Response to the public consultation on the Guidelines 07/2020 on the concepts of controller and processor in the GDPR

By Miloš Novović, PhD[1]
Associate Professor of Law
BI Norwegian Business School
Oslo, Norway

milos.novovic@bi.no

Summary:
While the Guidelines offer interesting insight into some of the most central terms of the GDPR, EDPB appears to be introducing arbitrary new rules without proper legal basis. As an example, EDPB unfoundedly insists that an Art. 28 agreement must contain clauses more detailed than those already contained in Art. 28, thus overstepping its Art. 70 mandate. In addition, EDPB again ventures into contractual questions, without any competence to do so. Significant revision is therefore recommended, with EDPB being more mindful of the scope of its tasks, the balancing of data protection right with other fundamental rights, and the general scope of reach of EU law.

I Introduction

European Data Protection Board ("EDPB") has recently adopted a public consultation version of *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* ("Guidelines"). Guidelines seek to provide additional details on the concepts of controller and processor under the GDPR, as well as to describe the nature of their relationship in greater detail. The Guidelines are therefore of great practical significance.

However, in the Guidelines, EDPB is *seriously overstepping its authority* – firstly, by introducing arbitrary new criteria that the GDPR never imposes on data controllers and processors; and secondly, by offering observations on contractual validity and interpretation, which it lacks formal and substantive competence to do.

It is disappointing that a body such as EDPB needs to be reminded of the scope of its competences and tasks. This document sets out to offer some short, non-exhaustive observations on the topic.

II EDPB lacks the competence to invent new data protection rules

By the virtue of Art. 70, EDPB has competence to "examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation". It is clear from the wording of the Art. 70

[1] All the opinions presented in this document are author's own, and do not represent the opinions of any organizations or institutions the author is affiliated with.

that the issuing of the Guidelines *must* be done with the sole purpose of encouraging harmonized, consistent application of the rules which are *already* in the Regulation.

If EDPB had a mandate to introduce new data protection requirements through its opinions, serious democratic problems would arise. In a clear violation of the Treaties, an agency with no legislative mandate would be introducing binding provisions, creating legal consequences for the Member States – and private and public organizations worldwide. Such rules would not be subject to judicial review, further cementing their illegitimacy.

Let us consider two examples from the Guidelines.

Firstly, EDPB repeatedly re-iterates that an Art. 28 agreement between a data controller and a data processor "should not merely restate the provisions of the GDPR; rather, it should include more specific, concrete information as to how the requirements will be met". *EDPB has no legal basis whatsoever for making this assertion.*

GDPR Art. 28(3) states that "[the] contract or other legal act shall stipulate, in particular…", and gives a *numerus clausus* list of obligations which have to be included in the contract or other legal act under Union or Member State law. The legislator has spoken: the mere inclusion of the clauses listed in Art. 28(3) is indeed *sufficient* for compliance with the Art. 28(3).

EDPB may offer its observations on the principle of accountability and state that the conclusion of data processing agreements should not become a pro-forma exercise. This would, indeed, naturally flow from the principle of accountability. But there is a vital difference from EDPB *recommending through due diligence and vetting* of processors, versus EDPB stating that an Art. 28(3) contract *must include additional clauses to satisfy Art. 28(3)*. The latter statement is *clearly disregarding* the wording of GDPR Art. 28.

The motives here are not hard to distinguish: EDPB wants to avoid a scenario where contracts are so short as to render supervision difficult. It is, indeed, easier for data protection authorities to check whether processing is legally compliant if all the details of processing are contained in a single contract. However, the fact that something makes supervision easier does not grant the EDPB the legal basis to invent new rules, *nor to force data controllers and processors* to assume *additional contractual* obligations.

The second example is the one pertaining to joint controllership arrangements, where EDPB states that a written contract is recommended because of the "legal certainty", and imposes the additional obligation to conclude an agreement "in plain *language*". Firstly, much like in the previous case, such requirement is nowhere to be found in the GDPR, and EDPB lacks the competence to introduce it. Secondly, it is unclear how EDPB has the competence to interpret the concept of "legal certainty". This is not a term defined in the GDPR, and not a term with an autonomous legal interpretation in the European Union. Consequently, EDPB has no basis to make such recommendations.

III EDPB has no competence to assess validity, formation, modification or interpretation of contracts

In the same vein as the Guidelines on Art. 6(1)(b), EDPB is *seriously overstepping its competence* by offering observations on contract formation, validity and interpretation.

As previously remarked, while data protection law is (to an extent) harmonized throughout EU through GDPR and other instruments, *contract law remains largely unharmonized* – barring sporadic provisions stemming from fields such as consumer protection. Consequently, data protection terms and provisions are meant to be interpreted autonomously, while the interpretation of contract law terms remains in the domain of different – and often diverging – *national contract laws*.

EDPB consequently has *no legal basis* to interpret national contract laws, or introduce rules on contractual formation, interpretation, form, validity, modifications or termination. Consider the following statements:

> To avoid any difficulties in demonstrating that the [Art. 28] contract or other legal act is actually in force, the EDPB recommends *ensuring that the necessary signatures* are included in the legal act.
>
> Even if a contract is silent as to who is the controller, it may contain *sufficient elements to infer who exercises a decision-making role* with respect to the purposes and means of the processing. It may also be that the contract contains an *explicit statement* as to the identity of the controller. If there is no reason to doubt that this accurately reflects the reality, there is nothing against following the terms of the contract.
>
> Any proposed *modification*, by a processor, of data processing agreements included in standard terms and conditions should be directly notified to and approved by the controller. The mere *publication of these modifications* on the processor's website is not compliant with Article 28.
>
> Therefore, for the sake of legal certainty, even if there is no legal requirement in the GDPR for a contract or other legal act, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject. This would provide certainty and could be used to evidence transparency and accountability. Indeed, in case of non-compliance with the agreed allocation provided in the arrangement, *its binding nature allows one controller to seek the liability of the other for what was stated in the agreement as falling under its responsibility*.

In all of these instances, EDPB is dabbling in questions ranging from contractual form (written form with signatures), the form of contractual modifications (website updates vs. direct notification), interpretation of contractual terms or contractual silence, and potential breach of contract claims between joint controllers. This comes in addition to a long section on Art. 28(3), where EDPB proposes a long list of terms to be included in the contracts, without any regard for the effects that these terms give rise to under different applicable laws.

This is important to note, as the rights and obligations of the parties *do not stem from the contractual text itself* – but rather, from the *interaction* between the governing (*contract*) law and various other elements *that contract law* deems *relevant* (such as the text of the contract, the

conduct of parties during negotiations, any prior or subsequent conduct, etc.). EDPB has *no legal basis* to select and comment on a random selection of these *elements* because their legal effects are not produced in vacuum; but rather, by interacting with the unharmonized field of contract law which EDPB has *no competence* to interpret.

It must also be mentioned that EDPB needs to be mindful of the fact that freedom of contract is *also one of the fundamental rights*, and that even if the Guidelines were revised to only offer observations on data protection issues, this would still need to be *balanced* as not to infringe on freedom of contract and other fundamental rights. As clearly stated in Recital 4: "The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality." It remains unclear why EDPB is ignoring freedom of contract in the guidelines which touch upon contractual questions.

IV Conclusion

The Guidelines offer an interesting insight into some of the problems stemming from the interpretation of the terms "controller" and "processor". They are written in an example-driven way, and they are more useful to the general public than a number of recent EDPB opinions.

Where the Guidelines fail, however, is when they start inventing data protection requirements not found in the Regulation, and offering observations on questions on national contract law.

Substantial revision is therefore strongly recommended.