User Privacy and GDPR

Privacy settings of a browser

Visitors can protect their online privacy through various browser settings. It is now common for browsers to prevent the installation of new cookies and to delete existing cookies. Adhese uses a cookie for data analysis and frequency capping. This cookie contains a unique value to identify a given user.

It is important to note that the above privacy settings disable the correct identification of unique visitors. Therefore, visitors who do not accept cookies will not be considered for campaigns with a frequency cap. The default Adhese setting is that campaigns with a frequency cap will not be served to the group of visitors who do not accept cookies.

GDPR

In terms of GDPR legislation and the use of Adhese (or online advertising), there are two parties involved:

- **Data controllers**, or the clients of Adhese. Data controllers determine which data to collect and how to use it. They must implement a way to obtain permission to use personally identifiable information (PII) for marketing purposes.
- **Data processors**, the role Adhese takes in this process. Everything is handled through the Adhese platform and data protection measures such as encryption are in place. However, Adhese cannot make decisions regarding the use of personally identifiable information.

Adhese acts as a processor of data under the GDPR in the EU. Adhese does not determine what Personally Identifiable Information (PII) is collected and how it is used, but our platform can and does process PII in certain implementations. Consent must be obtained from the controllers of the data that flows through the system before any Personally Identifiable Information (PII) can be used. To use PII, a consent flag must be passed with each Adhese request to enable PII use and the possibility to set any cookies.

Passing consent to Adhese

Without TCF integration

Adhese account owners can include the *tl* parameter in their request to specify whether or not personally identifiable information (PII) can be used for their Adhese application.

The *tl* parameter can have two values:

- *all*: There is user consent. All PII mentioned in the consent request can be used in campaigns.
- *none* (default): There is **no** user consent to track and use PII. Users can still see ads, but their activity is not tracked. Adhese will not set any cookies, which means that frequency capping cannot be applied. As a result, capped campaigns will be excluded. This is also the default setting if the *tl* parameter is left out or any value other than *all* is used.

> If the *tl* parameter is not present, no personally identifiable information (PII) will be used or logged. This means that no cookies will be used to identify browsers, no device IDs will be collected, no frequency capping will be applied, no fingerprinting will be performed, and no IP or derived geographical data will be logged.

With TCF integration

Adhese is a registered vendor for the IAB TCF framework and supports TCF v2.0 and TCF v2.2. The consent data can be send to the adserver by including it in the request using the *xt* parameter. Adhese will parse this data and handle all data accordantly.

TCF is a cross-industry voluntary standard that is intended to enable publishers of websites and apps (first parties) and technology partners that support the delivery, personalisation or measurement of advertising and content (third parties or vendors) to work together and provide users with a standardised experience when they make privacy choices.

TCF enables users to grant or withhold consent and also exercise their ‘right to object’ to data being processed. It includes minimum practical requirements that stems from guidelines of Data Protection Authorities and jurisprudence for informing users, providing them with privacy choices, and for respecting such choices.

Other measures to guarantee privacy

By default, Adhese does not use any personally identifiable information (PII). Additionally, Adhese has implemented several measures to ensure compliance with GDPR and ePrivacy regulations.

1. Each Adhese implementation operates as an independent platform with its own database and set of domains for public access. As a result, data cannot be shared between two Adhese instances. Implementations can run on the first domain to ensure that cookies remain within the context in which they were set and for which consent was given.
2. Adhese does not log any personally identifiable information (PII), even when consent is given. Therefore, users will never be identifiable in any log files.
3. If consent is given for a unique identifier for one day, the cookie ID will be logged as a hash with sufficient collision to ensure the original cookie ID cannot be identified. The ID is used to report unique browsers over one day.

More on the privacy policy of Adhese can be found on our website.

Revision #12
Created 7 June 2024 07:24:07 by Casper Steuperaert
Updated 17 February 2025 14:47:55 by Casper Steuperaert