mPulse-Compliance with EU Data Protection Laws

Dr. Anna Schmits
EMEA Data Protection Officer, Akamai Technologies
CIPP/E, CIPM

What is the mPulse service?

Akamai offers its mPulse service to customers to enable them to monitor and analyze real-time performance of its websites and web applications to help improve the overall digital experience for its end users.

How does the mPulse service work?

For mPulse to do its job, a bit of JavaScript code (mPulse snippet) must be inserted (tagged) by the customer in the HTML of all websites. This avoids blind spots in the data as the customer's website end users move from tagged pages to untagged pages. After setup, mPulse starts to collect beacons within seconds. Live dashboards in mPulse are available with the customer's data within a few minutes of loading time for data in the waterfall dashboard and for historic data collected more than 24 hours ago. The live dashboard is supported by a session cookie, storing session data for 30 minutes and technical data for seven days.

Depending on the configuration by the customer of the mPulse beacons, the real-time monitoring data gathered includes:

- performance timers (bandwidth and page load times),
- business metrics (bounce rate, conversion rates, and order totals), and
- user metrics (user location, device type, carrier speed, and application usage).

In addition, the mPulse beacons collect the end user's IP address to perform geolocation and mapping on the edge servers. Thereafter, the IP address will be discarded if the privacy-friendly configuration is set up (see below). If not, the IP address will be transferred to the mPulse dashboard.

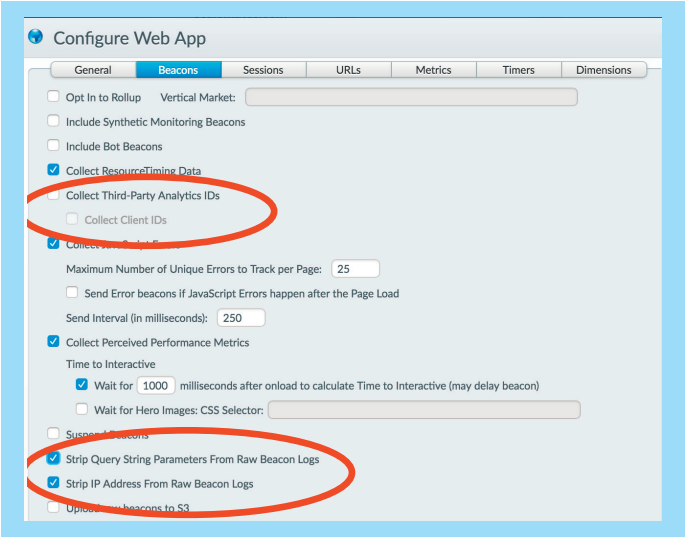
How does Akamai ensure EU data protection compliance?

Akamai's mPulse service complies with GDPR and other EU data protection laws. This is ensured by three safeguards that should be implemented in parallel:

Privacy-Friendly Configuration of mPulse

Akamai enables its customer to configure the mPulse service in a privacy-friendly manner in the mPulse portal, ensuring that the collection of personal data by the mPulse beacons is limited to the absolutely necessary, and deleted as early as possible after its collection:

The customer should uncheck the box "Collect Third-Party Analytics IDs". This will ensure that third-party analytics IDs (e.g., Google Analytics and unique Google client IDs) are not gathered by the mPulse beacons.



The customer should check the box "Strip Query String Parameters From Raw Beacon Logs". This will ensure that any personal data that might be included in the query string on the URL is discarded prior to being transferred from the edge server to the mPulse dashboard.

The customer should finally check the box "Strip IP Address From Raw Beacon Logs".

This will ensure that the IP address is discarded after the geolocation and mapping on the edge server is performed.

When these configurations are chosen, the data transferred from the edge server to the mPulse dashboard does not include personal data.

Data Protection Agreement

The mPulse beacons and cookie are so-called "first party" analytics techniques. As they collect personal data from the end users and transfer it to the edge servers, Akamai processes personal data when performing the mPulse services. The customer acts as a data controller and Akamai as

its data processor for this data collection. Akamai agrees on a data protection agreement with its customers to ensure the processing activities related to the provisioning of mPulse services comply with Article 28 GDPR.

Description of mPulse in Privacy Policy/Cookie Policy

To ensure a customer complies with its transparency requirement under GDPR, Akamai provides the customer with wording for implementation into its privacy policy or cookie policy to notify end users of the usage of the mPulse beacons and the cookie used to gather the real-time data.

In addition, Akamai has described its processing activities in its privacy statement, available at https://www.akamai.com/us/en/multimedia/documents/akamai/akamai-privacy-statement-july-2018.pdf.

Cookie Consent Exemption for mPulse

The mPulse beacons and the cookie are exempted from the cookie consent requirement under applicable EU data protection laws:

As stated by the Article 29 Working Party[1] in its guidance on cookie consent exemptions, first party analytics cookies and beacons are not likely to create a privacy risk when:

- they are strictly limited to first party aggregated statistical purposes
- they are used by websites that already provide clear information about these cookies in their privacy policy
  as well
- there are adequate privacy safeguards in place (opt-out mechanism and anonymization mechanisms for IP addresses)[2]

The Working Party recommends that "should article 5.3 of the Directive 2002/58/EC be re-visited in the future, the European legislator might appropriately add a third exemption criterion to consent for cookies that are strictly limited to first party anonymized and aggregated statistical purposes."[3]

Following and extending this guidance, the current draft of the e-Privacy Regulation dated July 10, 2018, exempts in Article 8 (d) web audience measuring from the consent requirement, provided that where the measuring service provider acts as a data processor, there is a data protection agreement in place.[4]

Akamai bases the processing of personal data gathered by the mPulse beacons on its legitimate interest to operate its business by offering its mPulse services. As Akamai puts a data protection agreement in place with its customers, complies with the applicable data protection principles, appropriately secures the personal data it processes, and has the required additional safeguards in place to ensure compliance with applicable data protection laws, its interest in providing the mPulse service is not overruled by the interest or rights and freedoms of the end users (the data subjects), which require protection of the personal data.

Summary

The compliance of mPulse services and its usage by the customer with applicable EU data protection laws depends on the cooperation of Akamai and the customer to ensure such compliance.

Akamai offers a privacy-friendly configuration of MPulse. The customer should implement such configuration to ensure that it complies with GDPR's principles (e.g., data minimization). Akamai requires that a data protection agreement is put in place with the customer to ensure the processing activities performed by Akamai relating to the mPulse service comply with GDPR. In addition, Akamai provides its customers with a statement as for the processing activities performed by the mPulse services, which the customer should implement into their privacy policy/cookie statement. Also, Akamai provides information about its processing activities related to the service in its privacy statement.

The privacy-friendly configuration, the data protection agreement, and the notification of the beacons and cookie usage to end users minimize the risks to the data protection rights of the end users. Consequently, no consent is required from end users to the beacons and cookie usage, and the processing of non-personal data by the beacons and cookie can be based on the legitimate interest to perform website analytics, which is not overridden by an interest or a fundamental right or freedom of an end user, which require data protection.

[1] The Article 29 Working Party was an advisory body made up of a representative from the data protection authority of each EU Member State under the EU Data Protection Directive. It has been renamed into the European Data Protection Board under GDPR.

[2] Doc. 00879/12/EN WP 194, WP 29 Opinion 04/2012 on Cookie Consent Exemption, adopted June 7, 2012, page 10, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

[3] Ibid.

[4] E-Privacy Regulation proposal draft document 10975/18 by the Austrian presidency of the Council of the EU, available at: https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/00/EU_30006/imfname_10827644.pdf.