1. What are the key differences and implications between joint data controllers and multiple data controllers?

The Article 29 Data Protection Working Party of the European Commission (now replaced by the European Data Protection Board) considered the concept of joint control of personal data, as referred to in Article 2(d) of Directive 95/46 EC, in its Opinion 1/2010 on the concepts of "controller" and "processor", WP169. The intervening period has seen some developments in the thinking on this concept, notably the expanded provisions of GDPR on joint control and certain decisions of the CJEU. Pending the publication EDPB's forthcoming updated guidance on controller and processor, WP169 remains a useful starting point for understanding the situation of joint control, and how it may be differentiated from multiple and separate control of data.

The definition of a data controller as the party which, "*alone or jointly with others* determines the purposes and means of the processing of personal data," appears in Article 2(d) of Directive 95/46/EC and represents an extension of the concept of the singular "controller of the file" as articulated in Convention 108 of the Council of Europe (1981). This reflects the possibility, indeed likelihood, of multiple actors involved in processing personal data given the range of activities that may be considered to be "processing". From the point of view of accountability and in order to understanding liability may lie for infringement, it is necessary for such multiple actors to evaluate their respective roles and responsibilities.

WP 169 recognises two key considerations in undertaking an evaluation of the interaction between controllers. First of all, "the mere fact that different subjects cooperate in processing personal data, for example in a chain, does not entail that they are joint controllers in all cases, since an exchange of data between two parties without sharing purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers." However, WP169 also recognises that the definition of processing in the Directive does not exclude, "the possibility that different actors are involved in different operations or sets of operations upon personal data." (The Directive's definition of processing is sufficiently similar to that of the GDPR to accept that this still stands).

This gives an indication of the complexity of the assessment of the roles and responsibilities of different actors. While it must be determined which parties determine the purposes and means of processing, it must also be considered that some processing may consist of multiple operations undertaken by multiple actors. WP 169 also advises that while contractual arrangements can be useful in understanding joint control situations, they "should always be checked against the factual circumstances of the relationship between the parties".

WP 169 suggests that the identification of joint control of data should mirror the assessment of "single" control suggested earlier in the guidance document. This involves a substantive and functional approach to the application of the "elements" of control and their potential attribution to each of the actors involved in processing the data.

In the first place, WP 169, looks at the meaning of the term, "determines". It suggests that the attribution of a determining actor, arising from an analysis the factual circumstances of the processing, may be understood through answering such questions as, "why is this processing taking place? Who initiated it?"

The Opinion goes on to suggest a typology of categories of situations in which actors may be designated as exercising a "determining" role in processing, and thus acting as a controller. These are 1) Control stemming from explicit legal competence, 2) Control stemming from implicit competence, and 3) Control stemming from factual influence.

This third category is likely to be of most relevance, and to give the clearest indication of the existence of situation of joint control. As noted in WP 169,

> "this assessment allows for the drawing of external conclusions, assigning the role and responsibilities of controller to one or more parties. This might be particularly helpful in complicated environments, often making use of new information technologies, where relevant actors are often inclined to see themselves as "facilitators" and not as responsible controllers"

In our view, this consideration may also be usefully applied to the complicated environments of scientific and health research.

WP 169 goes on to consider, in the assessment of "single" control, the implications of the meaning of "purposes and means of processing". Taking as a basis that, "determining the purposes and means amounts to determining respectively the "why" and the "how" of certain processing activities", the Opinion again suggests an interrogative approach to determining the level of influence on the "why" and "how" and whether this entails the qualification of an entity as a data controller.

In particular, this approach will assist in determining whether a party to a research project acts as a controller or processor. A processor may have a significant degree of independence in choosing the technical means for processing personal data, subject to a general instruction from the controller. The controller however, makes the wider decisions as to which data shall be processed, to whom it may be disclosed, when it shall be deleted etc…

The third element of the assessment of "single" control outlined in WP 169 focusses on the meaning of "natural person, legal person or any other body." In the context of health research, the elements discussed here are of general importance, as well as helpful in determining the allocation of roles and responsibilities among possible joint controllers. Noting that preference should be given to consider as controller the company or body as such rather than a specific person, the Opinion goes on to state that,

> "especially for big and complex structures, it is a crucial issue of "data protection governance" to ensure both a clear responsibility of the natural person representing the company and concrete functional responsibilities within the structure, for example by entrusting other persons to act as representatives or points of contact for data subjects"

The Working Party in this sense was prefiguring the role of the Data Protection Officer in the GDPR, and the obligations of controllers to implement technical and organisational safeguards. In the context of health research, this emphasises the importance for those engaging in collaborative projects to ensure that the company or body, which they represent or work within, is aware of the role and responsibilities it may be undertaking at the appropriate corporate level.

The approach suggested in WP169 for analysing controllership can be transposed to the post-GDPR environment, and augmented by an understanding of how the central concepts have developed since 2010, in particular influenced by decisions of the ECJ. This should assist parties in multiple actor research projects in understanding their roles and responsibilities.

The key trend in relevant judgements of the ECJ in this area (*Wirtschaftsakademie* and *Jehovan todistajat)* is a broadening of the concept of joint control and the circumstances in which it can arise between parties. The Court's thinking also seems to be led by a desire to maximise the defence of the data protection rights of individuals in its interpretation. The key implications of these judgements in assessing joint control were set out in our previous briefing document. To these I would add, in line with the Court's line of thinking, that a data subject focussed analysis of the processing might assist. Through consideration of which parties are in a position to facilitate the exercise of data subject's rights, including the communication of transparent information, gaps may become apparent. In determining how to close these gaps, the parties involved will come to a greater understanding of their respective roles and responsibilities with regard to the processing.

The final point to be drawn from this consideration is that an interrogative approach to the facts of the processing involved in a research project should appreciate both the macro and micro levels. As WP 169 notes,

> "it is likely that at micro-level the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at macro-level these processing operations should not be considered as a "set of operations" pursuing a joint purpose or using jointly defined means."

This indicates the level of detailed assessment that will need to be undertaken to accurately assess the relationship between the various parties.

In terms of the implications for the various parties, the best approach would appear to be to undertake a detailed analysis of the processing operations involved in the project and to delineate clearly the respective roles and responsibilities. Where a situation of joint control is determined to exist these compliance responsibilities should be set out in an arrangement as per Article 26 GDPR. Of principle importance in making these determinations, whether as multiple or joint controllers, will be the documentation of the decision making process and the rationale behind it, in accordance with Article 24 GDPR.

2. What is the latest thinking on data processors who might actually be (a) a joint data controller or (b) in a multiple data controller relationship?

On this matter, the legislation would appear to be relatively clear. Article 28(10) GDPR provides that,

> "without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in that respect"

The implication of this is that for a processor to take on the role of controller shall be an infringement. In appreciating the practical implications of this, it is useful to go back to the underlying principles and definitions.

Article 4(8) GDPR defines a processor as, "a natural or legal person, public authority, agency or body which processes personal data on behalf of the controller." Article 28(3) requires that the processing shall be governed by a binding contract stipulating, inter alia, that the processor process the personal data only on documented instructions from the controller. Were the processor to go beyond the documented instructions of the controller, this would de facto mean that they had determined separate purposes and means for processing as outlined in Article 28(10).

WP 169 in considering the relationship between controllers and processors, notes that a processor may have some leeway to determine the means of processing. A general instruction to process personal data for a given purpose need not be specific as to the precise technical means that are employed – this will likely fall within the professional competence of the processor. The essential means of processing however must be determined by the controller i.e. which data shall be processed, for how it shall be retained, to whom it may be disclosed.

A further requirement of Article 28 is that the processor must immediately inform the controller if it considers an instruction to process to be an infringement of data protection law. It would seem to be a corollary of this that should a processor consider that they may in fact be acting as a controller or joint controller (thus infringing the GDPR), they should inform the controller and jointly take whatever steps may be necessary to bring the processing into compliance; at all stages considering the risks to the rights and freedoms of data subjects.

3. In Article 26(2) of the GDPR, it talks about an "arrangement [to] duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects" and that "the essence of the arrangement shall be made available to the data subject." What does "essence of the arrangement being made available" mean particularly but not only in terms of (general) transparency?

Article 26(1) requires joint controllers to determine their respective responsibilities in a transparent manner by means of an arrangement between them. In particular this arrangement shall the exercising of the rights of the data subject and the duties to provide information to the data subject. It is the "essence" of this arrangement that must be made available to the data subject.

I would note that in the first instance the arrangement represents the means by which the controllers shall determine their respective responsibilities, *in a transparent manner*. The Article 29 Working Party's Guidelines on Transparency under GDPR, WP260, note that while transparency is not defined in the Regulation, it has some core elements such as the use of concise language, intelligibility and accessibility. It is also noted that, in contrast to a data processing agreement between a controller and processor, the arrangement is not a legally binding contract.

This would suggest that the purpose of the arrangement is to identify the responsibilities of the controllers in a clear manner, avoiding complicated or legalistic terms. In following the line of thought outlined above in WP 169, and in the decisions of the ECJ, this encourages data controllers to approach their responsibilities in a manner that will avoid gaps and maximise the protection of data subjects' rights.

Noting that the arrangement is required in particular to address the exercising of the rights of the data subject and the communication of transparent information on the processing, these elements may be what is intended to represent the essential components or "essence" of the arrangement.

Recital 79 of the GDPR may give some further insight into how the provisions of Article 26 shall be interpreted:

> "The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, *including where a controller determines the purposes and means of the processing jointly with other controllers* or where a processing operation is carried out on behalf of a controller"

This suggests that the clear allocation of responsibilities, as envisaged in the joint controller arrangement, is intended to encompass the full range of responsibilities of each controller including their interaction with the Supervisory Authority. It is not a requirement of Article 26(2) to provide the full content of the arrangement to the data subject but only the "essence". I would suggest that this means those parts that may be considered essential, such as how the responsibilities of the controllers with regard to the data subjects' rights are allocated, how the provision of information is handled, and whether a contact point has been established for further information.

4. Following directly from 3, what way do Article 13 and 14 work when a joint data controller arrangement is created?

As noted above, the joint controller arrangement shall, in particular, address the respective duties of the controllers to provide the information referred to in Articles 13 and 14. I would suggest that in the first instance the joint controllers consider in depth what information they are obliged to provide to data subjects. Secondly, they should devise a method of discharging their responsibilities that is in accordance with their shared responsibility under Article 13 to provide any such information, "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". For example, the information to be provided under Article 13 shall be provided at the time when personal data are obtained. It may thus be appropriate for the controller who is responsible for obtaining the data to provide information relating to the other controller(s) at this time.

5. Is data 'shared' information between data controllers or is there a 'disclosure' of information from one to another?

The term "disclosure" is not defined in the GDPR, nor is it defined in the Data Protection Act 2018. Article 4(2), GDPR, in defining 'processing' refers to, "disclosure by transmission, dissemination or otherwise making available". Thus it seems clear that the transmission of personal data from one controller to the other, whether "sharing" or "disclosure" is processing. As such the processing is subject to all requirements of the legislation including compliance with Article 5 (Principles relating to processing of personal data), Article 6 (Lawfulness of processing), and Chapter IV, Section 1 (General Obligation of the Controller and Processor).

The joint controller arrangement under Article 26(1) is without prejudice to the ability of the data subject to exercise his or her rights under the GDPR in respect of and against each of the controllers.

This would suggest that the purpose of the arrangement is to determine the respective responsibilities of the controllers and the manner in which they shall be discharged. The arrangement cannot obviate the requirement for any of the controllers to comply in full with their obligations.

6. Can a joint controller arrangement be retrospective or does it apply only to new personal data generated as a result of the creation of the joint controller arrangement?

As noted in WP 169, "being a controller is primarily the consequence of the factual circumstances that an entity has chosen to process personal data for its own purposes." A situation of joint control may arise in fact, whether a joint controller arrangement exists between the parties involved or not, as demonstrated in the ECJ cases discussed above. It thus appears that joint control is not contingent on the existence of a joint control arrangement; rather the arrangement is intended to clarify the compliance obligations of the joint controllers arising from their joint control of data.

A situation of joint control may arise as a matter of fact in relation to data that is transmitted from one controller to another for a shared purpose. Further, as noted in the judgements of the ECJ, access to the data in question is not required for a situation of joint control to arise. Joint controllership arises from the circumstances of the processing rather than the nature of the data, and while processing subject to joint control may generate new personal data, it seems possible that personal data that already exists may come within the scope of a joint controllership situation.