EORTC CONTRIBUTION TO THE PUBLIC CONSULTATION CONCERNING EDPB GUIDELINES 07/2020 ON THE CONCEPTS OF CONTROLLER AND PROCESSOR IN THE GDPR

19th October 2020

Prepared by EORTC International Affairs and Policies Team

Teodora Lalova Legal Fellow, **Iryna Shakhnenko** Privacy Manager, **Roxana Albu** DPO, **Stephane Lejeune**, Head of International Affairs and Policies Team

1. GENERAL COMMENTS

Since its coming into force on 25 May 2018, the European General Data Protection Regulation (GDPR) is the subject of significant debate among the scientific community, in particular concerning its interplay with the highly heterogeneous legal framework for clinical trials.[1] Lack of harmonisation continues to be one of the biggest hurdles for clinical research.

As an independent, non-profit cancer research organisation, the European Organisation for Research and Treatment of Cancer (EORTC)[2] has been active in sharing its decades of experience in the field. The EORTC has frequently expressed its concerns and proposals for solutions, and continues to do so.[3]

The EORTC welcomes the adoption of Guidelines 07/2020 on the concepts of controller, joint controller and processor in the GDPR (hereafter the Guidelines). The Guidelines play an important role in dispelling legal uncertainty concerning defining criteria for the legal capacity of data processing actors, as those provided by Working Party Article 29, some national data protection authorities, and the Court of Justice of the EU were sometimes conflicting.[4] This issue has been especially challenging

[1] See e.g. Evert Ben van Veen, 'Observational health research in Europe: Understanding the General Data Protection Regulation and underlying debate', European Journal of Cancer (104) (2018) 70–80; Jacques Demotes-Mainard et al., 'How the new European data protection regulation affects clinical research and recommendations?', Therapie (74) (2019) 31–42; Marcelo Ienca et al. 'How the General Data Protection Regulation changes the rules for scientific research. Study for the European Parliament Panel for the Future of Science and Technology (STOA)', July 2019, available at: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)634447

[2] https://www.eortc.org/our-mission/

[3] See e.g., EORTC contribution to the EMA Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures entitled "The General Data Protection Regulation: Secondary Use of Data for Medicines and Public Health Purposes Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures", 10th July 2020, available at: http://www.eortc.org/app/uploads/2020/09/EMA-_Secondary-use-of-health-data_Discussion-Paper_Stakeholders-consultation.pdf; Anastassia Negrouk and Denis Lacombe, 'Does GDPR harm or benefit research participants? An EORTC point of view', The Lancet Oncology (19) (2018) 1278–1280; Anastassia Negrouk, Denis Lacombe, Françoise Meunier, 'Diverging EU health regulations: The urgent need for co-ordination and convergence', 17 J. CANCER POLICY 24–29 (2018)

[4] See e.g., Yordanka Ivanova, 'Attribution of Responsibility under GDPR in the Context of Health Data Processing", in Maria Tzanou (ed.), 'Big Health Data and the GDPR: Data Protection, Privacy and the Law', Routledge Publisher (Forthcoming 2020)

for stakeholders involved in conducting health research (Sponsors, academic universities, investigators).

EORTC commends the inclusion of examples pertaining to clinical research, in particular linked to the relationship between Sponsor and health care research providers (investigators). However, some uncertainties, which will be discussed below, remain.

2. SPECIFIC COMMENTS: CONTROLLER-TO-CONTROLLER RELATIONSHIP

The Guidelines carefully outline the concepts of controller, joint controllers and processor under the GDPR, and clearly discuss the relationship between 1) controllers and processors, and 2) joint controllers. However, the relationship between controllers is not considered in a sufficient manner. This lack of consideration risks leading to incorrect allocation of responsibilities and further perpetuates legal uncertainty.

The controller-to-controller relationship pertains to personal data sharing from controller to controller. This type of data sharing is implicit in the GDPR (Article 14), but it is not explicitly named in the regulation.[5]

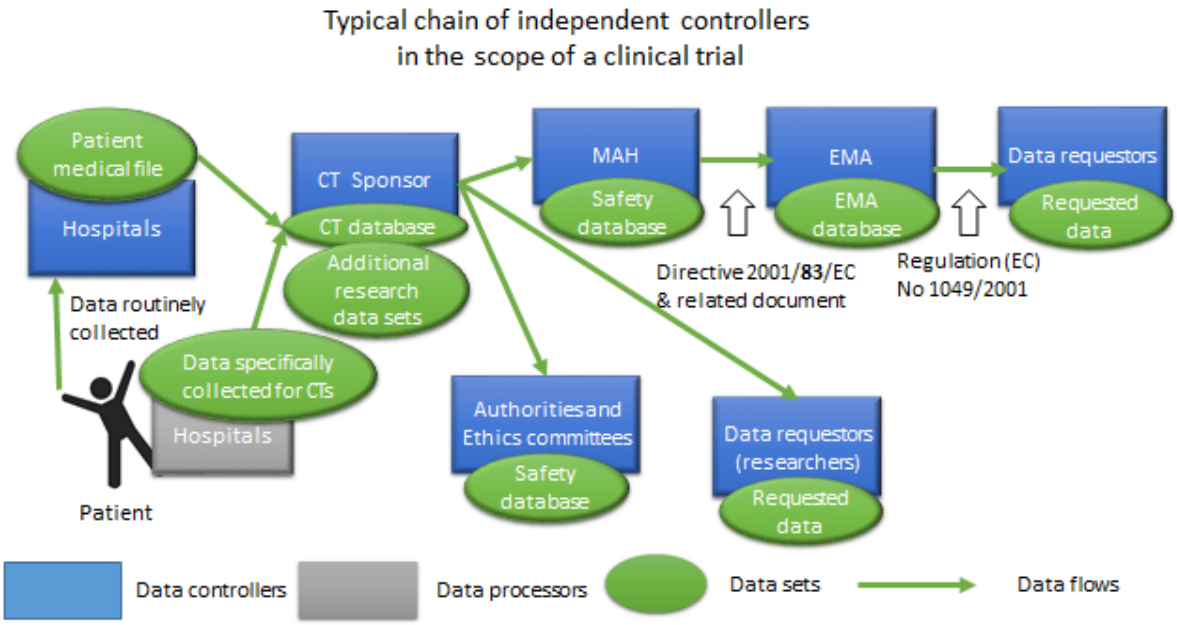
The Guidelines allude to it in paragraph 70, as an example of a situation where there is no joint controllership: *"(…) there can be situations where various actors successively process the same personal data in a chain of operations, each of these actors having an independent purpose and independent means in their part of the chain. In the absence of joint participation in the determination of the purposes and means of the same processing operation or set of processing operations, joint controllership has to be excluded and the various actors must be regarded as successive independent controllers".*

This explanation, however, is not overarching and misses to take into account, e.g., the intricacies of clinical research. There is also no direct link established with the discussion about recipients of personal data (Part I, Section 5 of the Guidelines).

The clarification is very relevant for the research community.

An example of such controller-to-controller data sharing (controllership chain) is illustrated in Figure 1 below. Clinical research relies on chains of controllers. Data sets are shared from one independent controller to another for achievement of sensibly different purposes. Differently from the joint controllers, independent controllers do not define purposes jointly.

[5] As previously pointed out in the EORTC contribution to the EMA Discussion Paper, available at: http://www.eortc.org/app/uploads/2020/09/EMA-_Secondary-use-of-health-data_Discussion-Paper_Stakeholders-consultation.pdf



Examples of datasets provided are either fully identified (patient medical file) or de-identified to a different degree, including to the extent to be considered as anonymous. In general, further the controller is in the chain as compared to the initial source of data, more difficult it becomes to re-identify the data subject. However, the full anonymization cannot be guaranteed at any step as the degree of de-identification depends on the needs of the activities/research at stake.

Therefore, from our organization experience with negotiations of agreements and pitfalls encountered in this regard, EORTC strongly believes that the controller-to-controller relationship must be further elaborated in a separate section of the Guidelines.

In particular, it is crucial that the consequences of controller-to-controller data sharing are clearly outlined, in order to avoid confusion with the consequences of joint controllership (See Part II, Section 2 and following of the Guidelines). Moreover, incorrect allocation of responsibilities and/or insufficiently specified rules for controller-to-controller data sharing could have serious detrimental effects for all actors involved in clinical research. First, there is a risk for a lack of protection of data subjects' rights in cases whereby controllers placed further in the chain could rely on Articles 11 and 14(5)(b) of the GDPR to release themselves from the transparency obligation. Second, study coordinators or other experts involved in clinical research might be discouraged to participate in studies if they risk being incorrectly regarded as joint controllers alongside the research sponsor.

At national level, the Belgian Data Protection Law is a good example of an act, which clearly identifies the controller-to-controller relationship.[6] The law stipulates that where personal data have not been collected from the data subject, the receiving data controllers (i.e. Controller 2) should conclude an agreement with the initial controller (i.e. Controller 1). Controller 2 is obliged to inform the initial Controller 1 about eventual restrictions on data subjects' right. According to scholars, the underlying

[6] Article 194, 30 Juillet 2018 Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

assumption of the law is that the initial controller acts as a "contact point" for data subjects and will fulfil their requests if they want to exercise their rights.[7]

EORTC applies the requirements of the Belgian Data Protection Law. When sharing data with other controllers, EORTC puts in place a data sharing agreement with additional clauses aiming to further protect data subjects' rights and ensure proper management of data breaches. EORTC requires assistance from the recipient controller (i.e Controller 2) in case of relevant data subject requests and prompt feed-back in case of any high-risk data breach or in case of incidental findings. [8]

In summary, based on the foregoing, the EORTC proposes the following updates to the Guidelines:

- Clearly define what are modalities and conditions of controller-to-controller data sharing and what are the eventual consequences in terms of obligations, risks, and liabilities for the involved parties;
- Provide specific examples of controller-to-controller data sharing, thus clearly dispelling any possible confusion between controller-to-controller relationship and joint controllership;
- Recommend the use of additional clauses in data transfer agreements that aim at protecting the data subjects' rights, namely following the example of the Belgian Data Protection Law, as specified above.

[7] R. Ducato, Data protection, scientific research, and the role of information, CRIDES Working Paper Series no. 1/2020, 10 January 2020; Computer Law and Security Review, forthcoming, available at: https://www.researchgate.net/publication/339213343_Data_protection_scientific_research_and_the_role_of_information

[8] See EORTC contribution to the EMA Discussion Paper, available at: http://www.eortc.org/app/uploads/2020/09/EMA-_Secondary-use-of-health-data_Discussion-Paper_Stakeholders-consultation.pdf