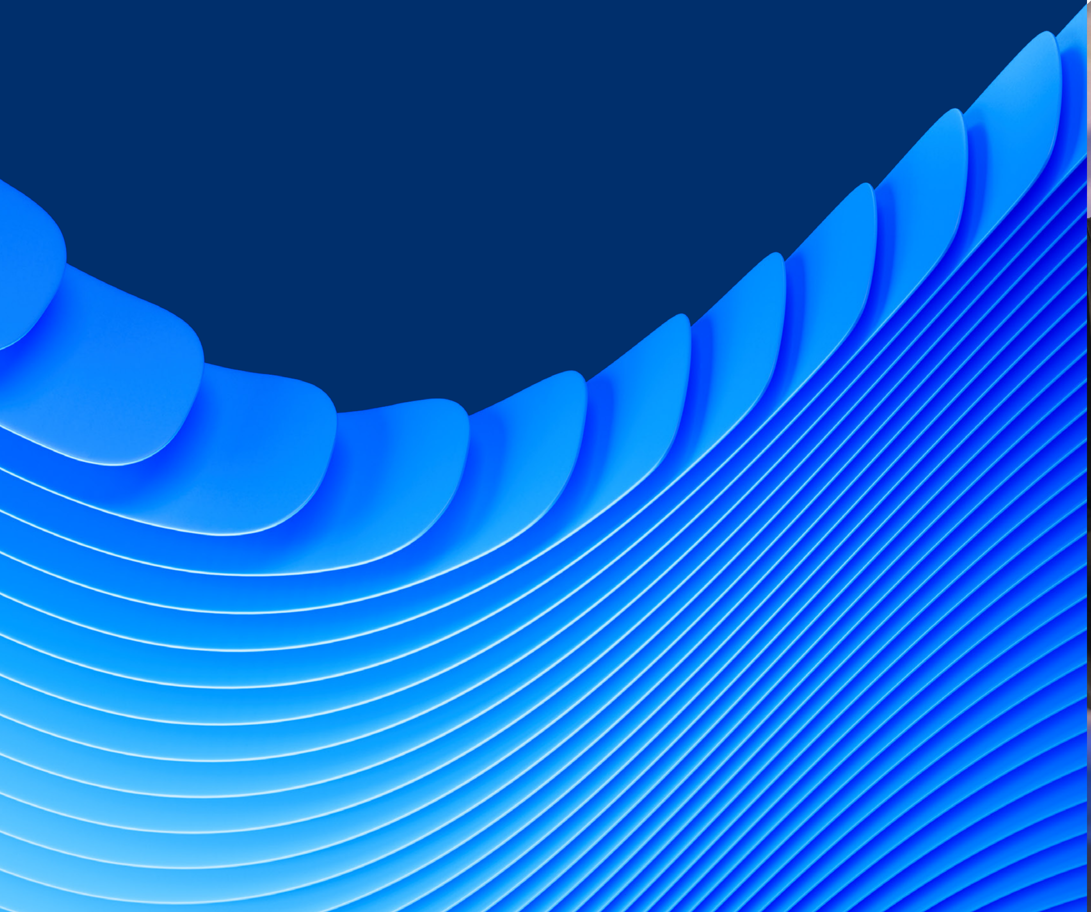
WHITE PAPER

Akamai mPulse Service

Compliance with Global Privacy Requirements



What is mPulse?

Akamai mPulse enables real-time performance monitoring and analysis of websites and online applications to help improve overall digital experience for your end users.

How does the mPulse service work?

JavaScript code, or an mPulse snippet, is inserted in the HTML of your websites to gather comprehensive data for measuring online performance. After configuration, the mPulse snippet collects mPulse beacons — invisible network requests that contain performance data and other page load characteristics — within seconds.

The performance data is converted in the mPulse dashboard into graphs and visual reports that show customers the real-time performance of their websites. The visualisation is available in the mPulse dashboard within a few minutes. Historical performance from data collected more than 24 hours ago is also displayed visually when available. Real-time data collection is supported with a cookie that stores session data for 30 minutes and technical data for 7 days.

You choose the types of data collected by the mPulse beacon:

- Performance timers, such as bandwidth and page load times
- Business metrics, including bounce rates, conversions, and order totals
- End-user metrics, like geolocation (at city level), device type, carrier speed, and application usage

Is mPulse compliant with data protection laws?

The Akamai mPulse service complies with all applicable data protection laws across the globe, including the EU General Data Protection Regulation (GDPR) and ePrivacy Directive, California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), Australian Privacy Principles (APPs), Singapore Personal Data Protection Act (PDPA), Argentina Personal Data Protection Law (PDPL), Japan's Act on the Protection of Personal Information (APPI), and many more. Akamai is committed to maintaining compliance with applicable data protection laws by applying privacy by design, including a variety of safeguards.

Privacy by design

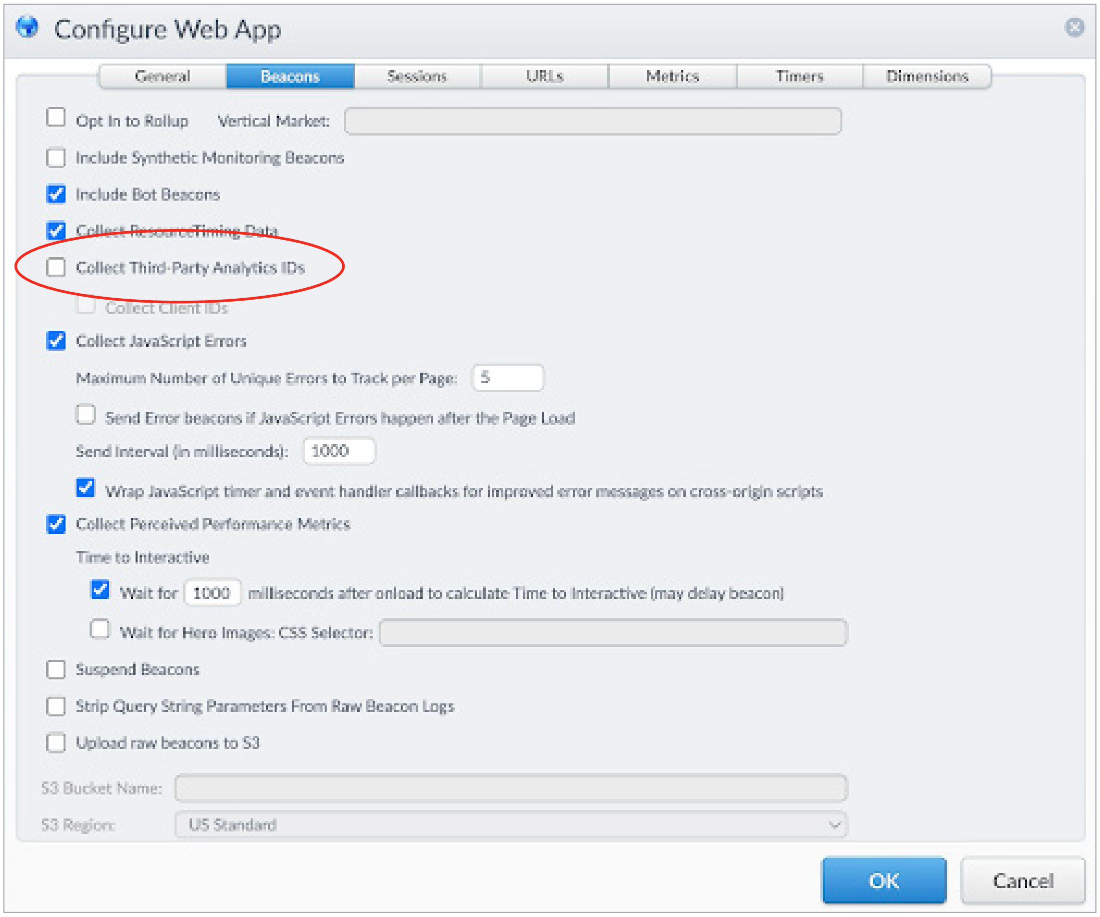
The mPulse service is designed in a privacy-friendly manner, and Akamai is permanently improving mPulse processing operations by applying data minimization.

As mPulse is a website performance service, the identification of individuals accessing the customer's website is not required for the service to operate. Thus, Akamai collects only the data absolutely necessary for website performance purposes and analyzes only website performances. It is doing neither profiling nor cross-site tracking on website visitors, neither for the mPulse service nor any other Akamai service.

Akamai continues to collect only data that is necessary for website performance analysis and has recently taken three additional steps to minimize data processing:

- Elimination of truncated IP addresses from the mPulse dataset
- Shortening the retention period for truncated IP addresses to 14 days in the system the data is stored in
- Reduction of the number of sub-processors used for mPulse service operations

Finally, Akamai maintains the ability for customers to uncheck the "Collect Third-Party Analytics IDs" box in the service configuration to further reduce the data collected.



□ Opt In to Rollup Vertical Market:

□ Include Synthetic Monitoring Beacons

☑ Include Bot Beacons

☑ Collect ResourceTiming Data

□ Collect Third-Party Analytics IDs

□ Collect Client IDs

☑ Collect JavaScript Errors

Maximum Number of Unique Errors to Track per Page: 5

□ Send Error beacons if JavaScript Errors happen after the Page Load

Send Interval (in milliseconds): 1000

☑ Wrap JavaScript timer and event handler callbacks for improved error messages on cross-origin scripts

☑ Collect Perceived Performance Metrics

Time to Interactive

☑ Wait for 1000 milliseconds after onload to calculate Time to Interactive (may delay beacon)

□ Wait for Hero Images: CSS Selector:

□ Suspend Beacons

□ Strip Query String Parameters From Raw Beacon Logs

□ Upload raw beacons to S3

S3 Bucket Name:

S3 Region: US Standard

Privacy and cookie management

The mPulse data is collected by Akamai on behalf of its customers.

In legal terms, this means customers act as data controllers (GDPR), businesses (CCPA), organizations (APPs and PDPA), information handlers retaining personal information (APPI), or the owners of a database (PDPL). Akamai in turn acts as a data processor (GDPR), service provider (CCPA), third party (APPs), another organization (PDPA), or the user of a database (PDPL).

Akamai publishes its data processing agreement covering these roles and related rights and obligations in the Akamai Privacy Trust Center.

The data processing agreement directs customers to the Cookie List for Akamai services that Akamai publishes for customers' cookie management purposes — as some Akamai services, including mPulse, are using cookie technology to collect data.

The mPulse beacon, a cookie technology, collects mPulse data. Akamai places the beacon on behalf of its customers as a first-party (the customers') cookie. Given Akamai's shared responsibility, customers are responsible for the service configuration, including cookie configuration and consent management. Akamai offers service configuration options, including consent management options for cookie technology where applicable, and is responsible for the operation of the services.

The mPulse cookie technology relates to website performance analysis, and the related consent management requirements vary by country. Akamai therefore offers the following configuration choices for the mPulse cookie technology to customers:

- The ***opt-in setup*** places mPulse cookie technology only in cases where an end user consented to its use.
- The ***opt-out setup*** places mPulse cookie technology when the website is loaded, unless an end user opts out.
- The ***no-choice setup*** places mPulse cookie technology when the website is loaded with no option to opt out, honoring a user's browser setting (e.g., "no session tracking" as browser setting is honored and no cookie technology is placed).
- The ***no data collection without opt-in setup*** places the mPulse cookie technology on the website, but data is collected only when an end user's consent is provided.

Akamai's "privacy by default" configuration for mPulse cookies ensures that:

- The data collected is limited to the absolute minimum required to perform website analysis
- The IP address is pseudonymized and discarded immediately once not needed anymore
- Individuals are not identified
- Individuals are not tracked across websites
- Individuals are not profiled
- Data processing is covered by Akamai's data processing agreement
- Customers can choose between configuration options to meet their performance analysis needs while meeting privacy requirements

Summary

The compliance of mPulse services with applicable data protection laws depends on the choices and activities of Akamai customers. When your organization uses the mPulse service, you determine the means and purposes of the data it collects and usage of cookie technology — and Akamai follows these instructions.

As a service provider, Akamai offers a variety of configurations for data collection and cookie management, and a data processing agreement to assist you in compliance with applicable data protection laws, in particular with transparency and consent management obligations. Akamai designed mPulse with privacy in mind, adhering to the “privacy by default” principle, and is always striving to improve its services and to minimize data collection and related privacy risks to customers.

For more information about data privacy, visit the Akamai Privacy Trust Center at akamai.com/compliance/privacy.