

This pdf is generated on March 29, 2024. Go to [the documentation page](#) for the most up-to-date version.

Compliance with Privacy Regulation

This page is meant for people with some background in legal.

In this page, we explain in-depth why Simple Analytics is fully compliant with Regulation (EU) 2016/679 (the GDPR), the Privacy and Electronic Communications Directive 2002/58/EC (ePrivacy Directive), and The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

Simple Analytics does not collect any personal data

The [what we collect](#) page on our website lists all the data we collect and process to provide analytics. None of these data qualify as personal data under Art. 4(1) GDPR in and of themselves. Additionally, these data do not allow to "single out" a user (Recital 26) when combined. Tracking or fingerprinting users through Simple Analytics is not possible.

Most of the data listed on the page are also optional to collect: the customer can tweak Simple Analytics' settings to exclude certain categories of data, should they want to.

Even under default settings, Simple Analytics does not collect personal data, making tracking possible. Simple Analytics is, therefore, perfectly compliant with the *data protection by default principle* under Art. 25 GDPR.

Simple Analytics processes IP addresses but doesn't collect it

IP addresses are personal data under the GDPR. Simple Analytics processes IP addresses of website visitors as an essential part of Internet communication. We only use this data to communicate with the user's terminal and do not log or store this data in any form.

For this reason, our processing of IP addresses falls under the notion of "data usage" under Art. 4(2), which is distinct from both "storage" and "collection" under the same comma.

Simple Analytics does not process any other personal data.

Simple Analytics does not require a cookie banner or any consent pop-up

Art. 5(3) of the ePrivacy Directive (as implemented in Member State legislation) and Art. 6 of the PECR both require consent as a condition for lawfully processing any information stored on a user's

terminal equipment (such as cookies) unless the data is only processed to make electronic communication possible or it is strictly necessary for providing the user with an information society service they require.

Simple Analytics does not process any data falling under Art. 5(3) ePD or 6 PECR because it doesn't read, write, or otherwise process cookies or any other data stored in a user's terminal. For this reason, websites using Simple Analytics do not need a cookie banner, nor are they required to collect consent in any way when collecting data through Simple Analytics.

We process data forwarded by the user's browser, but this data is not stored on the user's terminal and doesn't fall under the strict regimes of Art. 5(3) ePD and Art. 6 PECR. For example, IP addresses are forwarded from browsers but do not fall under the aforementioned Articles. This is confirmed by EU case law^[^1] and entirely uncontested in practice.

Simple Analytics does not require pop-ups of any kind

Under Art. 13 GDPR, the data controller is under an obligation to provide certain information to the data subject whenever it collects their personal data. This Article does not apply to the use of Simple Analytics because we do not collect any data that qualifies as personal data for the GDPR (as we explained, IP address is only processed for communication and never collected).

We still encourage our customers to be transparent and provide information on their use of Simple Analytics. This can be done by making a privacy notice available on their website, without any need to implement pop-ups or banners that would deteriorate user experience.

Data localization

Simple Analytics relies on two trusted and GDPR-compliant Dutch companies (Worldstream and Leaseweb) to process data. The data we collect doesn't qualify as personal data under the GDPR and could lawfully be transferred outside the EU in compliance with Chapter V. However; we keep the processing and storage within the EU to further ensure compliance with European data protection law.

Footnotes

[^1]: See e.g. CJEU cases 582/14 (the well known Breyer case) or 597/19.

This pdf is generated on March 29, 2024. Go to [the documentation page](#) for the most up-to-date version.