WHITE PAPER

# GDPR Data Management and Protection

## How the Akamai Intelligent Edge Platform Helps Mitigate Security Risks

Akamai

## Table of Contents



> GDPR is a game changer. To avoid high fines and reputation damages, state-of-the-art data management and security are necessary. Akamai's services help our customers to manage and secure their data as required under the GDPR."
>
> – DR. ANNA SCHMITS, EMEA DATA PROTECTION OFFICER, AKAMAI

## General Data Protection Regulation

The General Data Protection Regulation (GDPR), in effect since May 25, 2018, is the current European Union (EU) data protection law that aims to harmonize local data protection laws across Europe. Since its inception, the law has triggered organizations to bolster privacy policies and established data protection best practices across the globe.

The GDPR requires organizations to manage and secure any operation that involves processing EU personal data to protect against unauthorized access. Noncompliance with GDPR – such as failing to prove that personal data is adequately protected when processed or not maintaining control over a subject's data – can result in fines that materially impact an organization. Large financial penalties imposed by local data protection authorities – fines of US$230 million issued to British Airways and US$124 million to Marriott for data breach violations, for example – illustrate the consequences of not complying with GDPR requirements.[1]

## How Can Akamai Help With GDPR Compliance?

The GDPR requires that EU personal data processed by an organization be appropriately and sufficiently managed and protected. In a connected world, where millions of web applications and websites collect and use personal data, this is a significant challenge that encompasses people, processes, and technologies.

The Akamai Intelligent Edge Platform helps organizations meet this challenge with strong data management and security capabilities based on user-driven data controls, access to a team of qualified security professionals, and state-of-the-art technology offerings. Akamai provides personal information management and cloud security solutions and services that enable organizations to quickly address GDPR requirements.

## Identity Data Management in the Cloud

The GDPR shifts the responsibility of personal data protection to the organizations that collect and manage this information. The ability to ensure privacy and transparency in all data management processes is essential for GDPR compliance.

Akamai Identity Cloud is a cloud-based identity-as-a-service solution, also known as customer identity and access management (CIAM). Identity Cloud enables organizations to provide end users with control over the creation, use, and management of their data, all while ensuring personal information protection, data security, and regulatory compliance.

Identity Cloud includes registration, login, authentication, single sign-on, scoped access control, and preference and consent management, as well as other capabilities needed to collect, manage, and secure the personal data submitted by end users to utilize the organization's services.

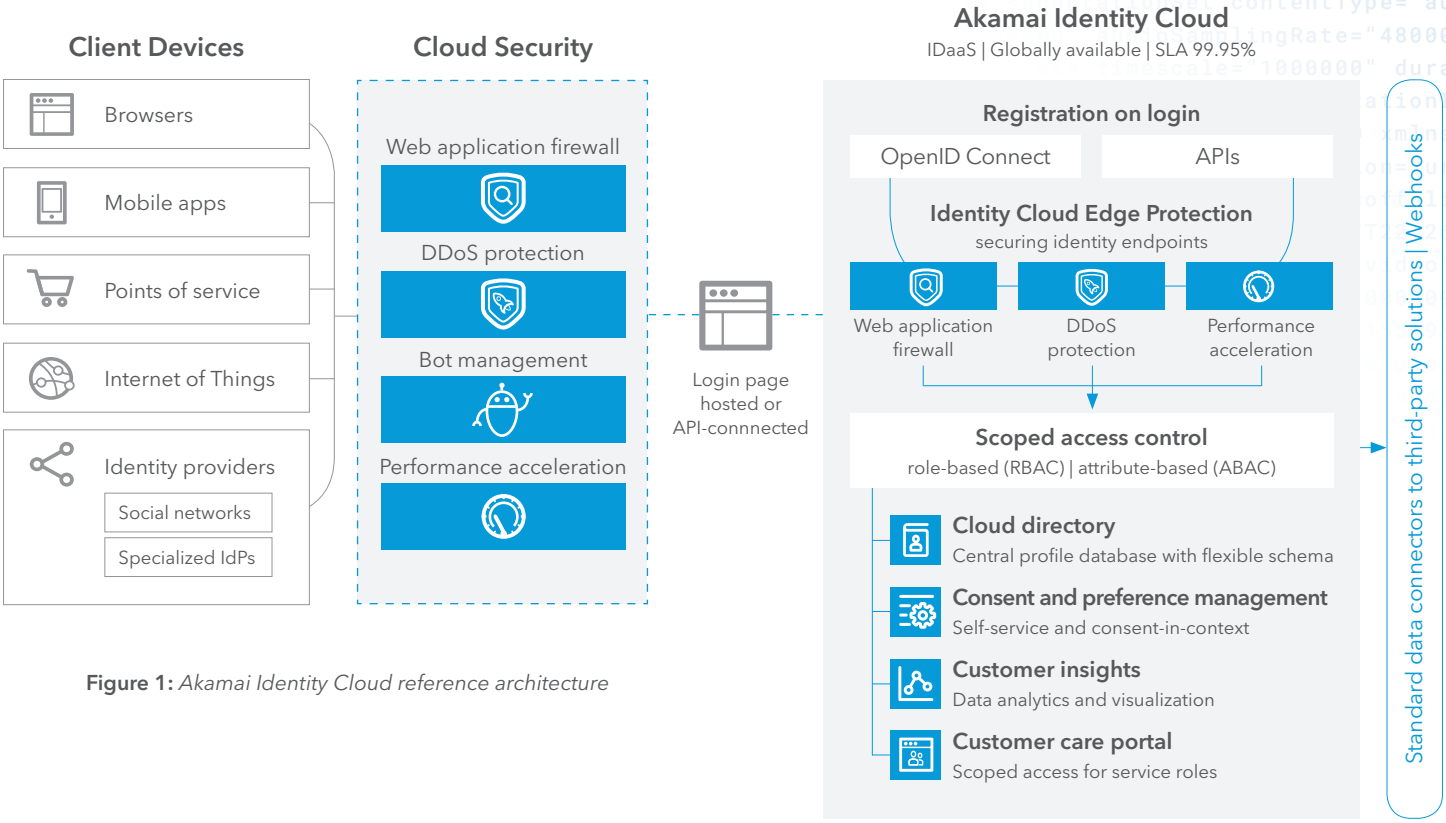


**Figure 1:** *Akamai Identity Cloud reference architecture*

## Manage Personal and Organizational Data

The data management features within Identity Cloud enable organizations to provide end users with control over their data by allowing them to choose the information shared. Individuals can opt in and update or correct their data anytime, on any device.

Identity Cloud also enables organizations to document when individuals provide, update, or delete data. Respective logs and audit trails are available for documentation purposes and enable organizations to comply with accountability requirements under the GDPR. Identity Cloud provides strong access control mechanisms that support both role-based access control (RBAC) and attribute-based access control (ABAC), and limits access to personal data. Fine-grained controls help mitigate the sprawl of toxic data, such as outdated permissions, and reduce the attack surface.

## Protect End-User Accounts

Identity Cloud provides field-level access control that allows organizations to define who has read or write access rights to specific user record fields. With the ability to grant the desired scope of data access, organizations increase data security by reducing the risk of unintentional exposures. Strong encryption for data in motion and at rest further supports state-of-the-art data protection.

The security and data protection safeguards in Identity Cloud are ISO 27001:2013, ISO 27018:2014, and CSA STAR Level 2 certified, and comply with the requirements of the U.S. Health Insurance Portability and Accountability Act (HIPAA).

> **Developed and designed to meet high data protection requirements, Identity Cloud is a key tool for organizations to implement the GDPR Privacy by Design principle, ensuring end users maintain control over their data."**
> – Mayur Upadhyaya, Senior Director, Akamai Identity Cloud, Akamai

| GDPR REQUIREMENTS | AKAMAI IDENTITY CLOUD CAPABILITIES |
|---|---|
| **Obtaining and managing consent**<br>Art. 4 (11), 7 (3) GDPR | Collects consent and provides self-service for users to view, modify, and revoke consent |
| **Parental consent for children under 16**<br>Art. 8 GDPR | Protects against the acceptance of personal data from children with age-gating functionality |
| **Right of access by the data subject**<br>Art. 15, 20 GDPR | Provides easy self-service data record access for users |
| **Right to rectification**<br>Art. 5 (1) d, 16 GDPR | Allows users and service representatives to edit data records |
| **Right to erasure ("right to be forgotten")**<br>Art. 17 GDPR | Enables secure deletion of data records, including deletion from backups |
| **Maintain record of processing activities**<br>Art. 30 (2) GDPR | Maintains an auditable record of all data record changes, and a general description of technical and organizational security measures |
| **Implement security safeguards appropriate to the risk**<br>Art. 28, 32 GDPR | Applies the appropriate safeguards to protect the personal data processed by Akamai and the privacy of the affected data subjects, including the safeguards specifically noted in Article 32, such as encryption of personal data in transit and at rest |

**Figure 2:** *Akamai Identity Cloud capabilities that address GDPR requirements*

## Data Security in the Cloud

Organizations that process personal information also need to secure the data against unauthorized access. The GDPR tasks organizations with demonstrating that appropriate security measures are protecting the data processed.

A data protection impact assessment (DPIA) is a powerful evaluation tool, required in some cases under the GDPR, to determine the potential impact of data processing operations. When conducting a DPIA, an organization must document in detail a number of factors, including:

- Planned data processing operations
- The necessity and proportionality of these operations
- An assessment of the risks of data breach associated with the operations
- The measures envisaged to address these risks, including safeguards and security measures, and mechanisms to ensure the protection of personal data[2]

The GDPR mandates a risk-based approach to data protection. Data security obligations are not stated in a vacuum, but rather developed based on a thorough analysis and understanding of the risks that each processing operation may have for the data subjects. While this approach offers the necessary flexibility to allow organizations to apply reasonable measures in light of costs, system architecture, and related factors, it nevertheless requires a rigorous cost-benefit and risk review of everything that the organization does with personal data. In many cases, this is a significant task.

How successfully an organization provides sufficient evidence of effective risk mitigation will depend on its understanding of the relevant privacy risks, as well as the strengths of the data management and security measures it chooses to implement in response to perceived risks. An organization's success also depends on the selection of partners that understand its security and data protection obligations, and take the necessary steps to manage and protect their own data and systems.

Akamai is committed to maintaining individuals' control over their data by managing and securing all data transmitted over its state-of-the-art platform. Its enterprise-wide information security program complies with the ISO/IEC ISO 2700x standard for information security management. Akamai is assessed annually against the ISO 27001, ISO 27002, and U.S. federal government FedRAMP standards. In addition, the Akamai content delivery network is reviewed annually for compliance with Payment Card Industry Data Security Standards and HIPAA. Akamai also undergoes annual SOC 2 Type 2 auditing and reporting.

Akamai Security Solutions support GDPR requirements by enabling organizations to manage risk, build evidence, deploy state-of-the-art technology, and implement a Zero Trust strategy.

## Work Risk-Based

Significant volumes of personal data are processed through Internet-facing applications. Organizations are required under the GDPR to implement appropriate technical and organizational measures to secure the personal data under their control.[3] Such measures include security technologies designed to protect Internet-facing applications and websites from attacks intended to access personal data.

The Akamai web application firewall (WAF) combines industry best practices such as those set out by the Open Web Application Security Project (OWASP) with intelligent scoring mechanisms to identify attack traffic.[4] In addition, Akamai security experts continuously monitor the web for new attacks with unmatched visibility into online traffic.

The Akamai WAF is a risk-based threat protection service by design. Built upon risk groups, the WAF immediately, effectively, and efficiently mitigates risks associated with the most sophisticated application-layer attacks. By deploying the Akamai WAF, organizations demonstrate that they've taken reasonable steps to prepare against known and unknown threats.

Application programming interface (API) traffic is increasing on the Akamai Intelligent Edge Platform, and the risks associated with underprotected APIs is an area that requires special attention, according to the OWASP Top 10. The Akamai WAF protects API traffic to secure both RESTful APIs and traditional XML-based web services, mitigating distributed denial-of-service (DDoS) attacks and data theft caused by excessive rate, slow post, parameter, and man-in-the-middle attacks. It is able to scale to the needs of the largest business asset owners and API publishers, providing analytics, value confirmation reports, and security information and event management integration.

Evidence that best practices are implemented from a reputable vendor as part of an information security management system is key to risk mitigation. The ability to demonstrate that appropriate security measures are in place helps to satisfy the Data Protection Authority (DPA).

## Build Evidence

In the event of a security breach that requires the reporting of the loss of personal data to a DPA, it is extremely important to supply evidence of the steps already taken to control the incident, as well as the planned mitigation procedures to minimize future impact.

For security measures to be effective, constant review against new and changing threats is required. Akamai Security Optimization Assistance helps organizations respond to the ever-changing threat landscape and provides the evidence that risks are actively anticipated and mitigated by creating and maintaining effective WAF rules.

Akamai provides extensive reporting and evaluation containing the type, quantity, and probability of attacks in a given period. As part of Akamai WAF services, a security expert proactively reviews security policies and makes suggestions for ongoing adjustments of the WAF rules specific to an organization's business.

## Use State-of-the-Art Technology

The GDPR describes appropriate security measures as those that consider the state of the art; implementation cost; and scope, context, and purposes of processing personal data – balancing these factors against the risks and impacts to the rights and freedoms of individuals.[5] An organization will take into account industry best practice as a guide to determine the appropriate and balanced measures.

DDoS attacks – combined with application-layer attack vectors such as Structured Query Language injection (SQLi), local file inclusion (LFI), remote file inclusion (RFI), and cross-site scripting (XSS) – are extremely dangerous combinations when it comes to the theft and leakage of personal data. Often, separate and siloed solutions from different vendors are installed in an organization's cloud data center, leading to delayed and ineffective security responses.

> **While applications and personnel are kept busy and many incidents are created, a very targeted attack can be launched, stealing specific sensitive information. Personal data can only be effectively protected by a solution that protects against both DDoS and application-layer attacks in a harmonized and coordinated way."**
> – Gerhard Giese, Senior Manager, Cloud Security Architects EMEA, Akamai

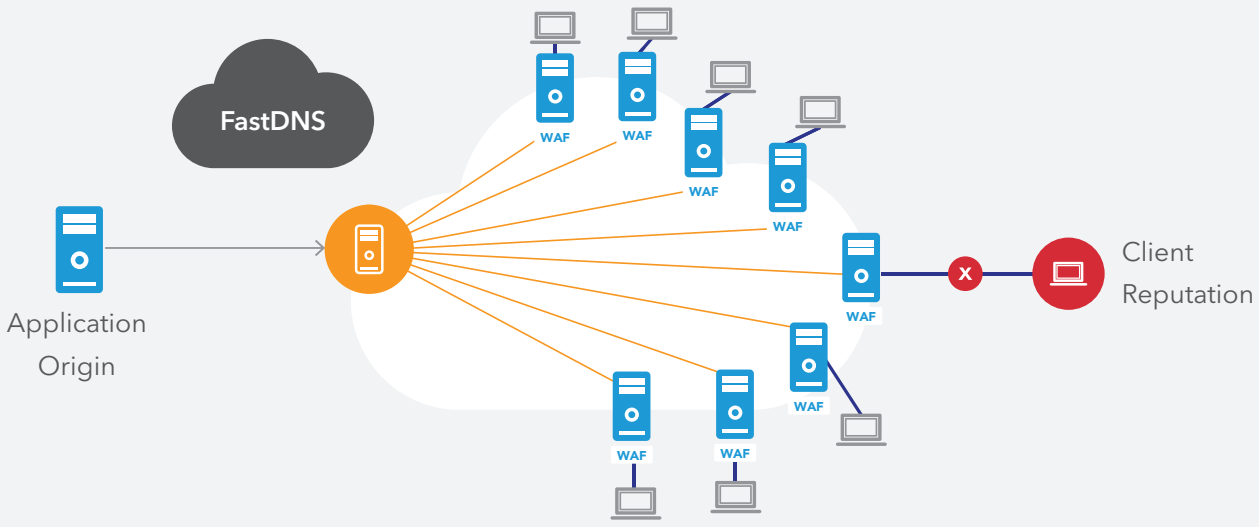


**Figure 3:** *Delivering performance and security from the Edge, where scale matters*

Part of the Akamai Intelligent Edge Platform, the Akamai WAF is designed to deliver customer content via the best available Edge Node for the user requesting certain web content. The best available Akamai Edge Node is, in many cases, the Edge Node that is physically closest to the user requesting the web content.

The Akamai Intelligent Edge Platform consists of a worldwide network of more than 240,000 servers at the edges of 1,700 networks in more than 130 countries. Attackers are stopped at the edge – not only before the attack hits the organization's website or application, but before it reaches the company's server or data center, where absorbing a large-scale attack becomes cumbersome. Without the need for expensive equipment investments or unpredictable costs of hybrid solutions, the Akamai WAF is installed on thousands of Edge Nodes, absorbing and mitigating attacks at no extra capital cost to the organization. Application-layer DDoS attacks, and attacks using ports other than 80 or 443, are immediately stopped at the Akamai Edge Node.

Specific WAF rules tailored to each organization are quickly rolled out across thousands of relevant Edge Nodes to secure web-facing resources worldwide. This innovative approach uniquely positions Akamai to protect the entire data processing and distribution chain of personal information for any organization's digital business.

The effectiveness of the Akamai WAF is enhanced by adding the reputation of the IP addresses accessing an organization's web resources. Akamai's Client Reputation database sees one billion IP addresses every quarter. A small percentage of these addresses are malicious and can be blocked by WAF rules. Every day, hundreds of millions of IP addresses are analyzed for malicious activity. The effectiveness of security controls is an important part of GDPR compliance.[6] The Akamai WAF approach results in measurable effectiveness, in most cases, with an accuracy of more than 95%.

Credential theft can very easily lead to the loss of sensitive personal data. People tend to choose simple passwords that they can easily remember, and reuse them often. Once credentials are hacked, it's possible that multiple data sources are exposed. Sophisticated botnets automatically and rapidly access websites worldwide using stolen credentials. Akamai mitigates these risks with dedicated bot management capabilities. Akamai Bot Manager installed on Akamai Edge Nodes inspects and rejects traffic to web resources using advanced machine learning algorithms designed to detect and mitigate bot activity.

## Implement a Zero Trust Enterprise Security Strategy

Implementing a Zero Trust enterprise security strategy makes GDPR compliance easier and less costly. Zero Trust is based on the concept that there is no distinction between internal and external network traffic. As the name implies, nothing and nobody is trusted inside or outside an organization's network until properly verified.

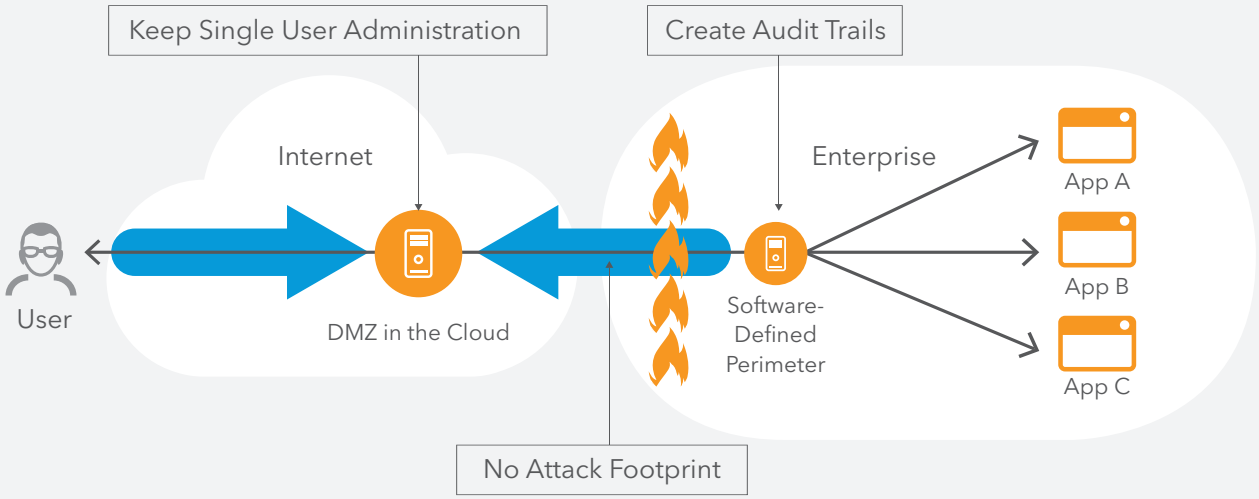


**Figure 4:** *Zero Trust isolates applications containing sensitive personal data*

As a first step, access is explicitly granted and confirmed by a central management system to all resources, and all traffic is always monitored and inspected. Second, the classic perimeter network design is transformed into an isolated services approach. Access via a cloud perimeter isolates apps from the Internet and keeps unauthorized users off the organization's network. Using the Akamai Intelligent Edge Platform, application and personal data can only be accessed via the platform, which obfuscates corporate infrastructure and resources, protecting personal data on- or off-premises. The ability to segment and isolate applications and data, combined with full-access logging, facilitates an audit or DPIA as well as security incident identification.

A Zero Trust strategy extends to users and their devices. Akamai inspects content within data packages, and monitors and logs every user action, providing organizations with full visibility into network traffic. Audit trails of employee and contractor activity are secured appropriately to easily provide the required documentation for any DPIA or audit.

Since the vast majority of malicious attacks use the domain name system (DNS) across the entire cyber kill chain, it's critical not only to monitor Internet-bound DNS requests, but also use DNS as an enterprise control point. The cloud perimeter inspects and evaluates all DNS requests – if untrustworthy links are clicked in phishing or ransomware attempts, it blocks the request to proactively prevent malware and DNS-based exfiltration across an organization. It only delivers apps and data to authorized and authenticated users and devices, never trusting without verifying.

## Conclusion

The GDPR requires evidence of a risk-based approach to data management and security. All organizations that process personal data of EU individuals must be prepared to demonstrate that they have taken the appropriate steps to manage and protect the personal data under their control.

The Akamai Intelligent Edge Platform surrounds everything from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Leveraging Akamai's data management and security expertise, customers manage and secure their digital assets, including personal data, against loss and unlawful access. Akamai is committed to helping organizations manage their data and mitigate underlying security risks as required by the GDPR. For more information, visit www.akamai.com/gdpr.

**Authors:**
Dr. Anna Schmits, EMEA Data Protection Officer, Akamai
Sven Dummer, Product Marketing, Identity Cloud, Akamai

**Sources:**

1) Hodge, Neil. "What we can learn from the biggest GDPR fines so far," *Compliance Week*, July 19, 2019. Available at: https://www.complianceweek.com/gdpr/what-we-can-learn-from-the-biggest-gdpr-fines-so-far/27431.article
2) Article 35 (7) (d) GDPR. Available at: https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A35
3) Articles 24 (1) and 32 (1) GDPR. Available at: https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A24 and https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A32
4) "How Akamai Augments Your Security Practice to Mitigate the OWASP Top 10 Risks," November 2018. Available at: https://www.akamai.com/us/en/multimedia/documents/white-paper/how-akamai-augments-your-security-practice-to-mitigate-the-owasp-top-10-risks.pdf
5) Articles 25 (1) and 32 (1) GDPR. Available at: https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A25 and https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A32
6) Article 32 (1d) GDPR. Available at: https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A32