Liferay Analytics Cloud

Data Privacy and Security Overview

Introduction

Liferay Analytics Cloud tracks customer profile and behavioral data, bringing them together into a unified view of the customer. Together, these elements help businesses transcend data silos and provide personalized experiences to their customers.

While these capabilities enhance understanding of customer behavior, they can also introduce data privacy and security questions for Liferay customers. This document aims to provide guidance around the key concerns regarding data security and handling within Liferay Analytics Cloud.

Legal Resources

When engaging in prospect/customer conversations, please be attentive to the following guidelines:

- For DXP customers purchasing Liferay Analytics Cloud as an add-on to on-prem based DXP; the relevant terms are set forth in the "Terms of Service" incorporated into the Subscription Appendix (Appendix 1).
- For DXP Cloud customers, the relevant terms are in Sec. 11 of the DXP Cloud Appendix (Appendix 4).
- For the purpose of GDPR compliance, our terms incorporate a DPA (Data Protection Addendum) which governs how we process data in accordance with GDPR requirements.
- All documents are available at https://www.liferay.com/legal.

Top Five Things to Consider for Data Security

1. Data Hosting

There are three areas to consider for questions around data hosting: Transmission and encryption, the hosting provider, and the available data center regions.

Secure Transmission and Encryption

Liferay Analytics Cloud encrypts data at the transmission level and the infrastructure level (where data at REST is hosted).

Data transmission occurs with forced encryption via HTTPS with TLS 1.2 protocol. On the infrastructure layer, data at REST is protected behind a private network and encrypted by the hosting environment provider with 128-bit GCM block ciphers and a 256-bit symmetric key (AES_256_GCM). The network is protected by robust firewall and inbound/outbound port configurations. The load balancer is monitored for DDOS attacks and inappropriate activity.

Liferay has a formal encryption policy that is defined by its infrastructure security committee and regularly revised to adapt to customer needs over time.

Data Isolation

By default, Liferay Analytics Cloud runtime and data at REST are separated per customer workspace.

Hosting Provider

Liferay Analytics Cloud (AC) is installed on top of Liferay DXP Cloud running on Google Cloud Platform (GCP), operated by Google Ireland Limited, Dublin, Ireland. Customer data will be saved in any of our data centers setup for Analytics Cloud, with the option for customers to choose which region their data will reside in.

Available Data Center Regions

The available regions for Analytics Cloud are Oregon (USA), São Paulo (Brazil), London (United Kingdom) Frankfurt (Germany) and Mumbai (India).

Data Availability

Liferay Analytics Cloud has an active Disaster Recovery (DR) and Business Continuity Plan (BCP) in place to support the product and ensure that business processes continue during a time of emergency or disaster.

2. Access Control

Monitoring who has access to your digital project and what their permissions are within the system is a critical part of maintaining data security. Liferay Analytics Cloud has a built-in access and privileges management tool to let workspace owners manage individual access and define permissioning.

Analytics Cloud users can only see workspaces they have been invited to within the company. Within each workspace, individuals can be granted Owner, Member, or Admin access by a Workspace Owner or Admin. A user can be deleted at any time by the Workspace Owner or the Admin. User accounts to access Analytics Cloud are created when users first access analytics.liferay.com.

All workspaces are protected by a Multi-Factor Authentication system provided by a third-party system (Okta).

On the infrastructure level (where the database and service account live), access is restricted to Analytics Cloud personnel only. No Liferay employee has access to the data stored in each customer workspace unless they have explicit consent from the customer.

To learn more, read the User Administration documentation for Analytics Cloud >

3. Information Security Policies

Liferay Analytics Cloud has a Security Committee that is responsible for designing, implementing, reviewing, and promoting internal policies and security standards.

At the infrastructure layer, monthly evaluations are performed for disaster recovery, security event monitoring, internal audits for security objectives, asset access compliance, and supplier agreement/compliance. In addition, the infrastructure undergoes routine evaluation from third-party auditors including penetration/hardening testing and ISMS certifications (SOC 2, ISO 27001). A full list of our technical and organizational security measures is available here.

In case of an incident, customers may use the following channels to contact Liferay: official email communication and Liferay's Help Center (reactive based on a ticket opened by the customer).

4. Data Minimization

The principle of data minimization involves limiting data collection to only what is required to fulfill a specific purpose. When an organization applies data minimization, any processing (the analysis of data to produce meaningful insight, for instance) will use the least amount of data necessary to accomplish the task. In Liferay Analytics Cloud, interaction data (page visits, clicks, scrolls, and other events) is pseudonymized by default. Interaction data is only merged with the data identifying an individual when the data reaches the cloud infrastructure layer, which requires a customer’s proactive action. This means that by default no personal data is exposed externally or transferred by any means. Individuals’ identity syncs are performed directly from the customer’s DXP and cloud instance. Additionally, all the data is transferred with HTTPS encryption to the cloud.

5. Data Retention

Liferay Analytics Cloud retains data for a period of 13 months by default. Customers can change the retention period in the control panel of the application settings to seven months. If they need data to be retained for more than 13 months, they can get in touch with Liferay Analytics Cloud Customer Support and define a custom retention period.

Furthermore, Liferay retains all data for 30 days after the expiration of a customer’s contact. Within 14 days from the end of a customer's subscription they have the option to request access to this data, which will be provided for the purposes of data retrieval for another 14 days. All data will be irretrievably removed 30 days after the expiration of a customer’s subscription.

Other Common Questions

What types of data does Analytics Cloud capture, process, and store?

Client-side browser data

The following data is captured and processed on the client side by a browser and is never captured or stored by Analytics Cloud service:

- **Browser Local Storage:** Liferay Analytics Cloud uses JavaScript to generate a unique anonymous visitor ID and stores it in the browser’s local storage.
- **Browser Cookies:** Liferay Analytics Cloud adds a first-party cookie to the set of cookies used by Liferay DXP customers. Liferay Analytics Cloud does not use cookies to process the data that is shown on reports.

Analytics Cloud service:

The following data is captured on the client side by a browser to be processed and stored inside Analytics Cloud service:

- **Events Data:** Liferay Analytics Cloud uses client side JavaScript to track visitor interaction data taken from visitor activity with Liferay DXP. This includes data related to Clicks, Scroll Depth, Views, Downloads, Submissions, and Page Loads. The interaction data is sent to Analytics Cloud services for reporting.
- **Geolocation and Technology Data:** Liferay Analytics Cloud service third-party libraries to determine two kinds of data: visitors’ geolocation and the technology (type of

browser, operating system) based on the captured Events Data. In order to ensure that no visitor data is exposed outside of Liferay Analytics Cloud, the library is hosted and run internally.

- **PII Data/Personal Data**: Personally Identifiable Information (PII) is a category of sensitive information that is associated with an individual person, such as an employee, student, or donor. All data, including PII, is encrypted via HTTPS in transmission; stored data is encrypted on the backend.
    - For Unauthenticated Visitors, Liferay Analytics Cloud tracks IP addresses and browser session information.
    - For Known Individuals/Authenticated Visitors, Liferay Analytics Cloud only requires an email address to be tracked as an identifier field for that visitor. All other PII will be up to the Liferay Analytics Cloud customer's own choice to sync (or not) to AC. For instance, if the customer doesn't wish to sync first name, address, and phone number into AC, the data mapping interface will allow the customer to remove these fields and AC will stop tracking these attributes from their data sources.
- **Individual Profile Information:** On top of tracking analytics event data from website visitors, Liferay customers can also enrich individual profile information with information stored in Liferay DXP, Salesforce, or through a CSV file import. This allows Liferay customers to aggregate behavior data and profile data, and help them understand their website visitors better. Any profile information imported into AC can be used to create multidimensional audience segments for more accurate personalization.

Which privacy regulations do you comply with?

In order to understand how Liferay helps companies comply with privacy regulations, it's important to understand the differing roles of the Data Processor and Data Controller.

With regard to the personal data processed through Analytics Cloud, Liferay is a Data Processor. Once data has been processed within Liferay Analytics Cloud, ownership of the data belongs to our customers, making them the Data Controller. The Data Controller is ultimately responsible for complying with privacy regulations, as they go beyond the scope of how software like Liferay handles data.

Although Liferay is not a Data Controller, AC has implemented capabilities to help our customers in their journey towards compliance. This includes tools to anonymize and export data, control the data retention period, and delete subject data.

Are customers notified immediately in the event of a security breach?

Liferay respects multiple data privacy regulations and will follow the appropriate timeline in the event of a security breach. Liferay's policy outlines an approach model for responding to and mitigating a data breach, security weakness, or a security incident involving the availability, integrity, or confidentiality of personal, restricted, or confidential data. Additionally, this document lays out the general principles and actions for successfully managing the response to an incident as well as fulfilling the obligations surrounding the notification to Data Processors, supervisory authorities, and individuals as may be required by local regulation.

Do you provide secure data deletion functionality in the event of service termination?

Yes, Liferay Analytics Cloud has established a set of processes for the secure deletion of all customer data in the event of service termination.

Conclusion

Data Privacy and Security requirements are critical to the success of any Liferay Analytics Cloud project. For more information, please contact sales@liferay.com or visit liferay.com/analytics.