Position Paper

Comments regarding Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0, adopted on 02 September 2020

******

Introduction

Floreani Studio Legale Associato welcomes the opportunity to provide a response to the European Data Protection Board's consultation on the drafts Guidelines 07/2020 on the concepts of controller and processor in the GDPR and invites the EDPB to evaluate the following proposals as well as to clarify the problems highlighted below.

Part I - CONCEPTS

DEFINITION OF CONTROLLER

2.1.2 "Determines"

Para. 23: "*In the absence of control arising from legal provisions, the qualification of a party as controller must be established on the basis of an assessment of the factual circumstances surrounding the processing. All relevant factual circumstances must be taken into account in order to reach a conclusion as to whether a particular entity exercises a determinative influence with respect to the processing of personal data in question".*

Comment: We would like to request the EDPB to confirm that the criterion of legitimate expectations of data subjects based on the visibility/image gived by the controller to the same referred to in the previous "*Opinion 1/2010 on the concepts of "controller" and "processor*" ("*Visibility/image given by the controller to the data subject, and expectations of the data subjects on the basis of this visibility*", par. III.1.a) e III.2. can no longer be used in case of doubt to identify the controller and, in the aforementioned hypothesis, to clarify the reasons in support of this choice, given the absence of explicit references from the Guidelines.

2.1.4 "Purposes and means"

Para. 35: "*In practice, if a controller engages a processor to carry out the processing on its behalf, it often means that the processor shall be able to make certain decisions of its own on how to carry out the processing. The EDPB recognizes that some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing. In this perspective, there is a need to provide guidance about which level of influence on the "why" and the "how" should entail*

the qualification of an entity as a controller and to what extent a processor may make decisions of its own".

Comment: It is suggested to the EDPB to specify through practical cases in which terms "*that some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing*". Furthermore, it is requested to clarify with concrete examples the prediction for which "*In this perspective, there is a need to provide guidance about which level of influence on the "why" and the "how" should entail the qualification of an entity as a controller and to what extent a processor may make decisions of its own*".

2.1.5 "Of the processing of personal data"

Para. 42: ***"It is not necessary that the controller actually has access to the data that is being processed. Someone who outsources a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data".***

Comment: We would like to request the EDPB to confirm that failure to access the data being processed does not imply the impossibility of considering as the controller the person who determined the purposes and essential means with which the processing is carried out by the processor.

3 DEFINITION OF JOINT CONTROLLERS

3.2.2 "Assessment of joint participation"

Para. 51: ***"Joint participation in the determination of purposes and means implies that more than one entity have a decisive influence over whether and how the processing takes place. In practice, joint participation can take several different forms. For example, joint participation can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities regarding the purposes and essential means".***

Comment: We would like to request the EDPB to clarify, with the use of practical examples, the distinction between the forms that the joint participation can take and, in particular, between the case in which the joint participation takes the form of a common decision taken by two or more entities and the one, on the other hand, resulted from converging decisions of two or more entities, regarding the purposes and essential means.

Para. 53: ***"(…). Decisions can be considered as converging onpurposes and means if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing. As such, an important criterion to identify converging decisions in this context is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. (…)".***

Comment: It is suggested to the EDPB to specify through practical cases in which terms – on the basis of what is stated from the case law of the CJEU - "*the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. (…)".*

DEFINITION OF PROCESSOR

4 Definition of processor

Para. 75: ***"A separate entity means that the controller decides to delegate all or part of the processing activities to an external organisation. Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a department within a company cannot generally be a processor to another department within the same entity".***

Comment: The last subparagraph of section 75 stipulates that "*On the other hand, a department within a company cannot generally be a processor to another department within the same entity"*. Here, since the Guidelines use the adverb *"generally",* we would like to ask the EDPB to avoid interpretative uncertainties and to specify which exceptions to the rule are foreseen and to evaluate the opportunity to reformulate the highlighted prediction with greater clarity.

Para. 82: ***"As stated above, nothing prevents the processor from offering a preliminary defined service but the controller must make the final decision to actively approve the way the processing is carried out and/or to be able to request changes if necessary. Example: Cloud service provider".***

Comment: We propose the EDPB to evaluate the opportunity to reformulate the example shown here ("*Cloud service provider*") since it is inappropriate. From a practical point of view, in the case considered here, it is difficult to hypothesize that a "*small*" controller may be able to intervene and/or request changes on the terms of processing (for example, storage periods, data deletion, etc.) performed by a cloud service provider ("*The cloud service provider has offered a standardized service that is offered worldwide*") with greater bargaining strength (for example, Big Tech).

PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES

1 - RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR

1.1. Choice of the processor

Para. 92: "*The controller has the duty to use "only processors providing sufficient guarantees to implement appropriate technical and organisational measures", so that processing meets the requirements of the GDPR - including for the security of processing - and ensures the protection of data subject rights. The controller is therefore responsible for assessing the sufficiency of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration".*

Comment: With reference to the requirement of the controller - if a processing needs to be carried out on his behalf – *to use "only processors providing sufficient guarantees to implement appropriate technical and organisational measures", so that processing meets the requirements of the GDPR - including for the security of processing - and ensures the protection of data subject rights*", we ask the EDPB to predict the case in which the controller is unable to identify a subject possessing the aforementioned characteristics and to clarify what the consequences may be in terms of relations with the external organization that carries out data processing activities on his behalf.

1.3. Content of the contract or other legal act

Para. 109: "*While the elements laid down by Article 28 of the Regulation constitute the core content of the agreement, the contract should be a way for the controller and the processor to further clarify how such core elements are going to be implemented with detailed instructions. Therefore, the processing agreement 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 and which level of security is required for the personal data processing that is the object of the processing agreement. (…)".*

Comment: We ask the EDPB to specify that the inclusion of additional elements and/or information with respect to the main content of the agreement must be the subject of a specific assessment made by the controller, in the light of the actual relationships with the processor ("*rather, it should include more specific, concrete information as to how the requirements will be met")* and not an obligation as it is not governed by the Regulation, since the minimum mandatory content of the contract or other legal act is already punctually regulated by article 28 (3) of the GDPR.

1.3.6. The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR).

Para. 133: "*Secondly, the processor must assist the controller in meeting the obligation to notify personal data breaches to the supervisory authority and to data subjects. The processor must notify the controller whenever it discovers a personal data breach affecting the processor's or a sub-processor's facilities /IT systems and help the controller in obtaining the information that need to be stated in the report to the supervisory authority".*

Comment: With regard to the processor's duty to assist the controller in compliance with the obligations referred to in articles 32 to 36 of the GDPR, we suggest the EDPB to mention in the Guidelines the case which the "*processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor"* (*Guidelines on Personal data breach notification under Regulation 2016/679,WP250 rev.01, 6 February 2018, p. 14*).

1.3.8. The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR).

Para. 141: "*Further details shall also be set out in the contract regarding the ability to carry out and the duty to contribute to inspections and audits by the controller or another auditor mandated by the controller. The parties should cooperate in good faith and assess whether and when there is a need to perform audits on the processor's premises. Likewise, specific procedures should be established regarding the processor's and the controller's inspection of sub-processors (see section 1.6 below)".*

Comment: With reference to the highlighted paragraph and, specifically, in relation to the possibility that inspections can be carried out by another person appointed by the controller, it is proposed to the EDPB to identify some examples in the Guidelines (for example, by recalling the DPO nominated by the controller or other subjects internal or external to the organization of the controller).

1.4 Instructions infringing data protection law

Para. 142: "*According to Article 28(3), the processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions".*

Comment: The evaluation and information obligations of the processor referred to in the paragraph in question refer exclusively to the "*GDPR or other Union or Member State data protection provisions*". It is proposed to the EDPB to evaluate the opportunity to foresee the case for which the instructions

provided by the controller infringes the GDPR other than those mentioned above and to clarify in the aforementioned hypothesis whether any liability issue is possible for the processor for infringe of article 28 (3) of the GDPR.

Para. 142: "*According to Article 28(3), the processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions".*

Comment: We ask the EDPB to clarify whether the controller has the right to refrain from executing such an instruction, if he considers that the instruction provided by the controller infringes the Regulation or other provisions on data protection and whether the execution of the information activities towards the controller may limit their responsibility profiles towards the controller.

1.6. Sub-processors

Para. 148: "*Although the chain may be quite long, the controller retains its pivotal role in determining the purpose and means of processing. Article 28(2) GDPR stipulates that the processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. In both cases, the processor must obtain the controller's authorisation in writing before any personal data processing is entrusted to the sub-processor. In order to make the assessment and the decision whether to authorise subcontracting, a list of intended subprocessors(including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor".*

Comment: We ask the EDPB to specify more clearly that, in addition to the nomination by the processor of the sub-processor, the latter can, in turn, nominate a further sub-processor ("sub-sub-processor") and, therefore, that said possibility of configuring a "chain of sub-processors" in light of the provisions of article 28 (2-4) of the GDPR is compatible with the Regulation.

2 - CONSEQUENCES OF JOINT CONTROLLERSHIP

2.2.2. Obligations towards data subjects

Para. 178: "*What should be covered by the notion of "essence of the arrangement" is not specified by the GDPR. The EDPB recommends that the essence cover at least all the elements of the information referred to in Articles 13 and 14 that should already be accessible to the data subject,*

and for each of these elements, the arrangement should specify which joint controller is responsible for ensuring compliance with these elements. The essence of the arrangement must also indicate the contact point, if designated".

Comment: With reference to the obligation to make the "essence of the arrangement" available to the data subjects pursuant to article 26 (2) of the GDPR, given the principle that the controller is not obliged to provide the data subject with the information he is already aware of, we ask the EDPB to provide in the Guidelines that the essence of the arrangement may omit the information referred to in articles 13 and 14 of the GDPR.

Para. 179: "*The way such information shall be made available to the data subject is not specified. Contrary to other provisions of the GDPR (such as Article 30(4) for the record of processing or Article 40(11) for the register of approved codes of conduct), Article 26 does not indicate that the availability should be "upon request" nor "publicly available by way of appropriate means". Therefore, it is up to the joint controllers to decide the most effective way to make the essence of the arrangement available to the data subjects (e.g. together with the information in Article 13 or 14, in the privacy policy or upon request to the data protection officer, if any, or to the contact point that may have been designated). Joint controllers should respectively ensure that the information is provided in a consistent manner".*

Comment: With respect to the provision in question, it may be appropriate for the EDPB to clarify whether the controllers are required to acquire a declaration of knowledge of the "essence of the arrangement" from the data subjects, in order to demonstrate the correct fulfillment of the obligations pursuant to article 26 (2) of the GDPR.

Para. 179: "*The way such information shall be made available to the data subject is not specified. Contrary to other provisions of the GDPR (such as Article 30(4) for the record of processing or Article 40(11) for the register of approved codes of conduct), Article 26 does not indicate that the availability should be "upon request" nor "publicly available by way of appropriate means". Therefore, it is up to the joint controllers to decide the most effective way to make the essence of the arrangement available to the data subjects (e.g. together with the information in Article 13 or 14, in the privacy policy or upon request to the data protection officer, if any, or to the contact point that may have been designated). Joint controllers should respectively ensure that the information is provided in a consistent manner".*

Comment: We ask the EDPB to specify in the Guidelines that any subsequent amendments to the agreement that concern essential aspects of the arrangement must also be made known to the data subject (in particular, as regards the relations of the joint data controllers with the data subjects).

2.3. Obligations towards data protection authorities

Para. 189: "*It should be recalled that data protection authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point. (…)".*

Comment: In this regard, in relation to the provisions of paragraph 171 of the Guidelines ("*Also, in line with the accountability principle, the use of a contract or other legal act will allow joint controllers to demonstrate that they comply with the obligations imposed upon them by the GDPR*"), we ask the EDPB to evaluate the opportunity to specify in the Guidelines that, with regard to the internal division of responsibility, the contents of the agreement may be assessed by the data protection authorities to reconstruct the roles of controllers in the context of the processing activities performed by each, although they are not, in themselves, opposable.

We would be grateful for your consideration of our comments and proposals and remain available for any clarification and further information.

Sincerely.

19 October 2020