Monday 21 September 2020

Participation to the public consultation for the European Data Protection Board on the concepts of Controller and Processor in the GDPR

Dear Madam/Sir,

My name is Mathilde Barbour I am a French lawyer specialized in personal data protection and e-health in France and I also work as an outsourced DPO.

Thank you for giving us the opportunity to participate and to give our opinion on this consultation.

I would like to share with you a practical case that several data specialists are facing in France and in Europe but for which we have no common or satisfactory answer.

I think it's important that the EDPB shed some light on this issue and that these guidelines are the right way to do it.

There are several services providers on the European market that offer e-health services, including: medical teleconsultation, online medical appointment scheduling, secure messaging between a patient and a healthcare professional, etc...

The services provider offers this service on behalf of healthcare professionals or on behalf of hospitals and does not in any case process patients' health data on its own behalf. The storage and hosting of health data are mostly provided by an approved health data host located in France, and the services provider never has access to the health data.

Consequently, it is perfectly normal regarding the provisions of articles 28 and 29 of the GDPR to consider the services provider as a processor and that with respect to the processing of health data, which must act on the basis of instructions from the health professional acting as data controller.

However, some people believe that these providers are data controllers or even joint controllers of the processing of health data for several reasons, in particular:
- the fact that the services provider is known on the market and that under the pretext of their visibility they necessarily process health data;
- it would be easier for patients to exercise their rights directly with this provider because it is complicated for patients to exercise their rights with each data controller.

Most patients who directly exercise their rights under Articles 15 and following of the GDPR with this provider are disappointed because they expect to obtain a file containing their health data (medical appointments, etc.) but they only obtain the data for which the provider acts as

data controller (i.e. administrative management of the account, information used for the sending of the newsletter).

Pressure is mounting on this issue and I thought of a solution that perhaps you could consider and set out in the guidelines.

The heart of the problem lies in the fact that the provider is "known" by the patient and has visibility in the market. As a result, the patient wants to exercise his or her rights with this provider because he or she believes that this provider has access to his or her data. However, the providers have strict privacy policies and inform the persons concerned about the processing implemented and their role within the meaning of the GDPR.
What is all the more disconcerting is that patients are not favorable to the fact that providers have access to and use their data.

The fact of qualifying the provider as the controller or joint controllers for the processing would lead to a lack of knowledge of the provisions of article 28 of the GDPR since the provider acts solely on behalf of the controller. In no case the providers act on its own behalf when offering its services.

This would therefore risk pushing the provider to process data (in particular health data) on its own behalf, although this was not the initial objective.

In my opinion, in this specific case, it is necessary to maintain the qualification of processor for these providers and to allow these providers to respond to requests to exercise the rights of the data subjects on behalf of the data controllers. The response to requests to exercise the rights of the data subjects would therefore be entrusted by the data controller to the service provider.

This would greatly facilitate matters and would make it possible on the one hand to comply with the provisions of Article 28 of the GDPR but also to allow each person concerned by a processing of personal data to be satisfied in the event of a request to exercise his rights.

It would be great to have any guidelines or advices on this subject.

I remain at your disposal for any further discussions or information.

Best regards

Mathilde Barbour