

What's New in the EDPB's Draft Guidelines on Controllers and Processors Under the GDPR? (Part 2)

Article By:

Stéphanie Faber

Asel Ibraimova

This is the second in our series of posts on the draft [Guidelines 07/2020 on the concepts of controller and processor in the GDPR](#) (the “draft Guidelines”) issued on 7 September 2020 by the European Data Protection Board (“EDPB”). This post focuses on the updates to the concept of *controller*. See our previous post regarding the concept of processors [here](#). Upcoming posts will address joint controllers, “third parties” and “recipients.”

Please note that the EDPB has invited businesses to provide their feedback on the draft Guidelines by 19 October 2020.

Part II: Focus on Data Controllers

What is New in the Draft Guidelines?

Although the draft Guidelines provide some additional clarity on the distinction between controllers and processors, there remain various uncertainties in the application of the criteria for determining these roles under the GDPR. Evaluation continues to require a careful assessment of the relevant criteria and regulatory risks. It is important to keep in mind that not every “service provider” will qualify as a data processor. Indeed, the regulatory approach proposed by the EDPB appears to continue the trend towards limiting the scope of the “processor” classification and categorising data recipients that play a role in determining the purposes or essential means of the processing as joint controllers instead of processors. Joint controller status will be the focus of our third blog in this series.

Controller determines purposes and means of processing

The basic criteria for determining what makes an organisation a controller remains the same as under the previous guidelines issued by the EDPB's predecessor in February 2010 (“[Opinion 1/2010 on the concepts of controller and processor](#)”). This is unsurprising, since the EU General Data Protection Regulation (“GDPR”) has not changed the definition of *controller* that was codified by the 1995 EU Data Protection Directive 95/46/EC. A data controller is defined 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” (Article 4(7) GDPR). The draft Guidelines reaffirm that the controller determines both the “purposes” and “means” of the processing of personal data. The purposes and means were interpreted as the “why” and the “how” of the processing in the 2010 Opinion. Control can be exercised over the entirety of a processing activity or only over a particular stage in the processing of the data.

Processors often have discretion as to the means of the processing, furnishing their own tools and technologies. The draft Guidelines suggest that this does not necessarily impact the role of the processors if such control is limited to non-essential means of the processing. As examples of such non-essential means, the draft Guidelines refer to *“more practical aspects of implementation”* – such as which hardware or software should be used. At the same time, controllers retain the sole control on the “essential means” of the processing, if they decide *“which data shall be processed”, “which third parties shall have access to this data”, “when data shall be deleted”, etc.*

The draft Guidelines offer as an example the situation in which a company appoints a payroll administrator and notes that the *“way in which the latter should carry out the processing is in essence clearly and tightly defined”* even if the payroll processor may decide on certain matters *“such as which software to use”*.

The draft Guidelines observe that in some cases there is a thin line between the role of controller and processor, such as when companies appoint accountants. Often the accounting firm *“decides itself, in accordance with legal provisions regulating the tasks of the auditing activities carried out by it that the data it collects will only be processed for the purpose of auditing the client and it determines what data it needs to have, which categories of persons that need to be registered, how long the data shall be kept and what technical means to use”*. In such cases, the accounting firm acts as a controller. However, *“[i]n a situation where the law does not lay down specific obligations for the accounting firm and the client company provides very detailed instructions on the processing, the accounting firm would indeed be acting as a processor.”*

The controller role may stem from applicable legal provisions, that is, when the law determines the controller or establishes specific tasks for the organisation. The draft Guidelines provide as an example the processing activity of a municipality that has the obligation to provide social welfare benefits to citizens depending on their financial situation. Classification as a controller may also result from *“factual influence.”* The draft Guidelines also provide the example of a law firm that acts with a *“significant degree of independence”* when representing a client (noting also that the mandate is *“not specifically targeted to personal data processing”*). Factual influence includes amongst other things the terms of a contract or the *“traditional roles and professional expertise that normally imply a certain responsibility”* (as in the case of an employer with respect to the processing of personal data of its employees).

Access to personal data is irrelevant to be a controller

The draft Guidelines clarify, consistent with case law from the Court of Justice of the European Union (*Facebook Fan page* (C-201/16) and [Jehovah's Witnesses \(C-25/17\)](#)), that organisations which do not have access to the personal data being processed on their behalf cannot exclude themselves from being a controller. So, for example, an organisation that engages a service provider to carry out a market study and only receives aggregated or statistical data will still be classified as a controller in relation to the personal data analysed in order to prepare the market study, if the organisation determines the means and the purposes for which personal data should be collected and the

parameters of the study.

Control cannot be artificially allocated

As set out in the draft Guidelines, “*it is not possible either to become a controller or to escape controller obligations simply by shaping the contract in a certain way,*” or by appointing a natural person within one’s organisation to implement a processing activity and designate such person as the controller.

Continuous obligation to ensure processors and sub-processors provide “*sufficient guarantees*”

Controllers have the primary responsibility for compliance with the GDPR due to the accountability principle and other obligations imposed directly by the GDPR on controllers. The draft Guidelines stress the obligation of the controller to only engage processors that provide sufficient guarantees that the processing will meet the GDPR requirements. The EDPB clarifies that this obligation also applies to granting authorisation for processors to engage a sub-processor. In practical terms, this means that controllers should add an extra layer to their due diligence process for engaging service providers when the latter in turn engage sub-processors. Controllers should have contractual restrictions on the processor’s right to engage a sub-processor without the controller’s prior authorisation. There should be controls in place to check that the sub-processors provide “*sufficient guarantees*”. Where the controller grants a general authorisation, controllers should have the right to be informed of any changes to the list of approved sub-processors and an opportunity to object to any new sub-processors. The obligation to check that engaged processors and sub-processors provide sufficient guarantees is a “*continuous obligation*”, which requires regular verification that is ultimately the responsibility of the controller, even if the controller delegated the vetting of sub-processors to processors.

Emphasis on purpose limitation when sharing data with other controllers or joint controllers

The draft Guidelines also emphasise the duty of each controller to ensure that the personal data disclosed to another controller or a joint controller are not further processed in a manner that is incompatible with the purposes for which the data was originally collected by the controller disclosing the data. In case the personal data is intended to be used for additional purposes by the controllers or joint controllers receiving the personal data, they should contractually commit to have a legal basis for such processing.

Contractual arrangements

The draft Guidelines also provide an interpretation of Article 28(3) GDPR reaffirming that written and binding agreements are necessary. The EDPB calls on controllers to add specific and concrete information on how processors are to comply with their GDPR obligations (additional detail may be found [here](#)). Specifically, the EDPB suggests adding procedures and template forms in contracts with processors to allow processors to assist controllers, where necessary (for example setting forth a detailed procedure that would apply in case the processor suffers a data breach or who does what in case the controller or the processor receives data subject requests, etc.) or to arrange for further instructions for such assistance.

A controller’s instructions should also cover international transfers of data outside the EEA. Where the processor is authorised to delegate some processing activities to other sub-processors, the

contract must be clear on whether the controller allows for transfers to processors in third countries, including the processor's own divisions or units in third countries.

The EDPB emphasises that the controller will not be able to escape responsibility in cases where it agrees to non-negotiable terms offered by large service providers acting as processors, and the terms violate the GDPR requirements. Consequently, controllers must assess their compliance risks and ensure that any such non-negotiable contracts do not impact their key processing activities involving personal data, key data subjects or major data flows.

© Copyright 2025 Squire Patton Boggs (US) LLP

National Law Review, Volume X, Number 289

Source URL: <https://natlawreview.com/article/what-s-new-edpb-s-draft-guidelines-controllers-and-processors-under-gdpr-part-2>