Protection of Personal and Sensitive Data

Lukasz Orzechowski, Senior Technical PgM, Akamai InfoSec
Agenda

1. Introduction
2. Types of Data
3. Where the Data is processed
4. Access Control
5. General Data Protection Regulation
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
Types of Data processed by Akamai

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

Cache

Secrets

Each data category will be further discussed on the following slides
It can be anything

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. Akamai must process IP addresses. IP addresses are important as they are considered to be personal data by the GDPR law. 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 cache sensitive or personal information (Akamai’s PS team can help you configure your services).

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
- business address
- Luna / API credentials
- email address

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

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

Bots
- Bot signatures
- Behavioral patterns
- Bots 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
- Encryption in transit
- No PII on disc
- Audits every 20 minutes
- Restricted inbound traffic
- Port hardening
- NOCC monitoring
- Access control
- Quarterly pentests
- Dedicated memory
Where is the data processed?
Akamai is a global platform

- 250,000+ servers
- 130+ countries
- 3,300+ datacenters
- 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 as for malicious activities 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*

Data that flows through the Akamai platform

Data about you as our customer

Data generated by Akamai

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

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.

Generated globally and processed globally.

Usage:
- services delivery,
- support, billing,
- audit trail,
- diagnostic,
- services improvement...

Cache

Processed and stored globally.

Secrets

Managed globally by secure Key Management Infrastructure.

Processed globally by Secure CDN Edge servers
Can you deliver us a list of countries?

| Albania | Angola | Antartica | Argentina | Armenia | Australia | Austria | Azerbaijan | Bahamas | Bahrain | Bangladesh | Barbados | Belarus | Belgium | Belize | Bermuda | Bolivia | Botswana | Brazil | Brunei Darussalam | Bulgaria | Cambodia, Kingdom of | Canada | Chile | Christmas Island | Colombia | Costa Rica | Croatia | Curacao | Cyprus | Czech Republic | Denmark | Djibouti | Dominica | Dominican Republic | Ecuador | Egypt | El Salvador | Estonia | Faroe Islands | Fiji | Finland | France | French Guyana | Georgia | Germany | Ghana | Gibraltar | Great Britain | Greece | Greenland | Grenada | Guadeloupe (French) | Guam (USA) | Guatemala | Guernsey | Guinea | Haiti | Honduras | Hong Kono | Hungary | Iceland | India | Indonesia | Iraq | Ireland | Isle of Man | Israel | Italy | Jamaica | Japan | Jersey | Jordan | Kazakhstan | Kenya | Kuwait | Laos | Latvia | Lebanon | Lesotho | Lithuania | Luxembourg | Macau | Macedonia | Madagascar | Malawi | Malaysia | Maldives | Malta | Martinique (French) | Mauritius | Mexico | Moldova | Monaco | Mongolia | Morocco | Mozambique | Myanmar | Namibia | Nepal | Netherlands | New Caledonia (French) | New Zealand | Nicaragua | Niger | Nigeria | Northern Mariana Islands | Norway | Oman | Pakistan | Panama | Paraguay | Peru | Philippines | Poland | Portugal | Qatar | Reunion (French) | Romania | Russian Federation | Rwanda | Saint Lucia | Saudi Arabia | Senegal | Serbia | Seychelles | Singapore | Sint Maarten | Slovak Republic | Slovenia | South Africa | South Korea | Spain | Sri Lanka | Sweden | Switzerland | Taiwan | Tanzania | Thailand | Trinidad and Tobago | Tunisia | Turkey | Uganda | Ukraine | United Arab Emirates | United States of America | Uruguay | Vanuatu | Venezuela | Vietnam | Zambia |

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

Production Network

Authgate
Akamai networks separation

Corporate Network

Authgate

Akamai Employee Grants

Time Access Purpose

Production Network
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
- Grants users indirect access to production machines
- Supports MFA
- Delivers UI to manage grants and keys
- Grants are time limited and provided on a must-basis
- Generates and stores logs
- There are no direct administrators
KMI and Secrets

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

- Port hardened
- Secure Memory allocation
- Dedicated admin channels
- Multi-Layered secret protection
- Inbound traffic only on 443 and 80
- No PII on disk
- Drop malformed requests
- Dynamic load balancing
- Fully enclosed secure racks
General Data Protection Regulation
What is General Data Protection Regulation (GDPR)?

An EU regulation set in place to protect all EU citizens’ data privacy rights.

Applicable to all companies that are processing EU citizens’ personal data, also outside of the EU borders.

Effective since May 25, 2018.

Non-compliance can have material, financial impact.
GDPR defines Data Processor and Data Controller

- **Data processor** processes Personal Data
- **Data controller** decides how the Personal Data is processed
For some Personal Data, Akamai is a Data Processor

Data that flows through Akamai platform

Data about you as our customer

Managed by you

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
### Akamai as a Data Processor

**“Customer Personal Data”**

<table>
<thead>
<tr>
<th>Contact Names</th>
<th>Telephone Numbers</th>
<th>Business Address</th>
<th>Title</th>
<th>Luna / API Credentials</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Akamai as a Data Processor

“Customer Personal Data”

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 operates as a Data Processor.

You decide

- business address
- contact names
- telephone numbers
- title
- Luna / API credentials
- email address
"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.

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 operates as a Data Processor.
Akamai as a Data Processor

“Personal Data in Customer Content”

Financial or other transaction information

Login Credentials

Subscriber name and contact information

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

Akamai acts as a conduit and processes data as you have told us to process it.
Akamai as a Data Processor

“Personal Data in Customer Content”

You decide

The Customer decides how the data is going to be processed and what will be sent through the Akamai platform and, as such, the Customer 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.)

Akamai acts as a conduit and processes data as you have told us to process it

<table>
<thead>
<tr>
<th>Financial or other transaction information</th>
<th>Login Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber name and contact information</td>
<td>Other information relating to the individual data subject as requested or provided by the customer through the use of its web property.</td>
</tr>
</tbody>
</table>
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
- and more...
Akamai as a Data Controller

“Logged Personal Data”

For some Personal Data, Akamai is a Data Controller

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).

Various logged data generated by Akamai

IP addresses
Geo location
Page activity and URLs
Telemetry data
and more...
Legal Perspective
DPA / Data Processing Agreement

Provisions in Agreements


It is highly recommended to use the above DPA in agreements with Akamai, as most DPAs are constructed with single role in mind and require extensive work to adjust them to contracted services.