Introduction

The article 26 of GDPR defines the role of joint controllers when "*two or more controllers jointly determine the purposes and means of processing*".

The EDPB guidelines on controllers and processors state that "*an entity will be considered as joint controller with the other(s) only in respect of those **operations** for which it determines, jointly with others, the means and the purposes of the processing. If one of these entities decides alone the purposes and means of operations that precede or are subsequent in the chain of processing, this entity must be considered as the sole controller of this preceding or subsequent operations"* (page 18, par. 55).

In my experience, as referent for personal data processing in a Research Institute that operates in health and well being, I noticed that many organizations wants to avoid the state of joint controllership, because (I guess) they are afraid of more responsibilities in the data processing, in favour of independent (or separate) controllership thought it couldn't be the right configuration of responsibilities among the parties (with respect the personal data processing).

Some examples

Example 1

A Research Institute participate as partner in a multi-centre research project (we call it PRI) with other partners and another Research Institute that act as Coordinator (CRI). The PRI executes assessments on biological samples and send the results, with pseudonimysed data, to CRI that insert them in a DataBase for research purposes. PRI and CRI with other partners, have received fundings from European Union on the basis of a project proposal defined together. PRI doesn't host patients in its centre then defines an agreement with an Hospital (HO) that can collect that samples. HO collects the samples (explicitly for the project, they are not collected for daily clinical activity, and the cost of this activity is covered by PRI and CRI), pseudonimyse the data, then send the sample and the data to PRI.

In this case we can clearly identify different and distinct phases of the processing and, consequently, different and distinct phases of responsibility. In my opinion, they are phases of a single and unique process and it can be compared with the examples ("Research project by Institutes" and "Clinical Trials") on page 21. PRI and CRI should act as joint controllers towards the data subject but they can define the separate responsibilities in the different phases, in the Data Sharing Agreement. HO, didn't define purposes and means, so it should be a Responsible and his activity is limited to collecting the samples and related data.

Instead, the configuration for the responsibilities of the processing, chosen by CRI, PRI and HO has been to act as independent (separate) controllers (nevertheless I suggest to them that it wasn't the right solution).

Example 2

A research Institute, that act as coordinator (CRI), with another Research Institute, as partner (PRI), and other Clinical Partner (CP1, CP2…), define together a research project. CRI designs and builds a software-as-a-service (cloud) platform to elaborate clinical and genetical data (with the aim to investigate correlations between phenotype and genotype). PRI defines and builds some hardware tools, to execute clinical tests, whose results are loaded onto the platform together with other clinical data. CP2, CP3 and CP4 access to the platform for uploading and manage clinical data while CP1, in addition to execute the same operations as the others, executes the elaborations with the aim to find the correlations. Also in this case some (five) areas of responsibilities can be defined. The "central" one concerns the management of the data inside the cloud platform. The other ones are the four areas where CP1-CP4 produce the data, upload them onto the platform and use the platform to manage them.

The processing stems from a project proposal, presented by all partners (hence they together define purposes and means) and funded by Regional Authority.

Also in this case, the example “Research Project by Institutes” can provide the key to define a joint controllership between CRI, CP1, CP2, CP3 and CP4.

PRI, for the design and construction of the tool, doesn’t access personal data but participated to the definition of project proposal, so it should be a joint controller, as well (as stated on par. 54, page 18).

Again in this case the partners decided for a separate and independent controllership towards patients (data subject) of each organisation.

Discussion

Referring to paragraph 55 (page 21) and to the flow chart on page 48 of the document, in particular, the sentence:

“You are joint controllers for the stages of the processing for which you determine purposes and means together and ***separate controllers for those processing operations where you determine purposes and means separately****”,*

in my humble opinion, they can generate ambiguity in interpretation.

In the case of a single processing, I think that more emphasis should be put where, even if more phases or areas of processing can be defined and even if the responsibilities of the different operations can be defined separately for the different controllers, cannot exists separate controllers, if there one single processing (corresponding to the same purposes) for the following reasons:

- the data subject should receive information from only one subject (the contact point) for a single processing (for the same and shared purposes). In the case of more separate controllers, each controllers have the duty to inform the data subject;
- in this way the data subject would receive information regarding the processing of their data from more subjects (the separate controllers) for the same purposes;
- in the case of the data subject wishes to assert their rights, who they should contact? How a data subject can know the different stages of a processing if all parties act as separate and independent controllers?

Surely, separate controllers can exists where different processing may stem by a single collection of personal data. A typical example could be the data collect for health and care by an organisation (as an hospital) and then used by a research institute for research purposes.

So, the sentence: “*If one of these entities decides alone the purposes and means of operations that precede or are subsequent in the chain of processing, this entity must be considered as the sole controller of this preceding or subsequent operations”*, should be followed by the explanation that, in these cases, these preceding or subsequent operations should (or must?) be lead to independent and separate data processing.

Several organisation consider the joint controllership a complication in the management of personal data and, for this reasons, they try to avoid it and the related Data Sharing Agreement (on the contrary, in my opinion, it is the best way to delimitate the specific responsibility inside a single data processing).

I’m afraid that those sentences could be an alibi for choosing a “more convenient” separate controllership.

Raffaele Conte

Consiglio Nazionale delle Ricerche - Italian National Research Council