1. INTRODUCTION

Since the concepts of controller and processor are functional and autonomous concepts, difficulties as to how they should be interpreted and applied arise often. These difficulties are not only faced by organisations which do not have a specialised data protection function but affect organisations of all sizes and in all sectors.

As the concepts are fundamental to data protection law, organisations should generally be able to understand their role and the obligations which arise from that role without the need to obtain specialist advice. The publication of guidance on these concepts by the European Data Protection Board ("**EDPB**") has therefore been highly anticipated to provide greater certainty for all organisations in the day-to-day application of the law.

Having reviewed the draft version of the guidance, we are of the view that certain aspects of them may not achieve the desired level of clarity. The guidance is unlikely to meet the expectation of businesses which had anticipated guidance to allow them to reduce time and resources used to assess their data protection relationship with other parties. We have set out below our comments on how we think that the guidance could be improved.

2. CONTROLLERS / PROCESSORS

2.1 Key elements

We welcome guidance which clarifies that the controller must determine both the purpose and the means of processing and not either the purpose or means, rectifying the position in the Article 29 Working Party Opinion. However, additional guidance is needed on the extent to which decisions about the means may be delegated to a processor. In our experience, it is often difficult to determine how much influence may be exerted in relation to such decisions for a party to be a controller.

The guidance does not clearly state that a single entity cannot be both a controller and a processor with respect to the same processing activity, nor does it explain how conflicting assessments between two or more entities with respect to a processing activity should be dealt with. Presumably, if an entity determines the purpose of a processing activity e.g. hosting as part of a broader purpose, the entity would not be considered a processor for the same activity. Additional guidance on this point to assist parties with an accepted method for approaching this type of situation would be welcome. We are of the view that such guidance will assist with reducing the large amount of time and costs expended by parties.

The distinction between "essential" and "non-essential" means does not always simplify / support the determination of the role of the parties. At times it even fuels debate in contract negotiations, providing parties with opportunities to exert their market power and negotiating position, which is contrary to the idea of clear allocation of responsibilities as envisaged by the General Data Protection Regulation ("**GDPR**"). Therefore, the guidance should further clarify to what extent decisions about the means of processing may be delegated to a processor.

As an example, if an organisation determines what data it needs to provide a service to another party, is this decision sufficient to prevent the other party from being classed as a controller? It is often the case that the controller has limited influence over the means of processing. For example, a processor could use a particular algorithm to process personal data and the controller could have no input into the decision to use that algorithm.

We would also welcome further clarity on how the assessment of a party's role should be made with reference to determining the purpose of processing where there is more than one party who will process the personal data. The guidance seems to go beyond the letter and intent of the law in some instances. As an example, paragraph 91 states that Article 28(3) GDPR "*imposes direct obligations upon processors, including the duty to assist the controller in ensuring compliance*". In our view, this is not in line with the intent, as the GDPR makes such obligations subject to a "*contract or other legal act*". If they had been intended as statutory obligations in their own right, such as the maintenance of processing records under Article 30 for example, there would not be a need for a contract or other legal act setting out such terms.

2.2 **Practical aspects**

The guidance breaks down the Article 28 requirements and provides much anticipated explanatory notes. It would be helpful if some of the points could be expanded upon to explain how much leeway controllers and processors have in relation to contractual terms in order to be able to deal with the practicalities of each processing situation. For example, in relation to audit rights, it is not clear if controllers can agree to have the right to carry out remote audits rather than on-site audits. If such points can be determined by the controller at their discretion, then the guidance should confirm this and provide points the controller needs to consider in its assessment of such contractual rights to meet its obligations.

The guidance in relation to the approach controllers and processors can take regarding technical and organisational security measures is helpful. However, the obligation on the processor to obtain the controller's approval before making changes to the security measures is likely to cause practical difficulties. For example, where a processor has thousands of customers for which it processes personal data, the processor would have to obtain approval from each customer to change its security measures. As the controller’s instructions may leave a certain degree of discretion, can the controller give general approval to allow the processor to make changes to such security measures without instructions where it trusts that the processor can best determine the most appropriate measures?

The guidance states that the controller must only use processors providing sufficient guarantees to implement appropriate technical and organisational measures and can take account of the processor’s expert knowledge, reliability, resources and adherence to an approved code of conduct or certification mechanism. In a similar way to the guidance the EDPB has approved in relation to the appointment of a Data Protection Officer, it would be helpful if it could expand upon the concepts of the expert knowledge, reliability, and resources of a processor to ensure that companies can apply these recommendations.

The appointment of sub-processors is an area which often requires extensive negotiation between parties. While the guidance states that the agreement between the parties should set out the process for obtaining the controller's approval for the appointment of a sub-processor, it doesn't expand upon how this might work in practice. In the same way that the guidance seeks to explain how involved the processor can be in determining the security measures, the guidance should confirm to what extent the obligation to carry out due diligence on sub-processors can be delegated to processors.

In addition, in circumstances where a controller objects to the appointment of the sub-processor, the EDPB should suggest possible options that can be applied. In many agreements we are seeing, the only remedy for a controller which objects to the appointment of a sub-processor is to terminate the agreement. Practically, this remedy is difficult for the controller to utilise and would require interruption to the processing or extensive costs for a controller, particularly if the processor is essential to the controller's business.

3. JOINT CONTROLLERSHIP

3.1 General

The guidance provides a welcome deep dive into what it means to jointly determine the purpose and means of processing. It moves past the general concept to expand upon the CJEU's views that joint controllers can be involved to different degrees.

The guidance on common decisions provides some much needed clarity on the conditions for joint controllership to arise, particularly by confirming that joint controllers must jointly determine both the purposes and the means of processing, rather than just one or the other as was suggested in the Article 29 Working Party Opinion.

However, the guidance seems to lean towards the importance of a jointly determined purpose and less so on a jointly determined means. It would be helpful if the guidance could clarify if this should be the focus of any analysis of the relationship, and if the concept of "essential" and "non-essential" means outlined in relation to controller-processor relationships is relevant here.

A particular point of confusion is whether the decision by an entity to allow another party to determine the means of processing is sufficient to jointly determine the means with that other party. The guidance uses the example that the use of an already existing technical system does not exclude joint controllership when users of a system can decide on the processing of personal data to be performed in this context. The question is: must the party using the other party's technical system demonstrate that they have provided some input into the decision to use the particular means or is it sufficient for that party to decide to allow the other party to make the decision?

In relation to determining the respective responsibilities of controllers, it is unclear why the joint controller arrangement should deal with compliance points such as international transfers and general data protection principles if each joint controller has direct GDPR obligations to ensure compliance. As controllers, the parties would not be able to delegate such responsibilities to another party.

In light of this, the guidance should clarify if the concept of joint controllers should be considered as a concept separate to that of controllers in relation to joint processing. If joint controllers do need to determine their respective responsibilities in relation to the Article 5 principles, the guidance should set out how this would work in practice. An example of how the EDPB sees such separate responsibilities working and why this would need to be determined as part of the requirement under Article 26(1) would be helpful for joint controllers to understand the requirements.

3.2 Converging decisions

We are of the view that the introduction of the concept of converging decisions goes beyond what is intended by the GDPR in relation to joint controllership. It is likely to cause extensive debate and confusion and may be unworkable in practice, particularly because it blurs the line between situations where two controllers act jointly and others where they pursue different albeit complementary purposes. We are aware of businesses which are already grappling with this aspect of the guidance.

In our view, the GDPR does not provide a basis for joint controllership to arise where decisions on the purpose and means merely converge. Although guidance on the concept of "inextricable link" is needed to bridge the apparent gap between the law and the recent judgements of the CJEU in cases such as *Wirtschaftsakademie,* the guidance emphasises secondary, indicative criteria rather than focusing on key determinative factors.

The guidance refers to joint controllership arising where there is a mutual benefit. It subsequently states that joint controllership does not arise out of the mere existence of a mutual benefit because if one party does not pursue a purpose of its own, it would only be a processor.

However, there are many situations where two independent controllers mutually benefit from processing but do not exert any substantial influence over each others' processing purposes.

The guidance also unduly focuses on the choice of processing systems and tools, suggesting that the requirement of determining the means may be satisfied merely on the basis that one controller adopts the means of processing made available by another; even though the guidance subsequently states that the use of a common processing system would not suffice.

The guidance points out that cases of joint controllership should be distinguished from controller – processor relationships, but further detail is needed on distinguishing situations where joint controllership arises from others where the parties simply act as independent controllers.

Many controllers exchanging data mutually benefit from the exchange and also use common means of processing. However, something more is needed for joint controllership to arise. As an example, a company buying another company may be provided with information about the selling company's employees as part of the due diligence exercise. The parties use common means of processing, mutually benefit from the sharing of the information, and even share the wider objective of completing the deal and transferring the employees if the deal goes ahead, however, the buying and selling companies would not be considered as joint controllers.

In our view an element which needs to be given more attention is that of a decisive influence which enables both the purpose and the means of processing. Additional focus on this element would help distinguish processing activities which are "inextricably linked" from others which are merely complementary. The judgements of the CJEU in *Wirtschaftsakademie*, *Fashion ID* and *Jehovah's witnesses* were driven by a need to ensure "effective and complete protection of data subjects"; however, such protection does not require joint controllership to arise in every case where processing activities are linked. We are also of the view that these judgements support an interpretation based on decisive influence / enablement.

4. OTHER CLASSIFICATIONS

4.1 Third party

Although the guidelines explain that the concept of third party is a relative concept, we have come across instances of controllers or processors assessing their role to be that of a "third party", without also being a controller or a processor. It would help if the guidelines explained, in simple terms, that any organisation which processes personal data will be a controller or a processor, and that third party is not an alternative to these concepts.

4.2 Persons acting under the direct authority of a controller or a processor

Some clarity on this concept, which is not defined in the GDPR, would be welcome. Apart from reference to the concept in the guidance on "third parties", the concept has practical implications when determining whether certain individuals act as processors. An employee of a controller or a processor is an obvious example of a person who acts under direct authority, but it is unclear how this applies to alternative arrangements. It is not uncommon for individuals to be engaged as independent contractors or to be seconded by agencies. In such cases these individuals would be "external" to the controller or a processor, but their treatment as processors is impracticable and does not reflect the reality of their relationship with the organisation. Some definitive criteria are needed.