ADIJ
Protection des données personnelles

COMMENTS ON THE GUIDELINES 07/2020
OF THE CONCEPTS OF CONTROLLER AND PROCESSOR IN THE GDPR
-
Data protection workshop at ADIJ (French association for the development of IT law)

19 October 2020

Dear Sir or Madam,

We thank the EDPB for the opportunity to provide the following questions and comments of our legal workshop regarding the guidelines 07/2020.

1. General comments

Consultation process. As a preliminary comment, we highlight that it is always difficult to meet the deadlines set out by the EDPB public consultations. They are usually limited to a month or so, and this is very short when an organization needs to consolidate the comments from several contributors.

We would also like to bring to the attention of the EDPB that the content of EDPB guidelines – specifically on essential notions such as these or on sectorial questions - could benefit from national prior consultations launched by national data protection authorities. We strongly believe that it would enable the EDPB to build its guidelines on elaborate reports and materials illustrating the diversity of issues and situations raised at national level. Indeed, not all the interested parties are in a capacity to answer consultations at EU level, in particular SMEs and the public sector. .

Scope of the guidelines. The guidelines aim to address the very complex concepts of controller and processor. However, we note that this draft covers other topics that falls within the scope of the legal regime applicable to controllers, processors and joint controllers. Part II regarding the consequences of attributing different roles is a typical example. Yet, the concepts of controller and processor and the identification of cases of joint controllership alone are already sufficiently complex to be the sole subject matter of the guidelines.

Covering both the concepts of (joint) controller and processor and the responsibilities and liabilities regime governing each qualification in one single set of guidelines is very challenging, when taking proper account of the critical need to clarify not only the concepts, but above all the interplay between those concepts. It is thus questionable whether on set of guidelines may cover both issues with the required level of precision. In any case, the objective to cover the entire subject should not be conducted to the detriment of the level of granularity of the analysis of the part covering the concepts.

We appreciate that further clarification is needed, in particular to address the following points:

- the criteria that may be used to determine the appropriate qualification (see below,

comment n°3.2);

- the illustration of how the case-by-case analysis should be conducted: the variety of the practical examples presented should include all environments, and not be principally on the online world; we appreciate that more examples should cover situations of the offline environment to answer the legitimate expectations of all the actors, and especially SMEs ;
- the articulation of the concepts of processor and controller with other concepts/roles : in this regard we appreciate a sectorial approach is necessary, especially on sectors such as healthcare, insurance, research and that a dedicated section should deal with the issues raised by the qualification in the public sector, especially on calls for tenders and on situations where more than one public stakeholder is concerned and where the controller is not nominated by or no specific criteria for its nomination are found in Union or member State law ;
- the qualification of cloud service providers in light of previous guidance given by the article 29 working party[1] and member state DPAs[2], which mentioned the possibility that a cloud service provider may under certain circumstances or for certain processing operations be considered as (joint) data controller;
- the interplay between the allocation of liability between joint data controllers under article 26 (1) of the GDPR and the provisions of article 82 (Right to compensation and liability) and 83 (conditions for imposing administrative fines) of the GDPR, in light of the statement (§56 of the guideline) that joint responsibility does not necessarily imply equal responsibility.

2. Concept of controller and processor

2.1. Consequences of adopting a broad interpretation of the concept of data controller (§14)

The guidelines state (§14) that "*the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data*", and thus, "*'the concept of 'controller' should be interpreted in a sufficiently broad way so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules*".

It would be quite helpful for stakeholders if the guidelines could provide further explanation on the

[1] "*Nevertheless based on concrete circumstances situations may exist where the cloud provider acts as a controller as well, e.g. when the provider re-processes some personal data for its own purposes*" : Opinion 05/2012 of the article 29 working party on Cloud Computing adopted on July 1st 2012 (Wp196), p.20 : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[2] " [*The] CNIL notes that in some cases of PaaS and public SaaS, although customers are responsible for their choice of service provider, they cannot actually give the service provider instructions and they are unable to check the effectiveness of the security and confidentiality safeguards put in place by the service provider. This lack of instructions and of means of control is due mainly to the existence of standard offerings that customers cannot modify, and to standard service contracts that do not allow them room to negotiate. In these situations the service provider could therefore, on the face of it, be considered to be joint controller according to the definition of 'controller' given in Article 2 of Directive 95/46/EC, because it participates in determining the purposes and means of the processing of personal data.*" : CNIL, " Summary of responses to the public consultation on Cloud computing run by CNIL from October to December 2011 and analysis by CNIL", 25 June 2012, accessible on https://www.cnil.fr/sites/default/files/typo/document/Summary_of_responses_to_the_public_consultation_on_Cloud_computing.pdf [last visited : 19 Oct. 2020]

consequences of adopting a broad interpretation of the concept of data controller.

In particular, does it mean that, when in doubt:

- the controller capacity should systematically prevail for all stakeholders?
- the interests of the data subject should be taken into account in identifying the capacity as data controller, and if so to what extent?

2.2. Clarification of the definition of acting "on behalf" (§75, 77, 78)

"Acting on behalf" is not equal to "deciding to delegate" (§75 and 78), as well as "upon instructions" is not equal to "for the benefit of" (§77). There are indeed examples where a delegate is a data controller: e.g. an insurance broker appointed by an insurer with a full conferral of management ("*délégation de gestion pleine et entière*").
We appreciate that in such case, it can be considered that the insurance broker, while acting as delegate, does not act under the direct authority of the controller, and is thus a joint controller, and not a processor.

The guidelines could perhaps present a more nuanced analysis given the diversity of the situations that may occur in practice.

2.3. What are the limits of the qualification as processor? (§79)

The guidelines state that *"Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions".*

It is however quite frequent that, in a contractual relationship, a processor that is strictly processing data on behalf of and under the documented instructions of a controller, has also the legal obligations to reuse the client data for a purpose of its own. As it does not stem from this that a common purpose and benefit is shared by both parties and thus, the guidelines could most relevantly clarify that there is in such case no scope of joint liability.

We also appreciate that the guidelines should elaborate on the circumstances under which a processor may act as data processor for certain data processing operations and qualify as data controller for other (§63 and 81). This specific case could most relevantly be illustrated by the reuse of personal data (in most cases, after implementing anonymisation/pseudonymisation techniques) by a data processor for service improvement and/or research and development (e.g. to create a learning data base for artificial intelligence), for benchmark or for statistical purposes, with or without the permission of the initial controller

2.4. Essential vs. non-essential means (§38 and §39)

Examples of essential and non-essential means. More examples should be provided regarding the

application of the criteria of essential vs. non-essential means in complex contexts such as cloud providers, clinical trials involving a contract research organization, connected vehicles with embedded applications, etc.

We appreciate that the guidelines could build on the work previously conducted by the article 29 working party on cloud computing, as well as on guidance issued by national DPAs mentioned above. The guidelines would gain in effectivity by presenting a table of the criteria to take into account in the context of a specific case and of the way to determine the appropriate weighting for each criteria.

Information on the means. In addition, we note that the guidelines state that "*In any event, the controller remains responsible for the implementation of appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation (Article 24). In doing so, the controller must take into account the nature, scope, context and purposes of the processing as well as the risks for rights and freedoms of natural persons.* ***For this reason, the controller must be fully informed about the means that are used*** *so that it can take an informed decision in this regard*".

Considering the above, what are the consequences for the parties, if the controller is not actually fully informed?

Answering this question is all the more pressing that in practice, controllers are not fully informed on the technical and organisational means, specifically since the controller requires the services of third party provider because it does not have the expertise and resources to undertake a thorough analysis of both the needs and the means to be implemented. This is more particularly relevant for SMEs. Even if the controller is informed, the controller may not always be able to challenge the relevance of the means implemented or may only do so at excessively high prices. This is particularly true when the controller uses cloud services.

Therefore, we appreciate that the guidelines could clarify the nature of the guarantees and information that must be obtained from the processor. For instance, would this obligation to be fully informed be fulfilled if a data controller chooses a provider that provides guarantees such as security and ISMS certifications, security audit reports, or other relevant global guarantees? May this obligation be nuanced based on the risk generated by the processing?

The guidelines should also specify (§39) whether the lack of information has any impact on the qualification of a service provider as processor: are there circumstances where the lack of information leads to consider that the processor is acting outside the instructions of the controller and qualifies as data controller?

3. Joint controllership

3.1. Definition of controller (§18 and §19)

The guidelines states that "*it is usually the organisation as such, and not an individual within the*

organisation (such as the CEO, an employee or a member of the board"). Since the guidelines do not exclude by principle this possibility, the guidelines should further explain in which circumstances an employee or a member of the board of a legal entity may qualify as data controller and elaborate of the nature of this liability (civil or criminal?): does it apply in circumstances where the said employee/member of the board act in their capacity as employee or board member or only where they act outside the scope of their functions? Even in such case, shouldn't the extent of the employee's or board member's personal liability be subject to national law?

Also, the guidelines states that "*As far as data processing within a company group is concerned, special attention must be paid to the question of whether an establishment acts as a controller or processor, e.g. when processing data on behalf of the parent company*". This complex issue should be further analysed by the guidelines, with examples. For instance, the guidelines provides an example in §69 that only addresses the relationship between affiliates using a shared database, but not the relationship between affiliates and the parent company in such a case (see below, 3.4).

3.2. <u>Assessment of joint participation (section 3.2.2.)</u>

A need for precise methodology. The guidelines provide a general analysis on how to assess joint participation, but we feel that a more thorough analysis of the criteria identified by the CJUE in the various quoted decisions would be helpful. For instance, a clear and express list of the relevant criteria, with a precise analysis on how to interpret each of them in a dedicated section.

A clear analysis of the way to implement in practice the CJUE methodology for this assessment would also be helpful. Indeed, the CJUE has notably ruled in Fashion ID that it is possible to distinguish between various data processing operations for the same data processing, with different data qualification for each (e.g. a limited scope of joint responsibility within the entire data processing). Additional guidance on how in practice data controllers should distinguish the various data processing operations (notably the level of granularity to be applied in distinguishing the various stages of the processing operations, the circumstances under which it can be considered that the "same purpose" is pursued by the controllers for a specific operation, the consequences of the distinction of the obligations of data controllers towards data subjects and on their overall responsibility and liability. This approach would be highly welcomed.

Another important topic requiring clarification is the interplay between the purpose and the "common benefit" criteria laid down by the CJEU in the Fashion ID decision (see below 3.5).
A need for practical examples. The examples provided by EDPB guidelines are always very helpful, as they offer an interpretation of the notion through a case study. We however note that the examples provided in these guidelines are scarce and generally cover textbook situations. It would be useful to obtain more examples, regarding various sectors that are not addressed by the guidelines (e.g. automotive industry, insurers and their intermediaries, ecommerce platforms and their business partners, IT providers specifically through Saas, etc.), and to address the issues that are not solved today. In our view, the guidelines are not designed to provide the general public with information but to provide thorough analysis to data protection law experts and practitioners. The examples provided in the guidelines might be too general and simple to provide answers to the questions that every sector faces today.

3.3. Clinical trials and research (§66)

The previous WP169 provided an interesting example (n°25) regarding clinical drug trials, according to which, in a detailed context where both trial/investigation centres and sponsors made important determinations with regard to the processing, a joint controllership could be identified:

- the pharmaceutical company "*sponsors the drug trials and selects the candidate trial centres by assessing the respective eligibility and interests; it draws up the trial protocol, provides the necessary guidance to the centres with regard to data processing and verifies compliance by the centres with both the protocol and the respective internal procedures*" (…) "*it does acquire the patients' data as collected by trial centres and processes those data in different ways (evaluating the information contained in the medical documents; receiving the data of adverse reactions; entering these data in the relevant database; performing statistical analyses to achieve the trial results*)";

- the trial centre "*carries out the trial autonomously – albeit in compliance with the sponsor's guidelines; it provides the information notices to patients and obtains their consent as also related to processing of the data concerning them; it allows the sponsor's collaborators to access the patients' original medical documents to perform monitoring activities; and it handles and is responsible for the safekeeping of those documents. Therefore, it appears that responsibilities are vested in the individual actor*".

The guidelines 7/2020 provide a similar example (p. 21), with a university sponsor and a health care provider (the investigator) that "*collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.)*". (…) "*In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial*".

Therefore, should it be construed as considering the drafting of the protocol as the main criteria to define the qualification of the parties? Indeed, other aspects of clinical trials such as those listed in the previous example still appear relevant to identify a scope of joint responsibility, even if the sponsor is the one elaborating the protocol. The criteria of the autonomy appears, in our view, quite important, not only to identify a scope of joint responsibility between the parties, but above all, that contradicts the processor qualification of the health establishment / professional. The latter appears to always have in practice, because of its expertise and deontology, a great deal of autonomy in the way the clinical trial and the health data processing is being carried out.

In addition, the guidelines do not mention the contract research organization, which a very frequent part of clinical trials. Before GDPR, CROs used to be considered as data processors, only because they were service providers. However, given their important involvement in the management of the clinical trials (health professionals database, drafting and management of the consent forms, management and monitoring of the entire clinical trial, etc.), there is a question on the qualification of such parties. This could be a case where a scope of joint responsibility between

three entities could be identified.

3.4. Groups of companies (§69)

Groups of companies definitely need guidance on usual issues regarding allocation of responsibilities and data protection capacities. The example provided in §69 is useful, since there are frequent cases of a group of companies sharing an infrastructure. However, this example does not cover the potential complexity of this kind of infrastructure.

Some of the usual questions in such contexts are:

- What is the qualification of the parent company, that usually is the one deciding on the implementation of such a shared infrastructure?
- What are the practical circumstances that should lead to consider that there is a case of joint liability between the mother company providing the system and the affiliates using the shared infrastructure? To what extent can the mother company be considered as a simple data processor taking into account that in most cases the use of system is imposed upon the affiliates.
- What if the mother company does not limit its services to the provision of the infrastructure, but also uses it in order to procedure aggregate data?

3.5. Joint controllership and the "common benefit criteria"

(§51) Also, the criteria of joint participation through a "common decision", i.e. "deciding together" and "common intention", is likely to be frequently met in any business agreement, where parties usually agree on the common purpose of the agreement, on the means and generally obtain a common benefit from it, otherwise there would be no cause for contracting. Of course, not every agreement has data processing for main subject matter, but in many sectors, data are now a main topic of business agreements. This fairly general criteria could thus be further explained by the guidelines.

4. Recipients and third parties (section 5)

In this section, the guidelines could clarify whether recipients can be specific services or departments of the same entity, e.g. the marketing or IT service of a data controller.

5. Relationship between controller and processor (part II, section 1)

The processor must **assist the controller for the fulfilment of its obligation to respond to requests** for exercising the data subject's rights (Article 28(3) (e) GDPR, and see section 1.3.5 of the guidelines). Under §127, this section provides that "*The details concerning the assistance to be provided by the processor should be included in the contact or in an annex thereto*." The guidelines should further explain whether the details concerning the assistance to be provided by the processor may also include the financial conditions under which such assistance may be provided. Such assistance indeed has a cost for data processors which should be taken into account.

Under § 145 of this section, **in case of instructions infringing data protection laws**, the EDPB

recommends the parties to negotiate and agree in the contract the consequences of the notification of an infringing instruction (section 1.4). What if the contract is unclear or does not provide with any specific clause in this respect? Must the data processor suspend the services in case of an instruction infringing data protections laws?

Regarding subprocessors, the **difference between a general and specific authorization** remains unclear. In §152, it is indicated that in the case of a general authorization the contract must include a list with the sub-processors in an annex. It is further indicated that 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.

In practice, the above is the same as specifically agreeing each sub-processor as in a specific authorization: if the sub-processors are initially listed in the agreement, they are nominatively agreed by the data controller from the start.

We draw your attention to the fact that this will create practical issues for data processors (please also see section 7 below). Could a general authorization also be possible for defined and specific categories of sub-contractors, e.g. for maintenance services, with a defined scope and appropriate guarantees/obligations set out in the contract (e.g. on the level of security required from the sub-contractors)?

In addition, does this obligation also applies to sub-contractors of the data processor's sub-contractors, e.g. if the data processor uses a cloud service provider to host the data: must the list of the sub-contractors of the cloud service provider also be provided in the contract?

Finally, the guidelines could indicate that the consequences of the data controller's objection to a sub-contractor should be defined in the contract (e.g. termination of the contract).

6. Consequences of joint controller ship (part II, section 2)

Regarding section 2.1, "*Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR*", it would be interesting to clarify how can joint controllers can in practice allocate responsibilities and the consequences for joint liability. For instance, can one of the joint controllers only be responsible for responding to data subjects' requests (§163)?

Data protection workshop – ADIJ
19 October 2020

Contributors: *V. Bachvarova, C. Borfiga, M. Depadt-Bels, L. Maisnier-Boché, N. Metallinos, E. Mertz*

@ADIJ_FR