai to manage the customer relationship.

Such purposes are determined by Akamai, as well as the data elements collected, categories of data subjects, processing systems and location, retention periods and security measures in place. The Customers do not participate in such determinations, they are not at all involved in these data processing activities and there are no instructions from the Customer regarding this personal data processing. The Service Logs, Contact Information, Account Data and Telephone Chat Data are collected independently by Akamai and it is solely Akamai determining the why, what and how of these processing activities[7].

As outlined above, Akamai complies with data protection requirements applicable to a Data Controller when processing such data, e.g., the privacy principles, security and notification obligations.

In case of questions about Akamai's processing of Personal Data as Data Controller and execution of related data subject access rights, data subjects shall contact Akamai directly as set forth in the Akamai Privacy Statement.

Sub-processors

While Akamai remains responsible for the processing of Personal Data as outlined herein, for certain Services we may use sub-processors within the Akamai group as well as third party sub-processors. For details on sub-processors used by Akamai please refer to Akamai's sub-processor list.

[6] See the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 30 and 41.
[7] See the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0, adopted on 07 July 2021, number 35.

International Transfers of Personal Data

Cloud Computing Services

The Customer Content Personal Data within Cloud Computing Services will be stored within Akamai Connected Cloud on the Akamai server chosen by the Customer and/or individual. The data transfer may take place depending on the Customer's and/or individual's location and chosen storage location.
For Cloud Computing Log Personal Data, the described processing activities require data transfers to the USA, as the backend systems the data is processed on, are deployed in the USA.

Delivery Services

For Customer Content Personal Data within Delivery Services, data transfer occurs only where the transmission of Customer Content between the individual, the Akamai servers and the customer origin server requires transfer of the Customer Content outside the individual's location.
The Akamai Connected Cloud is designed in a manner that routes traffic through the best available routes regardless of geographic boundaries. The way the Akamai Connected Cloud operates is that the Customer Content will always be delivered by the optimal Akamai server (which will usually be the server that is physically closest to the individual). This means that when Customer Content is accessed by e.g. an individual located in the European Economic Area ("EEA"), in general the Customer Content and the embedded Customer Content Personal Data will be transmitted via Akamai servers deployed in the EEA and there is no transfer of the Customer Content Personal Data to servers deployed outside the EEA, however, in some cases (e.g. internet congestion or BGP routing issues) traffic delivery may occur from servers located outside of the EEA, even if the individual requesting such data is located inside the EEA.

For Traffic Log Personal Data, the described processing activities require data transfers to the USA, as the backend systems the data is processed on, are deployed in the USA. In case of certain Traffic Log Personal Data, if the default configuration is not changed by the Customer, Traffic Log Personal Data of individuals located in the EU and UK is automatically localized and stored in the EU, however in case of Support Services remote access to or transfer of Traffic Log Personal Data will be required.

Security Services

For Enterprise Security Personal Data, Application Security Personal Data and API Personal Data, the described processing activities require data transfers to the USA, as the Akamai's security analytic systems the data is analyzed and processed on, are deployed in the USA.

In case of some Security Services (e.g., Guardicore Platform, AAP or API Security) Customer may decide to localize respective Personal Data in the EU processing location via its service configuration however in case of Support Services remote access to or transfer of Personal Data will be required.

Support Services

To ensure 24/7 availability of the Services, Cloud Computing Log Personal Data, Traffic Log Personal Data, Enterprise Security Personal Data, Application Security Personal Data or API Personal Data, as applicable, are for purposes of service issue resolution and system monitoring and maintenance, remotely accessed and processed by Akamai's support teams in the EU, EMEA, Americas, LATAM and APJ as listed in Akamai sub-processor list. Usually the regional teams (EU, EMEA, Americas, LATAM or APJ) are involved in the support services for the respective Customer.

In addition, Akamai support ticket systems are located in the USA therefore data will be also transferred to and processed in the USA.

For any international transfer within the Akamai group or to third party service providers, Akamai shall ensure that such recipients maintain appropriate contractual, technical and organisational safeguards and shall have in place required data protection terms to ensure protection of Personal Data to the same degree as required by Akamai and applicable Data Protection Laws (e.g., adequacy decision or Standard Contractual Clauses).

For details on international transfer and applicable safeguards please refer to the "Data Transfers by Akamai" section in the Akamai Privacy Trust Center and to Akamai's sub - processor list.

Additional information

Additional information regarding the data processed by Akamai as a Data Controller is published in the Akamai Privacy Statement to notify interested parties in a fair and transparent manner.

The data processing and data transfer agreement offered by Akamai to its Customers and Akamai's technical and organizational measures to secure the personal data processed as a Data Processor, are published in the Akamai Privacy Trust Center under the respective sections.