
MSA GDPR BING ADS FAQs

Updated May 18, 2018

GENERAL GDPR FAQs

What is the GDPR?

The GDPR is the European Union's new data protection law. It replaces the Data Protection Directive ("Directive"), which has been in effect since 1995. While the GDPR preserves many of the principles established in the Directive, it is a much more ambitious law. Among its most notable changes, the GDPR gives individuals greater control over their personal data and imposes many new obligations on organizations that collect, handle, or analyze personal data. The GDPR also gives national regulators new powers to impose significant fines on organizations that breach the law.

When will the GDPR come into effect?

The GDPR takes effect on May 25, 2018. Although the GDPR became law in April 2016, given the significant changes some organizations will need to make to align with the regulation, a two-year transition period was included. Organizations should not expect any grace period from regulators beyond May 25, 2018. Some EU member state regulators have already gone on record to say there will be no enforcement holiday for organizations that fail to comply.

Who does GDPR apply to?

The GDPR applies to companies, government agencies, non-profits, and other organizations that offer goods and services to people in the EU and that collect and analyze data tied to EU residents (personal data). The GDPR applies no matter where personal data is processed and imposes a wide range of requirements on organizations that collect or process personal data, including a requirement to comply with six key principles:

- Requiring transparency on the handling and use of personal data.
- Limiting personal data processing to specified, legitimate purposes.
- Limiting personal data collection and storage to intended purposes.
- Enabling individuals to correct or request deletion of their personal data.

- Limiting the storage of personally identifiable data for only as long as necessary for its intended purpose.
- Ensuring personal data is protected using appropriate security practices.

Although the rules differ somewhat, the GDPR applies to organizations that collect and process data for their own purposes ("controllers") as well as to organizations that process data on behalf of others ("processors"). In addition, unlike the current Data Protection Directive, both controllers and processors can be held accountable for failing to comply with GDPR.

What is personal data under the GDPR?

The definition of personal data is exceptionally broad under the GDPR. It includes any information relating to an identified or identifiable natural person ('data subject'). Under the law, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. If an identifier can be tied to a natural person, by Microsoft or by another else, it is personal data for purposes of GDPR compliance.

What is Microsoft doing to comply with GDPR?

Microsoft is leveraging its extensive expertise in protecting data, championing privacy, and complying with complex regulations, and currently complies with both EU-U.S. Privacy Shield and EU Model Clauses towards complying with GDPR. We believe that the GDPR is an important step forward for clarifying and enabling individual privacy rights and we are committed to GDPR compliance across our business, including Bing Ads, when enforcement begins May 25, 2018.

What are Processors and Controllers?

Under the GDPR, a controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the ***purposes and means*** of the processing of personal data.

A processor is a natural or legal person, public authority, agency or other body which processes personal data ***on behalf and under the direction of the controller***.

What are the responsibilities of a Controller and Processor?

A controller is directly responsible for complying with data protection laws. This includes requirements to:

- provide notice of processing to the data subject;

- confirm legitimacy and proportionality for the processing of personal information;
- assure that disclosures to third parties are made in accordance with appropriate contractual;
- terms and otherwise in compliance with applicable law;
- establish adequate measures to protect the cross-border transfer of personal information outside the EU; and
- establish appropriate controls over processors who process personal information on the controller's behalf, including:
 - assuring processors maintain appropriate security measures,
 - confirming the engagement of sub-processors in compliance with applicable rules, and
 - assuring adequate protections for cross-border transfers.

A processor, on the other hand, has relatively few direct responsibilities (for example, they must comply with technical and organizational data security regulations). A processor's main responsibility is to carry out the obligations imposed by its controller via contract. Processor duties may include, but are not limited to:

- Processing data only as instructed by the controller. Processors have no independent rights in the personal data and may not use the personal data for its own purposes beyond providing the service to the controller;
- Using appropriate technical and organizational measures to protect personal data;
- Assisting the controller with data subject requests; and
- Ensuring sub-processors, it engages meet these requirements.

Does Microsoft have a Data Protection Officer?

Microsoft has appointed a European DPO, Steve May, who is based in Dublin, Ireland. His chief responsibilities are representing our customers' data protection needs and rights in assessing Microsoft's data processing in an ongoing basis, as well as supporting Microsoft's ongoing engagement with European regulators relating to data protection matters.

Where can I learn more about Microsoft's approach to GDPR?

To learn more about the [General Data Protection Regulation \(GDPR\)](#) please visit www.microsoft.com/gdpr which has information about how specific Microsoft products can help you prepare to comply with the GDPR.

BING ADS GDPR FAQ

Does GDPR apply to Bing Ads?

To the extent Microsoft processes EU personal data, yes, GDPR applies in the context of Bing ads.

Is Bing Ads GDPR Compliant?

Microsoft is committed to being GDPR compliant when enforcement begins on May 25, 2018.

Is Microsoft a Processor or Controller under GDPR with respect to Bing Ads?

Microsoft's makes numerous decisions about the purposes and means of processing personal data we collect directly from Bing users, including how we use the data we collect for our services. Therefore, under GDPR, Microsoft is a controller and not a processor of that data.

Bing Ads service is delivered pursuant to Microsoft's data protection policies and procedures as a data controller, including:

- Microsoft maintains a [Privacy Statement](#) that explains to consumers how Microsoft collects and processes personal information as a data controller; and
- Microsoft maintains appropriate processes to select, contract with, and monitor the data processing activities of vendors that process personal information on behalf of Microsoft.

To the extent you have questions about what this means for your business, we encourage our customers to work with a legally qualified professional to discuss GDPR, how it applies specifically to their organization, and how best to ensure compliance.

Why is Microsoft a Controller and not a Processor of personal information processed when operating Bing Ads?

Microsoft determines the *purposes and means* of processing personal information collected when an individual uses Bing Ads. For example, Microsoft determines the means by which we collect search queries from users (e.g., user enters query on Bing homepage) and the purpose behind collecting that data (e.g., to provide a search result and, if applicable, relevant ad).

What is Microsoft's role under GDPR when working with advertising agencies or channel partners?

Microsoft is a data controller with respect to personal data processed in connection with Bing Ads regardless of whether an advertiser is working through an agency, channel partner, or directly with Microsoft.

Will Microsoft sign Data Processing Agreements with respect to Bing Ads?

Microsoft is a data controller with respect to personal data processed in connection with Bing Ads. Because Microsoft is a data controller and not a data processor, a data processing terms do not apply to Microsoft's role with respect to Bing Ads.

How can I ensure that my organization is compliant with GDPR when using Bing Ads?

To the extent you have questions about what GDPR means for your business, we encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to their organization, and how best to ensure compliance.

Is the Bing Ads Universal Event Tracking (UET) feature subject to GDPR?

Yes, because personal data is collected via UET, it is subject to GDPR. UET offers advertisers the ability to place a Microsoft pixel/tag on their sites that allows Microsoft to track users' activities on the advertisers' sites once users click on an ad served by Bing Ads.

Microsoft honors data subject rights through the standard controls and processes applicable to Bing Ads, including honoring the privacy settings chosen by data subjects through Microsoft's privacy dashboard.

Why is Microsoft the data controller with respect to Bing Ads' UET feature?

Microsoft determines the purposes and means of processing personal information collected directly from Bing users, including in the context of UET. As such, Microsoft is the controller of user personal data used to target Bing Ads, including through its UET feature.

UET enables Microsoft to collect user information directly from users visiting advertiser webpages. Microsoft provides advertisers with a UET tag which is then placed on the advertiser's site. This tag collects information from Bing users so that Bing can retarget and track conversions. Microsoft also uses that data more broadly to improve Bing Ads and related services. Advertisers do not have access to the data Bing collects via the tag, although advertisers may collect the same data independently of UET. Although the advertiser places the UET tag on its website, Microsoft still determines the purpose and means of processing data as opposed to acting under the advertiser's instructions.

Microsoft honors data subject rights through the standard controls and processes applicable to Bing Ads, including honoring the privacy settings chosen by data subjects through Microsoft's privacy dashboard.

For general information about Microsoft's privacy practices, please see our [Privacy Statement](#). User controls over individuals' personal data collected, processed, and retained by Microsoft are available on our privacy dashboard.

What data does Bing Ads UET collect?

For the specific data elements collected by UET, see [FAQ: Universal Event Tracking](#). Bing Ads retains this data for 180 days. UET will also collect the user's IP address, which is encrypted by Bing Ads, and will set the Microsoft cookie, which has an expiration date of 13 months. This cookie contains a GUID assigned to the user's browser and/or an ID assigned to a user who has been authenticated through their Microsoft account.

Bing Ads does not sell this data to third parties or share it with other advertisers.

How does Microsoft secure user data?

Microsoft uses a variety of security technologies and procedures to help protect personal data from unauthorized access, use or disclosure. In addition, Bing Ads follows industry standards as an [MRC \(Media Ratings Council\)](#)-accredited platform and through its annual participation in a Payment Card Industry Data Security Standards (PCI DSS) audit.

Where does Microsoft store Bing Ads data? Is it transferred out of the EU?

Although GDPR does not prohibit the transfer of personal data outside of the EU, it does require that organizations that move data outside of Europe have a lawful basis and use "appropriate safeguards" to do so. Microsoft uses Model Clauses (standard contract terms) and has signed on to the EU-US Privacy Shield, which are both recognized as "appropriate safeguards." Customers can find Microsoft's certification to the Privacy Shield [here](#).

Microsoft maintains major data centers in the Australia, Austria, Brazil, Canada, Finland, France, Germany, Hong Kong, India, Ireland, Japan, Korea, Malaysia, the Netherlands, Singapore, the United Kingdom, and the United States. Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a data center in another region. The storage location(s) are chosen to operate efficiently, to improve performance, and to create redundancies to protect the data in the event of an outage or other problem. Microsoft takes steps to ensure that the data collected under its [Privacy Statement](#) is processed according to the provisions of the statement and the requirements of applicable law wherever the data is located.