



Verda_Bulletin

No: 2021_30

Guidelines on the concepts of controller and processor in the GDPR

The European Data Protection Board (EDPB) has issued the final version of its guidelines on the concept of controllers and processors under the GDPR which also aims to clarify the fundamental concepts (of joint controller and processor). It includes updated wording and further clarifications in order to address comments and feedback received during the public consultation. The main purpose of the Guidelines is to clarify the application of the GDPR and examples of common scenarios of data processing are also provided.

Here are the features of the guidelines:

- In its executive summary, the EDPB has emphasized that, the concepts of controller, joint controller and processor play a crucial role in the application of the General Data Protection Regulation (GDPR), since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice.
- The concepts of controller, joint controller and processor are functional concepts in that they aim to allocate responsibilities according to the actual roles of the parties and autonomous concepts in the sense that they should be interpreted mainly according to EU data protection law.
- A controller is a body that decides certain key elements of the processing and in principle, there is no limitation as to the type of entity that may assume the role of a controller but in practice it is usually the organization as such, and not an individual within the organization (such as the CEO, an employee or a member of the board), that acts as a controller. Controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case.
- **In many cases, the terms of a contract can help identify the controller, although they are not decisive in all circumstances.** A controller determines the purposes and means of the processing, i.e. the why and how of the processing. The controller must decide on both purposes and means and it is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller.



- The GDPR introduces specific rules for joint controllers and sets a framework to govern their relationship. **The main criterion for joint controllership is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable.** The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand.
- A processor is defined as a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller and **two basic conditions are mentioned for qualifying a processor: that it is a separate entity in relation to the controller and that it processes personal data on the controller's behalf.**
- The processor must not process the data otherwise than according to the controller's instructions and those instructions may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means.
- **Any processing of personal data by a processor must be governed by a contract or other legal act which shall be in writing, including in electronic form, and be binding. The GDPR lists the elements that have to be set out in the processing agreement.**
- The processing agreement should not merely restate the provisions of the GDPR; 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.
- Joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the GDPR. The determination of their respective responsibilities must in particular regard the exercise of data subjects' rights and the duties to provide information.
- Each joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected.



- **The legal form of the arrangement among joint controllers is not specified by the GDPR. 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.**
- **Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers. Supervisory 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**

You may read the EDPB's press release in full and for links to the Guidelines and consultation, please click https://edpb.europa.eu/news/news/2021/edpb-adopts-guidelines-codes-conduct-tool-transfers-final-versions-guidelines_en

You may also reach the guidelines through : https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

The content herein is aimed at providing a general insight regarding the subject. For customized circumstances or for further information, please refer to your lawyer.