We would like to thank you for the opportunity to express our views and comments on concepts of controller and processor. As enforcement of GDPR is ongoing, it is important to have a common understanding of these concepts throughout European Union. Of course, we still must take into account the differences in member states laws and regulations, also backgrounds, which may lead to different interpretations of these concepts.

It is of essence to understand the concepts as uniformly as possible, as exchange of personal data between member states is becoming more and more common and widespread. Also, we need a thorough understanding of when an entity is considered a processor, a controller or offers just transmission services. To clarify this issue further, we propose to add some additional examples to the guidelines.

The nature of data and roles of different actors

When service provider adopts technical and security measures so the service provider has no means to access the personal data, different parties have argued that service provide could be still be considered as processor. This approach would consequently also lead to conclusion that all service providers and relevant actors are to be considered either (joint) controllers or processors, responsible for personal data processing. **We find this conclusion to be not in accordance with GDPR aims and provisions.** GDPR recital 26 points out that the principles of data protection should apply to any information concerning an identified or identifiable natural person. **The principles of data protection should therefore not apply to anonymous information.**

If the data is encrypted and person receiving data does not have any access nor has any available means to access personal data, being only holder of the “black box”, the receiving person should not be considered as processor. It is per se contradictory to the concept of processor, which in notion expects the processing of personal data. Several examples in draft guidelines refer to processor as not dependant on processing of personal data. This leads us to the scope of GDPR and whether the processing concerns personal data or should there be distinction made to data that shall not be considered personal data, as it is protected by privacy technologies. If all of the means are reasonably used and available technology at the time is considered and used to protect the personal data thus **rendering it through privacy measures anonymous to the holder of the data** (holder of “black box”), **the holder cannot be considered as processor** according to the GDPR recital 26.

It has been confirmed also in the Art 29 Working Party guidance and the existing Union law that a network service provider is not to be considered the controller for the personal data that is being exchanged. It is said that even when the message that is being transferred contains personal data and is being transferred by a network, whose only purpose is to deliver these messages, the person who created the message is

considered the controller of the personal message contained in the message not the person providing the transmission service[1].

Smart technical solutions can make personal data unidentifiable, so different data sets can be combined without having to process personal data. One example of such a solution is when data owners/donors encrypt the data and provide it to the service provider without giving the service provider access to the decryption key. This takes the reidentification capability out of the hands of the service provider. In this case, the service provider cannot be considered as a data processor in the means of GDPR. The solution transforms encrypted inputs into encrypted results without making the data available to the service provider.

Secure Multiparty Computation (SMC), a type of technical solution for research, allows for secure computation of sensitive data sets, such as health data, without having to trust a centralized entity. It refers to a field of cryptography that deals with protocols involving two or more participants who want to mutually compute a useful result without having to trust each other with their sensitive data. Every party will provide an input value and learn only the result of their own individual value so that nobody is able to access all the information. For example, in the case of a solution called Sharemind each party will receive one share of every secret value. The original secret can only be reconstructed by collecting all the shares of a value and adding them up. After the data has been transmitted and stored, the server can perform computations on the shared data; however, the server does not share the information with other servers so that none of them can reconstruct the input values. After finishing the computation, the results of the servers are transmitted and published to the client of the computation. The servers send the share of the results to the client who reconstructs the real result.

The secret-sharing of personal data by dividing it thus does not fall under the GDPR's scope, backed up by an analysis conducted by Prof. Dr Gerald Spindler[2]. This is because the solution divides the data, stores it on different servers and it is highly unlikely for any party to receive another's shares. If it is necessary for one data donor to specify whose information the other donor must provide, this has to be considered as processing of personal data. It would then be inevitable to identify the data subjects whose information is needed for the purposes of computation. But personal data will be processed only by one data donor, not all by all of them.

In case of Secure Multiparty Computation simply random fragments of personal data are used. The original data can only be restored (and thus turned into personal data) if all fragments are put together. Without the other parts, the file cannot be read in any way. One fragment itself does not contain information regarding a person and thus cannot be regarded as personal data. Theoretically, all server providers may collude and reengineer the personal data, however, this is highly unlikely since the providers of the server themselves have a high interest in ensuring safety and confidentiality of the SMC and may be legally bound by contract.

---

[1] Working Party 29 Opinion 1/2010 on the concepts of "controller" and "processor"page 11 also The legal guidance to telecommunication operators: recital 47 of Directive 95/46/EC

[2] https://www.jipitec.eu/issues/jipitec-7-2-2016/4440

The EDPB-EDPS Joint Opinion 1/2019 designated the European Commission as a data processor even though European Commission is only responsible for the core services in the eHDSI system, providing a secure private network (secure and encrypted connection) to Member States without having any access to the personal data. This raises concerns for modern techniques in scientific research, such as SMC, because if the European Commission is considered a data processor in eHDSI secure private network, then whoever provides or uses SMC would also be considered as a processor. Therefore, this decision raises questions and concerns. Should we apply this logic to researchers using SMC, we fear it would seriously hinder research efforts on health data across the EU, joint projects as envisioned under the Digital Europe Programme. This is because if a party is considered a data processor, it needs a legal basis for processing personal data under GDPR (e.g. permit from the ethics committee, data controller or a data subject's consent). The time and effort spent acquiring such a permit could constitute and undue barrier to research, because with solutions like SMC, no actual personal data is being processed – all data is anonymous from the perspective of the researchers.

Stepping further from the nature of data we would like to also deepen the knowledge about role division between different actors. For example, in the case of procurement procedures the roles could be understood quite diverse and these differences should be considered very carefully. Would the contractor be always relied on as processor or would it be subject to the substance of the procured service or its topic?

Considering the concepts, as given on page 3 of the draft guidelines, it is emphasized that 1) the controller must decide on both purposes and means, 2) the joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand and 3) the controller's instructions may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means.

Would it be possible to add an example to the guidelines, considering the following illustrative situation. Executive powers (government agency) procures an analysis on the purposes of policy development and the aim has been presented and decided by government agency. At the same time the means are left open to decide by the researchers as they have the best knowledge on the field, inter alia which method would be the best to achieve the result in a best manner. In this case, the government agency does not have any methods chosen or fixed, as they do not have this knowledge in-house. Would the researchers (who won the procurement) be considered as joint controllers, as they have the possibility to decide over the means (methods) or are they to be considered as processors?

To add another angle to the previous example, if the analyses would be funded from the EU funds, would it make any difference regarding the division of roles? For example, would European Commission, having set the aims for the use of certain fund and allocating the government agency the use of these funds for certain analyses, to be considered as joint controller, also? At the same time, we have to bear in mind that funding is given on a quite broad basis, for example European Commission probably

does not have any deeper insight to the topic than, eg assessing the recent developments of employment market for better policy making.

As conclusion of previous example and all its nuances, it is important to differentiate the situations and resulting consequences for all parties involved, as the rights and obligations are differentiated according to the role attributed. This would also be the main aim when supplementing the guidelines with different examples, as these can so lead to uniform understanding across EU, especially on borderline cases.

When also taking into account the status of recipient and third person, special attention is needed to distinguish the roles, as it is rightly so emphasized in the draft guidelines. Special attention should be given to differentiate which situations are considered as falling under the notion of jointly determined means and therefore as being a enough basis for designating a joint controllership. To provide an example at the national level, different bodies are consulted in the process of setting up a national database in Estonia and data sets are determined in legislative acts. This does not however mean that all the involved parties become joint controllers of the national database.

Regarding some insights in the guidelines, we would like to draw your attention to and query further the different aspects addressed in points 63 and 66 of the guidelines. Point 63 concludes that use of an already existing technical system does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context. At the same time, clinical trials example in point 66 refers in the event of investigator not participating to the drafting of the protocol to the investigator as a processor. It is not clear why the purpose of processing has not been considered in the case of investigator not participating to the drafting of the protocol. As per its nature, the clinical trial presumes the participation of health care provider and the processing as a whole is aimed at conducting the clinical trial. Against this background it is not clear how to clearly distinguish and deduce in this example when the investigator could be seen as processor.

We look forward to continuing dialogue between different actors thus achieving broad consensus and understanding on the core matters of personal data protection regulation and also on more specific concerns.