Stellungnahme

des Bundesverbandes der Unternehmensjuristen e.V.

durch die Fachgruppe Datenschutz

Response to public consultation on EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

2020 October 18th

Contact:
Bundesverband der Unternehmensjuristen e.V.
Hauptstadtrepräsentanz
Friedrichstraße 94, 10117 Berlin
Germany
Head:
Inga Vogt
+49 171-2044457, inga.vogt@buj-verband.de

Position Paper

Response to public consultation on EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

1. Introduction

Bundesverband der Unternehmensjuristen e.V. (BUJ) is grateful to the European Data Protection Board ("EDPB") for providing the opportunity for BUJ to comment on the important and complex discussion around the interplay between the concept of controller, joint controllership and processor.

The German Federal Association of Company Lawyers (Bundesverband der Unternehmensjuristen – BUJ) is the oldest, largest independent interest group for lawyers in the legal departments of companies, institutions, associations and corporations in Germany. The BUJ sees itself as the mouthpiece of in-house counsel in Germany. Its goal is to optimally bundle the interests of the association members. Therefore, the BUJ is actively involved in social and political debates in order to stand up for the interests of its members and to strengthen the position of the in-house counsel in companies, the economy and politics.

The concepts of controller and processor are key elements of the GDPR. They determine the obligations and liability of the parties involved in the processing of personal data. While the GDPR provides some basic definition of the terms and underlying concepts, it has led to numerous questions, resulting in different interpretations and solutions across the European Union. These critical interpretative issues undermine the objective of the GDPR ensuring a consistent and harmonized approach in all member states of the European Union regarding the application of the GDPR.

BUJ welcomes the clarification EDPB aims to provide with the paper and appreciates the reflection of the CJEU`s precedence. However, certain aspects still remain quite nebulous and provide complexity that will be difficult to apply in practice. While the EDPB picks up the criteria established by the CJEU, the guideline does not improve the clarity on how to apply such criteria in practice. The criteria presented use vague legal terms which, in practice, raise even more questions.

2. Definitions

2.1. **Definition of controller**

2.1.3 "alone or jointly with others" and 2.1.4. „Purposes and means"
EDPB recognizes the need to provide further guidance on the level of influence on the "why" and "how" of the data processing. In a more specialized world, companies may, however, actually not be able to influence the "how" of the processing, e.g.

- Supply of standard products/tools, e.g. standard software: Role of the supplier of an IT product as data processor or controller if the product is supplied with no possibility for the customer at all to adapt it to its requirements
- Supply of specialized tools/solutions: Role of the supplier of specialized services to customers in need of special expertise without having own expertise to exercise control over the process

EDPB uses level of flexibility left to the Purchaser to distinguish between controller and processor. It is necessary to be more precise in order to avoid that regulators and authorities oversee the actual practice in the market.

In globalized, connected and specialized markets, companies engage specialized service providers. While the company may decide to use a specific IT tool or service provider, the company may not have any insight or control over the process how personal data are processed. This may be due to the fact of high specialization or centralized IT infrastructure to bundle ressources within groups of companies. While the company may take the final decision to use the process (sometimes even upon instruction by the holding company, manufacturer, e.g. uniform sales systems) and actively approve the processing it may not be able to request changes in detail.

The main purpose of software as a service and the business model of specialized IT services and products rely on the fact that the Company which purchase the product does not want or is not able to develop the special skills inhouse. Thus, companies which does outsource specific functions, can only choose the vendor in a clear and responsible manner and it could decide regarding the general scope of the data processing and the purpose on a high level. But the more detailed it should be controlled the less the outsourcing make sense at all. The business case would collapse.

For small and medium sized companies, purchasing from a global player in software providing, it can only choose from a set of standard tools, provided by the vendor. It should be considered if the service provider is still the processor in this case, even if the controller would only be able to set instruction to a certain extent.

Concept of essential vs. non-essential means leaves uncertainty. Business reality is different. BUJ would welcome it if the EDPB could clarify the differentiation criteria for the question of whether IT support constitutes a controller/processor relationship. There is still a considerable grey area between the two examples presented, which could still cause uncertainty.

2.2. Definition of joint controller

- We are grateful for the many clarifications of the forms of joint controllership. Nevertheless, it must be recognized that the explanations on the assumption of joint controllership due to converging decisions lead to an extension of the concept of joint controllership. In business practice, this means that it is more difficult to differentiate from the data processing agreement (DPA) despite this guideline. Since this also involves liability issues, detailed explanations should follow by EDPB.
- The distinction between joint controllership and separate data controllers is ambiguous. The guideline focusses on the distinction between joint control and data processing. In addition to distinction to controller-processor relationship we would welcome practical criteria to distinguish joint control and converging decisions of controllers to separate controller situations. The EDPB uses the term “inextricably linked” as criteria for joint control. While we appreciate that the EDPB may not have had much flexibility considering the precedents on these concepts by the CJEU, business participants would welcome more precise criteria and clear position beyond repeating criteria used in the individual cases handled by the CJEU. Businesses involved in data sharing would appreciate the EDPB to draw an exact line to avoid endless discussions and negotiations with the other parties involved in the data processing.
    - Joint control: Criteria provided for level of joint determination, in particular in converging decisions, do not allow even after in-depth review of the factual circumstances:
    - Processing by each party is inseperable, meaning that parties cannot be exchanged without jeopardizing the processing activity?
- Affiliated groups of companies: Will holding companies which determine certain group wide processes involving processing of personal data or providing central IT-tools to be used by group companies be always determining the modalities of processing in a way that it will qualify as (joint) controller? Examples: Group internal processes, distribution networks using common IT-systems provided by the manufacturer, holding company.

- It should be considered that the legal entity structure does not always reflect the organizational structure within an affiliated group of companies. But the organizational structure reflects the allocation of roles and responsibilities much better than the legal entity structure.

- Supply of standard tools within an affiliated group of companies or business partners (e.g. distribution network with different sales levels): Standard IT-tools provided by a manufacturer, which is one affiliate within the group for different sales levels without possibility to adapt the tools to the requirements of an individual member of the group/distribution network

3. Consequences of attributing different roles

3.1. Relationship between processor and controller

- It is welcomed that it is recognized in recital 107 of the guidelines that, in view of the market power of some service providers, there is de facto no possibility of influencing the data processing agreement. It is also clearly understood that the contracting companies are responsible for the processing, provided they accept these contracts. Nevertheless, it is also the responsibility of the supervisory authorities to ensure that the contracts of such service providers comply with the GDPR.

- Reference is made at various points to Art. 28 para. 3 lit. f DSGVO, which standardizes the support obligations of the processor. In this context, there is no clarification as to whether a remuneration clause for any support obligations conflicts with Art. 28 para. 3 lit. f DSGVO. This also applies to any audit rights under Art. 28 para. 3 lit. h. DSGVO.

3.2. Consequences of joint controllership

- In recital 51 ff. (3.2.2.) of the Guidelines the EDPB clarifies that joint participation in the determination of purposes and means implies that more than one entity have a decisive influence over whether and how the processing takes place. For example, joint participation can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities regarding the purposes and essential means. As described above, the requirements for acceptance of a joint controllership are still unclear. In particular, the cases of converging decisions are difficult to identify in business practice and contain high (hidden) liability risks. However, even if this form of joint controllership is discovered, no distinction is made between the different forms in their explanations of the consequences of joint controllership. Here, concrete guidelines for the design of an agreement for joint controllership on a converging decision would be useful.

3.2. Written form of the data processing agreement

The BUJ would welcome a clarification whether (in para 147 of the Guidelines) the EDPB sees the written form requirement in Art. 28 (2) and Art. 28 (9) as differently strict. In Art. 28 (2), the reference to the "electronic format" is missing. However, this could also be an editorial error.

According to the eIDAS guideline the written form can only be replaced by a qualified electronic signature. Clarification if electronic form is possible at all and in which format exactly would be appreciated.

The BUJ would welcome clarification (in para 148 / 150 of the Guidelines) that the processor must actively inform the controller about new subprocessors and that the mere provision of links, lists, or the possibility to subscribe to an information service is not adequate.

Yours sincerely,

Bundesverband der Unternehmensjuristen e.V.