Practical Guidance for Exercising User Rights for Digital Marketing Companies

Introduction

The General Data Protection Regulation ("**GDPR**") expanded and strengthened the data rights provided to individuals, while also creating additional rights concerning personal data collected by businesses.

Depending on the circumstances, individuals may request to see their data held by the company, request that the data be corrected or deleted, ask to cease or restrict processing of the data, and ask for the data to be ported over to another service provider.

These practical guidelines were drafted to help digital publishers and advertisers (such as ad networks, agencies, DSPs and SSPs) find resources and tools that may help them meet new legal or contractual requirements relating to data subject rights under the GDPR.

Why is this important?

Many businesses are now required to handle requests to exercise data rights. **This requirement presents operational, legal and technical challenges for companies operating in the digital marketing ecosystem**, for various reasons:

- Digital marketing companies operate in different roles in the ad supply chain, whether as controllers or processors; this distinction impacts the company's responsibility to respond to the data right requests.

- Digital marketing companies traditionally collect and process indirect identifiers, such as IP addresses, cookie IDs, mobile device IDs or other pseudonymous information. While such identifiers may be regarded as "personal data" under the GDPR, they pose a particular challenge, as they do not typically identify an individual (but rather a browser or a device).

- Digital marketing companies do not typically have direct relationships with the individuals, thereby posing another challenge in responding to these types of requests.

Given these challenges, we have prepared the below guidance which is based on our experience and insights relating to exercising data right requests.

Please note that the guidance set out below should be evaluated on a case-by-case basis, and companies should always document their reasoning for their actions.

User Rights Practical Guidelines

1. Determine whether you are a controller or processor.

Companies in the digital advertising ecosystem (advertisers, publishers, ad networks or agencies, ad exchanges, DSPs, SSPs, etc.) act in different roles, either as a controller or as a processor.

In addition, these companies are generally subject to contractual obligations that typically specify their roles, and allocate the responsibilities between them and their respective partners regarding handling data right requests.

The distinction between a controller and a processor, together with the contractual obligations of the company, poses different responsibilities with regard to exercising data right requests:

- If the company acts as a controller – it is likely to be directly affected by data subject rights, and responsible to exercise it.
- If the company acts as a processor – it would be typically required to direct the request to the controller, and provide the controller with assistance in responding to the request.

➢ **Key takeaways:**

- **Determine whether you act as a data controller or data processor** – this would impact whether you are responsible to respond to the request. Data processors should not reply directly to access requests, unless directed by the controller in a contract or otherwise.
- **Implement technological measures that would facilitate your (or your partner's) obligation to respond to the request**, in particular the ability to identify the data, retrieve it, rectify it, suspend it from further processing, extract it in a machine-readable format, and delete it.

2. Understand if you are able to identify the requestor from the information you process.

Under certain conditions, **a company may refuse to exercise data rights if it is able to demonstrate that it is not in a position to identify the requestor**.

This exception is particularly relevant for digital marketing companies, who traditionally collect and process indirect identifiers, such as an IP address, cookie IDs, mobile device ID or other pseudonymous information, which identify a browser or a device – but not necessarily an individual.

Furthermore, while the request may include the requestor's name and email address, the company may not be able to act upon such request, as such data is not typically linked or attributed to the pseudonymised information recorded on its system.

However, note that this exception does not apply if the individual has provided the company with additional information enabling his or her identification.

➢ **Key takeaways:**

- In certain circumstances, **digital marketing companies may be able to demonstrate that they are not in a position to directly identify the individual, and may therefore reject the request and respond accordingly to the requestor**.
- Companies should consider **acting on data right requests tied to the identifier they use** – such as a cookie ID or mobile device ID. Companies should consider explaining to the requestor how to locate their cookie or mobile identifier on their devices.

3. Consider if you have taken reasonable measures to identify the requestor.

Companies are required to use all reasonable measures to verify the identity of an individual who request to exercise data rights access.

This is important in order to avoid processing a request filed by an unauthorised individual. Responding to this type of request without verifying the identity of the requestor may result in an adverse effect on the rights of other individuals, and may also be considered, in certain circumstances, a data breach.

This requirement is particularly relevant in the context of online services and online identifiers, as the data stored is not typically associated with a specific individual.

In practice, it is nearly impossible for a digital marketing company to truly verify a person's ownership of a cookie ID or a mobile device ID, as a single browser or device is shared by several individuals, resulting in a cookie ID being assigned to several individuals.

Furthermore, an IP address can be dynamic and allocated to other persons, or otherwise masked or replaced by fairly easy means (such as via proxy servers, VPNs or other means).

➢ **Key takeaways:**

- **Companies should take reasonable steps to confirm they have received a bona-fide data right request by asking for additional information that can validate that the cookie or device identifier is associated with the requestor**, such as by asking the requestor to:
  - Send a screenshot of the identifier to validate the request;
  - Send a declaration or affidavit that the cookie or mobile ID belongs to the data subject.

- **Companies should not ask for information that is unnecessary or disproportionate in order to validate the requestor's identity** (such as by requesting government issued-IDs, or personal information that is not recorded on the company's systems).
- Companies should consider building a mechanism (e.g. webpage) to automatically read the cookie from the individual's browser, to both validate and automate the exercise of data right requests.

4. Ensure you have appropriate procedures and policies in place to respond to the data rights, and record them.

Companies should create an internal, written policy around its data right response procedures, in order to enable the company to demonstrate its compliance with the GDPR.

This policy should set forth which data subject identifiers must be provided (e.g., cookie ID's or mobile advertising ID's), the required verification information, the technical aspects relating to exercising the request (such as data retrieval, extraction and deletion), as well as lay out the company's process for responding to such requests and recording them.

In addition, **companies should always maintain records of all data right requests they receive and all data access responses they issue, in order to demonstrate compliance with the GDPR**.

This record may include the data subject request itself, the date of the request, the company's response, the date of the response, along with a copy of the individual's identifier and timestamp, proof of verification, and who handled the request.

Note that companies may need to provide this information as evidence upon a supervisory authority inquiry. Therefore, companies should keep records of all correspondence with the individual concerned for a set retention period of at least 18-36 months.

➢ Key takeaways:

- Put in place adequate and robust written policies for handling data right requests.
- Record data right requests for at least 18-36 months.