Response to European Data Protection Board (EDPB) consultation on the concepts of controller and processor

19 October 2020

MedTech Europe welcomes the opportunity to provide comments to the EDPB's Guidelines on the concepts of controller and processor in the GDPR (the "Guidelines") and appreciates the efforts made by the EDPB to clarify the meaning of the concepts and the different roles and the distribution of the responsibilities between these actors.

Hereby, we aim to provide reflections and specific recommendations for increasing the impact and usability of the Guidelines.

How the concepts of controller and processor may be applied to MedTech companies

Medical technologies (medtech) cover any products, services or solutions used to save and improve people's lives and which can be used in a care setting, such as disposables, diagnostics, capital equipment and surgical innovations, through to implant technology, biomaterials and connected health IT such as eHealth, mHealth, human genome decoding, disease prediction, biobanks, biomarkers and many more.

Depending on the specific phase in the lifecycle of a medical technology and in which kind of context the medtech company performs, **their respective role may change**: they process health data in the research and development phase of a medical technology as a data controller, then process patient health data as a data processor when providing connected care and remote monitoring to health care professionals, and process data as a data controller in the context of vigilance reporting in accordance with mandatory requirements.

Other times, **medtech companies could be both a controller and processor for the same data** but for different purposes. For example, in context of digital health solutions, there is an evolution towards putting the patient in control of his care and developing direct-to-patient offerings. Thereby, a company may offer a remote monitoring solution that allows the patient to upload data at home. In that case, the data is available to the treating Healthcare Professional (HCP), but the company may also offer a patient-facing service that provides insights about the condition to the patient directly. With regards to the first activity (i.e. the remote monitoring solution), the company would qualify as a data processor and regarding the second one (i.e. the patient-facing service), as a data controller. In this context, it would be valuable to have more guidance to what extend such "additional services" could be conducted and without the approval of the controller of the remote monitoring service (i.e. the Healthcare Organisation in that case). There are a number of such scenarios applicable to medtech companies and it could become even more complex than in the provided example.

Taking into account the particularities of the sector, and outside of the specific set-up of direct-to-patient provision of technologies, medtech companies regularly find themself in multifaceted situations where it is not always clear whether they are controllers, co-controllers or processors.

Some scenarios may be more complex in reality

We value additional Guidelines on the concepts of controller and processor bring some clarity for the medtech industry, especially when it comes to scientific research.

We understand that the examples provided in the Guidelines have the goal to make the concepts more understandable. However, some examples, like the one on Clinical Trials (under paragraph 66) or the one on Market Research (under paragraph 42) can, in the industry's reality, be more complex. It may be worthwhile to put more emphasis on the fact that they are examples that cannot be applied to all scenarios, given that there are a number of different scenarios.

In particular, with regards to the Clinical Trials example, the set-up can be very complex. Without such a contextualization, and reference to GDPR provision of a case-by-case analysis, we fear that this proposed delineation of roles will be interpreted as the general rule and that Healthcare Organisations, contract research organisations or other stakeholders might want to use the qualifications as provided by the example without taking into consideration the different nuances of the specific clinical trial.

- **As such, it may be worth considering developing additional examples on the different legitimate setups, such as a (i) a processor, (ii) an independent controller, or (iii) a joint controller, tackling factors such as who initiated the study, how it is funded and by whom that could be taken into consideration to determine the right concept in a particular case.** Specifically, the impact of the qualification as joint controllers may merit further clarification, especially as the Guidelines acknowledge that the qualification may be limited to only those activities that are truly joint in nature, not necessarily the 'end-to-end data processing activity'. Also, especially when the 'joint' activity is limited to a small part of the data processing activity performed at one clinical site only, the impact of a joint controller qualification may easily become very complex[1]. Further, what impact a joint controller qualification has on the decision-making rights of the study sponsor. For example, regarding terminating the clinical trial early, involving a processor to perform certain data analytics services, etc. Jurisprudence has already addressed some situations where multiple controllers (co-)exist (jointly or not)[2]. Thereby, they stated that a controller is responsible only for those operations they are involved in, even if in the same processing context multiple controllers and other actors come into play.

[1] As an example of the need for further clarification, let's look at the situation in the Netherlands, where the CCMO indicates the investigator and study sponsor should be joint controllers, also if the study sponsor is solely responsible for the protocol, site selection criteria, patient eligibility criteria, etc.
[2] CJEU C-40/17, 136/17

- **Also, other situations with possible, or likely, joint controller relationships may merit further clarification; real-life situations, in particular in the technology and digital sectors, may feature multiple examples where a service provider supplies a large multitude of customers.** If such relationships all qualify as joint controller, what practical consequences would this have?

- **Given the above arguments on the Clinical Trials example, and the fact that this is one scenario among many others, we would recommend to re-write the provided example and simplifying it to a post-market registry scenario.** That way, the EDPB could still provide an example without risking simplifying those very complex scenarios and rigidly attributing the concepts of controller and processor to a specific party.

- **Furthermore, we would propose to the EDPB to address other scenarios where the roles may be different in future Guidelines which may be more healthcare research related.** Thereby, we would be more than happy to further exchange and discuss those different scenarios with the EDPB as well as providing more sector-specific examples.

- **In this context, it would also be very helpful if the EDPB came up with Guidelines on how to handle situations when the parties disagree with their respective roles or when authorities who are not entrusted with the enforcement of data protection rules (e.g. ethics committees, or other authorities outside the health sector) have different views about who should qualify as a controller, processor or else.** For example, there might be situations where negotiations stall or contracts are not executed because parties cannot decide what roles they have under the GDPR. Indeed, it is the GDPR that says that the controllers need to run self-assessments and they are also subject to the scrutiny of Data Protection Authorities and Courts (and only them).

Lastly, we would suggest indicating in the Guidelines, even if it might seem repetitive, that the examples serve only for educational purposes and that controllers/processors should not rely on them without undertaking a rigorous assessment of each particular data processing operation, as required under the accountability principle of the GDPR.

Other considerations

When it comes to a group of companies, the requirements and the application of the concepts of controller and processor might not always be easy to interpret and there may be many other, more complex scenarios to consider than those provided in the Guidelines. Overall, there are many nuances to consider and the Guidelines seem to be a bit rigid when it comes to situations where groups of companies are involved[3].

[3] For example, under paragraph 69 of the Guidelines, where it says *"[…] each entity decides independently on the access, the retention periods, the correction or deletion of their clients and prospects' data*".

Last but not least, we appreciate the efforts made by the EDPB to clarify those two concepts as well as to ensure consistency among their application. We value the Guidelines in their role of clarifying the different GDPR requirements. As such paragraphs 161-164 seem to go beyond the intended spoke, i.e. the requirements in Art. 26 GDPR and may appear as generate new or additional requirements. **We would therefore propose removing these paragraphs.**

Concluding, we would appreciate if the above considerations are taken into account by EDPB, especially with regards to the re-drafting of the Clinical Trials example, whether it is to update these Guidelines or for the development of additional ones, perhaps more focused on clinical/ healthcare research, and we would welcome a further discussion on the specificities of the medtech industry.

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our purpose is to make innovative medical technology available to more people, while helping healthcare systems move towards a more sustainable path. Our members are national, European and multinational companies as well as a network of national medical technology associations who research, develop, manufacture, distribute and supply health-related technologies, services and solutions.

For more information, please visit www.medtecheurope.org .

If you have any further questions, please reach out to:
Aline Lautenberg
General Counsel, MedTech Europe
a.lautenberg@medtecheurope.org