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

19 October 2020

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

Please find below the comments of Sanofi on the guidelines.

1) 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* ».

Sanofi agrees with the statement that, in the context of a clinical trial (unless the trial takes place upon a common initiative of the sponsor and the study site and unless they collaborate together to the drafting of the study protocol) **the sponsor should be considered as the controller for the purpose of performing the research whereas the study site should be considered as a processor for said purpose** (being noted, as also stated in the example, that the study site would remain the controller with respect of personal data processed for the purpose of patient care).

This « *purpose oriented* » approach, which differentiates between the various processing activities which are implemented simultaneously during a clinical trial, appears most relevant and the clarification at an EU level is welcome.

These qualifications, i.e. that the study site is a processor for the purpose of research and a controller for the purpose of care, will serve as a basis to define the respective obligations and responsibilities of the parties in terms of personal data processing. This further analysis of the parties' respective obligations and responsibilities could be done at the sector level, for example in the framework of a code of conduct.

With respect to the terminology used in the example:

- Sanofi considers that the reference to the "investigator" would benefit from being replaced by a reference to the "study site", since the legal entity will generally be the 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 3 of the executive summary of 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 could be adapted accordingly or to clarify the non-exhaustive nature of the example.

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*. »

Sanofi agrees with this statement, and the corresponding example concerning market research, according to which a party would be a controller if it has a determinative influence on the purpose and (essential) means of the processing, even though it does not have actual access to the personal data processed. 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. Sanofi would however like to stress, in addition to the above, that there are a number of various market research scenarios

and services which may accordingly lead to different qualifications depending on which entity(ies) determine the purpose and / or means of processing and how the processing is implemented (e.g. off the shelf v. ad hoc market research).

3) 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.* »

In the opinion of Sanofi, the explanations provided about essential versus non-essential means would deserve to be further elaborated on, notably because what is an essential mean versus a non-essential one is very context driven.

In this respect, a situation that raises questions in practice as to the qualification of the parties as controller or processor is 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 (for example where a company develops a medical device and supplies it to healthcare professionals and hospitals in order for them to better monitor patient care) but has no final say on whether or not the clients decide to use the services or products offered .

Sanofi would also like to comment on the 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* »: in the view of Sanofi technical and organisational security measures in such case should not be considered as essential means determining controllership, since said measures are at the core of the expertise of the hosting service provider.
Also, 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*". In the contemplated scenario, an essential mean would rather by for example the duration of the processing or storage period.

4) 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.

5) Comments on paragraphs 92 and 93 of the guidelines concerning technical and organisational measures:

Sanofi welcomes the clarification in paragraphs 92 and 93 that both controller and processor are responsible concerning the implementation of appropriate technical and organisational measures and that, in this respect, the processor shall provide sufficient guarantees to the satisfaction of the controller, and the controller is responsible for assessing the sufficiency of the guarantees provided by the processor.