Position Paper

Response to EDPB draft guidelines on the concepts of controller and processor in the GDPR

Our reference:	COB-DAT-20-072	Date:	19 October 2020
Referring to:	Guidelines 7/2020 on the concepts of controller and processor in the GDPR		
Contact person:	Áine Clarke, Policy Advisor, General Insurance	E-mail:	Clarke@insuranceeurope.eu
Pages:	5	Transparency Register ID no.:	33213703459-54

Introduction

Insurance Europe welcomes the European Data Protection Board's (EDPB) draft guidelines on the concepts of controller and processor under the General Data Protection Regulation (GDPR), as these guidelines deal with concepts that are of major importance for the insurance industry. While Insurance Europe welcomes that the draft guidelines shed light on the interpretation of a number of fundamental concepts, we invite the EDPB to further clarify the issues below in order to provide the necessary legal certainty to insurers.

General comments

- **Changes to the meaning of the concepts of controller and processor:** In the introduction, the EDPB mentions that these guidelines were drafted in response to many questions surrounding *"to what extent the GDPR brought changes to the concepts of controller and processor and their respective roles".* However, the guidelines do not provide an answer to this question, but rather state in paragraph 11 that, for the most part, the concepts haven't changed and that *"overall, the criteria for how to attribute the different roles remain the same*".

  Recommendation: We would welcome some insights by the EDPB as to where the differences may arise between the GDPR and its predecessor.

- **Qualification of controller/processor in public insurance contracts:** In FR, an issue has been raised surrounding the roles of the different parties in public insurance contracts. In a notable number of local authority insurance tenders, the qualifications/concepts employed by the public contracting parties do not seem to be consistent with those found in the GDPR. In these cases, the public purchaser qualifies as a data controller and the insurer (and its management delegate, where applicable) qualifies as a processor. However, ongoing work that is being carried out in the context of the project to transform the Compliance Pack highlights that, in the relationship between the insured party and the insurer, the latter must qualify as a

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

data controller and not as a processor, given that the status of a public entity or the mere existence of a call for tender has no impact on these qualifications. The Legal Affairs Department of the Ministry of the Economy has published a practical sheet entitled "The Impact of the GDPR on public procurement law" in which it defines the public purchaser as a "data controller" and the contract holder as a "processor" without any other distinction linked to the nature of the contract. This difficulty was raised with the French data protection authority. The Italian Data Protection Authority has established that, in public insurance contracts, insurers should in fact be considered as controllers.

Recommendation: we would welcome clarification from the EDPB that, in public insurance contracts, the insurer qualifies as the "data controller" while the public purchaser (insured party) qualifies as the "data processor", consistent with the qualification of these terms in the GDPR.

- **"Purposes and means":** Paragraphs 37-39 discuss the definitions of "*essential vs non-essential means".* Differentiating between the two can be especially difficult in cases relating to the cloud environment (incl. IAAS, PAAS) or Business Process Outsourcing.

  Recommendation: Clarification on the term "*essential vs non-essential means"* in the context of cloud and Business Process Outsourcing would be welcomed.

- **Comments on the criteria for determining controllership**

  - As the guidelines correctly 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 constitute controllership, even if past judgements of the ECJ may 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 differentiate between essential and non-essential means, the interpretation appears reasonable and generally provides clarity. The EDPB is correct to state in the guidelines that deciding about 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 purpose, otherwise the purpose and means of the data processing become 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.

    Recommendation: Clarify that the sole act of determining the essential means of the data processing does not alone constitute controllership.

    In contractual relations between joint controllers, it is necessary to encourage the parties to make use of common coordination tools. The RACI (responsible, accountable, consulted, informed) matrix of responsibilities in the field of management which indicates the roles of the stakeholders within each process and activity could be a relevant tool in this regard, listing the roles and responsibilities of each controller.

    Recommendation: These tools should be further explained in the context of joint controllership under the GDPR and their use should be encouraged.

- **Comments on joint controllership**

  - **Broad interpretation of "joint controllership":** The draft guidelines provide a broad interpretation of the concept of joint controllership. Reference can be made to paragraph 58,

which states: *"…joint controllership can be established when the entities involved pursue purposes which are closely linked or complementary"*. Furthermore, paragraph 62 states: *"It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing".* In our view there is no basis in article 26 GDPR for such a broad interpretation. In this light it is for example completely unclear what is meant by "closely linked". We stress that the concept of joint controllership should be clarified in conformity with the wording of article 26 GDPR and that the interpretation of this article should not overstretch the scope thereof. It is important that the concept of joint controllership will not be assumed too lightly, as joint controllership leads to impactful obligations for companies and the risk of joint liability.

Recommendation: The concept of joint controllership should be clarified in conformity with the wording of Article 26 GDPR, thereby not overstretching the scope of this article. The EDPB should provide more examples of joint controllership in order to avoid situations in practice in which joint controllership is assumed too lightly. This could come in the form of pre-configured models of distribution of responsibility that could be used to facilitate negotiations between parties.

The EDPB states in paragraph 50/51 that *"the overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation… (this) implies that more than one entity have a decisive influence over whether and how the processing takes places.".* However, in paragraph 23, the EDPB uses the term "*determinative influence with respect to the processing of personal data"* as among the criteria for determining controllership. It is important both to further clarify the meaning of these terms and to explain how one differs from the other.

Recommendation: Clarify the meaning of the terms "*decisive influence"* and "*determinative influence"* and provide a more objective way of determining the meaning of 'influence' in both contexts.

- **"Common decisions" and "converging decisions":** The EDPB states in paragraph 51 that *"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".* However, paragraph 70 states that *"there can be situations where various actors successively process the same personal data in a chain of operations, each of these actors having an independent purpose and independent means in their part of the chain. In the absence of joint participation in the determination of the purposes and means of the same processing operation or set of operations, joint controllership has to be excluded and the various actors must be regarded as successive independent controllers".* In order to avoid legal uncertainty in these situations, further clarification of the meaning of the terms *"common decisions"* and "*converging decisions"* is necessary so that a proper assessment of the relationship can be conducted. This is especially true as regards intercompany processing activities or (semi-)governmental processing activities.

  Insurance Europe also asks for clarification in the following areas:
  - What role does a company have when actors in a chain of operation process data simultaneously, or overlapping? Clarification of this role is also welcomed in the context of entities operating intragroup.
  - What role does a company in such a chain have when it processes personal data, but processing personal data is not its primary task/assignment?
  - We would like to see more examples, regarding e.g. largescale processing, or the processing of special categories of data (where the processing of data is not the

primary task/assignment). In the insurance context, perhaps the exchange of personal data between primary insurer and re-insurer would be a welcome example.

Recommendation: Provide further examples of joint controllership relationships and further clarify the meaning of the terms *"common decisions"* and *"converging decisions"* to assist in determining whether a joint controllership exists or not. Furthermore, provide clarification on the above questions.

- **Contents of the joint controllership agreement:** The guidelines stipulate that joint controllers should distribute the responsibilities for compliance not only for the areas 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. The law does not require that joint controllers determine more topics within the joint controllership agreement than what is explicitly enumerated in Art. 26 (1) GDPR. Otherwise, in practice, this can lead to overly extensive and bureaucratic contractual constructs being negotiated without creating any added value.

  Recommendation: Clarify that it remains left to the decision of the controllers whether they explicitly regulate additional aspects – beyond what is referred to in Art. 26 (1) – in the joint controllership agreement.

- **Relationship between controller and processor**

  - **Choice of the processor:** In paragraph 95, the EDPB states that the processor's *"expert knowledge"* and *"reliability"* should be taken into account by the controller in order to assess the sufficiency of the guarantees. Paragraph 97 states that *"the controller should, at appropriate intervals, verify the processor's guarantees",* however Article 28 (3)(h) GDPR infers rather that certain guarantees and controls could be established at the beginning and other guarantees could be established during the development.

    Recommendation: Guidance from the EDPB on ways for controllers to determine the level of expertise and reliability of processors would be welcomed. Furthermore, the term *"appropriate intervals"* should be revised in line with Article 28.3.h GDPR.

  - **Content of the contract or other legal act:** Paragraph 110 states that *"the contract between the parties should be drafted in light of the specific data processing activity",* however a number of questions remain open, including those surrounding the description of the level of detail in processing activities.

    Recommendation: Further guidance on the content of the contract would be welcomed, in particular on the necessary level of detail of the descriptions. Examples may provide clarity in this area.

    Insurance Europe notes positively that paragraph 107 states clearly that the mere publication by a processor of modifications (of data processing agreements included in standard terms and conditions) on the processor's website is not compliant with Article 28 GDPR, however it should be specified what can be considered as 'approval' on the part of the controller. For example, is the sending of a message or pop-up to be accepted considered an acceptance by the data controller? This is a mechanism that many providers (processors) use, which leaves data controllers unprotected.

Recommendation: Regarding the approval mechanism on the part of the controller, Insurance Europe would welcome clarification from the EDPB that any modifications must be formally accepted in the same that that the contract was accepted, in the way that if there is a signed contract, it must be updated with an update of the terms and conditions.

- **Sub-processors:** Paragraphs 147-157 outline the role of sub-processors, however, there remain areas where uncertainty arises. In the case of providers of non-essential services of the treatment provider, are they all sub-processors? Do they all have to be authorised? E.g. when entity X contracts company Y for a service by virtue of which it will act as the treatment manager for X, in practice it can be very complicated to authorise all of Y's sub-processors. The simplest example could be if they use Outlook/Microsoft as their e-mail provider or other tools they may use in their day-to-day business.

  Recommendation: Clarification from the EDPB on the qualification of sub-processor, particularly in cases such as the one raised above.