Bates Wells
10 Queen Street Place
London, EC4R 1BE

Tel: +44 (0)20 7551 7777
DX: 42609 (Cheapside 1)

European Data Protection Board
Rue Wiertz 60
B-1047 Brussels
Belgium

Direct Dial: 00 44 20 7551 7796
Email: v.hordern@bateswells.co.uk

Your ref:
Our ref: VH/MC2/199999/0888

19 October 2020

Public Consultation

Guidelines 07/2020 on the concepts of controller and processor in the GDPR

Bates Wells is a UK law firm that provides specialist data protection advice to a range of commercial, public sector and charity clients. We have the largest dedicated Charity and Social Enterprise team in the UK and we act for more UK charities in the top 3,000 (by size) than any other law firm. We regularly advise on data protection law, as the vast majority of our clients are impacted by it.

We welcome the opportunity to respond to this consultation. Our response draws upon our extensive experience in advising on the controller/ processor definition in practical situations and the common issues that our clients ask us to advise on. We consider there are some areas where the guidelines could be enhanced that would help to address these common issues. In particular, we would like to address:

(a) The role of independently appointed investigators;

(b) The implications of individuals acting as controllers/ processors and the lack of examples in the guidelines;

(c) When employees act as controllers; and

(d) What organisations need to demonstrate where the position is not clear.

1. **The role of independently appointed investigators**

1.1 Controllers may appoint independent investigators who process personal data provided by the controller in order to carry out an investigation. Frequently, but not always, these investigators are individuals. There are a variety of different scenarios where this could occur. For example, a controller often appoints an independent investigator to resolve an employer/ employee dispute. Or, in a professional regulatory setting, a controller may rely on individuals participating on independent panels to adjudicate on matters. What is critically important in these circumstances is that the investigator acts independently. If the investigator is considered to act on the instructions of the controller, that is likely to undermine the investigation they are undertaking. We note the reference to a clinical trials investigator in an example at paragraph 66 of the guidelines but there is no other guidance on the role of an independent investigator.

1.2 The guidelines do not adequately address these situations therefore. Paragraph 19 (on the definition of a controller) explores the Article 4(7) GDPR wording of "*determines*" and invites two questions; "*why is the processing taking place?*" and "*who decided that the processing*

should take place for a particular purpose?". Paragraphs 77 and 78 (on the definition of a processor) explore the concept of "*processing personal data on the controller's behalf*", stating, in particular, that "*a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means*". While the guidelines highlight the concept of "*essential means*", a dichotomy exists with respect to these examples.

1.3 An independent investigator is appointed for a specific and usually temporary purpose. Where personal data is involved, the investigator is appointed by the controller and will process personal data in order to carry out the investigation. Based on the guidelines, this scenario could be interpreted as the investigator *always* acting as a processor, based on the fact that:

(a) The processing is taking place on the controller's behalf;

(b) The controller decided that the processing should take place for a particular purpose (i.e. to carry out the investigation); and

(c) The investigator is implementing the instructions of the controller in carrying out the investigation.

1.4 However, the investigator will often decide the "*essential means*" in reality. For example, in an employer/ employee investigation, an investigator (and not the employer) may decide who to interview or which records to review. Paragraph 78 is unhelpful in this regard, as the investigator clearly has "*regard to the purpose of the processing*" (which is ultimately the employer's purpose) but, in fact, may solely determine the "*essential elements of the means*". This exposes a lack of clarity as to whether *both* criteria in paragraph 78 should be satisfied in order for the entity to be regarded as a processor.

1.5 The guidelines therefore fail to address the nuances of such a scenario. This is reflected in the clinical trials example at paragraph 66 which does not address the grey areas where an investigator may *partially* design or assist with designing a protocol.

1.6 The role of an investigator in a clinical trial should be regarded as different to the role of an independent investigator in the examples referenced above, taking into account the separate legal regime governing clinical trials.

1.7 With respect to the clinical trials example at paragraph 66, we suggest that it is clarified that a healthcare provider and sponsor may be joint controllers (for some/ all purposes) or *independent* controllers (for some/ all purposes) depending on the structure and purposes of the arrangement.

1.8 We suggest that the following changes to the guidelines are considered:

(a) A new example (or examples) is introduced to specifically address situations where an investigator has been appointed by a controller to act independently, explaining the potential nuances of the situation.

(b) The wording at paragraph 78 is reviewed.

(c) The controller/ processor determinations should be reviewed in the clinical trials example. One option is that the example be removed and addressed in a separate

publication from the EDPB on the roles of parties involved in clinical trials, as the controller/ processor roles within clinical trials is a complicated area of law.

2. The implications of individuals acting as controllers/ processors

2.1 The guidelines acknowledge that individuals may act as controllers or processors. However, it is often the case that individuals are not aware that they hold this status under data protection law and are not equipped to consider the implications.

2.2 Therefore, it would be useful if the guidance could set out the *practical* implications for an individual who is a controller or processor under data protection law. For example, an individual who is a processor is required under Article 28 to put a data processing contract in place with the controller. However, often, such a contract is unlikely to be implemented unless individuals are acting in an official capacity and are aware of their data protection status (for example, if the individual is a consultant to a company). Additionally, it would be useful for the EDPB to indicate to what extent an individual is held to the same standard of compliance as corporate entities with more resources.

2.3 We suggest that the following changes are considered:

(a) The guidelines include examples of situations where an individual acts as a controller or processor.

(b) In the examples, the EDPB sets out its expectations of those individuals' compliance with the GDPR.

3. When employees act as controllers

3.1 Individual employees can inadvertently or intentionally act as controllers, such as when they use personal data outside of their role. For instance, when an employee who receives personal data that he is authorised to receive for his role chooses to process that data for a new purpose not associated with his employment role. The UK Supreme Court recently decided that an employer controller was not vicariously liable for the actions of a rogue employee (found to be acting as a controller) who published personal data relating to his colleagues on the internet[1].

3.2 Paragraph 76 of the guidelines states that "*employees and other persons that are acting under the direct authority of the controller, such as temporary employed staff, are not to be seen as processors since they will process personal data as part of the controller's entity*". This statement does not explore the possibility, or outline the risks, that an employee can become a controller in certain circumstances.

3.3 We suggest that the following changes are considered:

(a) Wording is added to paragraph 76 to confirm that employees can act as controllers, indicate when this occurs and explain the associated risks; and

(b) A new example is created which demonstrates how an employee can act as a controller.

[1] *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12

4. **What organisations need to demonstrate where the position is not clear**

4.1 We understand that the guidelines aim to clarify *how* to make the determination of whether an entity/ individual is a controller or processor and to address grey areas. However, the guidelines do not set out what data protection authorities will look for when assessing whether or not a correct determination has been made. We suggest that this point is considered in order to help organisations understand how they may be examined by a data protection authority.

4.2 We further suggest that the EDPB sets out its view on how data protection authorities should treat entities who have made the wrong determination in good faith and can demonstrate that appropriate thought was put into the decision. This could be reflected in a new section which, for example, addresses how investigations should be carried out/ fines should be issued by data protection authorities in different scenarios. For example, an entity that has *clearly and deliberately* made an erroneous determination in order to avoid data protection obligations should be treated with less flexibility than an entity who has made a *questionably* incorrect determination but followed the correct process.

---------- END----------