Privacy Shield Policy Statement of Akamai Technologies, Inc.

Other Covered Entities: Janrain, Inc.

Effective: August 30, 2016

Akamai Technologies, Inc. (“Akamai”), including its wholly-owned subsidiary Janrain, Inc., and its other wholly-owned subsidiaries, complies with the EU (which shall include the United Kingdom in the event of Brexit) and US Privacy Shield Framework, including the Supplemental Principles, and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce (collectively, the “Principles”). Akamai has certified that it adheres to the Principles with respect to its services and the collection, use, and retention of certain Personal Data (as defined below) transferred from the European Union (“EU”) and Switzerland to Akamai in the United States (“U.S.”). This Policy sets forth the standards under which Akamai will treat such Personal Data. To learn more about the Principles and to view Akamai’s certifications, please visit: https://www.privacyshield.gov/.

U.S. Federal Trade Commission Jurisdiction

Akamai’s commitments under the Principles are subject to the jurisdiction and enforcement and investigatory authority of the United States Federal Trade Commission.

Required Disclosure

Akamai may be required to disclose Personal Data to the extent required to meet a legal obligation, including national security or law enforcement obligations and applicable law, rule, order, or regulation.

Definitions

"Data Subject" means the individual to whom any given Personal Data covered by this Policy refers.

"Personal Data" means information relating to an identified or identifiable natural person residing in the EU or Switzerland. If the information has been irreversibly stripped of all identifiers such that an individual cannot be identified or re-identified, it is not Personal Data.

"Sensitive Personal Data" means Personal Data regarding any of the following:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Health or medical condition; or
- Sex life.

Scope

Akamai provides solutions for delivering, optimizing and securing online content and business applications. In connection with providing these solutions to its business customers, Akamai generally serves as a conduit for the web properties it delivers and secures -- it is Akamai’s customers (and visitors to their web sites) that control the actual data, including Personal Data within

the web properties transmitted across the Akamai platform (e.g. messages, login information, financial data, website graphics, photos, etc). This Policy applies to the collection, use, and disclosure in the U.S. of Personal Data transferred from the EU or Switzerland to Akamai in the U.S. of: (i) internet end users who visit our business customers' websites and applications (with respect to which Akamai generally serves as a conduit), (ii) internet end users of Akamai's own websites and applications, and (iii) business contact information associated with our business customers.

Data Processed

In the context of providing solutions to its business customers and the Internet community, Akamai collects and processes certain data elements relating to the traffic on its network, including, Internet Protocol Addresses (IP Addresses), network, browser and device behavior data, DNS log data, and website performance data derived from browser activity on a website. To the extent that such data is capable of being used to identify (alone or in conjunction with other data, an individual), it is treated as Personal Data under this Policy. In addition, Akamai collects, uses, and discloses Personal Data of users of Akamai's own websites and applications, as well as contact information associated with our business customers -- such data is processed in accordance with Akamai's Privacy Statement.

Purposes of Data Processing; Disclosure to Third Parties; Choice

Akamai processes data that is transferred from the EU or Switzerland to Akamai in the U.S. for purposes of: providing, maintaining, protecting, developing, and improving the solutions it offers to its business customers; detecting and preventing potential fraud and security risks; and supporting Akamai's internal business operations (e.g. billing).

Akamai may use from time to time a limited number of third-party service providers, contractors, and other businesses to assist Akamai in providing its solutions to customers or in meeting internal business operation needs. These third-parties may access, process, or store personal data in the course of performing their duties to Akamai. Akamai maintains contracts with these providers restricting their access, use and disclosure of Personal Data in compliance with our obligations under the Principles.

Accountability for Onward Transfer

In the event Akamai discloses Personal Data covered by this Policy to a non-agent third party, it will do so consistent with any notice provided to Data Subjects and any choice they have exercised regarding processing and disclosure. Akamai will only disclose Personal Data to third parties that have given us contractual assurances that they will provide at least the same level of privacy protection as is required by this Policy and the Principles and that they will process Personal Data for limited and specific purposes consistent with any consent provided by the individual. If Akamai has knowledge that a third party to which it has disclosed Personal Data covered by this Policy is processing such Personal Data in a way that is contrary to this Policy and/or the Principles, Akamai will take steps to prevent or stop such processing. Akamai complies with the Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

Security

Akamai has put in place technical and organizational measures to protect Personal Data covered by this Policy from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

These measures take into account the risks involved in the processing, the nature of the Personal Data, and the state of the art and best practices in the industry for security and data protection.

Data Integrity and Purpose Limitation

Akamai will only collect Personal Data covered by this Policy that is relevant for the purposes for which it is to be used, and only use such Personal Data in a way that is compatible with the purposes for which it was collected or subsequently authorized. Akamai will take reasonable steps to ensure that such Personal Data is accurate, complete, current and reliable for its intended use.

Access

Data Subjects have the right to access Personal Data about them that is covered by this Policy and to correct, amend, or delete such Personal Data if they can demonstrate that it is inaccurate or incomplete (except when the burden or expense of providing access, correction, amendment, or deletion would be disproportionate to the risks to the Data Subject's privacy, or where the rights of persons other than the Data Subject would be violated). Data subjects may also provide instructions, including withdrawal of consent theyu may have given, regarding the processing or disclosure of such data.

Data Subjects may make requests by filling in Akamai's consent management form at https://app.onetrust.com/app/#/webform/b547fd1a-9fdd-4123-a7f0-d23482defb5f. Data Subjects should note that before Akamai is able to provide them with any access to information, correct any inaccuracies, or delete your personal data, Akamai may ask the Data Subject to verify the identity and to provide other details to help Akamai to respond to the request. Akamai will contact a Data Subject within 30 days of a request.

Enforcement; Recourse

Inquiries and complaints relating to Akamai's treatment of Personal Data and its compliance with the Principles may be directed to:

privacy@akamai.com

or

Akamai Technologies, Inc.
145 Broadway
Cambridge, MA 02142
Attention: Chief Privacy Officer

Akamai will respond to any such inquiries or complaints within forty-five (45) days. In the event that Akamai fails to respond or its response is insufficient or does not address the concern, Akamai has registered with JAMS to provide independent third party dispute resolution at no cost to the complaining party. To contact JAMS and/or learn more about the company's dispute resolution services, including instructions for submitting a complaint, please visit: https://www.jamsadr.com/eu-us-privacy-shield. Complaining parties may also, in absence of a resolution by Akamai and JAMS, seek to engage in binding arbitration through the Privacy Shield Panel.

Akamai will cooperate with the United States Federal Trade Commissions and any data protection authorities of the EU Member States ("DPAs") and/or the Swiss Federal Data Protection and Information Commissioner ("Commissioner") in the investigation and resolution of complaints that cannot be resolved between Akamai and the complainant that are brought to a relevant DPA.

Akamai also commits to periodically reviewing and verifying the accuracy of this Policy and the company's compliance with the Principles, and remedying issues identified. All employees of Akamai that have access to Personal Data covered by this Policy in the U.S. are responsible for conducting themselves in accordance with this Policy. Failure of an Akamai employee to comply with this Policy may result in disciplinary action up to and including termination.

Last Updated: April 8, 2020