Optimizely

# Privacy@Optimizely

October 2019

Optimizely is the world's leader in customer experience optimization, allowing businesses to dramatically drive up the value of their digital products, commerce, and campaigns through its best in class experimentation software platform. To minimize privacy and security risks and to help our customers avoid unnecessary compliance costs, we design our products to collect only a limited amount of data about your customers (whom we refer to as "visitors") when they visit your website and/or use your digital products. This document answers some frequently asked questions to help you understand our approach and assess the impact of using Optimizely on your organization's privacy program.

## What data does Optimizely collect?

### Visitor Data

Optimizely collects limited information about your customers when they visit your website and/or use your digital products, which we call "Visitor Data." This may include:

- Event Data:
  A string indicating the type of event logged by Optimizely, such as whether a visitor has clicked on a button on your website. This data can optionally include customer-defined attributes and event tags.
- End User ID (or Visitor ID):
  A randomly generated identification number (ID) assigned to a visitor on a per-project basis. For web experimentation and personalization, this corresponds to the optimizelyEndUserId cookie.
- End User IP Address:
  The IP address associated with a visitor. Optimizely anonymizes IP addresses by default at the project level, and can also be configured to always anonymize IP addresses at the account level.
- Campaign and experiment IDs:
  A randomly generated ID of the campaign or experiment a visitor participated in.
- Variation ID:
  A randomly generated ID of the variation tha a visitor saw (for instance, if you have a website with a blue button and create a variation with a red button, each variation will have a variation ID).
- Timestamp:
  The date and time the event occurred.
- Referring URL:
  The URL of the web page that sent a visitor to your site.
- User Agent Data:
  The standard "userAgent header" passed by the browser, which contains information such as OS type and browser version.

As an open platform, we allow you to provide us with additional data about your visitors, for example, attributes related to repeat buyers. The additional data collected depends on the specific features you use and your configuration (some popular features include Dynamic Customer Profiles (DCP), list attributes, adaptive audiences, feature flags, and integrations). To help minimize the amount of personal data we collect, please note that our terms of service prohibit you from providing us with additional personal data or with sensitive personal information, such as health information. Please consult our documentation for additional information.

### Product User Data

When your employees or other authorized users set up an account on Optimizely, we also collect basic account information from the individual, such as a person's username, name, work email address, work contact details, and job title, which we call "Product User Data."

## Does Optimizely collect any personal data about your visitors?

The Visitor Data Optimizely collects is, by default, tied only to the following types of indirect device identifiers:

- End User IDs may fall within the scope of some privacy and data protection laws under certain circumstances, though by default we do not associate End User IDs with email addresses or other direct identifiers. We also allow you to set a custom expiration time for the Optimizely cookies through our APIs.
- End User IP Addresses are anonymized by default, but may also fall within the scope of some privacy and data protection laws under certain circumstances if you choose to disable IP anonymization for a given project.

We collect this data on your behalf from individual visitors who use websites and digital products where you are running Optimizely, and process it to provide the Optimizely Services to you.

You can also configure some Optimizely services to use other identifiers you provide, but please keep in mind that we do not permit customers to process direct identifiers on our systems.

## How does Optimizely use the personal data collected?

We only process Visitor Data in accordance with your company's permission and instructions as set out in your agreement with us. We do not sell Visitor Data, and we do not allow other companies to use your Visitor Data to test with or target your visitors. If a visitor to your site or app uses one of our other customers' sites or apps, they will receive a different randomly generated End User ID.

## Does Optimizely have a GDPR-compliant data processing agreement?

Optimizely offers a GDPR-compliant data processing agreement (DPA) to customers. Your Account Executive or Customer Success Manager can assist you with signing the DPA.

## The EU requires a lawful basis for collecting personal data. What are Optimizely's grounds for collecting personal data?

When operating within your websites and digital products, we collect data from your visitors as a "data processor" to enable you, the "data controller," to test and personalize your content and features. As the data controller, you are responsible for providing appropriate privacy and cookienotices to your visitors, and for obtaining consent, if needed. You should also consider implementing appropriate options for visitors as described in our documentation. Like other services, Optimizely does not display a separate cookie pop-up or privacy policy to your end users. Instead, you may choose to integrate Optimizely with popular tag management and cookie banner tools.

## Does Optimizely maintain a record of when personal data was collected? How long is personal data stored?

The Visitor Data we collect receives a timestamp to indicate when it was received by Optimizely. Starting on May 25, 2018, Visitor Data, such as raw Event Data, is kept in association with an End User ID or End User IP Address (if applicable) for up to 1 year only. We retain other data, such as account information for authorized users and DCP data for as long as your account is active with us. Should you terminate your agreement with Optimizely, you will be provided with an opportunity to download your Visitor Data. Upon your request, we will also also delete your Visitor Data in our production instances.

## Where does Optimizely store personal data? Does it use any third-party processors?

Like most modern technology companies, Optimizely uses leading cloud providers and other service providers to help us deliver a robust service. We have listed each of the key Optimizely data processors who process personal data (also known as "sub-processors") for our product.

Our services are currently hosted on servers based in the United States.

We have certified to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks for customer-related data. This provides you with the option of relying on these frameworks for the transfer of data from the EU to the U.S. You can find more information on our Privacy Shield certifications in our Privacy Policy.

## How does Optimizely allow us to access and delete our visitors' personal data?

We will assist you should you receive a request from an eligible data subject for data access or deletion of Visitor Data within our control. Our support engineers are trained to export or erase the event data records associated with identifiers you provide. For data stored in DCP and similar databases you manage, you will need to identify the particular records you would like to erase and submit a request to us. To learn more about our access and deletion processes, please refer to our documentation.

## What technical and organizational measures has Optimizely implemented to help secure personal data stored on its systems?

Every day thousands of companies use Optimizely on their websites and in their digital products to deliver billions of experiences, so we have built our service with security in mind. For more information, please refer to our current security measures.

## Does Optimizely have a process for regularly testing, assessing, and evaluating the effectiveness of its security measures?

Our security program includes annual security reviews by security consultants, automated source code analysis to find common security issues, and a bug-bounty program to encourage disclosure of security issues. For more information, please refer to our current security measures.

## Does Optimizely have a notification process in place in the event of a data breach?

We will inform you promptly in the event we learn of any unauthorized access, disclosure, or destruction of your Visitor Data and Product User Data per the terms of your agreement with us.