19 October 2020

Dr. Andrea Jelinek, Chair
European Data Protection Board
Rue Wiertz 60, B-1047 Brussels

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

Dear Dr. Jelinek,

The European Federation of Pharmaceutical Industries and Associations (EFPIA) and the International Pharmaceutical & Medical Device Privacy Consortium (IPMPC) welcome the possibility to provide comments in response to this Consultation. EFPIA represents the biopharmaceutical industry operating in Europe. Through its direct membership of 36 national associations, 39 leading pharmaceutical companies and a growing number of small and medium-sized enterprises (SMEs), EFPIA's mission is to create a collaborative environment that enables its members to innovate, discover, develop and deliver new therapies and vaccines for people across Europe, as well as contribute to the European economy. The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical companies and medical device manufacturers. The IPMPC strives to be a leading voice in the global pharmaceutical and medical device industries to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.[1]

In addition, the following associations have joined the sections of these comments that are relevant to their activities, as reflected in the footnotes: the Association of Clinical Research Organizations (ACRO)[2], the Market Research Society (MRS)[3], the European Federation of Associations of Market Research Organisations

[1] More information about the IPMPC is available at www.ipmpc.org. This filing reflects the position of the IPMPC as an organization and should not be construed to reflect the positions of any individual member.

[2] The Association of Clinical Research Organizations (ACRO) represents clinical research organizations and technology companies that support the conduct of a majority of commercially-sponsored clinical trials in Europe.

[3] The Market Research Society (MRS) is the UK professional body for market, opinion and social research, insight and analytics. MRS is the world's largest research association, representing 5,000 individual members and over 500 accredited Company Partners in over 50 countries and has a diverse membership of individual researchers within agencies, independent consultancies, client-side organisations, the public sector and the academic community. MRS promotes, develops, supports and regulates standards and innovation across market, opinion and social research and data analytics. MRS regulates research ethics and standards via its Code of Conduct. All individual MRS members and Company Partners agree to regulatory compliance of all their professional activities via the MRS Code of Conduct and its associated disciplinary and complaint mechanisms. See www.mrs.org.uk.

(EFAMRO)[4], the European Pharmaceutical Market Research Association (EphMRA)[5], and the British Healthcare Business Intelligence Association (BHBIA)[6].

As noted in the Guidelines, the concepts of controller, joint controller, and processor play a crucial role in the application of the GDPR. The Guidelines explain each of these concepts and provide various examples of their application in practice. Our comments focus on the following examples provided in the Guidelines:

- Clinical trials (paragraph 66); and
- Market research (paragraph 42).

We believe these examples as presented are not fully representative of many clinical trial and market research scenarios and may lead to unwarranted, generalized conclusions. We recommend modification or removal to prevent confusion. We also suggest clarification of several places in the document where we believe the current wording is unclear and could lead to misunderstanding.

A. Clinical Trials[7]

Clinical research with human subjects is carefully regulated by law and long-standing ethical practices to ensure the protection of study participants. One of the key aspects of the clinical research process is the use of investigators at trial sites to administer and conduct the research trial. These investigators ensure the scientific validity of the study data, maintain the 'blinded' nature of the data to ensure that results are not unconsciously biased by knowledge of the study's progress, and use their independent medical judgement to look out for the best interests of participants. In addition, studies are conducted under the oversight of ethics committees, who are responsible for approving the study protocol, monitoring the study as it progresses, and providing oversight when unexpected or unusual issues arise. Although the study sponsor plays an important role in the design of the study, the selection of data collection methods, and the identification of study end-points, the investigator is responsible for the conduct of the clinical trial at a trial site and usually has direct obligations imposed on it by clinical trials legislation. This ensures the scientific validity of the study by reducing the opportunity for bias. The data collected by the investigator is reported back to the trial sponsor using 'case report forms' (or 'CRFs'), which summarize the information related to the study. The investigator assigns a code to each study participant and information is reported on the CRFs using the assigned codes. The decoding information that links the assigned codes to study participant identities is maintained confidentially by each trial site.

---

[4] The European Federation of Associations of Market Research Organisations (EFAMRO), founded in 1992, represents the interests of market, opinion and social research in Europe. Its members are national trade associations for research businesses.

[5] The European Pharmaceutical Market Research Association (EphMRA) develops and improves standards and techniques for global market research in the field of health and healthcare, and it supports its members in their international activities to create transparency to the general benefit.

[6] The British Healthcare Business Intelligence Association (BHBIA) is an industry association representing companies involved in healthcare market research and data analytics. It is a long established and highly regarded association and almost all pharmaceutical, medical device and biotech companies and business intelligence agencies with a UK base are members. Its members' work supports the measurement and understanding of disease, physician and patient needs, and informs drug development. The BHBIA's Ethics and Compliance Committee provides extensive and detailed guidance to members to help them comply with legislation and conduct market research to high ethical standards.

[7] This section of our comments is submitted jointly with ACRO. *See supra* note 2.

The Guidelines provide an example of a clinical trial involving a health care provider as an investigator and a university as a sponsor:

> 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 process followed in a clinical trial can vary quite significantly depending on the sponsor, the investigator, as well as the details related to the research, the medical intervention, and the therapeutic area under examination. We are concerned that the example above over-simplifies the role that an investigator often plays in a clinical trial. Pursuant to GDPR Art. 40, EFPIA is in the process of developing an EU code of conduct on scientific research (including clinical trials), and the code will holistically address the roles of the parties in a clinical trial of a medicinal product and the obligations of each party. Rather than providing an example in these more general Guidelines that does not fully reflect the complex relationship of a clinical trial sponsor and investigator, we encourage the EDPB to further consider these issues in the context of EFPIA's proposed code of conduct.

As an illustration of the complexity of the issues at hand and the relationship of the parties, it may be helpful to understand how a clinical trial protocol is developed and how the protocol relates to the conduct of a trial of a medicinal product. Under the Clinical Trials Regulation, responsibility for the drafting of the clinical trial protocol ultimately lies with the trial sponsor. However, the sponsor incorporates into the protocol the obligations that are assigned to an investigator under the Clinical Trials Regulation. In many cases, the investigator is consulted by the sponsor during the development of the protocol, and in all cases, the investigator must agree to conduct the trial in compliance with the protocol. As well as the obligations directly applicable to the investigator imposed by clinical trials legislation and standards, the investigator, as a health care provider, has independent legal and ethical duties towards patients, and the investigator's agreement to adhere to the protocol is more significant than the ordinary case of a processor who simply accepts the instructions provided by a controller. Once the protocol is approved by regulatory authorities and the relevant ethics committee, the investigator should not deviate from it without agreement by the sponsor and prior review and approval of the EC. However, the investigator is permitted – even bound – to deviate from the protocol where such deviation is necessary to eliminate an immediate hazard to study participants. Moreover, the investigator is responsible for all trial-related medical decisions. The investigator does not, therefore, merely follow the sponsor's instructions in its data processing.

The above example's analysis and conclusions also raise a number of important issues and questions that ought to be addressed in parallel to the question of the appropriate characterization of the parties in order to avoid unnecessary confusion:

- The EDPB's *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)* describes the processing of personal data in the course of a clinical trial protocol as falling within two categories – those processing operations related to reliability and safety purposes, and those processing operations purely related to research activities. How do the processing purposes described in the EDPB's 2019 Opinion align with the processing purposes described in the example in the Guidelines 07/2020? It should be noted, for example, that with respect to reliability, both the investigator and the sponsor have distinct responsibilities related to maintenance and archiving of their respective sections of the clinical trial master file (*e.g.*, the investigator is responsible for the investigator site files).[8]
- In a clinical trial that involves a therapeutic intervention, the data is collected both for research and for patient care. According to the latter part of the example above, the investigator should be viewed as creating and maintaining these clinical study records both as a controller for purposes of patient care and as a processor on behalf of the sponsor for purposes of research. How should this be described to research participants, particularly in relation to describing data subject rights and in consideration of the fact that the sponsor only maintains coded patient data?

Given the above considerations, many sponsors and clinical investigators have come to regard their relationship as that of independent controllers, with the sponsor controlling the processing of the sponsor trial master file (for purposes of (i) studying one or more health products with the objective of ascertaining the safety and/or efficacy or such product(s), and (ii) ensuring clinical trial reliability and safety, in accordance with the sponsor's legal and ethical requirements) and the investigator controlling the processing of the investigator site files (for purposes of (i) the health care of trial subjects, and (ii) ensuring clinical trial reliability and safety, in accordance with the investigator's legal and ethical requirements). Should the EDPB choose to retain a clinical trial example in the Guidelines, we request that it acknowledge this as an acceptable approach to compliance.

We appreciate the EDPB's efforts to develop harmonised EU guidance on the roles of the parties in a clinical trial. However, given the complexity of the issues, we believe that including a clinical trial example in these more general Guidelines may lead to further confusion. Therefore, we encourage the EDPB to delete the example and wait to address these issues in its consideration of EFPIA's proposed code of conduct. In the alternative, we urge the EDPB to add a caveat to the example that highlights the need for a case-by-case assessment based on the specific clinical trial arrangement at issue and acknowledges the acceptability of the approach we have described above.

B. Market Research[9]

The Guidelines explain 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.' The Guidelines then provide an example of the application of this statement to a market research scenario:

---

[8] See European Medicines Agency, *Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)* (6 December 2018) at § 3.1 ("The investigator/institution is responsible for all essential documents generated by the investigator/institution and should therefore have control of them at all times.")

[9] This section of our comments is submitted jointly with MRS, EFAMRO, EphMRA, and BHBIA. *See supra* notes 3, 4, 5, and 6.

> Company ABC wishes to understand which types of consumers are most likely to be interested in its products and contracts a service provider, XYZ, to obtain the relevant information.
>
> Company ABC instructs XYZ on what type of information it is interested in and provides a list of questions to be asked to those participating in the market research.
>
> Company ABC receives only statistical information (e.g., identifying consumer trends per region) from XYZ and does not have access to the personal data itself. Nevertheless, Company ABC decided that the processing should take place, the processing is carried out for its purpose and its activity and it has provided XYZ with detailed instructions on what information to collect. Company ABC is therefore still to be considered a controller with respect of the processing of personal data that takes place in order to deliver the information it has requested. XYZ may only process the data for the purpose given by Company ABC and according to its detailed instructions and is therefore to be regarded as processor.

This example provides an overly simplistic description of how market research often takes place, particularly in healthcare market research. Typically, market research starts with a company (the client) needing information to help it understand or assess opinions or behaviour within a specific sphere or market. The client then commissions a market research agency who assist in designing and executing a research project to obtain this information. In some cases, generally because of limitations in time or in-house market research expertise, the client may give the market research agency complete latitude to determine how to design and execute the project to best meet the client's information needs. In other cases, the client and market research agency may work collaboratively to develop research questions, identify the target audience, and decide on the approach to be taken (e.g. qualitative or quantitative, face-to-face, or online) and the topics to be addressed during fieldwork. So, in reality, there are a range of approaches that can be taken to the commissioning, design, and execution of market research that involve different working and decision making relationships between the client and the agency.[10]

---

[10] As a further example of the complexity of various market research arrangements, *see* the market research example provided by the UK ICO at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/how-do-you-determine-whether-you-are-a-controller-or-processor:

> *A bank contracts a market-research company to carry out some research. The bank's brief specifies its budget and that it requires a satisfaction survey of its main retail services based on the views of a sample of its customers across the UK. The bank leaves it to the research company to determine sample sizes, interview methods and presentation of results.*
>
> *The research company is processing personal data on the bank's behalf, but it is also determining the information that is collected (what to ask the bank's customers) and the manner in which the processing (the survey) will be carried out. It has the freedom to decide such matters as which customers to select for interview, what form the interview should take, what information to collect from customers and how to present the results. This means the market-research company is a joint controller with the bank regarding the processing of personal data to carry out the survey, even though the bank retains overall control of the data because it commissions the research and determines the purpose the data will be used for.*

The example and analysis provided in the Guidelines suggests that in most, if not all, circumstances, a market research agency or supplier will be a processor on behalf of the organization that commissioned the market research (the client). This would have implications in terms of (i) GDPR transparency requirements - *i.e.*, potentially requiring identification at the time when the personal data are obtained of the client as the 'controller' of the data; and (ii) data subjects rights - *i.e.*, potentially imposing an obligation on the client to respond to data subject requests to exercise their rights. As further described below, the example's construction raises a number of challenges.

First, disclosing the name of the client up front may introduce bias (which undermines the scientific integrity of the research). Naming the client (or the sponsor of the research) also creates possible conflicts with other sector relevant regulations. The client may wish to avoid reference to any corporate or brand names so as to avoid any risk of the market research being viewed as promotional (which raises particular concerns in the context of prescription medicines and medical devices) and to avoid any risk of conflict with anti-corruption legislation (which is of particular concern in the context of pharmaceutical and medical device company interactions with health care professionals). In these circumstances, the market research agency often acts with a significant degree of independence, for example in deciding what information to use, how to use it and choosing the respondents. The market research agency may recruit participants from its own pool of potential subjects, independently determine the sampling techniques and develop the questions to ask research subjects, use its own notice and consent forms, follow its own policies and procedures, and have autonomy in determining what information to include in the final report provided to the client. In these circumstances, the market research agency could possibly be viewed as the controller of personal data processing, and the client could be viewed as simply the recipient of a report containing aggregate, anonymized data.

Second, the example may lead to confusion with respect to the exercise of data protection rights and thereby actually prove detrimental to data subject rights. The client ordinarily has no ability to respond to data subject requests as the client receives no information identifying participants. The client would need to forward such requests to the market research agency for action, resulting in a delay in responding.

All of these issues support assessing the data processing roles within market research work on a task-by-task basis. To avoid the example provided in the Guidelines being presumed to be representative of all market research and the data protection conclusions misapplied to other market research scenarios, we recommend either providing additional examples that address a broader range of market research scenarios or deleting the example in this guidance document and instead working with the industry to provide more holistic guidance concerning the application of the GDPR to market research. We would welcome the opportunity to discuss this latter option with the EDPB should it be of interest.

C. Miscellaneous Additional Comments

The wording of the guidance in several places should also be reconsidered to ensure clarity. Specifically:

- Paragraph 65 currently reads: '[T]he choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities. This follows from the Fashion ID case . . . .' We suggest rewording as follows to more closely adhere to the CJEU judgment in the Fashion ID case: 'Where an entity chooses to use a tool developed by another entity (the 'tool provider') with the knowledge that the use of such tool will result in a disclosure of personal data to the tool provider for further processing (as determined by the tool provider), the entity's choice to use such tool can amount

to a joint decision (with the tool provider) on the means by which the tool provider is able to obtain personal data.'[11]

- Paragraph 79 currently reads: '[A] processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.' We suggest rewording as follows to make clear that whether the processor violates the GDPR in processing data for its own purposes depends on whether such further processing is permitted in its agreement with the controller (or as otherwise permitted based on written instructions provided by the controller in addition to those set out in the agreement): '[A] processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing <u>in contravention of its contract with the controller or any other written instructions provided by the controller following contract signature</u>. The processor will be considered a controller in respect of that processing and may be subject to sanctions for <u>violating its contract with the controller and</u> going beyond the controller's instructions <u>(including those that may be provided to the processor following contract signature)</u>.'

Conclusion

EFPIA and the IPMPC support the European Data Protection Board's efforts to provide further guidance on the concepts of 'controller' and 'processor', and we appreciate the EDPB's efforts to apply the guidance to real-world scenarios. However, due to the range and complexity of clinical trial and market research scenarios, we are concerned that the examples provided may lead to misunderstanding and confusion. With respect to the market research example, the guidance should address other scenarios that may result in different controller/processor determinations or it should be removed and could instead be addressed in sector codes. And given EFPIA's efforts to develop an industry code of conduct for scientific research by drug manufacturers, we believe clinical trial-related data protection issues can be more holistically addressed in the EDPB's consideration of that proposal.

[11] *See Fashion ID* case at para. 76 ('By contrast, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations.')