Public consultation
19/10/2020

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

EuroCommerce

EuroCommerce is the voice for over 5 million retail, wholesale, and other trading companies. Our members include national federations in 31 countries, Europe's 35 leading retail and wholesale companies, and federations representing specific retail and wholesale sectors.

Introduction

EuroCommerce welcomes the opportunity to provide a contribution to the public consultation on the guidelines on controller and processor. Below we provide an overview of our main concerns and detailed comments. In these we ask for clarification of the scope of the joint controllership relationship when processing data and of the legal basis of processing in a controller to processor relationship. The delineation between between processors, controllers, and joint controllers is not always (despite the useful contribution made by this draft guidance) clear cut. In those cases where it is not, we would ask for guidance to data protection authorities to avoid an immediate resort to enforcement before engaging in constructive discussion with market actors where they believe their analysis has not gone the right way.

Our key asks

1. Clarification of the legal basis of processing in a joint controllership relationship.
2. Clarification on liability where contracts are unilaterally drafted by the data processor.
3. Clarification of the legal basis of processing in the controller-to-processor relationship.
4. Clear and simple definition of the scope of multi-actor environments.
5. National data protection authorities (DPAs) to avoid unilateral interpretation of the relationship, and encouragement of dialogue and cooperation on outcomes rather than immediate resort to enforcement action.

General recommendations on the guidelines on controller/processor

- ***On the definition of processor (in executive summary of the draft Guidance):*** We would ask for the paragraph:
  "The processor must not process the data otherwise than according to the controller's *written* instructions.''
  Additionally, since the processor is allowed to determine non-essential means, the text should be clear about the instructions which should pertain to the purpose and the essential means of the assigned processing activities. We suggest adding the words in red to achieve this:
  "The controller's instructions *should pertain to the purpose and the essential means of the assigned processing activities. The processor is* allowed a certain degree of discretion about how best to serve the controller's interests in choosing the most suitable technical and organizational means ('non-essential means')."
  The conclusion in the last sentence of this paragraph describes a processor who changes becomes a controller. Changing colour should only, in our opinion, be limited to the situations where a processor determines the purpose(s) and essential means of the assigned processing. This would also align this paragraph with paragraph 37 of the guidelines. If determining even the smallest number of 'means' turns a processor into a controller, keeping the concept of

processor becomes redundant, as in practice none would exist. We would suggest the following **alternative wording**:

"A processor infringes the GDPR, however, if it goes beyond the controller's instructions and starts to determine its own purposes and *essential* means of the processing. The processor will then be considered a controller in respect of that processing and may be subject to sanctions for going beyond ~~the~~ *such* controller's instructions."

- ***On paragraph 9:*** The last sentence of this paragraph ("At the same time, it should be recalled that processors must always comply with, and act only on, instructions from the controller.") would seem to imply that in all instances a processor should follow the instructions of the controller. The scope of the instructions to be given by the controller should be limited to instructions pertaining purely to the purpose and the essential means of the assigned processing activities, aligning this paragraph with paragraph 37 of the guidelines. We would ask for **additional wording to clarify that the controller may only give written instructions which are in conformance with applicable law.**

- ***On paragraph 38:*** This paragraph should avoid any impression that a separate processing agreement needs to be concluded between parties. The GDPR does not prescribe such a separate agreement. We suggest **deleting the wording**: "and a data processing agreement according to Article 28 must be concluded." As paragraph 38 explains, when determining the means, a distinction can be made between essential and non-essential means where "essential means" are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller. In many cases, IT and online services are standardised services, where the essential means are already predefined. Alterations to the services offered are either not possible or associated with high costs for the buyer. It would be helpful to have further clarifications on how to assess these types of standardised services where the "essential means" already are predefined and if there can be situations where a "processor" is actually treated as a controller when offering a standardised service. If possible, it would be helpful if the EDPB could **provide a standardised template to be used in data processor agreements**.

- ***On paragraph 42:*** Some of our members do not consider classic marketing research as a controller-processor relationship. A research agency delivers a report based on statistical processing of the data derived from filed questionnaires. Equally, a public directory or its own panel database does not represent a controller/processor relationship as described. There are a number of points which need to be taken into account:
  - Results are statistical results e.g. 23% of members of Z generation thinks that brand A is better than brand B
  - For the company that ordered the research, the data is aggregated and completely anonymised.
  - The situation changes where a company provides a database of contacts drawn from its customer base, and this becomes a classic controller-processor relationship.

- ***On paragraph 101:*** The current draft guidelines state that each data processing should be on a legal basis (…) "in respect of the communication of data between the controller and the alleged processor''. It is not clear whether the data sharing between controller and processor should be subject to a specific legal basis or whether the processor with an unclearly defined role should be regarded as acting in another capacity (as a controller or a third party), thus raising the problem of the lack of a legal basis. The guidance needs to reflect that a processor carries out no data processing for its own purposes, nor independently from the data controller. The lawfulness of data processor's activities is already conditional on the existence of a data processing agreement, Article 28 of the GDPR and the processor's adherence to it. We therefore see no need for a separate legal basis to cover data sharing between a data controller and data processor

- ***On paragraph 109:*** As explained above, this paragraph should avoid giving the impression that a separate processing agreement needs to be concluded between parties. The GDPR does not prescribe the need for such a separate agreement. We suggest the following amended wording (changes in red):

"~~While~~ *In addition to* 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~~ the controller and the processor *should* ~~to~~ further clarify how such ~~core~~ elements are going to be implemented with detailed instructions."

- ***On paragraph 164:*** We see a strong need to clarify the legal basis of processing data in a joint controllership relationship. According to the draft Guidelines each disclosure of data requires a legal basis to be set in place, 'regardless of whether the recipient is a separate controller or a joint controller' (ftn. 59), presumably in the context where 'personal data are shared by one controller to another' (para. 164). However, the lawfulness of data exchange between joint controllers – unlike in the case of separate controllers – can already be ensured by a contractually binding joint-controllership arrangement. As currently drafted, this provision would contradict the intent behind either form of joint participations laid out in the draft Guidelines***.***

- ***On security measures:*** The controller is responsible for ensuring and demonstrating compliance with the GDPR according to Article 24. This includes responsibility for implementing appropriate technical and organisational measures. In addition, Article 28.1 lays down that the controller can only use processors who provide sufficient guarantees to implement technical and organisational measures. Moreover, the processor must be able to demonstrate compliance to the satisfaction of the controller, cf. paragraph 93. In many cases, the service provider has the sole responsibility of implementing security measures appropriate to the risk, and the controller has an obligation to conduct audits and inspections to ensure that the security measures are sufficient (Article 28.3 (f) and (h)). Article 24.3 allows for approved certification mechanisms referred to in Article 42 to be used as an element to demonstrate compliance. Considering the above, we wish to highlight that existing information security standards, such as the SOC 1, SOC 2, and SOC 3, can be used to assess whether a service provider satisfies "good information security practices". With this mechanism in place for auditing information security measures and obtaining reasonable assurance through these reports, it would be beneficial if data controllers could demonstrate compliance also under the GDPR by relying on existing standards regarding information security measures implemented by their processors. By using existing standards, controllers would have better tools to assess information security measures as part of their obligations under the GDPR, and processors have a clear framework for ensuring a high level of information security in their services. Such an approach would thus work to improve protection of data subjects' rights. In this context, we welcome the statement from EDPB that certain existing standards indeed could serve to demonstrate compliance under the GDPR, e.g. regarding implemented information security measures.

- ***On fines:*** It would be helpful if explicit wording were included to the effect that DPAs shall, when imposing fines, take into account the degree of responsibility of the controller and/or processor with regard to a violation. There is a significant degree of confusion about this, leading to clauses being included in agreements between parties to shift the responsibility of an imposed fine upon the other – often smaller – party, even though this party is not in fact responsible for the actual violation of the GDPR. Indeed, according to Article 83.2 (d) of the GDPR, a DPA should consider the degree of responsibility of the controller or processor when imposing a fine. We would ask EDPB to include a clear statement that DPAs shall impose a fine on the party that actually violates the GDPR (whether the controller, the processor or both parties), taking into account the degree of responsibility of the parties with regard to the violation.

Contact:
Ena Salihovic - +32 2 737 05 83 - salihovic@eurocommerce.eu **Transparency Register ID: 84973761187-60**