"What is the GDPR?"

The General Data Protection Regulation ("GDPR") is a comprehensive EU data protection law, which goes into effect on May 25, 2018. The GDPR expands the privacy rights of EU individuals, and places heightened obligations on companies that process EU personal data in the context of providing goods or services to those individuals.

For more details, check out this Guide to the GDPR published by the UK Information Commissioner's Office.

As a Webtrends client, does the GDPR apply to me?

Companies within the EU, or who process the personal data of EU residents in the context of providing goods or services, will need to comply with GDPR. As a Webtrends client collecting data via our Software-as-a-Service (SaaS) solutions, you are likely a data controller under the GDPR.

Clients will need to evaluate their obligations under the GDPR, in part, based on: (1) the type of client data that you collect via Webtrends SaaS solutions, and (2) the legal basis on which you rely for the collection of this client data.

What about Webtrends?

Webtrends serves as the data processor for the data you collect via our SaaS solutions, as further described in this GDPR FAQ. For some limited data types (e.g. your login data), Webtrends is the data controller.

What personal data is collected and processed via Webtrends' solutions?

Webtrends' SaaS solutions collect a limited amount of personal data by default - (1) IP address; and (2) randomly generated GUID. Clients have control over, and are responsible for, any additional collection and use of personal data.

Clients should be aware that combining multiple data elements, even if not considered personal data when taken alone, may result in them being considered personal data when combined.

Can I avoid collecting personal data when using Webtrends' solutions?

Webtrends provides functionality to allow clients to truncate IP addresses. In addition, clients may contact Webtrends' Technical Support team to discuss other options for minimizing the collection of personal data.

Are there certain types of data that cannot be collected and processed via Webtrends' solutions?

Yes. Webtrends' SaaS solutions are not intended for processing data that could be legally considered sensitive in any applicable jurisdiction (e.g. government-issued identification or credit card numbers). Webtrends calls this "Prohibited Data", and the default configurations of Webtrends' tagging methods do not collect Prohibited Data. Webtrends prohibits clients from using its solutions to collect, store, process, or analyze Prohibited Data, and does not accept liability for Prohibited Data.

When does Webtrends delete client data?

Webtrends deletes client data, including backups, within ninety (90) days following termination of the agreement. Please refer to Webtrends' Data Retention Policy (Exhibit B to Webtrends' Terms of Subscription Service) for more information about data retention during the term of the agreement.

Does Webtrends provide clients with the option to delete client data?

Webtrends supports the deletion of client data; however, this needs to be done in conjunction with Webtrends' Technical Support team pursuant to a Statement of Work.

Does Webtrends utilize augmentation data?

Yes. Webtrends uses augmentation data from NetAcuity and Device Atlas to provide additional geographical and device information in reports.

Where is the data held?

Webtrends leverages data collection centers in Australia, Netherlands, and the United States. All data is processed and stored in the United States.

Webtrends' Commitment to Data Protection

Webtrends will be ready for the GDPR when it becomes effective on May 25, 2018.

- **New Data Protection Addendum.** In early 2018, Webtrends will offer a Data Protection Addendum reflecting our commitments under the GDPR.

- **Protections for Data Transfer outside the E.U.** Webtrends offers Model Contract Clauses to address to EU data transfer requirements. Webtrends has also certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce's Privacy Shield List

- **Robust Security Practices.** Webtrends employs technical and organizational measures designed to prevent unauthorized access, use, alteration, or disclosure of Client Data collected via Webtrends' SaaS solutions). Further, Webtrends has more than 15 years of experience in operating highly secured SaaS solutions with security controls that are continuously updated to meet industry standards and emerging threats. This is described in detail in Webtrends' Security Statement:

---

webtrends ®

Europe, Middle East, Africa
+44 (0) 1784 415700
emea@webtrends.com
www.webtrends.com