Questions about the *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* of the European Data Protection Board

---

1. **Determination of purposes and means.**

> *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.*
>
> *(…)*
>
> *The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand.*

If one entity decides the purpose of the processing and another one decides the means, can there be joint responsibility between them? For example, a company decides to carry out an advertising campaign among its clients and for this, hires an advertising agency to study the case who decides that the best option is a certain mail delivery system. Would it be an order or a joint responsibility?

2. **Joint responsibility in purposes and means determined by law.**

> *The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. 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, 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. 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, i.e. inextricably linked.*

To understand that there is joint responsibility and not independent responsibilities, **is it essential that the parts decide the purposes and means or can they be included in a law?**

For example, in the Spanish legal system, the law regulates the figure of the "temporary work company" that provides "the user company" with temporary workers. Each of these companies assumes, by law, different obligations towards the worker in matters such as salary, command capacity, training or payments to Social Security, all with an impact on data protection. However, the

law also provides for the **subsidiary responsibility** of one of the entities in case that the other does not assume its functions (for example, the payment of salaries corresponds in origin to the "temporary work company" but the law determine the subsidiary responsibility of the "user company"). Furthermore, the "temporary work company", has no reason to exist without the "user company", so **there is no independence between them**

All this, would lead to think that there is a joint responsibility rather than independent responsibilities or commission.

3. Role of law firms.

The processor must not process the data otherwise than according to the controller's instructions. The controller's 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 organisational means.

(…)

Example: Law firms The company ABC hires a law firm to represent it in a dispute. In order to carry out this task, the law firm needs to process personal data related to the case. The reasons for processing the personal data is the law firm's mandate to represent the client in court. This mandate however is not specifically targeted to personal data processing. The law firm acts with a significant degree of independence, for example in deciding what information to use and how to use it, and there are no instructions from the client company regarding the personal data processing. The processing that the law firm carries out in order to fulfil the task as legal representative for the company is therefore linked to the functional role of the law firm so that it is to be regarded as controller for this processing.

If a company outsources legal advice and defence services and hires a law firm, **it is questionable that the firm acts as a responsible.**

The client company sets the purposes of the processing and makes the decision to take legal action against a specific third part or to defend herself in case that those actions are directed against her. The law firm receives this assignment and acts for the benefit of its client and for the purpose set by him. Certainly, **it may happen that the firm decides what personal data needs to process**, **but that decision will have just one objective, the fulfilment of the purpose set by the client or by the law** (for example, the content of the action is fixed in the law). This making-decision capacity of the lawyer should not make him responsible, as EDPB recognizes in other cases.

Moreover, it should be clarified that **any order or delegation of services by a data controller responds to the professionalism of the entity that receives the order and that turns to be an expert in this field. The controller trusts the processor to apply the measures that, given his experience, he considers most suitable to achieve the purpose of the controller.**

As an **example**, we can highlight the following cases in which the engagement relationship is not discussed and are quite similar to hiring and external legal service:

- When hiring an external **IT service**, where the controller is rarely going to tell to his IT service, which programs, tools or specific infrastructures he should enable. It will just ask you to do everything possible, given your knowledge and experience, to ensure the security of your information.
- When hiring a company for the **prevention of occupational risks**, the employer responsible of the processing has to guarantee the safety of its employees at work and for this, it resorts to that company, which acts as processor. However, this processor, **given her professionalism, may decide that needs to process certain employee health data, their time habits, workplace, etc. Likewise, the company may decides that needs to process these data of just some of the employees, depending on the risk that has been found due to their functions or personal characteristics.**

4. <u>Role of bank entities.</u>

Example: Bank payments As part of the instructions from Employer A, the payroll administration transmits information to Bank B so that they can carry out the actual payment to the employees of Employer A. This activity includes processing of personal data by Bank B which it carries out for the purpose of performing banking activity. Within this activity, the bank decides independently from Employer A on which data that have to be processed to provide the service, for how long the data must be stored etc. Employer A cannot have any influence on the purpose and means of Bank B's processing of data. Bank B is therefore to be seen as a controller for this processing and the transmission of personal data from the payroll administration is to be regarded as a disclosure of information between two controllers, from Employer A to Bank B.

In the case proposed by EDPB, it does not seem that the purpose that justifies the action of the bank is "performing banking activity". Rather, **the purpose of the processing would be to make the salary payment commissioned by the employer through its management company.**

Again, the fact that the bank request for certain information to carry out this order should not make it a data controller. **It is the employer who decides which people are paid, which amount of money and at what time, while the bank only executes the order using the means it has as a bank.**

Moreover, the fact that the bank keeps the data beyond the assignment will normally respond to legal obligations (for example, the legislation on the prevention of money laundering). **This retention of data, should not compromise the condition of processor of the bank.**

5. Role of data hosted.

Example: Marketing operations in a group of companies using a shared database: A group of companies uses the same database for the management of clients and prospects. Such database is hosted on the servers of the mother company who is therefore a processor of the companies with respect to the storage of the data. Each entity of the group enters the data of its own clients and prospects and processes such data for its own purposes only. Also, each entity decides independently on the access, the retention periods, the correction or deletion of their clients and prospects' data. They cannot access or use each other's data. The mere fact that these companies use a shared group database does not as such entail joint controllership. Under these circumstances, each company is thus a separate controller.

Should the hosting of data make the host a processor? In the case raised by the EDPB, the hosting of data by the parent company **may indicate a desire to control that company**, rather than a service that is provided to the group companies. In this way, it is not clear that the group companies determine the purpose of the processing, much less the means.

6. Responsibilities.

Can you clarify joint or subsidiary responsibility in the case of relationships between controller and processor, independent responsible and jointly responsible for claims and sanctions?