Identity Cloud Service Privacy Statement

Effective as of March 1, 2019

This Privacy Statement explains how Akamai Technologies, Inc., and any of its affiliates (collectively "Akamai") processes your personal information when providing our Cloud Identity services to our customers.

For information about

- any other processing activities performed by Akamai (e.g. in the course of the provisioning of other services to our customers, when you are visiting our websites, when we marketing to you or when we perform recruitment services to you),
- about how to contact us,
- contact details of our supervisory authority
- how to file a complaint

please read Akamai's main privacy statement at: https://www.akamai.com/us/en/multimedia/documents/akamai/akamai-privacy-statement-july-2018.pdf.

1. Our Role and Practices Related to Client Data when Providing our Identity Cloud Services

As a provider of Identity Cloud services, we receive and host on our customers' behalf such personal information and other data which our customers may provide to us in the course of the provisioning of our Identity Cloud services to them (collectively, "Client Data"). Our customer are the data controllers of Client Data and we are the data processor for each of our customers with respect to Client Data. In processing personal information on behalf of our customers, we follow their instructions with respect to the information they control. We do not determine how our customers collect and use Client Data, and we will not access or disclose Client Data except as directed or agreed to by our customers or required by law.

Akamai acknowledges that you have the right to access your personal information that is Client Data. Nevertheless, we do not have a direct relationship with you and do not know what personal information of you we process when providing our services

to the customers. As you have the relationship with our customers and they control your personal information, please contact the customer that you interact with directly to enforce your rights as a data subject.

Depending on the customers' configuration of our services, our customers can access, and delete Client Data, including an individual record, via an application provider interface or API. If requested by a customer to remove/access personal information we will respond within thirty (30) days. Following the deletion of personal information in a database we host, the related backup data will be deleted, generally within ten (10) days.

To comply with our legal obligations, resolve disputes, and enforce our agreements we will retain your personal information as necessary and may deny a customer's request to delete Client Data.

We will retain your personal information we process on behalf of our customers for as long as needed to provide services to our customers. In addition, as stated, we retain your personal information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

We transfer personal information to our suppliers that help us provide our Identity Cloud service:

- **Amazon Web Services, Inc.**, 1200 12th Avenue South, Suite 1200Seattle, WA 98144, USA, used for hosting services
- **Looker Data Sciences, Inc.**, 101 Church Street Santa Cruz, CA 95060, USA, used for data analytic services*
- **CI&T, Inc.**, 25 Broadway, Suite 10-069 New York, NY 10004, USA, used for support services
- **Ciklum group**, Amosova Str. 12, BC Horizon Park, 03038 Kyiv, Ukraine used for support services

*Looker Data Sciences, Inc., is only acting as a subprocessor if customer, while utilizing the Identity Cloud customer insights tool, requests a production of Personal Data underlying a report. Otherwise this entity is not acting as a subprocessor.

The transfer to such suppliers is covered by a data processing agreement with these suppliers, including the EU Model Clauses and or a privacy shield reference, where applicable, and by the service agreements with our customers.

Notice and Choice: You submit personal information to our customers through the use of the website registration and login services we provide to our customers. (Some of these services may have a notice that they are "powered by Akamai's Identity Cloud Services"). This personal information is submitted with notice to, and the consent of, you as the individual user via identity providers' permission screens, or voluntarily provided by you at registration. Once Akamai has successfully facilitated the transmission of personal information to a customer's database that is not hosted by Akamai's supplier, it is that customer's responsibility to guard the personal information against unauthorized access or transmission.

Cookies Related to Our Social Login Service

The following table shows how cookies are placed on user browsers in connection with our Social Login service. Each is required to deliver critical functionality or complete the users' service requests.

Type	Cookie Name	Created	Stored Data	Usage
Session	login_tab	When the user clicks on a social sign-in link	Identity provider name or identifier	Records which identity provider has been selected by the user, for use during the transaction
Session	expected_tab	After a successful social sign-in transaction	Identity provider name or identifier	Records which identity provider has successfully authenticated the user, for use during the transaction
Permanent	welcome_info_name	After a successful social sign-in transaction	Display name of user as returned by identity provider	Retrieves a display name for providing visual confirmation to end user

An individual using our Single Sign On service will have three cookies placed on his or her browser: session_id; visited; and janrain_sso_checked <domainspecifier>. These cookies are required to enable the service.

Statistics

To assist our customers and partners, and to market our services, we may disclose aggregated, statistical information related to the use of our services by some or all of our customers and their users. Such information will not contain any personal information or identify any customer or user of our services.

2. Our Policy Towards Children

Our Identity Cloud services are not directed at persons under 16. Children are not eligible to use our websites and we do not knowingly collect personal information from children under 16. If you become aware that your child has provided us with personal information, without your consent, please contact us at privacy@akamai.com so that we can take steps to delete your child's information and terminate any account your child has created with our customers using our services.

3. Security

Akamai uses appropriate technical, operational, and administrative safeguards to help protect the security, confidentiality, and integrity of the personal information and other data submitted to us by our customers. We cannot guarantee, however, that data may not be accessed, disclosed, altered, or destroyed by a breach of our safeguards. The security of your personal information also depends on your protection of your account. Please do not disclose your website login credentials to unauthorized people. Also, be sure to sign off when finished using a shared computer.

4. Cross-Border Data Transfers and Privacy Shield Notice

We process personal information both inside and outside of the United States when providing our Identity Cloud services to customers and rely on legally-provided mechanisms to lawfully transfer data across borders. These mechanisms include the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and European Commission-approved standard contractual data protection clauses to safeguard the transfer.

Privacy Shield Notice

For its Identity Cloud services Akamai participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. Akamai is committed to subjecting all personal data received from European Economic Area (EEA) and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce's Privacy Shield List: https://www.privacyshield.gov/list.

Akamai is responsible for the processing of personal data it receives, under each Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. Akamai complies with the Privacy Shield Principles for all onward transfers of personal data from the EEA and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Akamai is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission.

In certain situations, Akamai may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider Trust Arc group (free of charge) at https://feedback-form.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield website https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint, you are entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.