Privacy & Consent

Information on how user privacy and consent is handled by Adhese.

- Adhese & Privacy
- User Privacy and GDPR
- Consentless advertising
- Adblockers & first domain setups
- An introduction to cookies
- Bot filtering

Adhese & Privacy

Adhese puts user privacy first. On this page, you will find articles on our website that provide more information about our efforts to promote privacy in advertising.

You can find our full privacy policy here:

- https://adhese.eu/privacy-policy/

Articles:

- https://adhese.eu/article/privacy-and-compliance/

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.

Consentless advertising

> This article can also be found on our website.

Adhese offers a robust consentless advertising capability, ensuring that you can continue to offer effective advertising campaigns to advertisers while fully respecting user privacy and adhering to strict data protection regulations.

what is no-consent or consentless advertising?

Consentless advertising refers to digital ads that do not require user consent for tracking and targeting. This advertising is used for users who have not given consent or when consent has not been asked.

Since the introduction of GDPR, retail media owners and publishers across Europe have installed consent management platforms. Users get a choice between accepting or refusing the use of personal data. For users who do not consent, no cookies can be stored in a browser, and no unique id can be assigned to a visitor/browser by any other means for advertising purposes.

your AdTech needs to be ready for no-consent advertising

In many cases, AdTech only functions with a unique id to execute some form of identity-based marketing. As a result, none of these visitors gets to see advertising. The media owner gets no revenue from that traffic. It’s no surprise that Adhese is able to effectively deal with this!

no-consent traffic is growing

As GDPR adoption evolves and it becomes easier for users to refuse consent. This makes the share of anonymous media larger and the search for revenue even more urgent.

contextual advertising

Contextual advertising does not rely on personal user data but focuses on the webpage’s context or media content where the ads are displayed. This method targets ads based on the relevance of content to the advertisement, ensuring high engagement without needing explicit user consent.

first-party data

First-party data with consent is used to create detailed but anonymized audience segments, allowing targeted advertising that does not compromise personal privacy or require additional consent beyond the initial interaction.

segmentation and targeting

Advanced segmentation and targeting do not depend on personal identifiers. Media owners can effectively reach their desired audience based on non-personal criteria such as device type, content preferences, and behavioural patterns observed within the same session.

future of consentless advertising

Adhese ensures that all advertising practices meet legal standards for privacy and data protection, giving you peace of mind and safeguarding against legal risks.

Adhese consentless advertising is crucial for media owners who want to balance effective advertising with stringent compliance and user privacy concerns in a cookie-less world.

Read how Adhese’s targeting capabilities support consentless advertising.

Check out the whitepaper on consent-based advertising.

Adblockers & first domain setups

Ad blockers are browser plugins that prevent websites from requesting or loading ads. Depending on how they work Adhese will not be able to deliver ads, display ads or track ad impressions.

Ad blockers can work in different ways:

1. Ad requests are filtered out by blocking domains linked to known adservers.
2. Ad requests are filtered out by blocking all requests that contain certain keywords. For example sub domains or paths that contain the word 'ads': `ads.yourpublication.be` or `www.yourpublication.be/ads`
3. HTML elements that contain specific ID or CLASS values are set invisible by adding extra CSS

There are a couple of things you can do to minimise the impact of ad blockers:

1. Adhese can be implemented as a first domain solution. A subdomain, for example `content1.yourpublication.be`, or a path like `www.yourpublication.be/content1` , is then set as an alias of the Adhese servers. It is more challenging for an ad blocker to block the correct URLs without interfering with the proper and smooth functioning of a website.
2. Don't use ad related keywords when setting up new (sub)domains or paths.
3. Obfuscate HTML / CSS classes and ID's

> Setting up a first domain solution will require work on your and our end. Contact Adhese support for more questions or to get this process started.

An introduction to cookies

Adhese uses cookies to support a number of Adhese ad-serving features. **Cookies** are small packets of data that a server sends to a browser's directories when a visitor opens a web page. When the visitor subsequently accesses the same website, the browser retrieves the cookie and returns it to the relevant server. The browser will only return a cookie to the server that sent it in the first place.

> For user privacy concerning cookies, see User privacy GDPR. More on the privacy policy of Adhese is available on our website.

Adhese & cookies

Why does Adhese set cookies?

Adhese uses a single cookie, called `adhese2`, for data analysis and frequency capping. The adhese2 cookie contains a unique value to identify a previous visitor but does not collect any personally identifiable information. This cookie enables publishers to keep track of, for example, the number of unique visitors and the number of times a specific ad has been served to a particular visitor.

In addition, Adhese uses cookies for behavioural targeting. For example, if you want to target visitors who have expressed an interest in sports, you can place a sports cookie in your visitor's browser.

How does Adhese set cookies?

The Adhese Ad Server sends a cookie to a browser when a visitor opens a web page of a publisher for the first time. More specifically, Adhese sends the `adhese2` cookie when it receives the first initial request from the browser.

Bot filtering

Bots are computer programs that can perform human tasks autonomously, such as visiting a webpage. This results in invalid traffic to your website, since these tasks are not performed by humans. Adhese implements bot filtering to prevent invalid bot impressions from being counted.

Bot filtering automatically excludes impressions from bots. Adhese logs requests from detected bots, but their impressions are not included in Adhese's reporting tools.

Bots are detected by their IP addresses. Clients can choose to implement their own list of invalid IP addresses, or they can use a list that has been defined by the IAB. Adhese can also add invalid IP addresses when a new bot is identified.