19 October 2020

EBF_042951

EBF response to the European Data Protection Board's consultation on the Guidelines 7/2020 on the concepts of controller and processor in the GDPR

Key points:

- The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board's consultation on the draft guidelines on the concepts of controller and processor in the GDPR.
- The more practical approach of this draft Guidance is welcome. However, the current wording would **imply a considerable increase in the requirements for companies in managing their service providers who access personal data,** particularly considering the level of detail provided on the provisions that will have to be included in the contracts.
- Regarding joint-controllership, **we caution against the approach to extrapolate the conclusions of two specific CJEU cases - *Wirtschaftsakademie* and *Fashion ID*- to all situations.** In many situations where firms collaborate / have an arrangement, both should be considered controllers, but this does not mean they need to be joint controllers. **There should be a case-by-case assessment, based on the facts of the situation, and responsibilities determined accordingly. Forcing joint controllership unnecessarily will create significant complexities for firms, without clear benefits to individuals.**

EBF position:

The European Banking Federation (EBF) welcomes the European Data Protection Board (hereafter 'EDPB') draft guidelines on the concepts of controller and processor in the GDPR. You will find below technical comments on the draft guidelines.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

1. Introduction

We welcome the intention of the EDPB to clarify aspects related to the role of controllers and processors, as well as on the concept of joint controllers in accordance with the GDPR and the recent rulings of the CJEU. **EBF members also welcome the more practical approach in the draft guidance.** However, with regards to the relationship between the controller and processor section, we have concerns about the contractual guarantees that should be set between the controller and the processor.

The current wording of the guidelines would imply a considerable increase in the requirements for companies in managing their service providers who access personal data, particularly considering the level of detail provided on the provisions that will have to be included in the contracts. Any changes should therefore be applicable only to future contracts. Companies should be of no obligation to revise and re-conclude all past contracts which might be amounted in hundreds or even thousands.

Overall, the process of drafting the contract should be more efficient, reducing the details given on the specific guarantees to be incorporated. It would be helpful for the EDPB to produce – with comprehensive industry consultation – **a set of voluntary model contractual clauses which could be easily used by entities**, including a brief description of the processing and the data affected, and without the need to adapt in each case excessive fields (similar to the current Standard Contract Clauses).

Regarding joint controllership, we caution against trying to apply, by default, the conclusions of the two CJEU cases *Wirtschaftsakademie* and *Fashion ID*[1] to other situations for which the facts may not be the same. **In many situations where firms collaborate / have an arrangement, both should be considered controllers, but this does not mean they need to be joint controllers.** EBF members are concerned that forcing joint controllership unnecessarily will create significant complexities for firms, without a clear benefit to individuals.

PART 1 – Concepts

A. Definition of controller (Section 2)

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

Paragraph 17 (p.10) of the draft Guidance 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*

[1] CJEU, Judgment in *Wirtschaftsakademie*, 5 June 2018, C-210/16, ECLI:EU:C:2018:388; CJEU, Judgment in *Fashion ID*, 29 July 2019, C-40/17

the GDPR." We would recommend a reference to the discussion in paragraph 86 (p.27) below to put the term "*usually*" in context. Without this link, the current wording could cause uncertainties.

We would also like to note that in large companies with multiple entities, the controller can be the parent company and/or its branches and/or its subsidiaries.

2.1.2 "Determines"

In paragraph 21 (p.10), the draft Guidance notes that "*…this presupposes that the legislator has designated as controller the entity that has a genuine ability to exercise control."* In EBF member's view, the organisation that has **been specifically identified by legislation as being a controller - should have confidence that they are indeed legally a controller (as should the other firms that are interacting with it).** Therefore, we would also recommend to replace the word "determinative" with "definitive" in the following sentence: "*Where the controller has been specifically identified by law this will be* ***determinative*** *for establishing who is acting as controller*."

Paragraph 25 (p.11) includes an example relating to a Law Firm. We recommend to expand this to align to the example included in paragraph 38 (p.14) relating to Accountants. The level of instruction provided to a law firm or an accountant should be highlighted as a relevant determinant. It is referenced in the Accountant example but only alluded to in the Law Firm example, yet a Law Firm can also receive detailed instructions from, for example, the inhouse legal team of a company.

2.1.4 "Purposes and means"

In paragraph 35 (p.13), the draft Guidance writes that "*In this perspective, there is a need to provide guidance about which level of influence on the "why" and the "how" should entail the qualification of an entity as a controller and to what extent a processor may make decisions of its own."* However, it is not very clear **how and where this information should be provided by the controller and the processor**. We would welcome clarification on this point.

Further in this section, in paragraph 39 (p.15), the draft Guidance notes that "*Even though decisions on non-essential means can be left to the processor, the controller must still stipulate certain elements in the processor agreement****, such as – in relation to the security requirement, e.g. an instruction to take all measures required pursuant to Article 32 of the GDPR."*** It would be useful to have a clarification on the instruction on measures pursuant to Article 32 GDPR to be provided by data controller to the data processor, given that paragraph 38 (p.14) states that the detailed security measures are left to the decision of the processor.

2.1.5 "Of the processing of personal data"

Paragraph 42 (p.16) states that it is not necessary that a Controller actually has access to the data that is being processed. We would welcome a clarification to this point as a controller should have the legal ability to access the personal data being processed on its behalf by a processor. It should also be noted that the Wirtschaftsakadamie case referenced in the paragraph relates to *joint controllership* (see comments in the Introduction).

In the Market Research example following paragraph 42, it appears that the "no access required" conclusion in the CJEU Judgment in *Wirtschaftsakademie* is also given too broad an interpretation. The definition of "controller" requires that the controller determines *both* the purpose and the means (see paragraph 34). Company ABC has no control over the means by which XYZ collects data and ABC has not provided any personal data to XYZ. ABC has no control over which respondents XYZ selects. ABC has only instructed XYZ what questions to ask to respondents – this is not personal data. Also, in real life situations it is probably often XYZ that would identify the relevant questions and how to formulate them, based on ABC's general scope outline, since it is typically XYZ who have the relevant expertise on this. To impose, under such circumstances, the role of controller on ABC does not seem realistic.

B. Definition of Joint-Controllers (Section 3)

With regard to paragraph 46 (p.17) which mentions CJEU case law related to "joint controllers**", we would like to note that the recent CJEU rulings concerned two specific cases.**[2] The Guidelines **should be cautious about extending this joint controllership interpretation, by default, to too many relationships between data controllers**, (e.g. where one of the controllers is the beneficiary of the advertising undertaken by the other controller targeting its own databases). Indeed, the court cases referred to in the guidance related primarily to situations where a firm was claiming to have *no* responsibility. Provided both of the firms involved in the arrangement are acting as controller (where applicable), **existing GDPR provisions, e.g. on the legal basis of processing, accountability, and transparency requirements**, **should be capable of addressing most if not all data protection risks. It is not necessary to go as far as to insist that there must be *joint* controllership in situations where two controllers have an arrangement beyond the specific scenarios covered in the relevant case law.**

Requiring that controllers with some kind of arrangement together must be joint controllers will likely add complexity to the legal arrangements between them, without

[2] CJEU, Judgment in *Wirtschaftsakademie*, 5 June 2018, C-210/16, ECLI:EU:C:2018:388; CJEU, Judgment in *Fashion ID*, 29 July 2019, C-40/17

adding to data subject protection. This observation applies to the whole issue of joint-controllership.

3.2.2 Assessment of joint-participation

The concept of converging decisions, as described in paragraph 53 (p.18), is too broad. All commercial arrangements will involve converging decisions as this is the process by which agreement is reached. **A distinction should be introduced to reflect decisions which converge following independent assessment and consideration**. In addition, regarding the reference to processing activities being 'inextricably linked', it should be acknowledged that mutual benefit and economic interest can be independent and relate to separable factors e.g. two parties can derive economic benefit from a processing activity that both participate in but for different purposes and motivations. The application of the Wirtschaftsakadamie CJEU case to all circumstances and purposes of processing is misleading.

Paragraph 55 (p.18-19) notes that "If *one of these entities decides alone the purposes and means of operations that precede or are subsequent in the chain of processing, this entity must be considered as the sole controller of this preceding or subsequent operation.*" We recommend the Guidance to include concrete examples of the context described here, and in the paragraph overall. Otherwise, we would recommend to remove this paragraph.

3.2.2.1 Jointly determined purpose(s)

We would like to highlight that the key element to qualify joint controllership is that both controllers actually jointly define the purposes of the processing.

Paragraph 58 (p.19) : "*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.

Finally, we note that paragraph 60 is rather confusing. It should be made clear that in those situations where one of the parties provides its services on behalf or to the other party, and the latter pays for such services, we may not be facing a joint controller relationship between these parties, even if both parties have a mutual benefit. It will depend on all facts and circumstances, but we may be facing a processor-controller relationship.

3.2.2.2 Jointly determined means

With regard to paragraph 62 (p.20), it should be acknowledged that a party can independently assess the use of means provided by another controller and conclude that they are satisfactory for the processing purpose. This should not always amount to a joint determination as the assessment and decision making can happen independently.

We believe the following text in paragraph 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, also 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 paragraph 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 not to extend the concept of joint controllership beyond the specific scenarios in recent case law.

In paragraph 65 (p.20),the draft Guidance writes that *"Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data**, will likely amount to a joint decision on the means of that processing by those entities**."* EBF members have concerns on this point and note that the conclusions of the FashionID case should not be applied by default to all scenarios, as the facts vary case by case and should be assessed accordingly. Extending the concept of joint controllership in this way could cause substantial complexity. To qualify joint controllership, a joint determination of the purposes of processing is necessary.

In addition, we would like to point out that the fact that different entities cooperate in processing personal data, for example in a big group, does not entail that they are joint controllers, since an exchange of data between two parties without deciding together purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers.

Overall, regarding the arrangement mentioned in Paragraph 66 (p.20), 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 voluntary standard model contract clauses could be useful for companies.

Regarding the same paragraph, the example of the Clinical Trials (p.21), appears to conflict with earlier points raised in the draft Guidance. In EBF members' view, acceptance of the protocol without participation in the drafting leads to a processor status. In addition, in the same example, it also recognizes the processor status to those who did not participate in the protocol drafting.

C. Definition of Processor (Section 4)

In paragraph 72 (p.24), the draft Guidance writes that "*the GDPR lays down obligations directly applicable specifically to processors as further specified in Part II section 1 of these guidelines. A processor can be held liable or fined in case of failure to comply with such obligations or in case it acts outside or contrary to the lawful instructions of the controller*".

The generality of this statement and various other similar statements throughout these Guidelines may be misunderstood. The reader may easily get the impression that *all* processors are subject to the obligations of the GDPR. For clarification purposes, we encourage that the Guidelines confirm that GDPR's obligations on processors are only applicable to those processors who fall within the territorial scope of the GDPR. (Another thing is that the controller must instruct *all* processors in order for the controller to ensure compliance with the GDPR.)

In paragraph 75 (p.24), we would recommend the deletion of "generally" from the following sentence "*On the other hand, a department within a company cannot **generally** be a processor to another department within the same entity*" to avoid creating confusion.

We would recommend to add certain consulting arrangements as an additional example to the following in paragraph 76 (p.24) "*Employees and other persons that are acting under the direct authority of the controller, such as **temporarily employed staff**, are not to be seen as processors since they will process personal data as a part of the controller's entity."* It is not unusual that consultants are appointed to serve as a full time resource within a company (the controller) in a manner which in all material respects may be compared to that of a regular employee of the company; i.e. instructions on work assignments are made by the controller, work is performed in premises and on systems and resources provided by the controller, etc. Although the consultant is employed by the consultant company, the consultant should, under the described circumstances, be considered to process personal data as a part of the controller's entity.

In paragraph 78 (p.24-25), the draft Guidance writes that "*In the case of data protection law, 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."* We would like to see further elaboration and also some clarifying practical examples about the required level of instructions by the controller to the processor and the margin of manoeuvre which may be left to the processor.

One real-life example could be services provided by a (digital) service provider, operating as a joint venture, offering highly regulated services and/or standardized services to its customers. If the services are subject to regulatory requirements, does it have an impact in the actual assessment of the parties' roles in processing?

D. Definition of Third Party/ Recipient (Section 5)

The two examples on IT support (General IT support and IT consultant fixing a software bug) under Paragraph 81 (p.26), appear to both relate to incidental processing of personal data. We therefore suggest that the Guidelines clarify the distinction between the two scenarios.

In paragraph 84 (p.27), the draft Guidance writes that " *Article 4(10) defines a "third party" as a natural or legal person, public authority, agency or body other than the data subject, the controller, **the processor and** persons who, under the direct authority of the controller or processor, are authorised to process personal data."* We would recommend to clarify the distinction between the third party and a processor, especially as in paragraph 83 (p.27), the draft Guidelines state that "*A recipient of personal data and a third party may well simultaneously be regarded as a controller or processor from other perspectives."*

Part II – Consequences of Attributing Different Roles

A. Relationship between controller and processor (Section 1)

1.1. Choice of the processor

Under paragraph 93 (p.29-30), the draft Guidance notes that "*the guarantees "provided" by the processor are actually those that the processor is able to demonstrate to the satisfaction of the controller, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its obligations."* The current wording of this concept is confusing, and we would recommend the EDPB to clarify the meaning.

1.2 Form of the contract or other legal act

We welcome the statement from the EDPB in paragraph 104 (p.31) that "*there is no obligation for controllers and processors to enter into a contract based on SCCs, nor is it to be necessarily preferred over negotiating an individual contract. Both options are viable…".* We also welcome including the point in paragraph 107 that "*any proposed modification, by a processor, of data processing agreements included in standards terms and conditions should be directly notified to and approved by the controller*" and that "*mere publication of these modifications on the processor's website is not compliant with Article 28.*

We would also like to flag that the requirements of Article 28 GDPR can be incorporated into any type of agreement, including SLAs. The draft Guidance refers to a "data processing agreement" but we would suggest to clarify that this does not have to be a separate agreement.

1.3. Content of the contract or other legal act

EBF members have several general observations on this section:

- Although it can be helpful for the Guidance to set out potential content that *could be helpful* to include in contracts, it should not *require* material to be included in contracts that goes beyond GDPR Article 28.
- **The issue of liability is, overall, scarcely covered in the draft Guidelines**. Article 82 GDPR contains various rules on liability between controller and processor and on liability of controllers and processors vis-à-vis data subjects; **however, this Article is not mentioned in the draft Guidance. It is crucial to bear liability in mind when negotiating and reviewing data processing agreements**. It would therefore be helpful for the Guidance to clarify the application of Article 82 – we interpret it as being primarily in relation to joint controller relationships, but it could be helpful to clarify whether it also relates to arrangements between independent controllers.

EBF members are encouraged by the statement in paragraph 110 (p.33) that "*Generally speaking, the contract between the parties should be drafted in light of the specific data processing activity. For instance, there is no need to impose particularly stringent protections and procedures on a processor entrusted with a processing activity from which only minor risks arise: while each processor must comply with the requirements set out by the Regulation, the measures and procedures should be tailored to the specific situation. In any event, all elements of Article 28(3) must be covered by the contract.*"

However, **it would be useful to clarify what kind of elements the contract should include** that may help the processor in understanding the risks to the rights and freedoms of data subjects arising from the processing, in reference to the following "*At the same time, the contract should include **some elements** that may help the processor in understanding the risks to the rights and freedoms of data subjects arising from the processing*."

In regard to paragraph 111(p.33), in many cases, the required content can be understood from the contractual arrangement and it would be helpful to state that this need not always be included as a standalone clause, schedule or appending to a contract.

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 paragraph 119 (p.35), the draft Guidance notes 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.

1.3.4 The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art.28(3)(d) GDPR)

Regarding paragraph 125 (p.38), we would recommend to also include the point from or make a reference to paragraph 107, that "*any proposed modification, by a processor, of data processing agreements included in standards terms and conditions should be directly notified to and approved by the controller*" and that "*mere publication of these modifications on the processor's website is not compliant with Article 28.*

In the context of this paragraph, a clarification on whether it is possible for sub-processors to engage other sub-processors, would also be welcome.

1.3.7 On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies (Article 28(3)(g) GDPR)

We would recommend to include in paragraph 139 (p.38) that where a processor retains data for its own purposes (e.g. compliance with regulation) it will assume the role of a controller.

1.6 Sub-processors

In paragraph 151 (p.39), EBF members would recommend to add a clarification that the processor is responsible for ensuring that it has obtained "sufficient guarantee" from sub-processors. There should be no inference that the controller is responsible for this.

We welcome the statement in paragraph 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*". However, would suggest to add a clarification that the processor is responsible for the management of contractual arrangements with sub-processors. There should be no inference that the controller is responsible for this.

B. Consequences of joint controllership (Section 2)

In general, we would note that the guidelines only seem to cover joint controllerships in which both(all)controllers are subject to the obligations of the GDPR, but not where one of the controllers is not within the territorial scope of the GDPR.

In addition, we would like to note once more that CJEU case law established joint controllership in two concrete online situations. **Joint controllership should not be applicable to all situations where a controller benefits from the marketing activity of another controller made to that second controller's clients or data base.** Each controller should be responsible for the GDPR compliance of only the processing for which it is the responsible controller. **This will depend on the details of the case, particularly the level of influence over the means and purposes of processing of that first controller.** We would also recommend to explore developing a model joint-controllership agreement, like for standard contractual clauses (SCCs). These should be prepared using a full public consultation and should remain voluntary.

ENDS

For more information:
Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu