Power and protect life online
Akamai Services

Data Flow & Data Transfers
Delivery and Security Service

Ion, DSA, GTM, Media, Kona
The end-user request accesses the Akamai edge server that is closest to the end user. Where the end user is located in the EU, an edge server in the EU will answer the request (grey lines).

The edge server transmits the request via the Akamai platform to the origin server of the customer. On the way back to the end user, the origin server forwards the web properties via the Akamai platform back to the end user (orange lines).

The customer chooses the security of its web properties. For sensible web properties, Akamai recommends choosing the Akamai Enhanced TLS Platform for transmission.

On the Enhanced TLS Platform, the TLS connection is terminated for an instance by Akamai at the edge server to perform routing and mapping and security checks. Immediately thereafter, the TLS connection is reestablished.
Delivery of Web Properties via the Akamai Platform

- The customer determines whether the web properties are cached/stored on the edge servers or not.

- Where customer’s web properties consist of personal data, Akamai recommends choosing a no-cache configuration for such data, to avoid the accessibility of such data by any end users that are accessing the customer’s web properties (which is the idea of cache).
Delivery of Web Properties via the Akamai Platform

- Where malicious activities are recognized at the edge server, the request is blocked (red lines).
- Where requests are legitimate, they are transmitted via the Akamai platform (grey dotted lines).
- As Akamai does not know when and where an end-user request hits a specific edge server, it does not control which server delivers a given web property or when and where a TLS termination for a given web property occurs.
So, by nature of the Akamai platform, the Privacy by Design principle is met: Where an end user located in the EU is requesting web properties of a customer, the web properties and the embedded personal data (if any) are processed on Akamai servers deployed in the EU, except for corner cases in which transmission on EU servers is not possible.

With more than 100,000 Akamai servers deployed in the EU region, a fast, reliable and secure delivery is ensured within region per default.
Security of Web Properties via the Akamai Platform

- Customer security rules, Akamai rules, and Akamai’s threat intelligence are applied locally at the edge server.

- When an end-user request hits an edge server, the security analytics are performed on the edge server:
  - legitimate requests are transmitted
  - malicious requests are blocked

- For **legitimate requests** by end users located in the EU, the customer’s web properties are **processed in the EU**. No data is transferred outside the EU, except for corner cases.

- Log files of suspicious requests are transferred to the USA for analytics on Akamai’s security systems deployed in the USA.

- The processing of the log files for analytic and service support purposes is outlined on page 31.
Akamai Platform Data Flow

User Agents
- Browsers
- Mobile apps
- IoT devices

Akamaized domains
www.customer.com
api.customer.com
login.customer.com

Akamai Enhanced TLS

Customer managed
Edge services
- Bin
- Kona (WAF)
- Client Reputation
- Bot Manager
- ...

Origin (customer) domains
origin.customer.com
origin.api.customer.com
origin.login.customer.com

End user opens customer domain
www.customer.com
in a browser

The request is directed to the Akamai Edge server

The Akamai server terminates TLS connection and decrypts the request in a memory for processing

The server checks customer configuration to know how the request should be processed

The server re-encrypts the request and sends it to the customer Origin. The request content is now encrypted and is not retained on the server.

The Akamai server terminates TLS connection and decrypts the request in a memory for processing. Then customer configuration is checked to determine whether the response should be cached for future requests. If the response should not be cached, it is immediately re-encrypted, never stored on a disk. Then the response is sent to the end user over encrypted channel.

Origin (customer infrastructure) receives the request and processes it on the customer side.

The response from the Origin is sent to the Akamai Edge server over encrypted channel.
Enterprise Application Access

EAA
Based on the Zero Trust principle, EAA’s purpose is to ensure that only authorized and authenticated individuals access the applications they need to access.

The EAA Client (running on user’s computer) connects to the EAA Cloud (i.e., a proxy that runs in the cloud).

The EAA Connector runs behind the customer’s firewall in the customer’s data center and continuously makes “outbound” connections through the firewall to the EAA Cloud, checking for incoming client connections.

When the Connector detects an inbound connection from an EAA Client to the EAA Cloud, the Connector performs the dual tasks of (i) Authentication (i.e., “who are you?”) and (ii) Authorization (i.e., “what are you permitted to do upon access?”). The Connector relies on the customer’s employee directory and IDT to authenticate and authorize.

Then, the Connector “stitches together” the two connections, providing a tunnel through the firewall and into the customer’s networks so that the user can access authorized resources.
Enterprise Application Access

**Front-End Authentication**: Occurs between the user’s browser and the EAA Cloud server to which the user connects to use the EAA service. Usually, this step prompts the user for a username and password (if the user has not already authenticated to the EAA SSO service).

**Back-End Authentication**: Occurs between the EAA Cloud and the Application server. This process uses the authentication method that the requested application is programmed to accept (e.g., Kerberos, SAML, etc.).

**Authorization**: Whereas Authentication confirms who the requestor is, Authorization confirms which resources the requestor is permitted to access.

The Front-End Authentication ensures that EAA collects the information needed to craft the proper Back-End authentication method – so the user only logs in once.
Enterprise Application Access

The customer’s directory with the employee corporate contact details gets copied into the EAA Cloud.

The EAA Cloud runs on AWS, and EAA can be configured so that the customer’s employee directory in the EAA Cloud is stored in-region.

With this Privacy by Design feature, EU personal data for legitimate access is processed within the EU only.

Logs of malicious events (e.g., brute-force attack) are transferred to the USA and analyzed in Akamai’s security analytic systems. Such events are not performed by individuals, but by bots, so the related IP addresses are not to be classified as personal data.
Enterprise Threat Protector

ETP
Enter the Threat Protector

ETP offers different use cases:

- DNS-based threat detection only (for companies with full security stack inside)
- DNS + suspicious web traffic via security proxy (companies who are in the cloud transformation phase or have completed this phase)
- DNS + all traffic via security proxy (companies who want additional visibility and security on top of cloud security)

ETP protects at 3 layers:

- DNS inspection at DNS servers
- URL inspection at ETP proxy platform
- Payload analysis at ETP proxy platform

Malicious traffic is determined in accordance with:

- Customer rules
- Akamai rules, if desired
- Akamai’s threat intelligence

Recognized malicious traffic is blocked at the Akamai platform.

Legitimate traffic is forwarded to the internet.
Enterprise Threat Protector

• By design of the Akamai platform, end-user requests within the EU are answered by DNS servers deployed in the EU.

• Akamai’s threat intelligence is applied locally at the edge server. Legitimate traffic is passed through to the global internet.

• Logs are generated on the edge server when performing ETP services and transferred to Akamai’s log collection system in the USA for traffic and security analytics (see page 31).
Enterprise Threat Protector

- Data elements embedded in the logs:
  - End-user IP address
  - Time stamp
  - DNS data
  - Browser data
  - Network data

- The end-user IP address may relate to a corporate proxy. So it is not necessarily classified as personal data.
Edge DNS and Global Traffic Management

- Edge DNS and Global Traffic Management are Akamai’s external authoritative DNS services.
- Edge DNS provides DDoS resilient zone management.
- Global Traffic Management provides secure and extensible Layer 3 global service load balancing.
- Personal data processed is end-user IP address. IP address might relate to a corporate proxy and may not necessarily be classified as personal data.
- The customer determines security rules to apply. Akamai may apply additional rules. Finally, Akamai’s threat intelligence is applied, and the rules and the intelligence are rolled out to the DNS servers.
- In accordance with the rules and the intelligence, safe requests are forwarded to the internet and malicious requests are blocked.
Bot Manager Premier

Account Protector and Page Integrity Manager
Data is collected to determine whether access has been made by a **human or a bot**.

- Data elements include network, browser, and behavior data.
- Akamai’s threat intelligence is applied.
- End-user IP addresses are **pseudonymized** data for Akamai.
- Akamai does identify bots, but **does not identify the end users**.
- Akamai is not creating end-user profiles.

Web property’s access is **forwarded or blocked**, in accordance with the customer’s security rules, Akamai’s rules and Akamai’s threat intelligence.

The cookie technology used is **strictly necessary** for state-of-the-art operation of the customer’s website and offering of its services.

Bot Manager Premier has been developed with **Privacy by Design** in mind.

The log files are processed as outlined on page 31.

Details are outlined in the **Privacy by Design** white paper.
Prolexic

DDoS Protection
Prolexic Services

- Prolexic is a DDoS mitigation solution.
- The personal data element processed is the end-user IP address.
- When the service is enabled, the inbound traffic to the customer is directed to a scrubbing center on the Prolexic platform.
- There the traffic is analyzed for Layer 3, 4, and 7 attacks (http only). Where the traffic is encrypted, it remains encrypted. A TLS termination is not required (as no https traffic analytics are in scope of Prolexic).
- Legitimate traffic is forwarded to the customer’s infrastructure.
- Malicious traffic is blocked and further analyzed in the scrubbing centers.
- The security event logs are transferred to Akamai’s security systems in the USA for further analytics. In most cases the IP addresses relate to devices used by bots, not by humans. In this case the IP is not personal data. Logs are stored in the USA as outlined on page 31.
• Scrubbing Centers are deployed on the Prolexic Platform in the EU, Asia, and the Americas to ensure global coverage and best protection against DDoS attacks.

• While per default for EU traffic scrubbing centers in the EU are chosen, depending on the workload a failover to scrubbing centers in other regions may be used, in particular in case of large attacks, to ensure the availability of the customer website, notwithstanding the attack.

• Akamai does not limit the usage of scrubbing centers to one region to ensure best mitigation of DDoS attacks.

• Log processing for support purposes is described on page 31.
Akamai Identity Cloud Services

- Identity Cloud is an end-user identity management service on top of Akamai’s web performance services.

- Personal data elements processed relate to the identity of the end user, e.g.,
  - Name
  - Email
  - Address
  - Phone number
  - Age
  - Gender
  - Shopping history (e.g., shoe size, preferred toothpaste)

- Personal data elements are collected by the customer, not by Akamai. Akamai hosts and secures the data in Identity Cloud only.

- Identity Cloud runs on AWS as Akamai’s sub-processor.

- The customer determines via the service configuration the storage location of the end-user identities (USA, EU, or APJ).
Akamai Identity Cloud Services

- Akamai’s web performance service ensures availability and security of the customer web properties via the Akamai platform (see pages 2–8).
- Log files are processed as outlined on page 31.
- For details about how Identity Cloud helps to comply with data subject rights and other privacy requirements, see this Identity Cloud privacy white paper.
Privacy by Design resulted in the following access controls:

- **Limited access** to end-user identities for the customer employees based on roles, responsibilities, and application type/use.
- Access only in accordance with need-to-have principle.
- Fine-grained control down to the level of individual data record fields and columns.
- Access is logged and can easily be tracked in case of abuse.
mPulse
Web Performance Services
mPulse Service

- mPulse is a website performance analytic service. No end-user analytics are performed.

- The personal data element processed is the end-user IP address. It is anonymized at the edge server.

- Where the edge server is deployed in the EU, personal data is processed only in the EU (the IP is collected as part of the log file creation on the EU-based edge server and anonymized).

- The log files (with the anonymized IP) are transferred from the edge server to the mPulse portal deployed in the USA and analyzed there.

- Analytic reports are created and made available to the customer via the Akamai Control Center.

- Details are outlined in the white paper mPulse Compliance with Global Data Protection Laws.
Log Processing
Performance and Security Analytics and Support Services
Traffic and Security Analytics

• Log files consist of metadata collected at the edge server the moment a request hits an edge server.

• The logs are transferred from the edge servers to Akamai’s log collection system deployed in the USA, for traffic analytics.

• The logs are forwarded to Akamai’s security analytic system, deployed in the USA, for security analytics.

• Reports of the analytics are created and made available to customers in the Akamai Control Center. For some services, Akamai also provides the customers with logs.

• Log retention periods:
  • Couple of hours on the edge server
  • 14 days on the log delivery system
  • 90 days on the security analytic system

Where required from a security perspective (e.g., to include new attack vectors to the security algorithm), logs are retained for 180 days.
• In case of a service incident, a support ticket is created.

• The ticket is stored in Akamai’s Salesforce instance, which is deployed in the USA.

• Akamai’s AkaTech team handles the support case by collecting logs related to the request in question from the log collection system or the edge server.

• Logs consist of end-user IP address. So personal data is processed as part of the support service performed.

• Personal data in the support tickets are deleted 120 days after ticket closure.
Risks of Access to Logs by Third Parties

• The data transferred by Akamai to the USA is in most of the cases the end-user IP address. For Akamai, though it does not edit the IP address, the IP address is a pseudonymized data element, as Akamai does not hold the additional data to identify the individual using the device the IP address relates to, nor has it the legal means to request the additional data required.

While in the understanding of regulators it suffices that any third party with reasonable effort can identify an individual using additional data, in case of Akamai’s data transfers, it requires a significant effort to request the data from relevant third parties (e.g., a data access request directed toward the third party).

• Akamai is not classified as an e-communication service provider under U.S. laws. While the term is read very broadly, Akamai is processing IP addresses to perform mapping, routing, and security services. It does not process the IPs to perform communication services. So, FISA 702 is not applicable to Akamai. Respectively, Akamai has not received a data access request under FISA 702.

• Akamai has also not received a data access request under the CLOUD Act.

• These facts are supported by the confirmation by the U.S. government in a white paper on data access that data accessed must serve surveillance purposes, and therefore many data elements that in theory could be requested to access in fact are out of scope: [https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF](https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF). Where multiple data access requests are needed to collect data that serves surveillance purposes, the likelihood is high that there are other data access request recipients available to serve the surveillance purposes more easily.

• Akamai is not a cloud service provider, so use case 6 of the EDPB’s recommendation 01/2021 does not apply.
Risks of Access to Logs by Third Parties

• Respectively Akamai denies most of the data access requests by local law enforcement agencies (e.g., the local police) it receives because it does not hold the requested contact details of individuals. It serves the access request using the IP as determiner where to serve the requested web properties and whether the request is legitimate or malicious.

• Akamai secures the logs of the IP address by encryption in transit using TLS 1.2 and integrity protection at rest. An overview of Akamai’s tight access controls securing the data at rest is available upon request under NDA.

• As contractually committed in the EU SCCs 2021, Akamai has a law enforcement process in place ensuring that the request is reviewed by Akamai’s legal team, denied if Akamai is not in the possession of the requested data, challenged if the request is excessive or illegal, and reported on, as applicable.

Given these facts, Akamai assesses the data access risk for the IP address it transfers to be low. Akamai has taken the described technical and organizational supplemental measures to mitigate this low risk. Therefore, Akamai is of the opinion that the benefits for the state of the global internet resulting from Akamai’s web performance and security services outweigh the associated mitigated data transfer risk.
Akamai’s Privacy Trust Center: www.akamai.com/compliance/privacy