Ecommerce Europe's contribution the EDPB Public Consultations - Comments to the Guidelines 7/2020 on the concepts of controller and processor in the GDPR

Introduction

Ecommerce Europe is the sole voice of the European Digital Commerce sector. It represents, via its 25 national associations, more than 100,000 companies selling goods and services online to consumers in Europe. Ecommerce Europe acts at European level to help legislators create a better framework for online merchants, so that their sales can grow further. We welcome the opportunity to provide our feedback to the recently published EDPB's Guidelines 7/2020 on the concepts of controller and processor in the GDPR.

General remarks

Ecommerce Europe overall finds that the assignment of roles in multi-actor environments should be clarified and simplified in the guidelines. Companies should be able to act through roles assigned on an 'overall' processing level that will prevent extensive administrative burden.

In practice, most personal data processing activities include multiple parties. The guidelines are unclear on how granularly parties should define roles in personal data processing. Roles defined on a purpose or processing activity level will very likely lead to blurrier controller-processor relationship where processors are also controllers for certain activities and face joint controllership for others. Processors and controllers would be required to conclude contracts where the roles change based on processing activity.

Extensive granularity would not provide any value for individuals whose data is processed while significant overlaps in roles would emerge. As a result, informing individuals in a clear and simple manner and facilitating individual rights would become effectively impossible. Such approach would create legal uncertainty for both the data subjects and the parties involved in processing, running contrary to the EDPB's objective of ensuring full and comprehensive protection of data subjects' rights.

For further insights into Ecommerce Europe's general view on the published guidelines and the role of online retailers as joint controllers in data processing, we would kindly like to refer you to our reply to the consultation on Guidelines 08/2020 on the targeting of social media users.

Remarks on the Guidelines 07/2020 on the concepts of controller and processor in the GDPR

In this section you can find Ecommerce Europe's feedback on several paragraphs in the Guidelines:

- **Executive Summary, Joint controllers (p 3)**

"converging decisions by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing."

Ecommerce Europe is of the opinion that the concepts of converging decisions or decisions that complement each other, could significantly widen the applicability of Article 26 GDPR and may cause legal uncertainty. The wording of Article 26 rather suggests a common decision, not a complementary decision. The extension of the concept renders it more difficult to distinguish between a controller-to-controller situation (separate controllers) and a joint controller situation which, in our view, does not contribute to a better understanding of this provision.

❖ **Paragraphs 38, 42**

Ecommerce Europe calls on the EDPB to clarify paragraphs 38 and 42 and the examples that are used in the Guidelines. In the example used in paragraph 42, the essential information on from which data pool the test persons come and who decides on the selection, appears to be missing.

❖ **Paragraphs 51, 52, 53**

Paragraphs 51, 52 and 53 refer to the qualification of joint controllership on the basis of converging decisions. Similar to the comment raised above on the executive summary, Ecommerce Europe would like to stress that Article 26 GDPR suggests a common decision, rather than a converging decision. In addition, the basis of converging decisions for the identification of joint controllership may cause uncertainty as it entails that two entities taking converging decisions and being unaware or not-willing-to, could in the end qualify as joint controllers without factually being able to meet their legal obligations under the GDPR (i.e. drafting of an arrangement allocating responsibilities).

❖ **Paragraph 58**

Paragraph 58 states that "when the entities do not have the same purpose for the processing, joint controllership may also, in light of the CJEU case law, be established when the entities involved, pursue purposes which are closely linked or complementary." Similar to the comments above, this statement substantially broadens the scope of the concept of joint processor compared to a common understanding of the word 'jointly'. In the view of Ecommerce Europe, such an extension cannot be justified by wording of the GDPR provision or the CJEU case law.

❖ **Paragraph 64**

Paragraph 64 argues that an administrator of a Facebook fan-page, "by defining parameters based on its target audience and the objectives of managing and promoting its activities, must be regarded as taking part in the determination of the means of the processing of personal data related to the visitors of its fan page." Ecommerce Europe calls on the EDPB to clarify this statement as it is not clear whether this interpretation would also apply to providers in the advertising value chain such as SSPs, where the publisher sends an ad request or integrates a script that calls for the SSP to set a cookie. However, in such a case, the publisher does not define what data exactly is collected and will not be setting any parameters, as in practice it will be mostly the case and would normally lead to separate/independent controllership. In that perspective, Ecommerce Europe is concerned that the broad interpretation of joint controllership as elaborated in this document, would most likely cause confusion amongst all the different players in the advertising value chain and certainly will not contribute to a better understanding of the complex processing systems nor enhance protection of data-subjects.

❖ **Paragraph 82, Example (p 27)**

In the example in paragraph 82, the guidelines argue that a municipality that uses a cloud services provider for handling information on school and education services, as a joint controller, "must also make sure that their specific instructions on storage periods, deletion of data etc. are respected by the cloud service provider regardless of what is generally offered in the standardised service." Ecommerce Europe would like to point out that, in practice, it can be very difficult or even impossible for the joint controller to comply with this obligation, as service providers often do not allow to deviate from their preliminary defined settings arguing that they cannot accommodate variations of the standard services offered for individual clients.

❖ **Paragraphs 83-90**

Paragraphs 83 to 90 describe the concepts of recipient and third party. Unlike the concepts of controller and processor, the Regulation does not lay down specific obligations or responsibilities for recipients and third parties. The Guidelines explain them as relative concepts in the sense that they describe a relation to

a controller or processor from a specific perspective, e.g. a controller or processor discloses data to a recipient. Although the Guidelines explain the roles of recipients and third parties as such, Ecommerce Europe would welcome further information on the role of controllers/processors towards recipients or third parties, and on whether there is anything controllers/processor should be doing in the form of a contract.

- **Paragraph 93**

Paragraph 93 states that an exchange of relevant documentation between the controller and processor often is required, so that the controller can assess the processor's compliance with its obligations. This information would include for instance "privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external audits, recognised international certifications, like ISO 27000 series)." In Ecommerce Europe's view, it is generally quite difficult for online retailers to get this type of information from their processors, in particular when processors provide a standardised service at relatively low cost on a "take it or leave it" basis (e.g. a CRM tool) and with no factual influence of the online retailer on this processing.

- **Paragraph 97**

Paragraph 97 builds on the previous paragraphs and argues that "the controller should, at appropriate intervals, verify the processor's guarantees, including through audits and inspections where appropriate." As mentioned before, Ecommerce Europe would like to flag that, in practice, it is often difficult or factually impossible for controllers to comply with these obligations, as processors of standardized services usually argue that they cannot allow such controls/audits to their many clients and in consideration of the relatively low contractual sums. In that perspective, Ecommerce Europe would like to have guidelines for Controllers, joint controllers and processors on how to perform GDPR obligations they factually cannot deliver.

- **Paragraph 99**

In Paragraph 99, based on the fact that any processing of personal data by a processor must be governed by a contract or other legal act, the Guidelines argue that such a legal act must be in writing, including in 'electronic form', and "to avoid any difficulties in demonstrating that the contract or other legal act is actually in force, the EDPB recommends ensuring that the necessary signatures are included in the legal act." Ecommerce Europe calls on the EDPB to provide more clarification on this paragraph, as its guidance on this issue seems to reflect a rather restrictive interpretation of 'electronic form', excluding click-through contracts or conclusion by reference in the underlying contract (written link that enables to identify which version of a DPIA has been included by the parties).

- **Paragraph 101**

The guidelines state in this paragraph that although each data processing relation should be based on a written contract or other legal basis, a controller-processer relation could still be held to exist in absence of a written processing agreement or other legal basis. (footnote. 35). However, this would imply a violation of Article 28(3) and, moreover, it would raise in certain circumstances the problem of the lack of a legal basis on which every processing should be based, 'e.g. in respect of the communication of data between the controller and the alleged processor'. Ecommerce Europe would welcome further clarification on this concept, i.e. on whether data sharing between controllers and processors should be subject to a specific legal basis, or whether the processor, with no clearly defined role, should be regarded as acting in another capacity (as a controller or a third party). In Ecommerce Europe's view, the lawfulness of a data processor's activities is already sufficiently and adequately conditioned on the existence of a data processing agreement and Article 28 GDPR and the processor's adherence to it. Setting out a separate legal basis covering data sharing between a data controller and a data processor should therefore not be required.

- **Paragraphs 106/107**

Paragraphs 106 and 107 describe that contracts between controllers and processors may sometimes be drafted unilaterally by one of the parties. Which party or parties will draft the contract may depend on several factors including the parties' position in the market and contractual power, their technical expertise, as well as access to legal services. Some data processing service providers in their role as processor tend to unilaterally set up standard terms and conditions, which include data processing agreements. The guidelines state it is generally no problem that processors draft processing agreements unilaterally while maintaining the role of a data processor. However, the processor should directly notify any modification of the data processing agreement to the controller to be approved by the (joint) controller. Ecommerce Europe would welcome further clarification to what extent the EDPB position in these paragraphs is applicable in situations where processors mandate part of the processing done on the controller's behalf to third parties (sub-processors).

❖ **Paragraph 160**

According to the guidelines, Article 26(1) GDPR provides that joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the Regulation. Joint controllers thus need to set "who does what" by deciding between themselves who will have to carry out which tasks. Paragraph 160 adds that "The objective of these rules is to ensure that where multiple actors are involved, especially in complex data processing environments, responsibility for compliance with data protection rules is clearly allocated in order to avoid that the protection of personal data is reduced, or that a negative conflict of competence lead to loopholes whereby some obligations are not complied with by any of the parties involved in the processing. It should be made clear here that all responsibilities have to be allocated according to the factual circumstances in order to achieve an operative agreement."

In this context, Ecommerce Europe explicitly wants to draw attention to the fact that online retailers as joint controllers are in practice not in a position to influence the data processing agreement. This applies especially in the context of online data processing services that are offered to online retailers as a standard product on a "take it or leave it" basis and where the provider of these standard data processing services is dominantly deciding on purposes and means of the processing (like social media plug-ins, data analytics etc.) and where the online retailer, as user of this services and joint controller, has hardly any or no influence or decisive power on the processes conducted by the data processing service provider. In that perspective, Ecommerce Europe strongly recommends taking this unequal position into account when allocating responsibilities between controller and processor.

❖ **Paragraph 179**

Paragraph 179 refers to the obligation to ensure that the data subject is aware of the "essence of the arrangement". The obligation to make the essence of the arrangement available to data subjects is important in case of joint controllership in order for the data subject to know which of the controllers is responsible for what. What should be covered by the notion of "essence of the arrangement" as well as the way such information shall be made available to the data subject is not specified by the GDPR. Paragraph 179 specifies that "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."

Ecommerce Europe would like to point out that, specifically in the martech (marketing technology) and adtech (advertising technology) space, there is potential for many providers being qualified as joint controllers. In that context, it is almost impossible to provide information for all these situations in a consistent manner in a Privacy Notice or Cookie Notice. This extensive information obligation by all participants in the data-processing would probably cause information overload and information fatigue, and

thus will not be effective. To avoid double information and information overload, Ecommerce Europe calls on the EDPB to emphasise, in their guidance, that it is not necessary to include all this information into Privacy Notices, but that it can also only be made available upon request. In the latter case, it would be useful to have guidance on what type of information would still need to be included in a Privacy Notice (using a layered approach) and which participant would be most equipped to provide this information.

- **Paragraphs 188/189**

Paragraph 188 specifies that joint controllers should organise in the arrangement the way they will communicate with the competent supervisory data protection authorities. Moreover, paragraph 189 adds that 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. Therefore, the authorities can contact any of the joint controllers to exercise their powers under Article 58 with respect to the joint processing. Ecommerce Europe calls on the EDPB to clarify to what extent supervisory authorities are allowed to go beyond parties' valid agreements, to make sure it does not create any legal uncertainty for the joint controllers involved.