Guidelines 07/2020 on the concepts of controller and processor in the GDPR

Feedback in the public consultation by the Luxembourg National GDPR Working Group for Research

Regina Becker, Adrian Thorogood (ELIXIR-Luxembourg)
Sara Bonomi (Luxembourg Institute of Science and Technology, LIST)
Katrina Bramstedt (Luxembourg Agency for Research Integrity, LARI)
Anne Drochon (Institut National du Cancer, INC)
Chloë Lellinger (Luxembourg Institute of Socio-Economic Research, LISER)
Sandrine Munoz (University of Luxembourg)
Laurent Prevotat (Luxembourg Institute of Health, LIH)

Contact: Regina.Becker@uni.lu

Introduction

The Guidelines 07/2020 are very welcome by our Luxembourgish research community. The Guidelines help to provide more clarity and guidance in the controversially interpreted criteria to assign the roles as (joint) controller and processor. In addition, the detailed description of the associated responsibilities and the corresponding requirements of accountability and transparent agreements between the parties will provide a good guidance for data sharing agreements in the future.

Criteria to determine controller, joint controller and processor

- *Manage complexity*

The criteria given help in defining the roles of controller, joint controller and processor but guidance should also be provided about the conclusions if the criteria are only partly fulfilled, so as to be logically exhaustive.

Background: Explanations including criteria, leading questions and examples that illustrate how determining the purposes and the means of the processing can lead to the identification of controller and processor have been provided. While the Guidelines state in section 34 that the controller cannot settle with only determining the purpose, it is not discussed what the consequences are if a party only determines the means but not the purpose.

For instance, it might be possible that a party determines the purpose and with another party, they jointly define the means. Such a situation could actually apply in the example of the clinical trial. It often happens that the sponsor, e.g. a pharmaceutical company, determines the purpose of the clinical trial – the test of a newly developed drug candidate. They would then engage a contract research organisation or a clinical partner with whom they jointly develop the means – the protocol of the clinical trial. The gain of the contract research organisation is purely financial. However, they will largely define the research protocol as their experience will be key for the development. Such situation is currently not solved with the criteria provided in the guidelines.

Another extreme can be that one party determines the purpose while another party determines solely the means. As such, no party fulfils the criteria defining the controller. This could be the case in policy development. A ministry selects a public research organisation, on the basis of a financial offer, to provide them with information on the socio-economic situation and the corresponding influences in the population. If the ministry selects the research organisation purely based on the financial offer without influencing the methodology, the subject recruitment or the analysis. All the means will be defined by the research organisation that, on the other hand, has not defined the purpose.

Guidance should be given how in such cases the roles with respect to the processing can be a defined. Would the situation be different if the research organisation has an own benefit, such as a scientific publication of the results? Would it be different if the proposal on the conduct of research is part of the organisation's offer to the ministry?

- *Interpretation of case law*

We believe that some of the phrasings in the guidance derived from case law may lead to misunderstandings among the stakeholders. The sections 58 and 63 could be rephrased or better explained to avoid misinterpretations or too broad scope for interpretation.

Background:

Concerning section 58

It should be made clear that only where parties jointly determine the purpose of the processing they can be jointly accountable for this purpose and that, where several purposes are involved in a chain of processing, a granular analysis of the processing chain and purposes and means for the different processing elements may be required.

In the *Fashion ID* case, the CJEU rules that Fashion ID and Facebook jointly determine the purpose (and the means) of the collection and transmission, where the purpose is to benefit from a commercial advantage through visibility on the Facebook platform(s). The specific benefit in this case is different as Fashion ID profits from the advertising of its products in the social networks while Facebook uses the data subsequently for its own commercial gain based on the analysis of the data collected. Indeed, the CJEU makes it clear that Fashion ID is not accountable for this subsequent processing operated by Facebook.

We are concerned that stating that not having the same purpose for the processing could lead to joint controllership can lead to confusion in the interpretation. The subsequent interest in and benefit from the availability of the data in the Facebook platform should be more separated from the jointly determined purpose of making the data available in the platform for commercial benefit.

Concerning section 63

The section would benefit if it were more clearly targeted towards an explanation what "determining the means" can imply in the case of internet platforms. The guidelines could mention that in a typical situation where an entity merely provides infrastructure, the entity is clearly a processor. It could be made clear that the decision of using a platform will lead to controllership and that the platform user needs to be aware of a potential joint controllership where platform providers pursue an own benefit of the platform use. As the Facebook-related CJEU rulings are driving this section, it should be made clear that in such

cases the benefit of the platform provider is based on the data processing or enabled by the platform user.

Examples to determine controller, joint controller and processor

- *Research needs more detailed discussion*

The Guidelines should include at least one more complex example for collaborative research projects, otherwise there is a danger many institutions will conclude that all joint research projects will therefore lead to a joint controllership for all operations in a research project.

Background: The Guidelines 07/2020 propose an example for scientific research where the joint determination of the research, the joint agreement to host the data in a platform provided by one partner in the consortium and data contribution by all partners leads to a joint controllership.

We have serious concerns that many institutions will assume this to be the case for all research projects. However, often big research projects are more complex with respect to the participation in decision making and also the analysis of different elements in the processing chain (following e.g. the considerations of the CJEU in *Fashion ID*). Two examples are described below.

1. In many projects, a biobank as a partner is included in the project with the sole role to hold the biosamples and some associated data provided by the other partners, sometimes also generating genetic/molecular data by analysing the samples. The biobank was not involved in planning the research project, sometimes added only at the last stage of the project planning and would therefore in our understanding serve as a processor. The current example in the guidance treats one research institute providing a platform as a joint controller (but that institute is also contributing data). A clarification note could be included stating that in the case where one partner provides only the hosting infrastructure, it may still be a processor.
2. There may also be more granular situations where the consortium partners jointly agree on the research to be performed, but the individual partners in a consortium decide what data (if any) they make available for the project, and to which specific partners. This data is then transmitted to a central platform hosted by one of the partners, who manages granular access rights to the data on behalf of the submitting partner. The data provider decides which consortium partners can actually have access to the data and gives written instructions to the partner providing the platform about such access.
   In contrast to the example described in the Guidelines, not all partners have the same role in determining purpose and means. There are different roles in determining the purpose and means along the chain of processing that can also overlap to varying degrees with respect to data contribution, platform provision and data use. We believe therefore that even in a joint research project, different roles may apply to consortium partners, which may be indicated (where applicable) by separate work packages.

We would appreciate if the EDPB considered to include another example on a complex research consortium where the roles for the project are more differentiated with respect to the processing. Alternatively, clarification notes could be included under the research example, explaining the consequences if certain variables were changed. It is important for

us that the Guidelines exemplify that joint controllership for all consortium partners may not be applicable to all research projects.

- *Include trusted third parties as a pseudonymisation service as example*

The Guidelines should include again the example of trusted third parties who provide pseudonymisation as a service to clarify the role of such trusted third parties in relation to national legislations that may determine their work fully, in part, or not at all.

Background: The previous Opinion 1/2010 stated that an intermediate organisation offering coding of data in a research context may be considered a controller pursuant to specific national regulations, and it is subject to all resulting obligations including, among others, informing the data subject, notification. The justification then builds on the argument that ”when data from different sources are brought together, there is a particular threat to data protection, justifying the intermediary organization's own responsibility”. It would be helpful if the example would be re-evaluated with the criteria provided in the Guidelines and foreseeing different scenarios. This may be particularly relevant as pseudonymisation is introduced explicitly in the GDPR as a very important safeguard.

A research consortium building up a patient cohort engages an intermediary organisation (in the following, a trusted third party, TTP) for performing a pseudonymisation of data coming from different sources and being shared with different partners in the consortium with their own organisation-specific pseudonym. The use of TTPs for pseudonymisation in research may or may not be required by national law that determines safeguards according to Art. 89 GDPR. The research consortium will decide the purpose (research cohort), will determine the data subjects to be included and determine the rules under which and by whom a pseudonymisation can be reversed. The research consortium will further decide which TTP to engage depending on the methodologies used to realise the pseudonymisation. The TTP will not have any other benefit in this purpose beyond the service provision and the associated monetary gain. They may be able to decide that requests for de-pseudonymisation may not comply with the rules communicated and refuse the de-pseudonymisation for that reason. However, they would have to accept if the research consortium changes the rules for de-pseudonymisation unless such processing would violate data protection law.

Another scenario is that a TTP that was set up by law and has the legal obligation to provide sector-specific pseudonyms as realised e.g. in Austria. Here, the rules and services are not defined by the customer but by legal provisions in a law that establishes the tasks and duties of the TTP.

It would be very helpful if the role of the TTP as controller or processor could be discussed. Where without legal provisions, a TTP has a role as processor, it would be relevant to have criteria what scope of legal provisions could change such role.

Consequences of joint controllership

- *Influence of the joint controllership on the processing*

Guidance should be given how the individual controllers in a joint controllership may influence the entire processing. If the controllers in a joint controllership have to apply different rules for the processing, a clarification is needed on how the joint controllers deal with these differences.

Background: The underlying legal person or the nature of a controller has an influence on the processing such as on the legal basis that can be used. Where a legal basis is not available for one of the controllers, would the same processing be done under different legal bases by the different controllers? In particular, if there is an imbalance between the data subject and one of the controllers, would this exclude consent as a legal basis for all controllers or could the same processing be performed under consent and e.g. public interest at the same time?

A potential conflict can also arise where joint controllers are located in different countries. The territorial scope of national implementations of the GDPR is often defined by the location of the controller or processor. Where there are different implementations of the GDPR such as the restrictions on processing special categories of data or the implementation of safeguards according to Art. 89 were introduced in the countries of the joint controllers, which legislation would be applicable to the processing?

We would appreciate if the EDPB provided guidance in all cases where ambiguities may arise due to the different legal entity, nature or location of joint controllers.