EDPB GUIDELINES 07/2020 ON THE CONCEPTS OF CONTROLLER AND PROCESSOR IN THE GDPR

Deadline 19th October 2020

PRELIMINARY REMARKS

Unipol Group S.p.A. (hereinafter "Unipol Group") welcomes the EDPB guidance on the concepts of controller/processor as well as the clarification efforts and concrete examples provided with respect to these concepts on the basis of the GDPR's rules on definitions in Article 4 and the provisions on obligations in Chapter IV. In light of the accountability principle introduced by the GDPR, as underlined by the EDPB, it is indeed of paramount importance that the precise meaning of these concepts and the criteria for their correct use are sufficiently clear and shared throughout the EU and the EEA.

With this in mind, the Unipol Group would like to share its concerns and clarification requests on the following circumstances.

***

DEFINITION OF CONTROLLER and DEFINITION OF PROCESSOR

Under paragraph 42 of the draft Guidelines, the EDPB states that it is not necessary that the controller actually has access to the data that is being processed. Someone who outsources a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data.

Under paragraphs 140 and 141, however, the EDPB clarifies that the processor should provide all information on how the processing activity will be carried out on behalf of the controller. Such information should include information on the functioning of the systems used, security measures, retention of data, data location, transfers of data, access to data and recipients of data, sub-processors used, etc. Further details shall also be set out in the contract regarding the ability to carry out and the duty to contribute to inspections and audits by the controller or another auditor mandated by the controller.

With this in mind, the Unipol Group would like to ask the EDPB to **clarify whether the controller**, *via* a data processing agreement, **may entrust a processor of a processing activity regarding certain type of personal data that it would not be (e.g. legally) entitled to process directly**.

Such a circumstance in the market practice has already given rise to a number of conflicting views and it would be very helpful to clarify, from a more general standpoint, what actually the concept of "delegation" entails in the context of a processing agreement.

Under paragraph 78, the EDPB explains that *Processing personal data on the controller's behalf* requires that the processing must be done on behalf of a controller but otherwise than under its direct authority or control. Acting "on behalf of" means serving someone else's interest and recalls the legal concept of "delegation". In the case of data protection law, the EDPB précises that 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. The lawfulness of the processing according to Article 6, and if relevant Article 9, of the GDPR will be derived from the controller's activity and the processor must not process the data otherwise than according to the controller's instructions.

Given the above, and taking into account the civil law principle according to which "one cannot transfer to another more rights than they have" (*Nemo plus iuris ad alium transferre potest quam ipse habet*), we call on the EDPB to further elaborate on the concept of delegation to **clarify the scope and content of "powers" that can be delegated by the controller to the processor *via* a processing agreement**.

***

RELATIONSHIP BETWEEN THE CONTROLLER AND THE PROCESSOR

When looking at the relationship between the controller and the processor, **under paragraph 106**, the EDPB recognizes that contracts between controllers and processors may sometimes be drafted unilaterally by one of the parties. Which party or parties that draft the contract may depend on several factors, including: **the parties' position in the market and contractual power**, their technical expertise, as well as access to legal services. For instance, as the Group has observed in practice, **some service providers tend to set up standard terms and conditions, which include data processing agreements**.

The EDPB further explains, **under paragraph 107**, that the fact that the contract and its detailed terms of business are prepared by the service provider rather than by the controller is not in itself problematic and is not in itself a sufficient basis to conclude that the service provider should be considered as a controller. Also, the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law, nor can it discharge the controller from its data protection obligations. The controller must evaluate the terms and in so far as it freely accepts them and makes use of the service, it has also accepted full responsibility for compliance with the GDPR. **Any proposed modification, by a processor, of data processing agreements included in standard terms and conditions should be directly notified to and approved by the controller**. **The mere publication of these modifications on the processor's website is not compliant with Article 28**.

With respect to the above guidelines, we would like to call the attention of the EDPB on the following issues.

While we certainly agree that data controllers even when facing big service providers as counterparties must comply with the data protection obligations, we would like to stress the difficulty to engage with those counterparties not only to request and implement contractual changes - regardless of what they generally offer worldwide in standardized terms - but even to negotiate and enter into an agreement in a first place.

On this specific point, Unipol Group would like to refer to those situations where for example the processor is able to exert market power because *de facto* is the only provider in the market to whom/which the controller can assign the services related to data processing or it is the best in the market for the quality of the services provided.

Should this be the case, the data controller may then find itself in a weaker negotiating position and be able only to decide either to enter into an agreement by accepting the terms and conditions already set out by the service providers or to quit (with potential negative consequences for its own business activity).

The processor instead takes a decision-making role with respect to the purposes and means of the processing and has to be considered as a controller in respect of that processing, although "ontologically" it may not cover such a role.

Under paragraph 146, the EDPB clarifies that if the processor infringes the GDPR by determining the purposes and means of processing, it shall be considered as a controller in respect of that processing (Article 28(10) GDPR). With this respect, we would suggest the EDPB to clarify whether the controller may still incur into a violation of Article 28 of the GDPR and provide suggestions, whether possible, on **how the controller may overcome the imbalance in the contractual power to enter into in an agreement with the processor** and to have the latter following the controller's instructions.

In particular, it would be very helpful if the EDPB could further clarify the circumstances indicated under paragraph 107 where it is stated that any proposed modification, by a processor, of data processing agreements included in standard terms and conditions should be directly notified to and approved by the controller, since the mere publication of these modifications on the processor's website is not compliant with Article 28. Certain big service providers decide indeed to publish exclusively on their own website the terms and conditions for data processing (usually by including them in an internal policy document) and do not agree to explicitly attach them to the contracts they sign. Actually, **they establish that any future modification (unilaterally introduced) to the data processing agreement is published only on their website**.

Such a market practice not only prevents the contractual counterparty to negotiate any proposed modification to the contract and eventually to approve or reject them but also to get a direct notification on their insertion into the contract and on their consequent implementation.

More precisely, specific negative consequences may emerge from this practice when the changes introduced by the processor concern the engagement of other players in the chain that are indicated in a list of approved sub-processors which is then made available only online, on the processor's website.

According to paragraph 150, in cases where the controller decides to accept certain sub-processors at the time of the signature of the contract, a list of approved sub-processors should be included in the contract or an annex thereto. The list should then be kept up to date, in accordance with the general or specific authorisation given by the controller.

If the controller chooses to give its specific authorisation, it should specify in writing which sub-processor and what processing activity it refers to. Any subsequent change will need to be further authorised by the controller before it is put in place. If the processor's request for a specific authorisation is not answered to within the set timeframe, it should be held as denied. Alternatively, the controller may provide its general authorisation to the use of sub-processors (in the contract, including a list with such sub-processors in an annex thereto), which should be supplemented with criteria to guide the processor's choice (e.g., guarantees in terms of technical and organisational measures, expert knowledge, reliability and resources).

In this scenario, the processor needs to inform the controller in due time of any intended addition or replacement of sub-processor(s) so as to provide the controller with the opportunity to object. It derives that if the list of sub-processors is made available only online by the processor in its website, the requirement to inform the controller "in due time" may not be considered satisfied by the processor since the controller may not become aware of the list and miss the opportunity to object it (see also paragraph 125) (for example in case a non-EU sub-processor is entrusted).

Therefore, in light of the above, we reiterate to the EDPB the request to (i) **clarify whether the controller, in case of modifications to the contract introduced by the processor not included in the contract or attached in an annex thereto, may still incur into a violation of Article 28 GDPR** and (ii) hence to confirm that the practice of the mere publication of the modifications to the data processing agreements, including the list of sub-processors, on the processor's website, **is not compliant** with Article 28.

***

INSTRUCTIONS INFRINGING DATA PROTECTION LAW

As it is clarified by the EDPB under **paragraphs 142-145**, the processor has a duty to comply with the controller's instructions (i.e. *contractual obligation*), but it also has a general obligation to comply with the law. Therefore, an instruction that infringes data protection law seems to cause a conflict between the aforementioned two obligations.

On this specific point, the EDPB clarifies that once informed that one of its instructions may be in breach of data protection law, the controller will have to assess the situation and determine whether the instruction actually

violates data protection law. In case of inaction from the controller, the EDPB provides a practical solution and recommends the parties to negotiate and agree in the contract the consequences of the notification of an infringing instruction, by for example inserting a clause on the termination of the contract if the controller persists with an unlawful instruction.

While we appreciate the clarifications and suggestions provided, we would like to call the attention of the EDPB on the circumstances where terminating a contract does not always represent a viable and easy-to-implement solution, if not even economically detrimental for the processor.

With this respect, we would like to refer for example to the circumstances related to the call for tenders and more generally to those situations where the imbalance in the contractual power between the controller and the processor prevent the latter to effectively renegotiate the clauses and terms of the contract to include a termination clause in case of inaction from the controller.

As regards to the tenders, for example, the majority of procedures to which the Group participates are procured via open procedures. This means that anyone can bid on a contract to supply services or goods in line with the contractual requirements that have been already set, without the possibility for the selected company to further negotiate certain aspects of a contract, including the fee. It derives then, should the tender documents include instructions that may be in violation of data protection law, the processor/applicant to the tender can decide not to participate to the tender but it has to consider as well the consequences of the loss of (usually significant) business opportunities.

In addition to the above, there might be also cases where the instructions provided by the controller are not clear-cut violations of data protection law, thus triggering potential divergent interpretations between the controller and the processor as to whether these instructions infringe the law. Taking also into account the possibility of a potential imbalance in the negotiating power between the two parties (with the controller being in a market power position), it may be difficult for the processor to implement the solution proposed by the EDPB and agree with the controller on the consequences of the notification of an infringing instruction.

In light of the above, it would be very helpful if the EDPB could clarify the cases above mentioned and agree with the possibility to foresee under paragraph 145 of the Guidelines the insertion of "**a release from liability clause" for the processor who has formally notified the controller of an infringing instruction**. Such a recommendation may provide for an alternative solution in circumstances where inserting a clause on the termination of the contract if the controller persists with an unlawful instruction is not feasible.

***

SUB-PROCESSORS

As correctly pointed out by the EDPB under paragraph 147, data processing activities are often carried out by a great number of actors, and the chains of subcontracting are becoming increasingly complex. The GDPR

introduces specific obligations that are triggered when a processor intends to engage another player, thereby adding another link to the chain.

In this context, the EDPB maintains that although the chain may be quite long, the controller retains its pivotal role in determining the purpose and means of processing and recalls that Article 28(2) GDPR stipulates that the processor shall not engage another processor without prior specific or general written authorisation of the controller.

In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. In both cases, the processor must obtain the controller's authorisation in writing before any personal data processing is entrusted to the sub-processor. In order to make the assessment and the decision whether to authorise subcontracting, a list of intended sub-processors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor.

With this respect, and taking into Article 28(4) of the GDPR according to which, regardless of the criteria suggested by the controller to choose providers, the processor remains fully liable to the controller for the performance of the sub-processors' obligations (see also paragraphs 125 and 126 of the Guidelines), we would request the EDPB to **clarify whether the controller has to be informed and has to authorize each subsequent transfer of data between the processor and the sub-processors in the chain**.

While guidelines under paragraphs 156-157 seem to exclude such a requirement for the controller, it would be helpful to have it explicitly excluded.

UNIPOL GRUPPO S.p.A.
Head of Regulatory Affairs
Luca Giordano