Data Processing Terms

Effective date: 29 January 2020

1. Client is responsible for making sure that End-User Data does not contain Sensitive Data. Personal Data such as but not limited to name, age and email address can be sent if Client has explicit consent from Data subject. End-User Data sent by integration libraries to connect Client's product with Service, such as, but not limited to using (cookie based) user identifiers, IP address (which is anonymized and not stored "in rest"), browser/device info, and all other necessary to fulfill Service to Client, needs explicit consent from the Data Subject where necessary, such as where GDPR legislation applies. Any extraneous or accidental tracking of Personal Data or Sensitive Data can be removed by Stormly data removal tools, see next point below.

2. End-user Data can be removed by opening the Stormly application and using the "Data Management" page. Automatic End-User Data removal can also be done programmatically using the API, as described in the "Data Management" page. For more details see the "Data Management" page within the Stormly application.

3. Stormly accept no liability whatsoever for Sensitive Data, whether in connection with a Security Incident or otherwise.

4. Deployments, Plugins, Intelligence results, reports or insights ("Results") are normally constructed as generalized models or reports that should contain no Personal Data. But it is technically possible to create models or reports that do have Personal Data embedded, for example a machine learning model that knows when your name is "John Doe" it should recommend "jeans". Stormly will not be responsible that Results may contain Personal Data. The client is responsible for making sure such data is not tracked and not used directly in Results. Client needs to make sure Personal Data is removed when Data Subject submits data removal requests. Stormly provides the necessary data removal tools.

5. To generate Results, snapshots of raw user and event data is needed. These snapshot datasets may contain Personal Data, depending on whether Client is tracking such data and sends it to Stormly; Client is responsible for collecting consent to do so. Snapshot datasets are only kept as long as is necessary to generate Results. This can be from a minute up to a few days, but afterwards those are automatically removed. If Data Subject decides that they don't want to be tracked, they may still be in this snapshot data, but will automatically be removed after the Results are not needed anymore.

6. Stormly needs data from Data Subjects so that Stormly can analyze this data and generate Results. This is done through tracking or importing data. For more information on what is exactly tracked, see the "Data Processing Agreement".

7. Stormly has a maximum retention period for Client data of 36 months, or less depending on the Client's Subscription plan.

8. Stormly reserves the right to present and use, for Stormly's or Client's business purposes, aggregate categories of End-User Data such as but not limited to: conversion rates, absolute number of users, revenue per user, internet browser usage, rates or generally any averaged measure, in such a way that these aggregates cannot be linked to Client. These may be used for, but not limited to, benchmarks and industry level reporting.

Pricing

Try For Free

Schedule a Demo

Reports

Data Integration

Stormly vs. Amplitude

Stormly vs. Google Analytics

Stormly vs. Pendo

Stormly vs. Heap

Stormly vs. Adobe Analytics

Stormly vs. Power BI

Stormly vs. Tableau

Stormly vs. Looker

Privacy Policy

Data Processing Agreement

Terms of Service

Contact us

AI-powered analytics platform