Overview of Akamai's Personal Data Processing Activities and Role

Last Updated: April 2018

This document is maintained by the Akamai Global Data Protection Office

Introduction

Akamai is a global leader in content delivery and cloud security services designed to make the Internet fast, reliable and secure for its customers. Akamai operates a server platform consisting of over 240,000 servers, in over 1,600 networks within more than 130 countries. Akamai follows a data protection and privacy framework designed to comply with data protection obligations around the globe and takes its obligations under the EU General Data Protection Regulation ("GDPR") and similar 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 Network Data**", as defined in Akamai's Terms and Conditions, means all models, reports, analyses, statistics, databases and other information created, compiled, analyzed, generated or derived by Akamai in connection with delivery of services and the operation of Akamai's network, regardless of the media in which such Akamai Network Data is embodied.

"**Customer Content**", as defined in Akamai's Terms and Conditions, means content and applications, including any third party content or applications, provided to Akamai for delivery via the Akamai network.

"**Data Controller**" means an entity which, alone or with others, determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that processes Personal Data on behalf of and subject to instructions from the Data Controller.

"**Data Subject**" means the natural person to whom the Personal Data relates.

"End User" means the natural person that visits a customer's web property or otherwise uses a customer's services on the Internet.

"**General Data Protection Regulation**" or "**GDPR**" means General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Session**" or "**Web Session**" means a single visit by an individual or automated client to a particular website 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.

Categories of Personal Data

In providing the various services to its customers, Akamai Processes the following categories of data:

(i) **Personal Data in Customer Content**: Personal Data about visitors to web properties included within Customer Content that is; cached or stored on Akamai's servers for purposes of optimization and transport, is provided by a customer for storage on Akamai servers for delivery to its end users, or that otherwise transits the Akamai servers as part of an end user's session with the customer's web property ("End User Personal Data"). End User Personal Data may include,

a. Login credentials

b. Subscriber name and contact information

c. Financial or other transaction information

d. Other information relating to the individual data subject as requested or provided by the customer through the use of its web property.

(ii) **Personal Data in Akamai Logged Data:** Akamai Network Data, logged by Akamai servers, relating to the delivery of information over the Akamai platform, 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"). Logged Personal Data may include,

a. End user IP addresses

b. Page activity data and URLs of sites visited with time stamps (when combined with an associated IP address)

c. Geographic location based upon IP address and location of Akamai server (no more granular than city level)

d. Telemetry data (e.g. mouse clicks, movement rates, and user agent and related browser data)

Akamai Network Data means all models, reports, analyses, statistics, databases and other information created, compiled, analyzed, generated or derived by Akamai in connection with delivery of services and the operation of Akamai's network, regardless of the media in which such Akamai Network Data is embodied.

(iv) **Personal Data in Customer Contact Information**: Personal data of customer employees and representatives collected and maintained by Akamai to support the customer relationship ("Customer Personal Data"). Customer Personal Data may include, by way of example only,

a. contact names

b. title

c. business addresses

d. email addresses

e. telephone numbers

f. Luna Control Center customer portal or API credentials

Akamai's Policy Towards IP Addresses

IP addresses generally are treated as personal data under the GDPR and other data protection laws because some 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 vast 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, however, that a given IP address is not associated with an individual (such as IP addresses associated with a corporate firewall) should that party treat the IP address 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 transaction. 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 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 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. Rather, processing 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 by Category

Personal Data in Customer Content: End User Personal Data

Akamai operates largely as a conduit for End User Personal Data collected, processed and transmitted by its customers via the Akamai services. The customer determines; what End User Personal Data is collected or otherwise used by its Web Property, whether

and for how long such End User Personal Data should be cached by Akamai's servers, whether to use secure services offered by Akamai for encrypted delivery of its web traffic, and whether and for how long End user Personal Data is stored on Akamai's NetStorage servers. Akamai determines how such End User Personal Data is transmitted by determining optimal routes and caching, and other necessary service parameters based upon numerous factors including customer configurations, Internet congestion, and best available routes.

As described above customer determines through design and configuration of its Web Property and instructions entered via Akamai's service portals (e.g. Luna), what End User Personal Data will flow across Akamai's servers. The customer, therefore, will be 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 End User Personal Data transiting Akamai's servers (e.g. PCI compliant services)).

Absent customer request, Akamai does not store or otherwise process End User Personal Data other than as required to provide the services purchased by the customer.

Personal Data in Akamai Logged Data: Logged Personal Data

Akamai conducts analysis of traffic traversing its network both from system logs and data collected from the web site session or an end user's browser, which sometimes includes Logged 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's web property, 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.

Log Personal Data may also be processed for purposes of billing, service issue resolution and service improvement (e.g. mapping decisions), service troubleshooting, and aggregate reporting (i.e. the report does not identify any customer or the data subjects visiting their web properties) such as Akamai's "State of the Internet" report.

Personal Data in Customer Contact Information: Customer Personal Data

Akamai collects and processes Customer Personal Data to provide access to and use of services, communications with customers, and to manage customer relations. This data is stored by Akamai in its portal(s) (such as Luna), customer community and developer sites, and in internal business process tools.

General Principles in Data Processing

Akamai processes Personal Data in compliance with the principles set forth in the GDPR and similar laws and regulations around the world. Akamai processes only the personal data necessary and proportionate to meet the purposes outlined above, 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. As discussed above, 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 (such as browsers) on the Internet, such as determining whether an action on a website is being performed by a human or a Bot.

Transfers Outside of the EU

Akamai operates a global platform architected in a manner that routes traffic through the best available routes regardless of geographic boundaries and, therefore, in some cases traffic delivery will occur from servers located outside of the EU, even if the end user requesting such data is located inside the EU. In addition, certain servers Akamai operates are located in the USA only and, therefore, data will be transferred to and processed in the USA. To ensure that the transfer of personal data to the USA complies with applicable data protection laws, including the GDPR, it has certified under the EU and Swiss Privacy Shield programs and agrees to EU Standard Contractual Clauses with its customers.

To ensure round the clock availability, Logged Personal Data may, for purposes of service issue resolution and system monitoring and maintenance, be processed by Akamai's support teams in the EU, the USA and India. To cover these transfers, members within the Akamai group of companies have entered into EU Standard Contractual Clauses.

Once the GDPR has entered into force, Akamai intends to implement Binding Corporate Rules in addition to the existing safeguards.

Akamai's Role Operates Both as a Data Controller and a Data Processor Under the GDPR

In reviewing any processing of Personal Data under the GDPR 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 an agreement have simply designated any service provider as a Data Processor 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.

Akamai has worked with outside counsel to guide the company's GDPR compliance program. As part of its efforts to scope and document its data processing activities in a manner compliant with GDPR requirements, counsel has confirmed that, under the GDPR and similar laws, Akamai's activities as described above make it a data processor with respect to End User Personal Data and Customer Personal Data and a data controller with respect to Logged Personal Data.

---

[1] "the concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and [it is] thus based on a factual rather than a formal analysis'. Opinion 1/2010 of the Article 29 working party of 16 February 2010 on the concept of 'controller' and 'processor', 'Opinion 1/2010', p. 10.

[2] Opinion of Advocate General BOT delivered 24 October 2017, Case C-210/16, p. 60

[3] *Id.*

Under the GDPR, 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.

With respect to End User Personal Data, Akamai's customer determines what such data is processed by its Web Property or services. Customers then purchase services, set certain configuration options (e.g. what data on a web site should be cacheable on Akamai servers) made available by Akamai via Akamai's service portal(s), make choices regarding security and encryption, and control many other settings and options in order for Akamai to provide services to accelerate and secure their web properties and provide analytics and related services.

In the above scenario, Akamai has no control or visibility into the specific Personal Data that may flow across its servers. Absent Customer instruction, Akamai does not store or otherwise process End User Personal Data other than as required to provide the services purchased by the customer. Akamai Processes End User Personal Data only on behalf of the Customer and subject to its instructions for such Processing. operates as a Data Processor with respect to End User Personal Data and, therefore, is a Data Processor in this context.

Similarly, with respect to Customer Personal Data, Akamai is provided this data by the Customer and stores it in its service portals as necessary to support the services to the customer. The customer determines what data is provided and when contact names and the like must be changed. Therefore, with respect to Customer Personal Data, Akamai also operates as a Data Processor.

The analysis is different, however, for Akamai's processing of Logged Personal Data. With respect to this data, Akamai determines the data that must be collected and processed, the purposes of that processing (such as, for example, mapping/routing, threat analysis, service improvement and development, fraud management, billing), and the technical means for conducting the processing (such as development of algorithms, and delivery techniques and systems). The customers do not participate in such determinations which are largely transparent to them.

Through these actions, Akamai is thereby exercising a level of control over the purposes and means of processing of much of the personal data on its platform inconsistent with the role of a mere Data Processor—Akamai, therefore, operates as a Data Controller under the GDPR for Logged Personal Data. New data product development efforts include a review and analysis of potential data protection, security, and privacy concerns not only to comply with applicable laws and its obligations as a Data Controller, but also

to ensure that it follows processes and procedures necessary to maintain the trust placed on it by its customers and to protect the fundamental rights of end users.

Akamai® is the leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 40 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.