braze
FORMERLY APPBOY

GDPR Compliance FAQ

Is Braze GDPR compliant?

Braze is materially compliant with the European General Data Protection Regulation ("GDPR"). As part of Braze's GDPR implementation plan, Braze is actively involved in partnering with its customers to ensure that they understand how the Braze Services enable customers to comply with their extensive obligations as Data Controllers under the GDPR.

Does Braze have data centers in Europe?

Braze offers its customers the option to store their data either in the United States or in Europe. Braze uses AWS as its hosting provider. In Europe, the data is hosted in Frankfurt, Germany, with back-up in Ireland. Braze will not transfer for storage the Personal Data of any of its customers from the country where it is originally stored, in conformance with customer's instructions as the Data Controller.

Does Braze have any customer-facing documentation about its GDPR compliance?

Yes. Braze has materials on its website, including a new GDPR-compliant Privacy Policy. Braze continuously updates the materials on its website to enable its customers to understand how Braze processes personal data and the ways that the Braze Services enables its customers to comply with GDPR.

How did Braze technically implement the right of rectification, right of erasure, and right of access?

Braze fully understands and supports the requirements of the GDPR which give Data Subjects control over their Personal Data. In fact, Braze's focus, as a Data Processor, was to automate, as much as is technically feasible, the ability of its customers, as Data Controllers, to respond to requests from Data Subjects. For example, Braze has updated its Services to enable its customers to identify individual end users within the Services. This enables compliance by our customers with their end users' right of rectification, right of erasure and right of access. We updated our SDKs to enable data subjects to request a halt to the processing of their data.

Can customers use Braze to track the explicit consents needed for processing of Personal Data under the GDPR?

Braze can be used by its customers to send targeted messages to the end users of the customer's app or website. Customers, as Controllers, will determine the content of their messages, the audience to receive the messages, and the particular use case of the Braze Services. Customers can configure the Braze Services to track consents to processing (as required by GDPR) .

Is Braze a Data Processor or Data Controller?

With respect to the use of the Braze Services by Braze's customers, Braze's customers are the Data Controllers, and Braze is the Data Processor. As such, Braze will follow the instructions of its customers in connection with the processing of personal data. Braze is a Data Controller for data it collects from its EU employees and, with respect to EU data subjects, from visitors to the Braze website, or other personal data that we may collect in connection with our marketing programs.

Exactly how will Braze implement the right to restrict processing of specific categories of data of EU data subjects?

The Braze Services can be configured by customers to cease processing the data of a particular data subject. The Braze Services, however, cannot freeze the processing of specific categories of data for a single data subject. If a data subject wishes to halt the processing of certain categories of data, customers are able to halt the processing of all data for that data subject, but the Braze Services cannot technically distinguish between specific items of data.

Does the GDPR apply to data collected prior to May 25, 2018 (the day that the EU Data Protection Authorities began enforcing the GDPR)?

Yes. Under the GDPR, EU data subjects have control over their personal data, regardless of when the data was collected.

What data can customers collect from EU data subjects and what data can customers not collect?

The GDPR does not limit the types of personal data that can be collected. Instead, the GDPR requires companies that are collecting that data to demonstrate "Data Security by Design" – a dedicated policy that evidences sound principles of security designed to protect that personal data from unauthorized access, use or other types of processing. Braze protects all data that it collects from its customers to the highest standards and in connection therewith, has completed its SOC 2, Type 1 audit, is undergoing its SOC 2, Type 2 audit, and is currently working towards ISO 27001 certification.

Is there a way to "turn off" the Braze SDK at an individual user level?

Yes. The Braze Services can be configured by customers to stop processing the personal data of an individual.

How will Braze enable its customers to stop collecting personal data from an EU data subject who has either not given consent to the processing of their personal data or has withdrawn consent to such processing?

Our customers, as Data Controllers, are responsible for obtaining and documenting consent from EU data subjects to the processing of their personal data. The Braze Services can be configured by our customers to cease the collection of personal data from an individual data subject who has not given consent, or has withdrawn consent, to such processing.

Do the Braze Services (i) restrict personal data from being available to employees who don't need it in their role, (ii) enable the deletion of all personal data about a consumer upon request (including in third party services), and (iii) record the dates on which marketing consents were changed?

Personal Data within the Braze Services can only be accessed or processed by Braze employees who have a need to access or process that personal data to provide the Services, to provide support, as required by law, or as directed by the customer. Customers have the ability to export or delete all personal data about a particular end user from the Braze Services. Third parties chosen by customer whose services are used in connection with the Braze Services are, like Braze, data processors with customer being their Data Controller. As such, those data processors must comply with requests made by customers on behalf of their data subjects, to delete that data subject's personal data. It is important to note, however, that Braze has no involvement in those relationships between customers and their third-party providers. Braze does require that its sub-processors are able to comply with the requirements of the GDPR and has written contracts in place with each Braze sub-processor to enforce this requirement. Under the GDPR, Braze's customers, as Data Controllers, are responsible for keeping records of the dates on which consent was given or revoked.

How do the Braze Services ensure that a data subject who has asked to be forgotten is excluded from all further processing?

With respect to collection of data, when a data subject asks to be forgotten on the web, the Braze Services drops a cookie that recognizes that anonymous end user as an end user who has exercised its right to be forgotten. Without that cookie, there is no way for the Braze Services to know that that particular end user does not want their personal data to be collected or processed. The Braze mobile SDKs offer similar capabilities to cease processing of data. If, however, that particular end user clears their cookies in their browser,

gets a new mobile device, or uninstalls and reinstalls the app again, the opt-out tracking identifier will no longer be effective and the Braze Services will not be able to recognize that end user as an end user who has asked to be forgotten. The end user will have to opt out again.

Braze customers, as Data Controllers, are responsible for ensuring that the data subject is then removed from the Braze Services via an API call to the Braze Services, to delete the user profile of that data subject. Braze will not be able to identify if a 'forgotten' user subsequently attempts to log into or re-register with the customer's app or service — to address this, customers may refuse to allow login or obtain positive confirmation that the user consents to being remembered. The Braze Services cannot create blacklists of user identifiers or email addresses on behalf of customers.

How does Braze ensure that its sub-processors are also in compliance with GDPR?

Braze is responsible for the acts and omissions of its sub-processors and is responsible for ensuring their compliance with GDPR.

Does GDPR mandate any suppression of data capture or processing based on age?

Braze cannot provide legal advice to its customers. If a customer has a question about whether the GDPR requires certain actions, it should seek the advice of its counsel.

Will the GDPR impact data being transported out of the EU?

The GDPR does have a provision requiring appropriate safeguards for the transfer of personal data to a third country. Braze validates the transfer of personal data from the EU to the United States by entering into the Standard Contractual Clauses (Model Clauses) with its customers upon request.

This is a set of contractual commitments signed by the Data Controller (customer) and the Data Processor (Braze).

Pursuant to the Model Clauses, Braze agrees to apply data protections that are more stringent than those required by US privacy laws.

How will the user profile lifecycle be impacted by the GDPR?

Customer Data Controllers may only process the personal data of EU data subjects for so long as, and for the explicit purpose, for which the data subject gave its consent.

In what format will Braze make data exports available to end users of customers?

Customers can export any and all data from the Braze Services.

How customers make that data available to end users is up to customers, as the Data Controllers, and is not related to the Braze Services, or Braze's responsibilities as the Data Processor. If customers are not sure what is required by the GDPR, they should seek the advice of their legal counsel.