

Comment

of the German Insurance Association (GDV)

ID-number 6437280268-55

on the

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

**Gesamtverband der Deutschen
Versicherungswirtschaft e. V.**

German Insurance Association

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Phone: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Contact:
Datenschutz/Grundsatzfragen

E-Mail: data-protection@gdv.de

www.gdv.de



Executive summary

The EDPB's draft guidelines 07/2020 provide much needed guidance on the concepts of (joint) controllers and processors. In order to ensure further legal certainty the German insurance industry recommends additional clarification regarding the following aspects:

- Criteria for determining controllership
- The example on market research
- The obligation of the processor to obtain the controller's approval before making changes and
- The content of the controllership arrangement

1. Introduction

The GDV welcomes the EDPB's efforts to provide more guidance on the concepts of controller and processor and how to distinguish between these roles. The concept of joint controllership in particular has proven to be difficult to assess for the parties involved in the processing of personal data. However, we believe that further clarification is needed to ensure more legal certainty:

2. Criteria for determining controllership

As the guidelines state the controller must decide on **both** the purpose **and** the means of the processing (p. 13 para. 34). Merely determining the means of the data processing cannot by itself already constitute controllership. Past judgements of the ECJ have expanded the concept of (joint) controllership to a degree that correctly identifying and distinguishing between controllers and processors has become increasingly difficult. While the GDPR does not explicitly distinguish between essential and non-essential means, the differentiation appears reasonable and is generally appropriate to provide necessary specification. The EDPB is certainly correct that deciding certain key elements (essential means) of the data processing can constitute controllership since essential means are closely linked to the purpose of the processing. However, solely determining the essential means should not automatically be equated with also having determined the purposes of the data processing. Otherwise, purposes and means of the data processing would be indistinguishably merged with each other. This would in turn run the risk of potentially extending the concept of controllership beyond the already extensive and unclear interpretation in the ECJ case law and counteract the EDPB's attempt to provide clear guidance.

In addition, we would ask for further clarification and guidance to the differentiation between essential and non-essential means. In practice, clearly distinguishing between both will prove to be challenging.

3. Example: market research

As the EDPB correctly states access to the data being processed is not a defining requirement for controllership. Although we agree with the deliberations in page 16 para. 42, we believe that the "Example: Market research" is phrased too generally and should be complemented with additional scenarios since it could currently falsely imply that when conducting market research the controller is always the initiating company while the market research institution is always a processor. In practice, market research institutes are involved because of their expertise in

determining the fundamental parameters for correct market research, for example by determining the relevant group of people. In practice, the initiating party also rarely gives (detailed) instructions, but rather supplies the market research institute with a topic or question of interest. The market research institute then establishes the general conditions of the research and conducts the research on its own. Afterwards, the initiating party only receives anonymized or aggregated results. In these cases when the initiating party only gives the mental impulse for the data processing, but does not otherwise determine purposes or any means, considering the initiating party a controller would not accurately reflect the factual circumstances of the data processing. It would rather be correct to consider the market research institute the sole controller.

4. Obligation of the processor to obtain the controller's approval before making changes

Page 35 para. 123 implies that every processing contract needs to include a provision that the processor requires the controller's approval for **every** change to the data processing. It should be clarified that this only applies to significant changes or changes to the purposes or essential means of the data processing. The processor can determine the non-essential means (e.g. choice of specific hard- or software or the detailed security measures, page 14 para. 38) on his own, so a requirement for approval of such changes would run counter to this authorization. A requirement for approval of all changes however small they are would furthermore hardly be practically realizable because of the enormous bureaucratic and documentational effort.

5. Content of the joint controllership arrangement

The guidelines stipulate that joint controllers should distribute the responsibilities for compliance not only for the topics referred to in Art. 26 (1) GDPR, but also for other obligations under the GDPR (p. 41 para. 161 – p. 42 para. 163). Ensuring compliance with the GDPR is naturally part of the accountability obligation of any controller. Nevertheless, the EDPB should clarify that it remains left to the decision of the controllers whether they explicitly regulate these additional aspects in the joint controllership agreement. We concur that Art. 26 (1) GDPR is not exhaustive with respect to the list of responsibilities of the joint controllers. However, the law does not require joint controllers to determine more topics within the joint controllership agreement than what is explicitly enumerated in Art. 26 (1) GDPR. The lawmaker has made clear which aspects he deems most important and has thus expressly stated what has to be accounted for in the joint controllership agreement. In contrast to the more extensive list of elements which have to be subject to a processing agreement (Art. 28 (3)

GDPR) the lawmaker made the decision to leave it up to the joint controllers whether they deem it sensible to regulate additional elements in the joint controllership agreement depending on the specific circumstances of the data processing. This can be attributed to the fact that joint controllers already have an elevated interest in ensuring compliance with data protection law by virtue of their own accountability. If joint controllers were required to always include the elements described in p. 41 para. 163 without regard to the necessity thereof, overly extensive and bureaucratic contractual constructs would have to be negotiated in practice without creating any meaningful added value.

Berlin, 19 October 2020