The European Federation of Insurance Intermediaries
La Fédération européenne des intermédiaires d'assurance

Andrea Jelineck
Chair
EDPB
Rue Wiertz 60
B-1047 Brussels

Brussels, 19 October 2020

Dear Mrs Andrea Jelineck,

We are writing to you in relation to the consultation on **the EDPB guidelines 07/2020 on the concepts of controller and processor in the GDPR.**

As the main actors in the distribution of insurance products, acting as a link between insurers and insured, insurance intermediaries are confronted daily with problems relating to the processing and free movement of personal data. The data that insurance intermediaries process is necessary to provide quotations, arrange insurance cover, manage claims, for client relationship management and conducting internal conflict checks. They use personal data for general insurance purposes including marketing and client profiling, offering renewal, research and statistical analysis, crime prevention, credit assessments and other background checks, internal record-keeping and meeting legal and regulatory requirements. Arranging insurance may involve certain disclosures of personal data to insurers and service providers, including but not limited to consultants, market research and quality assurance companies, other group companies, industry regulators and auditors and other professional advisors. Depending on the circumstances, these disclosures may involve a transfer outside of the European Economic Area.

In legal terms insurance intermediaries represent a distinct legal entity with regard to insurance companies. In essence, most undertakings involved in the distribution of insurance products other than the insurance companies and their employees are insurance intermediaries. This includes mainly insurance agents and insurance brokers.

In most cases, insurance intermediaries will be processing personal data on their own account and will act as data controllers. In some others, intermediaries will act under clear processing instructions from a data controller and will be a data processor.

BIPAR generally welcomes the EDPB guidelines 07/2020 on the concepts of controller and processors in the GDPR that address many of the issues raised during the EDPB stakeholders' event organised on these concepts in March 2019 and **that bring helpful clarifications for our sector**. It will be crucial that

these guidelines are followed by the national DPAs so that they help in **achieving consistency** in the EU market on these key issues in the application of the GDPR.

BIPAR's comments and questions are set out in the annex to this letter. **BIPAR main concerns concern the possible overlapping of qualifications from different regulations/legislations and its impact of the the autonomous character of the concept of controller, the cumulative criteria to act on the purposes but also on the means of a processing operation to qualify as joint controllers, the criteria that are used to determine the qualification of different actors involved in the same processing activity and different requirements pursuant Article 32.**

We are grateful to you for your attention to this letter and annex.

Yours sincerely,

Isabelle Audigier

Legal director

bipar

Av. Albert-Elisabeth, 40 - 1200 Bruxelles - Tél: 0032-2-735.60.48
Fax: 0032-2-732.14.18 - bipar@bipar.eu - www.bipar.eu

The European Federation of Insurance Intermediaries
La Fédération européenne des intermédiaires d'assurance

Annex 1: BIPAR comments on EDPB guidelines on the concepts of controller and processor in the GDPR

I. Useful clarifications

BPAR welcomes EDPB draft guidelines that brings very helpful clarifications. Whilst there are unfortunately no examples specific to the insurance industry, there are a number of examples which are analogous to insurance intermediaries' use of personal data and that will enable a read across.

However, it would be very useful not to always have to work through analogies and to have a few examples for the insurance sector in the EDPB guidelines.

We have found the following clarifications helpful in particular in addressing intermediaries' position *as data controllers*:

- Paragraph 25 reference to "*existing traditional roles and professional expertise that normally imply a certain responsibility will help in identifying the controller*…" is useful. As professional service providers, we believe that this section – as well as paragraph 80, will be of significant assistance in justifying, when needed, that intermediaries are data controllers in the provision of their services.
- Paragraph 50 reference to "Not all processing operations involving several entities give rise to joint controllership" is useful as in our industry you can have a scenario where there is a chain of independent data controllers.

Depending on the concrete activities they carry out in specific context, intermediaries can act *as processors* for certain processing operations, and *as controller* for others.

This is for example the case of an insurance agent acting **as a data processor** in her/his relation to an insurer from which he/she has received a mandate (for the collection and management of data by the insurance agent for the purpose of carrying out the mandate he/she has received from the insurer)and as **a data controller** for the collection and management of data outside the execution of the mandate.

In the Employee Health & Benefits business, an intermediary may also act as both a data processor and data controller except where regulation stipulates that insurance intermediaries are categorised as data controller. The concept of being able to act as both controller and processor in the B2B2C space is extremely helpful for the intermediary, enabling it to use de-identified data for analytics purposes for example.

Paragraph 24 and the explanation that "the same entity may act at the same time as controller for certain processing operations and as processor for others" is therefore useful in addressing those situations. It would be useful to have the above example in the Guidelines.

II. Requests/need for further clarifications

- **The autonomous character of the concept of controller - Overlapping of concepts**

In its Annex 1 on the "*Flowchart for applying the concepts of controller, processor and joint controller in practice",* it is referred to the following question: "*Is the processing necessary in order to carry out a task for which you are responsible according to a legal act? (implicit legal competence*)".

We understand that this reference is in line with the useful paragraph 19 and in particular that "*controllership may be defined by law".* In many EU countries, intermediaries have legal and regulatory obligations in respect of the use of personal data and obligations to the regulators that are independent to their relationship with clients.

However, Annex 1 of the Guidelines also leads us to wonder about the possible overlapping of qualifications from different regulations/legislations.

In the context of the so-called "Solvency II" Directive[1], the insurer may decide to outsource to third parties (such as insurance intermediaries) certain tasks relating to the execution of the insurance contract (for example, and without this being exhaustive: delegation of management of the insurance contract, delegation of the subscription of the contract, delegation of premium collection, etc.).

In the context of this outsourcing activity, this third party is a services provider '(or " un sous-traitant" in French for example).
In the light of Solvency II, some might apply a parallelism of forms and consider that the insurance intermediary must therefore be qualified as a "processor" within the meaning of the GDPR for the processing of data carried out in this outsourcing framework. Indeed, too often incorrect assumption that any service provider is a processor leads to inappropriate terms being issued and time-consuming negotiations to put in place more appropriate wording that reflects the actual position.

For these outsourced activities, some intermediaries will have considerable leeway in defining the scope of the outsourcing and the execution methods to be implemented. Thanks to their expertise or added value on certain services, they have developed their own tools and processes and will thus benefit from significant autonomy and thus act directly on the determination of the purposes and essential means of processing in conjunction with the insurer.

It would therefore seem relevant to explicitly mention **that legal qualifications from other regulations do not automatically impact the qualifications retained in the context of the GDPR** and to thus reintroduce in the Guidelines 07/2020 the following clarification that was included in the Opinion 1/10 on the concepts of "controller" and "processor" and which clearly stated that "*A last characteristic of the concept of controller **is its autonomy**, in the sense that, although external legal sources can help identifying who is a controller, **it should be interpreted mainly according to data protection law**. The concept of controller should not be prejudiced by other - sometimes colliding or overlapping - concepts in other fields of law, such as the creator or the right holder in intellectual property rights. Being a right holder for intellectual property does not exclude the possibility of qualifying as "controller" as well and thus be subject to the obligations stemming from data protection law. "*

We are aware that this useful clarification is included in paragraph 13 of the Guidelines under item 1 on General Observations. However, we believe that it should be introduced under item 2 on definition of controller and in particular under 2.1.2 "determines". It would bring greater legal clarity.

- **Determining the purposes and means of processing**

According to the draft guidelines n°07/20, joint controllership arises from the joint participation of the entities in the determination of the purposes **and** means[2]. In other words, we understand that in order

[1] Directive 2009/138/EC of 25 November 2009
[2] Paragraph 50 and 51 of the draft guidelines

to qualify as joint controllers, it is necessary for the entities to act on the purposes but also on the means of a processing operation, these criteria **being cumulative**.

However, according to Opinion 1/10 on the concepts of "controller" and "processor", the autonomy of[3] the notion of "essential means" was recognised while maintaining the predominance of the notion of "purpose" of the processing.[4]

Since the GDPR has not altered this balance and in order to take into account the reality of operational processes, **we believe that it is important to maintain this distinction, which we have illustrated with the example that you will find below.**

Example n°1: Broker A is going to design an insurance product and will solicit insurer B to accept to carry the risk covered by this contract. Broker A will autonomously define certain elements of the insurance contract, such as price, guarantee, etc. As such, he enjoys substantial latitude in carrying out this task.
Insurer B, in its capacity as risk carrier, will cover the insurance risk proposed by broker A after making any necessary changes.
Broker A, who has a great deal of autonomy and expertise in this area, will determine jointly with Insurer B not only the aims but also the essential means of the processing.

- **Qualification criteria in case of intervention of several actors**

Opinion 1/10 listed a number of criteria that could be used to determine the qualification of different actors involved in the same processing activity. One of these criteria included the *"**visibility/image** given by the controller to the data subject, and expectations of the data subjects on the basis of this visibility".*

This criterion is no longer clearly stated in the draft guidelines. However, if we take Example 1 where the intermediary designs an entire insurance product, the intermediary's brand will generally be predominant and highlighted from a marketing point of view, so that the insurance policyholder will primarily identify the intermediary's brand.

Therefore, we believe that this criterion may in certain situations, and when combined with other criteria, be taken into account in determining the qualification of joint controllers.

- **Authorisation for use of sub-processors**

We would like to raise a particular concern regarding situations where specific authorizations are used by the processor to inform the controller about the use of another processor.

As explained in the draft guidelines, if the processor's request for a specific authorisation is not answered to within the set timeframe by the controller, it should be held **as denied**.

[3] *"In this perspective, joint control will arise when different parties determine with regard to specific processing operations **either** the purpose **or** those essential elements of the means which characterize a controller (see supra paragraph III.1.a to c)."*
[4] *"Against this background, while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply **control only when the determination concerns the essential elements of the means."***

While in most cases intermediaries when acting as processors, rely on the general authorisation process, there are some circumstances where they are required to accept specific authorisation clauses by their clients.

- **Processor and Article 32**

The draft guidelines explain the following:
82. "*As stated above, nothing prevents the processor from offering a preliminary defined service but the controller must make the final decision to actively approve the way the processing is carried out and/or to be able to request changes if necessary*."
and
123 "*…the processing contract should not merely restate the provisions of the GDPR. The contract needs to include or reference information as to the security measures to be adopted,* ***an obligation on the processor to obtain the controller's approval before making changes****, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time."*

Insurance intermediaries use CRMs (back office systems) and quote systems. For these activities, the providers of these systems are data processors for the broker who is the data controller.
The CRMs, as outsourcing processors, often have hundreds of intermediaries' clients, (thousands in other EU member states) and it would be unreasonable to expect data processors to obtain approval from each data controller before making changes to their security measures. It should be sufficient for the data processor to advise each data controller that the security measures are at a minimum to the same standards as before.

In paragraph 124 of the guidelines, it is explained that "*The level of instructions provided by the controller to the processor as to the measures to be implemented will depend on the specific circumstances. In some cases, the controller may provide a clear and detailed description of the security measures to be implemented. In other cases, the controller may describe the minimum security objectives to be achieved, while requesting the processor to propose implementation of specific security measures.* ***In any event, the controller must provide the processor with a description of the processing activities and security objectives (based on the controller's risk assessment), as well as approve the measures proposed by the processor.*** *This could be included in an annex to the contract. The controller exercises its decision-making power over Adopted - version for public consultation the main features of the security measures, be it by explicitly listing the measures or by approving those proposed by the processor*."

Again, using the above examples, how could an insurance intermediary be expected to provide the CRM provider with a description of the processing activities and security measures when the purpose and the function, and existence of the CRM is to provide data processing back office solution to intermediaries.

It is generally the CRM that will provide the contract to the insurance broker as, (as explained above) they have thousands ofintermediary clients and operating on the basis of economies of scale they would rely on using standard data protection provisions for all clients. It would be technically unworkable and financially unviable for such providers to agree multiple distinct data processing agreements, each with slightly different reporting times and audit rights to suit each data controller. This reasoning also applies where the insurer is acting as data processor to the broker.

- **1.3.6 – The processor must assist the controller in ensuring compliance with the obligations pursuant to Article 32 to 36**

In paragraph 133 of the Guidelines, it is explained that "…*Thus, the processor's notification to the data controller should also take place without undue delay. The EDPB recommends that there is a specific time frame of notification (**e.g. number of hours**)*."

It is however not clear what the processor's notification to the data controller should include. Should it include for example a notification, an investigation, an identification, a remedy and a solution? Then this "number of hours" would represent a big challenge for organisations and would not represent a realistic timeframe.

Any over ambitious notification requirement may cause a business to delay work mitigating the effects of the breach and rectifying the position in order to meet the reporting deadline instead.