

UK Association of Online Publishers (AOP) Data Privacy Good Practice Guidance

1. Introduction

- The EU General Data Protection Regulation (GDPR) – reforming existing national data protection laws across the region - will apply from 25 May 2018.
- This guidance has been developed by a dedicated AOP Working Group and builds upon a comprehensive matrix of publisher data use cases and data processing activities, including those involving third parties (e.g. advertising technology companies).
- **This guidance does not constitute legal advice: individual companies should seek their own and, when using this guidance, AOP member companies will need to take into consideration other relevant laws, in particular Article 5(3) of the ePrivacy Directive (as transposed into national laws) which requires the user's consent, having been provided with clear and comprehensive information, for the storing of information, or the gaining of access to information already stored in the terminal equipment of a subscriber or user.**

2. Objective

- **This guidance is relevant to AOP member companies looking to comply with both the GDPR and the existing ePrivacy Directive (as transposed into national laws).** AOP member companies should be aware that EU legislators are currently reforming the ePrivacy Directive and this guidance will be updated when the new law is applicable. Third party suppliers will also need to consider their roles, responsibilities and obligations under both the GDPR and ePrivacy Directive (as transposed into national laws).
- This guidance is intended to help AOP member companies with their own efforts to comply with the GDPR by **(a) categorizing general uses of publisher data; (b) including specific sub-uses; (c) applying distinct data processing activities or purposes for each sub-use; and (c) suggesting a possible lawful basis (or legal bases) under the GDPR for each purpose.**
- When selecting a lawful basis for each purpose, companies need to be aware of all the available legal bases to process personal data under the GDPR (Article 6). In particular obtaining the user's consent (Article 6a), the performance of a contract to which the user is party to (Article 6b) and a company's legitimate interests (except where they may be overridden by the interests or rights of the user) (Article 6f). In the case of legitimate interests, a very clear 'balancing test' should be undertaken. Whatever the legal basis chosen, the decision should be documented.
- This guidance may also help companies in meeting some of their other GDPR obligations, such as recording data processing activities (Article 30), informing users about them (Articles 12-14) and building processes to meet the individual rights (Articles 15-22).

3. Data Controller / Data Processor

- It is particularly important for companies to ascertain their legal 'status' under the GDPR: **are they a Data Controller or Data Processor?** Article 4 (7-8) specifically defines **Data Controllers** as "the 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" and **Data Processors** as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

- Whilst it is up to each company to determine their status as a Data Controller or Data Processor, companies will need to consider their relationship with third parties (and whether those third parties are Data Controllers and / or Data Processors), as well as their obligations and responsibilities in this context. Under the GDPR, both Data Controllers and Data Processors are liable for non-compliance.
- Please note that, in some cases, companies may be 'Joint Controllers' which is defined in Article 26 of the GDPR as when "where two or more controllers jointly determine the purposes and means of processing..." or when two parties may act as independent Data Controllers of the same or similar data sets.
- Under the GDPR, AOP member companies - as publishers - will be Data Controllers. In some scenarios AOP member companies will have further business models potentially warranting a different legal status. There will also be scenarios (e.g. customised advertising) where they will also work with other Data Controllers (possibly as 'Joint Data Controllers') as well as Data Processors (and also Sub-Data Processors).**

4. Publisher Uses of Personal Data

Whilst each individual publisher will have different, varying and sometimes distinct data uses, AOP member companies may consider the below categories of publisher user data:

A. Advertising

This involves the processing of personal data (usually in the form of identifiers such as cookies or mobile advertising IDs) to personalise advertising (such as using first party data observed or inferred to make advertising more relevant) as well as customised advertising (often involving the use of third party specialists to tailor the ad to a group of users interested in similar things). Depending on the circumstances, data may be collected across sites, apps and / or devices.

B. Performance Marketing

This involves the processing of personal data to direct marketing (both B2C and B2B) at both existing customers and potential new ones, including affiliate marketing, as well lead generation methods aiming to ascertain new customers.

C. Site Analytics

This involves the processing of personal data to analyse digital property (e.g. website, app) usage & performance for product research & development, measurement and product effectiveness purposes.

D. eCommerce

This involves the processing of personal data to implement purchase activity (including payment and delivery) as well as product & service recommendations.

E. Network Security

This involves the processing of personal data for information security purposes, including fraud prevention, as well as meeting other legal obligations (e.g. law enforcement).

F. Content Personalisation

This involves the processing of personal data to personalise the content and performance of the digital property (e.g. website, app) as well as the use of social media tools for sharing content.

5. Publisher Data Processing Purposes under the GDPR

- Within each data use case will be a different sub-use, each with its own data processing purposes. Where these involve the collection, receipt and / or use of personal data, publishers must consider the purpose(s) of such collection, receipt or use – and establish a lawful basis under the GDPR.
- Please note that, regardless of the legal basis that a publisher relies upon, users should be provided with transparency regarding data collection and use, including for example, who the Data Collection is, the type of personal data that is being collected, any Data Controllers with whom the personal data will be shared and the purposes for which it will be used.
- For more information on the data processing purposes which may be applicable to each data us, please see the AOP Data Purposes Spreadsheet.

6. Useful Links

In addition to this guidance, AOP member companies may find the following GDPR sources helpful:

- AOP GDPR FAQs - www.ukaop.org/hr-and-legal/the-eu-general-data-protection-regulation-gdpr-faqs- (NB member log in required)
- UK Information Commissioner's Office (ICO) - <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>
- EU Article 29 Working Party (group of EU regulators): Draft guidance on consent under the GDPR - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- EU Article 29 Working Party (group of EU regulators): Draft guidance on transparency under the GDPR - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- Data Protection Network: Guidance on the use of legitimate interests under the GDPR - www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/
- IAB Consent Framework – www.advertisingconsent.eu

Confidentiality Statement

Please treat all documents and other communications issued to AOP Members and all discussions that take place in the Group meetings as STRICTLY PRIVATE AND CONFIDENTIAL and that no disclosure will be made to any person outside the membership of the Association or be published in any journal without first obtaining the permission of the AOP.