Request or delete records for EU General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA)

Skip Ahead

- Your access and deletion obligations
- Submit a GDPR or CCPA access or deletion request through the Optimizely UI
- Automate GDPR or CCPA requests with the Optimizely REST API
- Retrieve the data from a completed access request
- Confirm data deletion
- Rectification Requests
- Disclaimer

THIS ARTICLE WILL HELP YOU:

- Submit GDPR or CCPA Access or Deletion Requests

This article describes how Optimizely can help you respond to an EU or California data subject’s request for access, rectification, erasure, or portability of their personal data. Please read this article carefully to understand how we can help you respond to such requests for the data Optimizely is processing on your behalf, and the implications for your organization.

Please keep in mind that:

- Data cannot be recovered once it has been deleted. Read this article carefully to understand the implications for your account.

- Data exports may contain information that your company considers confidential, such as the change history for a particular project. It is your responsibility to review this information before providing it to the requestor.

- This process covers information that Optimizely processes on behalf of its customers as part of its online SaaS
services. If you would like to file a request related to personal data that Optimizely controls, you should email privacy@optimizely.com. Please review our privacy policy for more information about this type of data and your options.

It is your responsibility to review this information before providing it to the requestor.

To learn more about the data Optimizely processes, please review our Privacy@Optimizely FAQ. To learn more about your role as a data controller, or for more detail about meeting your privacy and data protection obligations for other Optimizely products, see our Privacy and Data Protection page.

Your access and deletion obligations

Under the EU's General Data Protection Regulation (GDPR), each EU citizen has a right of access to their personal data. Upon request, you (as the data controller) have an obligation, with certain exceptions, to inform the individual (often referred to as data subjects under GDPR) where their personal data is being held and for what purposes. In addition, each EU citizen has a right to erasure (sometimes known as the right to be forgotten). Upon request, you have an obligation, with certain exceptions, to delete the personal data of a data subject.

The California Consumer Privacy Act (CCPA) provides similar access and deletion rights to California residents.

To make the process easy for our customers, Optimizely offers two options for customers who receive a request to begin the deletion or access process:

- A UI that is easy to use for a small number of access or deletion requests.
- A REST API to automatically submit access or deletion requests to Optimizely.

You may only make a request if you hold a collaborator role of Administrator on your company's Optimizely account.

Submit a GDPR or CCPA access or deletion request through the Optimizely UI

You can submit a GDPR or CCPA access or deletion request directly from the Optimizely application.

1. Navigate to Account Settings > Access or Deletion Requests.
2. Click Create New Request.
3. Fill in the following information:

- **Request type**: You can submit two types of requests:
  - **Delete**: Removes all data within an account that is associated to the identifier defined in the identifier field
  - **Access**: Finds all data stored in Optimizely systems associated to the identifier defined in the identifier field and exports it to an AWS S3 bucket for you to access.

- **Data type**: Any access or deletion request will apply to one of two data types:
  - **User data**: End users (also known as collaborators) who are added to the accounts of our customers. A user can be a collaborator on multiple accounts.
  - **Visitor data**: Individuals who visit or use our customers' websites, apps, and other digital products. Optimizely stores visitor data to calculate experiment results and to tailor content.

- **Identifier type**: User data is identified by the email address used to create the end user account. The form does not display the Identifier type field (see below) if you selected User as your data type in the previous step. If you selected Visitor, the form will display these five options for personal identifier types:
  - **DCP ID**: Any ID used to identify targeting records in Optimizely.
  - **Email Address**: The email address of a visitor.
  - **Full Stack ID**: The unique identifier used for Full Stack experiments.
  - **optimizely_end_user_id**: An Optimizely-generated user cookie.
  - **Other**: Any other identifier that was uploaded to Optimizely.

- **Identifier**: The identifier value you would like us to use when searching. If you selected User in the previous step, the identifier will be the email address for the user.

If you use DCP or list attributes, please submit the primary keys used to identify records in DCP data sources and list attributes. We need these keys to identify relevant records in these data sources; they cannot be searched using other identifiers. You may submit these keys using either the DCP ID or Other data type.

Please note that under our current terms, email addresses and similar personally identifiable information should not be uploaded into DCP. For more information, see PII: Personally identifiable information in Optimizely.

5. Click **Submit Request**.

---

**Automate GDPR or CCPA requests with the Optimizely REST API**

Optimizely customers can automate the requests using the REST API. These API endpoints are documented in our
The same considerations apply when using the API:

- Data cannot be retrieved once it is deleted.
- Data exports we provide may contain information that your company considers confidential, such as the change history for a particular project.
- DCP users must provide the DCP ID for us to identify the applicable record. We cannot search these records with other identifier types.

The endpoints that Optimizely offers are:

- List all the existing Subject Access Requests
  
  GET https://api.optimizely.com/v2/subject-access-requests

- Get an existing Subject Access Request
  
  GET https://api.optimizely.com/v2/subject-access-requests/{request_id}

- Create a new Subject Access Requests
  
  POST https://api.optimizely.com/v2/subject-access-requests

Retrieve the data from a completed access request

Where we receive a data access request, we search the records for the identifiers you provide and place matching records in an Amazon S3 bucket. When an access request is completed, you can call the existing Subject Access Request API as described in the Automating GDPR or CCPA requests with the Optimizely REST API section above. Alternatively, you can log into your account to view and download one or more existing requests.

Confirm data deletion

Where we receive a data deletion request, we search the records for the identifiers you provide and overwrite any matching data. When the request is completed, you can get the status of your request in the UI or with the REST API.

Note that we may retain some User Data in Change History logs and for other security purposes to ensure you have an audit trail of significant changes that may have been made to your account.

Rectification Requests

Optimizely users may correct their own data by signing into http://app.optimizely.com and editing the data in User Settings.
Rectification is not applicable for visitor data because the nature of the requests—records of events for users’ interactions with websites and apps, such as clicking on a button—isn’t compatible with the rectification process.

Disclaimer

This document is for informational purposes only and does not constitute legal advice. Readers should always seek legal advice before taking any action with respect to the matters discussed herein.