WIRTSCHAFTSKAMMER ÖSTERREICH

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

The Austrian Federal Economic Chamber provides the following comments:

Executive Summary, last paragraph: It should be clarified, that the Guidelines 8/2020 and the jurisdiction of the ECJ declare that the level of responsibility of joint controllers may vary (i.e. differences in fines, too).

Part I

2.1.1 "Natural or legal person, public authority, agency or other body"

No. 17 of the draft Guidelines reads that "*In practice, however, it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR*." We would recommend a reference to the discussion in No. 86 (p.27) below to put the term "*usually*" in context. Without this link, the current wording could cause uncertainties.

Please clarify if having distinct legal personality is a prerequisite for the qualification as a "controller". The term "body" is ambiguous and could also apply to legally dependent branches of foreign corporations, unincorporated entities, or partnerships/societies constituted under civil law ("*Gesellschaften bürgerlichen Rechts*") that do not have legal personality under Austrian Law.

2.1.2. "Determines"

No.22 is actually very vague. Particularly with a view to community law´s contact tracing, it would be appropriate to clarify that a person responsible must have a minimum amount of possibility to make decisions with regard to the purposes or means.

2.1.4. "Purposes and means"

No. 35: We would recommend the term "level of influence" to be defined in more detail. It needs to be clarified who has to provide the "guidance" mentioned in the paragraph. In this context, practical examples would be helpful and desirable.

Furthermore, as the law firm example is given, the Federal Bank and Insurance Division notes, that it would be very helpful for the banking sector to mention banks as examples of controllers. This would facilitate some discussions in an international context about the role of banks in this context.

No. 38 regarding accountants: Controllers are apparently those accountants responsible who carry out the "auditing activities in accordance with legal provisions". This basically corresponds to our Codes of Conduct "Bilanzbucherhalter" (= accountants). In order to draw a clear and predictable linie, there is no plausible reason for the distinction between "specific" and "general" obligations, when carrying out auditing services. Both determine the processing of the accountant alike and therefore should lead to their classification as a "controller". To avoid legal uncertainty regarding the difference between "specific" and "non-specific" obligations and „detailed" and „very detailed" instructions, we suggest the following adaption:

"In a situation where the law does not lay down ~~specific~~ obligations for the accounting firm and the client company provides ~~very~~ detailed instructions on the processing, the accounting firm would indeed be acting as a processor."

3.2.2.1 Jointly determined purpose(s)

No. 58: "*In addition, when the entities do not have the same purpose for the processing, joint controllership may also, in light of the CJEU case law, be established when the entities involved pursue purposes which are closely linked or complementary.*" It would be useful to clarify when the purposes can be considered "closely linked or complementary" through some concrete examples.

3.2.2.2 Jointly determined means

We believe the following text in No. 63 (p.20) could create uncertainties "*The 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*". We therefore recommend to clarify this provision, through some concrete, practical examples, particularly of when an owner of platforms, standardized tools, or other infrastructure allowing the parties to process the same personal data should be considered as a controller, processor, or joint controller.

With regard to No. 64 (p.20), we would like to point out that joint controllership will be difficult to put in place, especially in case of imbalances between contractual parties. We would therefore ask the EDPB to provide further guidance, including one or more model contract clauses on joint controllership, to be used in this context.

Regarding No. 66 (p.20), we agree with the recommendation that the arrangement between the controllers should be made in the form of a binding contract. In this regard, it would be helpful to provide guidelines on the content of this arrangement so companies might determine and clearly understand the respective responsibility of each party with respect to the obligations set out in the GDPR. As mentioned above, one or more standard model contract clauses could be useful for companies.

4 Definition of Processor

In No. 79: Please provide guidance for instances where the processor may be bound by law to carry out processing for its own purposes (i.e. statutory archiving/logging obligations).

Part II

1.3.1 The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR)

Under No. 119 (p.35), the draft Guidelines note that "*The contract must say that the processor needs to ensure that anyone it allows to process the personal data is committed to confidentiality. This may occur either via a **specific contractual agreement**, or due to statutory obligations already in place.*" Regarding the text in bold, we would welcome a statement from the EDPB as to whether confidentiality provisions in the employment agreement between the processor and its employees would be sufficient from a GDPR point of view. In our view, the answer should be that it is.

1.6 Sub-processors

We welcome the statement in No. 157 (p.40) that "*Imposing the 'same' obligations should be construed in a functional rather than in a formal way: it is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the obligations in substance are the same*".

Regarding TOMs: We criticize that the level of detail outlined in the Guidelines is improper, unrealistic and requires an extreme amount of documentation.

Best regards

Dr. Rosemarie Schön
Director

Legal Policy Department
Austrian Federal Economic Chamber