Protection of Personal and Sensitive Data in Akamai CDN and Security Services

Lukasz Orzechowski, Senior Technical PgM, Akamai InfoSec
How Akamai operates

Akamai acts as a conduit

Between you and your end users
You can send any type of data through Akamai

You decide
Purpose of the presentation

This deck will help you navigate current law landscape, understand what data Akamai processes and how this data is processed & protected.
Types of Data processed by Akamai

- **Data** that flows through Akamai platform
- **Data** about you as our customer
- **Data** generated by Akamai

Each data category will be further discussed on the following slides.
Data that flows through Akamai Platform

Akamai respects your privacy and will act as a mere conduit for data in customer content. The data will be processed exactly in the way you have configured, without inspecting it for sensitive or private information.

We encourage you to implement a data classification mechanism and select Akamai services adequate to the type of data you are sending.

Akamai must inspect requests to process them in the way you have ordered us to.

IP addresses are important as they are considered to be personal data by certain privacy laws. More about it later.
Cache

You have full control on what will be cached by Akamai

Only data selected by the customer is cached to be shared. That’s why you should not configure the services to cache sensitive or personal information (Akamai’s PS team can help you with the configuration).

Elements cached will be served by Akamai which offloads your infrastructure.

Cache integrity is ensured by checksums. Cache is not encrypted at rest for performance reasons.

Cache has transient nature and an expiration date. As a temporary copy, it is not backed up.
Data about you as a customer

Personal information
- contact names
- title
- telephone numbers
- Luna / API credentials
- business address
- email address

Regular information
- services configurations
- runbook rules
- property information
- notification preferences
- your certificates
Data generated by Akamai

End users
- IP addresses
- Geo location
- Page activity and URLs
- Telemetry data

Bots
- Bot signatures
- Behavioral patterns
- Bot activity
- Attack patterns

Administrative
- Authgate grants
- Grants usage
- Systems monitoring
- Secret keys management

Internet
- IP reputation
- Optimal routing
- Traffic congestions
- Emerging threats

...
What about secrets?

Certificates and Keys

Used to encrypt connections in the Standard and Enhanced TLS CDN. Stored and distributed using Akamai Key Management Infrastructure.

Protection

- Physical protection
- Encryption at rest
- Quarterly pentests
- Encryption in transit
- Dedicated memory
- Port hardening
- NOCC monitoring
- Access control
- No PII on disc
- Audits every 20 minutes
- Restricted inbound traffic
Processing Locations
Akamai is a global platform

- 300,000+ servers
- 2,300+ datacenters
- 130+ countries
- 1,600+ networks

Data as of September 2017
Servers are close to the end users
Everything is processed globally*

Data that flows through the Akamai platform

Processed globally by the edge servers that are the most optimal for the end user.

Edge server inspects end user requests and then processes them as defined by the customer.

IP data and geolocation is used to determine optimal servers and routing
Everything is processed globally*

Data that flows through the Akamai platform

Processed globally by the edge servers that are the most optimal for the end user.

Edge server inspects end user requests and then processes them as defined by the customer.

IP data and geolocation is used to determine optimal servers and routing

Data about you as our customer

Personal information is stored in Luna & Salesforce cloud and processed by Akamai support centers globally

Regular information (configuration) is distributed globally and processed by servers delivering services.
Everything is processed globally*

Data that flows through the Akamai platform

Processed globally by the edge servers that are the most optimal for the end user.

Edge server inspects end user requests and then processes them as defined by the customer.

IP data and geolocation is used to determine optimal servers and routing

Data about you as our customer

Personal information is stored in Luna & Salesforce cloud and processed by Akamai support centers globally.

Regular information (configuration) is distributed globally and processed by servers delivering services.

Data generated by Akamai

Generated globally and processed globally.

Usage:
- services delivery,
- support,
- billing,
- audit trail,
- diagnostic,
- services improvement…
### Everything is processed globally*

<table>
<thead>
<tr>
<th>Data that flows through the Akamai platform</th>
<th>Data about you as our customer</th>
<th>Data generated by Akamai</th>
<th>Cache</th>
<th>Secrets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processed globally by the edge servers that are the most optimal for the end user.</td>
<td>Personal information is stored in Luna &amp; Salesforce cloud and processed by Akamai support centers globally.</td>
<td>Generated globally and processed globally.</td>
<td>Processed and stored globally.</td>
<td>Managed globally by secure Key Management Infrastructure.</td>
</tr>
<tr>
<td>Edge server inspects end user requests and then processes them as defined by the customer.</td>
<td>Regular information (configuration) is distributed globally and processed by servers delivering services.</td>
<td>Usage: services delivery, support, billing, audit trail, diagnostic, services improvement…</td>
<td></td>
<td>Processed globally by Secure CDN Edge servers</td>
</tr>
<tr>
<td>IP data and geolocation is used to determine optimal servers and routing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

*Data Protection © 2020 Akamai | AKAMAI PUBLIC DOCUMENT*
Can you deliver us a list of countries?

As of 1st September 2019


* Please note that China and Russia CDNs are offered as separate products and servers in these countries are not used in the regular CDN
Access Control
Akamai networks separation

Corporate Network

Authgate

Production Network
Akamai networks separation

Corporate Network

Production Network

Authgate

Akamai Employee Grants

Time Access Purpose
Akamai networks separation

Corporate Network

- Authgate
- Akamai Employee Grants
- Time Access Purpose
- Proxy Logs
- Grant reviews

Production Network
**Authserver**

- Authenticates users using 2048 bit RSA key
- Sends shell commands to Authgate gateway
- Delivers UI to manage grants and keys
- Generates and stores logs
- Grants are time limited and provided on a must-basis
- Supports MFA
- There are no direct administrators

Grants users indirect access to production machines
KMI and Secrets

- Private key
- TLS Certificate Bundle
- AES-256 Encryption
- Separate encrypted transfer of decryption key

Key Distribution Center
Secure Edge Server
Audit Server
Hardened servers

- Port hardened
- Secure Memory allocation
- Dedicated admin channels
- Inbound traffic only on 443 and 80
- Multi-Layered secret protection
- No PII on disk
- Drop malformed requests
- Dynamic load balancing
- Fully enclosed secure racks
Privacy Laws
Privacy laws define the processing roles

The party that processes Personal Data on behalf of the determining party

The party who determines how the Personal Data is processed

The roles’ name vary by country: Data Processor/Controller, Service Provider/Business, Data Intermediare/Organisation…
Akamai processing on behalf of the customer

For some Personal Data, Akamai is processing on behalf of you as the Akamai customer.

You decide what will be cached
You decide what you will send
You decide what services will be used and therefore how the data will be processed.

Data that flows through Akamai platform
Akamai processing on behalf of the customer

“Personal Data in Customer Content”

Financial or other transaction information

Subscriber name and contact information

Login Credentials

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

Akamai processes Personal Data exactly as you have told us to process it.
Akamai processing on behalf of the customer

“Personal Data in Customer Content”

Financial or other transaction information

Subscriber name and contact information

Login Credentials

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

You decide

You as Akamai’s customer decides how the data is processed and what will be sent through the Akamai platform and, as such, you are responsible for compliance with applicable laws for such processing (e.g. appropriate end user notices or consent and having chosen services appropriate for the type of End User Personal Data transiting Akamai’s servers.)

Akamai processes Personal Data exactly as you have told us to process it
For some Personal Data, Akamai is a Data Controller

Akamai determining the purpose

“Logged Personal Data”

Various logged data generated by Akamai

IP addresses
Geo location
Page activity and URLs
Telemetry data

Data about you as our customer
Akamai as a Data Controller

“Logged Personal Data”

For some Personal Data, Akamai is a Data Controller

Various logged data generated by Akamai

IP addresses
Geo location
Page activity and URLs
Telemetry 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).
Akamai as a Data Controller

“Customer Personal Data”

<table>
<thead>
<tr>
<th>corporate address</th>
<th>Job title</th>
</tr>
</thead>
<tbody>
<tr>
<td>contact names</td>
<td>Business phone numbers</td>
</tr>
<tr>
<td></td>
<td>ACC / API credentials</td>
</tr>
<tr>
<td></td>
<td>business email address</td>
</tr>
</tbody>
</table>

Data about you as our customer

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.

Akamai determines what data it collects from its customers (e.g. business address of the company), the data retention and the purposes such data is used for (Marketing and Relationship Management). Therefore, with respect to Customer Personal Data, Akamai operates as Data Controller.
Privacy Laws require a DPA

DPA sets forth the right and duties associated with a processing role.


The Akamai DPA cover the role of Akamai as a content delivery and security service provider. Customer’s DPAs require extensive work to adjust them to the Akamai services.
Summary

1. Introduction
2. Types of Data
3. Processing Locations
4. Access Control
5. Privacy Laws
Thank You