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

Background: pharmacist, internal DPO in a French pharmaceutical company between 2009 and 2013 and data protection consultant for healthcare industry/external DPO for several pharmaceutical companies in France since 2013.

Please find hereunder my comments:

1) **Comments on paragraph 38 concerning essential versus non-essential means and on the example concerning hosting services, pages 14 and 15 of the guidelines**

Paragraph 38 of the guidelines indicates that: « "*Essential means" are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller. Examples of essential means are the type of personal data which are processed ("which data shall be processed?"), the duration of the processing ("for how long shall they be processed?"), the categories of recipients ("who shall have access to them?") and the categories of data subjects ("whose personal data are being processed?"). "Nonessential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on*. »

The explanations provided about essential *versus* non-essential means would deserve to be further elaborated on, as in the previous version of the guidelines.

The draft guidelines also provide an example about hosting services, indicating that « *Employer A must provide the necessary instructions to H* [hosting service] *on, for example, which technical and organisational security measures are required* ».
As it is currently drafted, this example seems to contradict the statement of paragraph 38 according to which *"Nonessential means" concern more practical aspects of implementation, such as the detailed security measures which may be left to the processor to decide on".*
I kindly suggest that "technical and organizational security measures are replaced by a more obvious essential mean such as the storage period.

Besides, the guidelines could address the scenario where the service provider anticipates the needs of its clients and thus determines in advance part of the essential means of the processing.
Example: a company providing a software for the management of human resources would anticipate the needs and legal obligations of its clients (employers who will actually use the software to manage their employees). For example, the vendor would not provide a section relating to religious beliefs when it offers its services to a French employer but it will include the possibility to collect this data if the HR software is to be used by an employer in Germany. The vendor would indeed anticipate the fact that employee's religious affiliation will be collected by German companies in order to manage withholding tax.
The example may be declined with other essential means, e.g. the vendor would pre-define the categories of data subjects, storage period, etc.
This example could also illustrate paragraphs 19 and following of the guidelines.

DP Conformity - SARL unipersonnelle au capital de 10 000 euros
Siège social : 115 rue Saint-Dominique 75007 Paris Tel : 09 70 40 30 23 Email : info@dpconformity.fr
SIREN 844 852 673 R.C.S. Paris - SIRET 844 852 673 00012 - Code APE 7022Z - TVA intracommunautaire FR 23 844 852 673

2) Comments on paragraph 42 and the example concerning market research, page 16 of the guidelines

Paragraph 42 of the guidelines provides that: « *It is not necessary that the controller actually has access to the data that is being processed. Someone who outsources a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data.* »

Although this statement may seem obvious, in practice it is a useful and relevant reminder to avoid the pitfall of considering that the lack of access to personal data suffices to exclude the application of the GDPR, without further analysis about the role of the entity regarding the purpose and means of processing.

In the example mentioned in the guidelines, the company requesting the market research does determine the purpose and essential means which is the reason why it is considered as a controller. Please note that there are a number of various market research scenarios which may lead to different qualifications depending on which entity(ies) determine the purpose and / or means of processing. This could be reminded in the example, to avoid any misinterpretation in the field of marketing research activities.

3) Comments on the example concerning clinical trials, pages 21 and 22 of the guidelines

The example provides that:
« A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller.
In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial ».

The role of investigation centers or investigators is a recurrent question and the divergent positions of data protection authorities - taken during the past years - are difficult to manage in the context of international researches. A common position at the European level is therefore very welcome.

First, it is useful that the draft guidelines remind the necessity to precisely consider the processing activities at stakes prior to defining the role of a party.

As a healthcare organization or a healthcare professional, a hospital or a doctor would certainly act in the capacity of controller for the purpose of patient care, independently of any research conducted in parallel.
The research activity being a separate processing activity, the role of the healthcare organization or professional would have to be assessed with regards to the research, without reconsidering or affecting their role as controller for the purpose of patient care.

DP Conformity - SARL unipersonnelle au capital de 10 000 euros
Siège social : 115 rue Saint-Dominique 75007 Paris Tel : 09 70 40 30 23 Email : info@dpconformity.fr
SIREN 844 852 673 R.C.S. Paris - SIRET 844 852 673 00012 - Code APE 7022Z - TVA intracommunautaire FR 23 844 852 673

Secondly, the EDPB's interpretation on the roles and responsibilities of a sponsor (controller) and an investigator (processor) for the purposes of a research is very relevant and appears to be already implemented without major issues in countries such as France and the United Kingdom.

The following elements support the EDPB's approach:

1. The sponsor (a pharmaceutical company, a university, a hospital, etc.) drafts the protocol of a research and therefore defines the purposes (objectives of the research) as well as its essential means (inclusion criteria defining the categories of patients involved, categories of data to be collected, etc.).
Even if healthcare professionals (HCPs) may help the sponsor while drafting the protocol, the ultimate decision remains with the sponsor. These HCPs - usually 4 or 5 experts - may also later participate in the research as investigators. However, in a multicenter research, investigators - which number is usually much higher than the number of HCPs who helped drafting the protocol - are only involved after the protocol is validated and approved by the authorities.
This means that investigators have no influence neither on the decision to implement a research nor on the purposes or essential means of the corresponding processing activity.

2. An investigator participating in a research remains a healthcare professional taking care of their patients. In the context of a research, the investigator (as a processor) shall strictly follow and cannot deviate from the instructions of the sponsor.
However, if a healthcare professional thinks that the research activity could harm the patient or is not anymore appropriate, they remain free to withdraw the patient from the research and freely process their personal data. In that case, they will be acting in their capacity as doctor (not investigator) and as controller (not processor).
Any data collected by the healthcare professional in contradiction or in disagreement with the study protocol would populate the patient's medical file and will not be processed for the purposes of the research.

3. The draft guidelines suggest that a sponsor and an investigation center could be joint controllers if they jointly define the purposes and the means of the processing. This approach is relevant and raises no questions or comments.
However, it should be kept in mind that a joint controllership between the sponsor and each of the investigation centers (or investigators) is almost impossible to consider. Indeed, if each investigation center was able to define the purpose and/or essential means of the processing jointly with the sponsor, there could be as many studies as there are investigation centers. It also never happens that the sponsor jointly defines the purposes and/or essential means of the research jointly and at once with all investigation centers. As mentioned in point 1. above, the investigation centers are involved in the research after the purposes and means are defined.

Finally, with respect to the terminology used in the example:
- the reference to the investigator should be better replaced by a reference to the study site or investigation center, since the legal person would be the controller/processor rather than the natural person (the investigator is generally employed by, or under a contract with, the study site); this would be in line with paragraph 17 these same guidelines providing that « *in practice it is usually the organisation as such, and not an individual within the organisation that acts as a controller* »
- also, the sponsor could be in practice a pharmaceutical or medtech company, or any other research institute, not necessarily a university, thus the wording may be adapted accordingly.

DP Conformity - SARL unipersonnelle au capital de 10 000 euros
Siège social : 115 rue Saint-Dominique 75007 Paris Tel : 09 70 40 30 23 Email : info@dpconformity.fr
SIREN 844 852 673 R.C.S. Paris - SIRET 844 852 673 00012 - Code APE 7022Z - TVA intracommunautaire FR 23 844 852 673

4) Comments on the example concerning headhunters, page 22 of the guidelines

Although the underlying reasoning is relevant, it seems that the situation described in the example is not very common in practice.

Most usually, employers will simply provide a job description to headhunters and the latter will proceed with interviews, screenings, etc. based on their own database and processes. The headhunter will then present the most suitable applicants to the employer. The employer may process any job application it may receive independently, without necessarily sharing it with the headhunter.

Could the role and responsibilities of the employer and the headhunter be clarified in such situation, in addition to the current example?

5) Comment on paragraph 139 concerning deletion or return of the personal data by the processor, page 38 of the guidelines

As mentioned in paragraph 139, in accordance with Article 28(2)(g) of the GDPR, the processor must delete all existing copies of the data, unless EU or Member State law requires further storage.

Thus, in some situations, although the controller does determine the storage duration of the personal data, the processor will store the data for a longer time period due to obligations arising from Member State or EU law.

It would be useful to clarify in the guidelines that in such case the longer storage period by the processor does not affect the initial qualification of the parties.

6) Comment on paragraph 164 concerning legal basis, page 42 of the guidelines

The draft guidelines state that *"In this respect, both* [joint] *controllers always have a duty to ensure that they both have a legal basis for the processing."*

A processing activity that is under the responsibility of several joint controllers remains "one unique processing activity" that shall be defined by a unique legal basis leading to specific data subjects' rights.

It would be very useful to clarify that joint controllers should not only ensure that they have a legal basis for the processing but this legal basis should be the same.

DP Conformity - SARL unipersonnelle au capital de 10 000 euros
Siège social : 115 rue Saint-Dominique 75007 Paris Tel : 09 70 40 30 23 Email : info@dpconformity.fr
SIREN 844 852 673 R.C.S. Paris - SIRET 844 852 673 00012 - Code APE 7022Z - TVA intracommunautaire FR 23 844 852 673