Comments on the draft Guidelines 07/2020 of the European Data Protection Board

This paper exclusively reflects the views of its author.

On 7 September 2020, the European Data Protection Board published its draft Guidelines 07/2020[1] *"on the concepts of controller and processor in the GDPR"* (hereinafter referred to as Draft Guidelines or Draft).

The Draft Guidelines replace the WP29 Opinion 1/2010 on the concepts of "controller" and "processor" (one of the best papers of the WP29—if not the only legally correct and thorough one). Although the Draft "inherited" some merits of the previous WP29 Opinion but it cannot meet its objective *"to clarify the meaning of the concepts"* of controller and processor. It fails to achieve this objective both "internally" (among the provisions of the Draft) and "externally" [vis-à-vis other EDPB Guidelines, especially EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)].

1. Elements of the concept of data controller

It is repeated like a mantra that the controller is the entity that determines the purpose and means of the data processing, while it has been lost that the situation is (should be) more subtle:

a) Although the Draft refers to the fact that *"controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case"* (paragraph 19), it fails to *clearly* distinguish between these two cases.

In the case of "controllership by law", both the controller and the purpose of the data processing are determined by law [cf. Articles 4(7) and 6(3) respectively], and the designated controller may have a (sometimes very limited) room for manoeuvre regarding the determination of "means". But the law may also determine the means (e.g. special software, templates to be used etc.) of the data processing as well. Therefore, the EDPB should make it clear that whenever the law determines the person of the controller, the purpose and/or the means, the room for interpretation of the GDPR is quite limited, and the controller is (almost) only the *addressee* of the obligation imposed by the GDPR (and is not in the position to "determine" the purpose and/or means of the data processing).

There are, however, some other questions, emerged in the practice, that the EDPB should focus on regarding the "controllership by law". For example:

- Can the law establish joint controllership? Or does paragraph 169 exclude this?
- If joint controllership by law is possible, must the law declare this clearly or is it enough if the provisions of the legal instrument point to this direction?

[1] See at the following link
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

- What are the minimum requirements, content-wise, that a law must meet in order to establish joint controllership?

b) In the definition of "controller", one can find reference to the "purpose" and "means" of the data processing, while the data processing has many other aspects to be determined by the data controller: the legal ground, the scope of data, the retention period, the recipients etc. [see—for example—Article 6(3)]. The fact that Article 4(7) does not contain these elements can be considered as the (usual) failure of the GDPR (and the drafters of it).

The Draft should emphasise that determination of these elements are also independent elements of the controllership (and should have been regulated in this way in the GDPR). While it is understandable that the Draft Guidelines would like to squeeze in any of the existing elements of controller, but what the Draft Guidelines chose—namely classifying these elements as part of determination of "means" (cf. paragraph 38)—is totally wrong and contradicts even to the Draft Guidelines, since *"the type of personal data which are processed ('which data shall be processed?'), the duration of the processing ('for how long shall they be processed?'), the categories of recipients ('who shall have access to them?') and the categories of data subjects ('whose personal data are being processed?')"* can be derived from the *purpose* of the data processing, and, therefore, are part of the "what" rather than the "how".[2]

c) The attitude of the Draft Guidelines towards technology providers that provide software, applications for the purpose of data processing is not convincing at all. While *Draft Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* tend to declare those technology providers as data controllers[3] by "encouraging" them to fulfil the obligations of controllers, these Draft Guidelines try to take them out of the scope of data controllership.

But the situation is quite controversial: paragraphs 62 and 65 make it clear that the party providing the "means" is a joint controller, and even only the choosing of a tool provided by another entity constitutes joint controllership… (while in paragraph 82, the same situation is described as a controller-data processor relationship). At the same time, in some examples (e.g. examples "Market research" (p. 16) and "Independent controllers when using a shared infrastructure" (p. 23), etc.) the Draft Guidelines "handsomely" fail to mention the "means" of the data processing to be able to classify one of the actor in the case as data processor.

Unfortunately, the term "determines the means of the data processing" leaves actually no room for excluding these technology providers from being "controller". In other words: while the efforts of the EDBP to finetune the GDPR (which could have been done by the legislator) is meritorious, the rigidity of the GDPR sets (and will always set) limitations. The word "processes" in the term of data processor "processes personal data on behalf of the controller" cannot be interpreted in such a way that the data processor does anything that is reserved to the data controller.

[2] See, for example Article 18(1) of the Rules of Procedure of the EDPB, where „means" means *technical* thing.
[3] See, for example, para. 1 and 86 of the Draft Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

With regard to the "technical and organisational measures" (cf. para. 78.), Article 24 assigns the task of their determination[4] to the controller, while Article 32 mentions only implementation as a task of data processor. See along with this the line "Example: Hosting services"(page 15).

d) The draft's assessment of some examples (n.b. not examples should be presented but clear criteria on how to separate different roles) is also not convincing:

- in such cases, where two entities are in a mandator-mandatary relationship, the fact that the mandatary must act as determined by/upon instruction of the mandator (e.g. client-attorney-at-law relationship, see "Example: Law firm" after para. 25.) cannot be missed. In my view, the statement *"the law firm acts with a significant degree of independence, for example in deciding what information to use and how to use it, and there are no instructions from the client company regarding the personal data processing"* is a quite liberal interpretation of civil law and the laws on attorney-at-law. Would you mandate an attorney-at-law who does *not* follow your instruction in any case, including the determination of what you, as the client, want (c.f. "determines the purpose"), while all the negative consequences fall on you? Generally speaking, "representatives" should always be considered as part of the controller (in case of a legal entity's representative) or the same entity as the controller (in the case of natural persons);
- the example "Market research" (page 16) seems to be inadequate, and "Hosting services", after paragraph 38., are the same in terms of the "data processor" to determine.

2. Contradictions

a) It is recurring in some chapters that a (theoretically) correct statement at the very end of the chapter is preceded by questionable statements in the same topic. For example:

- Subchapter *3.2.2.1 Jointly determined purpose(s)*: while it is true that *"the mere existence of a mutual benefit (for ex. commercial) arising from a processing activity does not give rise to joint controllership"* (paragraph 60.), the statement regarding the Wirtschaftsakademie-case (paragraphs 58-59.), where the "mutual" benefit is missing, in my view (since the parties are not benefited from the other party's activity), contradicts it;
- Subchapter *3.2.2.2 Jointly determined means*: while it is true that *"the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers*" (paragraph 66.), the statements in paragraphs 63. and 65. (namely *"the use of an already existing technical system [by other entities] does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context"*, and especially *"the choice made by an entity to use for its own purposes a tool or other system developed by another entity,*

[4] Although Article 24 uses the word "implement," it is obvious that the controller's obligation is to determine these TOMs.

allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities") clearly contradict it.

What is common in these points is that the first statements are theoretically and legally correct, the rest of the statements tries to justify the unjustifiable, namely the born-in-pain decisions in the *Wirtschaftsakademie* case and the *Fashion ID* case.

b) The Draft Guidelines mention the EDPB Guidelines 3/2018 on the territorial scope of the GDPR only in footnote but fail to realise the contradiction between the Draft and the Guidelines 3/2018.

Paragraph 75 states—theoretically and legally rightly—that *"within a group of companies, one company can be a processor to another company acting as controller,* ***as both companies are separate entities****"* (emphasis added), as well as paragraph 87 states rightly that *"within a group of companies, a company other than the controller or the processor is a third party, even though it belongs to the same group as the company who acts as controller or processor"*. Although these statements are made in relation to "data processors" but—hopefully—it is not difficult to realise that this is true if one examines the status of two "separate entities" in the case of (joint) controllership. It is hard to deny that in the *Google Spain* case the Google Spain *"possesses separate legal personality"*[5] which does not take part in operation the search engine,[6] therefore Google Spain did not take part in determining the purpose and means of the data processing (related to search).[7] In the light of these, Google Inc. and Google Spain are two separate legal entities, two different data controllers in two different data processing operations. Only convoluted justification (doing violence to law) could conclude in the Google Spain case that these two separate entities should be considered as one data controller.

Generally speaking, the Draft Guidelines fail to realise that, in the case of "group of undertakings" (Article 4(19) of GDPR), it is not evident that the "group of undertakings" (i.e. the totality of separate legal entities) is the controller, but it must be carefully examined in each and every data processing operation who can be considered as data controller: in the case of data processing operations of local importance (inc. data processing operations ordered by local laws), the local branch of the "group of undertakings" can exclusively considered as controller, and the "group of undertakings" as such(!) can only be considered as controller in the case of such data processing activities that are decided at the level of the "group of undertakings". It also affects the imposition of administrative fines: in the case of violation of GDPR by a local branch of a "group of undertakings" acting as controller of its own data processing activity of local importance, only the total worldwide annual turnover earned by this local branch can be taken into account and not the "total worldwide annual turnover" of the "group of undertakings".

---

[5] Cf. Case C-131/12 para. 43.

[6] Ibid.

[7] *„The operator of a search engine is the 'controller' in respect of the data processing carried out by it since it is the operator that determines the purposes and means of that processing."* (C-131/12, para. 23), and *"Google Inc. designated Google Spain as the controller, in Spain, in respect of two filing systems registered by Google Inc. with the AEPD; those filing systems were intended to contain the personal data of the customers who had concluded contracts for advertising services with Google Inc."* (C-131/12, para. 43.)

* * *

In sum, the Draft Guidelines—while struggling to "adjust" the old fashioned terms of the GDPR to the current situations—fail to meet its objective to interpret the concept of controller in such a way that it can ensure avoiding "lacunae" and "circumvention of the rules". Anyway, the aim of legal interpretation is not to provide a given kind of answer at any cost, but the aim should be to provide a coherent and contradiction-free interpretation. Unfortunately, the Draft Guidelines failed this.

Zsolt Bártfai