CONTROLLER-PROCESSOR CRITERIA

Working Paper 05/2018

IAB Europe
GDPR Implementation Working Group

Version 1.0
19 July 2018

About IAB Europe

IAB Europe is the voice of digital business and the leading European-level industry association for the interactive advertising ecosystem. Its mission is to promote the development of this innovative sector by shaping the regulatory environment, investing in research and education, and developing and facilitating the uptake of business standards.

About the GDPR Implementation Group

IAB Europe's GDPR Implementation Working Group brings together leading experts from across the digital advertising industry to discuss the European Union's new data protection law, share best practices, and agree on common interpretations and industry positioning on the most important issues for the digital advertising sector. The GDPR Implementation Working Group is a member-driven forum for discussion and thought leadership, its important contribution to the digital advertising industry's GDPR compliance efforts is only possible thanks to the work and leadership of its many participating members.

Acknowledgements

This working paper on controller and processor definitions has been prepared by the members of the IAB Europe GDPR Implementation Group under the leadership of Alan Chapell, of Chapell & Associates.

Contacts

Townsend Feehan (feehan@iabeurope.eu)
CEO, IAB Europe

Matthias Matthiesen (matthiesen@iabeurope.eu)
Director, Privacy & Public Policy, IAB Europe

Chris Hartsuiker (hartsuiker@iabeurope.eu)
Manager, Privacy & Public Policy, IAB Europe

Contents

Overview

On 27 April 2016, the European Union adopted the General Data Protection Regulation ("GDPR").[1] The GDPR became directly applicable law in the European Union ("EU") and European Economic Area ("EEA") on 25 May 2018, replacing previous national data protection laws.

The GDPR does not only apply to companies based in the EU but also to companies all over the globe offering goods and services to people based in the territory of the Union, or monitor the behaviour of individuals located within it. Data protection law regulates the processing of personal data, defined broadly as any information that relates to an identified or identifiable natural person, which may include, amongst others, online and device identifiers that can be used to single out a natural person, for example for digital advertising purposes.

The GDPR grants data protection authorities the power to levy significant administrative fines against businesses found in breach of the law. Depending on the severity of the infringement, fines can reach up to €20,000,000 or 4 per cent of a company's annual global turnover – whichever is higher.

This document has been prepared by members of the IAB Europe GDPR Implementation Group (GIG) to provide guidance to companies across the globe on the definition of controllers and processors.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter 'GDPR', available at http://eur-lex.europa.eu/eli/reg/2016/679/oj/.

Key Terms for this Guidance

Client

As used herein, the term Client generally refers to an adtech platform's customer.

Data Subject

The GDPR defines a data subject as "an identified or identifiable natural person."[2] Adtech companies typically refer to data subjects as Internet users.

Data Controller

The GDPR defines a data controller 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."[3] In other words, the data controller is the entity that makes decisions about processing activities, regardless of whether that entity actually carries out any processing operations. Please note that the specific requirements for data controllers and data processors may be addressed in separate guidance. As noted by the Article 29 Working Party, "[t]he determination of the "means" of processing can be delegated by the controller, as far as technical or organisational questions are concerned." [4] However, the working party also states that "[d]etermination of the "purpose" of processing is reserved to the "controller". Whoever makes this decision is therefore (de facto) controller."[5]

Data Processor

The GDPR defines the term "processor" as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[6] In other words, while the data controller is the entity that makes decisions about processing activities, the processor is any entity contracted by the data controller for carrying out the processing. The data processor generally cannot use the data except as directed in writing by the data processor. Processors might still be entitled to determine some of the means of processing (it could even be delegated by the controller), but not the purposes according to the Article 29 Working Party. Technical and organizational measures might therefore be determined by a processor as long as they do not constitute essential elements of

[2] GDPR Article 4(1)
[3] GDPR Article 4(6)
[4] Article 29 Working Party: Opinion 1/2010 on the concepts of "controller" and "processor" ("WP169"), 16/02/2010, p. 17 at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.
[5] Ibid. See also example number 3 on page 14 which notes the the "decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this processing operation."
[6] GDPR Article 4(8)

processing.[7] Please note that the specific requirements for data controllers and data processors may be addressed in separate guidance.

SubProcessor

The GDPR offers rules for a data processor that engages another data processor – the latter being considered a sub-processor. In adtech, a sub-processor is often either a hosting company, a third-party developer with some level of access to personal data, or another entity that otherwise assists a data processor. The GDPR requires the data processor to obtain the data controller's authorization to appoint sub-processors. This can be given in a general way, so long as the data processor informs the data controller of any sub-processors so that the data controller may have the opportunity to object.[8] Sub-processors also are subject to the same requirements under the GDPR.

UID

A User ID or UID is a pseudonymous identifier such as a cookie ID or mobile Advertising ID (e.g., IDFA in iOS). A UID which is used to identify a browser, computer, or device over time is considered a "digital identifier" under GDPR and is considered personal data.

Processor vs. Controller – Criteria to consider for adtech companies

EU privacy law has only two primary categories of entities which collect and process data: data controllers and data processors. Contrast the EU approach with the three classifications used widely in the U.S. adtech world: First Parties (i.e., websites and advertisers), Third Parties (mostly adtech companies) and Service Providers (essentially agents of the First Party). Advertisers are First Parties in multiple contexts (i.e. when they interact with users directly on their sites, or if there is a pre-existing relationship), but if they are loading in the context of another website than their own, they act as Third Parties.

Service Providers in the U.S. are roughly analogous to Data Processors in the EU – in that both are agents of the First Party /Data Controller. Thus, one of the key differences between U.S. adtech privacy rules and EU privacy rules is that the two primary categories in the EU privacy rules (e.g. who is the processor/controller) do not cleanly align with how data flows among, and the relationship between, the parties in the adtech model. Some third-parties make use of First Party data outside the ambit of the instructions provided by the First Party. This notion goes back to the "ad network" model *circa* 1997

[7] Article 29 Working Party, WP169, p. 14.
[8] GDPR Article 28(2).

– where a network would take data from website 1 and website 2 and use that data to create a targeting segment for website 3.[9]

Adtech business models[10] are unique in many respects. As a result, there's been some marketplace confusion regarding characterization of the various roles (i.e., controller vs processor) within the adtech models. Moreover, a recent ruling by the Court of Justice of the European Union[11] indicates that EU Data Protection Law casts a wide net by design when it comes to apportioning responsibilities across various roles when more than one entity is directly or indirectly involed in the processing of data. Therefore, adtech companies need a set of criteria they may point to in order to ascertain whether they are a processor or a controller. After receiving input from data protection regulators in the EU, and after considerable internal discussion, the GDPR Implementation Group's Controller / Processor Working Group offers the following considerations designed to assist adtech companies in ascertaining whether they are acting as a controller or a processor of personal data. While not providing legal advice, this working group offers a few criteria that may be helpful in determining whether your company is acting as a processor or a controller.

1. UID Creation and Use

- Does your company create a UID solely or even partly for your company's own purposes? If your company creates a UID either solely or partly for your own purposes, the presumption is that your company is a controller of that UID. Conversely, if your company creates a UID solely for the purposes of your Client(s), the presumption is that your company is considered a processor of that UID (unless your company shares or uses the same UID across Clients in a manner that could make you a Controller, as provided in #2 below). Companies leveraging the advertising IDs created by third-parties such as the mobile O/S platforms have not "created" those UIDs and should look to the next set of criteria.[12]

  A single UID may be tied to multiple separate sets of data processed by a single entity (eg. behavioural data from a specific website processed on behalf of a particular Client, ad serving data from publisher's website used for service optimisation). In such cases, the entity

[9] Note the ad network model dates back to 1997. Some of the very first ones include: ValueClick (1997 was its first ad server), FlyCast (1997), Narrowline (1997), Advertising.com (launched 1998 as "Teknosurf.com"), and Specific Media (launched 1999 as "advertisementbanners.com").

[10] The WG recognizes that there are many different digital advertising models which may find this guidance useful, including but not limited to: ad servers, ad exchanges, SSPs, DSPs, DMPs, ad networks, attribution vendors, market research companies, data companies, affiliate marketing companies and cross device vendors. Moreover, the WG group recognizes that each digital advertising company has its own unique characteristics making it challenging to create guidance that perfectly fits all models. The guidance is intended to act as a helpful tool for digital advertising companies to be used in conjunction with guidance and feedback from privacy counsel.

[11] *See* generally, the EU Court of Justice opinion in Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH at http://curia.europa.eu/juris/documents.jsf?num=C-210/16.

[12] Mobile advertising companies that create and use their own UID (e.g., a fingerprint) in addition to the mobile advertising ID offered by the mobile O/S companies are deemed to have created their own UID for the purposes of these criteria.

concerned may be considered both a controller and a processor of a UID forming part of different data sets.

As an example, if your company creates a UID that is used or shared across Clients (and is used solely for the purposes of your Clients) and that UID is synced with the UID of another vendor as part of a transaction initiated by or on behalf of the Client, such syncing may be considered part of the technical and organizational measures of processing. As a result, such activity may be considered that of a processor.

2. UID Segregation

- Does your company silo its UIDs? In other words:

  Does the UID referenced in paragraph 1 get shared or used across your company's Clients so that the same User ID is leveraged across one or more of those Clients,[13] or:

  Does each Client have their own UID for each user so that the same user might be UID123 for Client1 and UID456 for Client2?

  Building on the above criteria, if your company creates a UID for its own purposes and/or shares or uses the same UID across Clients and you are not contractually or technologically restricted from using the UID for any purpose other than carrying out the instructions of a Controller, the presumption is that your company is a Controller of that UID. As per the Article 29 Working Party's Opinion, determining the means in terms of technical and organizational measures can, to an extent, be delegated to Processors as long as they do not concern the essential elements of the means.[14]

  If we consider the case of making use of the same UID across several clients, it could be the case that a Controller has contractually delegated the technical and organizational means, such as a 'shared' UID, to its processor, but at the same time provides specific instructions on the purposes for which the UID can be processed for that Controller. However, it must also be borne in mind that when the common UID could be considered an essential element of the 'means' of processing, i.e. where the processing would not be possible with separate UID's per client, this may make the company using the 'shared' UID a controller.

[13] Companies leveraging mobile advertising IDs are likely to be deemed as using that same UID across multiple clients.
[14] Article 29 Working Party, WP169, 16/02/2010, p. 14.

3. Data Use

- Does your company insert or use an (additional) UID or co-mingle or otherwise combine data across Clients, i.e. for ad serving optimization[15] such as frequency capping across multiple sites or apps? If YES, then you are likely to be considered a Controller of that data.

  This working group has decided against compiling a comprehensive analysis of the practices of the adtech marketplace. Instead, the members of the group agreed that companies engaging in multi-site ad serving optimization across Clients are generally considered controllers of that data. The working group opted to set the bar at ad serving optimization and let each individual company determine how their use of data compares to ad serving optimization after consultation with counsel.

Accordingly, if your company: 1) creates or uses a UID for your own purposes, 2) uses the same UID across Clients without restriction, and 3) uses the data associated with that UID across Clients for ad serving optimization such as multi-site frequency capping, your company is likely to be considered a controller. Any of the three criteria could cause a company to fall within the scope of being a controller – but the concepts of controllers and processors are functional and will depend on the circumstances. A given company may be a controller in relation to one set of data and a processor in relation to another. In specific circumstances, the scopes of these separate data sets can overlap to a certain extent. These criteria are meant as a guide to help indicate to which extent a company in the online advertising ecosystem needs to consider their status.

[15] In other words, if data is being co-mingled across clients even for ad serving optimization such as frequency capping, many EU regulators have taken the position that this use case would indicate that the adtech company is a controller of that data.

About the IAB Europe GDPR Implementation Working Group

IAB Europe's GDPR Implementation Working Group brings together leading experts from across the digital advertising industry to discuss the European Union's new data protection law, share best practices, and agree on common interpretations and industry positioning on the most important issues for the digital advertising sector.

The GDPR Implementation Working Group is a member-driven forum for discussion and thought leadership, its important contribution to the digital advertising industry's GDPR compliance efforts is only possible thanks to the work and leadership of its many participating members.

For more information please contact:

Townsend Feehan (feehan@iabeurope.eu)
CEO
IAB Europe

Matthias Matthiesen (matthiesen@iabeurope.eu)
Director, Privacy & Public Policy
IAB Europe

Chris Hartsuiker (hartsuiker@iabeurope.eu)
Manager, Privacy & Public Policy
IAB Europe