Position Paper

Bitkom views on EDPB Guidelines 7/2020 on the Concepts of Controller & Processor in the GDPR

19/10/2020

Federal Association
for Information Technology,
Telecommunications and
New Media

Rebekka Weiß, LL.M.
Head of Trust & Security
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Introduction and Overview

Bitkom welcomes the opportunity to comment on the European Data Protection Board's (EDPB) Draft Guidelines on the concepts of controller & processor in the GDPR. We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty.

1. Summary

We welcome the EDPB's public consultation on this important issue and the opportunity for stakeholders across all industries to provide input.

We would like to point out the following areas of concern and make a few initial suggestions where we believe the guidelines should be adjusted to account for the current state of technology and practice. In summary, we believe that the scope and notion of both controller as well as controller-processor relationship are described too broadly and need clarifications to take practical circumstances into account.

2. Scope and Notion of Controllership

While the obligations placed on controllers are vital for the protection of the rights of individuals, these guidelines propose language that would broaden the interpretation of a 'controller' to a degree that could: (a) create new uncertainties; and (b) fail to reflect important nuances contemplated by the

language of the GDPR and inherent to the state of practice.

Paragraph 14 states that *´[a]s the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, the concept of 'controller' should be interpreted in a sufficiently broad way´*. Comprehensive protection of individuals' personal data is indisputably a priority. With that understood, it is also worth bearing in mind that the GDPR contemplates the concept of a third party, i.e. a party other than the controller or processor that still may have an interest that is being pursued with the processing in question.

The interpretation of controller (and processor) cannot be made so broad as to eliminate the existence of this concept and we believe this needs to be emphasized at the outset of the Guidelines.

Additionally, an expansive understanding of the controller concept does not necessarily result in more effective and comprehensive protection of personal data. A multitude of controllers for a given data processing activity has the potential of diluting responsibility in practice. And every additional controller also adds an entity carrying rights vis-a-vis the data subjects.

Paragraph 22 states that *´the law may also impose an obligation on either public or private entities to retain or provide certain data. These entities would then normally be considered as controllers with respect to the processing that is necessary to execute this obligation´*. This can put entities into a very challenging position. E.g., a processor may be compelled by EU Member State Law (e.g. in the area of criminal tax law) to disclose personal data that it processes on behalf of a controller. If the processor is deemed to be a fully-fledged controller for the purpose of that disclosure, it would suddenly be required to carry out all controller obligations, such as informing data subjects (etc.), which may be difficult or impossible in practice. We encourage the EDPB to acknowledge that concern in their guidance, and maybe envisage the concept of a controller whose obligations are limited by ´the framework of its responsibilities, powers and capabilities´ as established by the CJEU in multiple decisions.

Paragraph 28 states that *´the word 'determines' means that the entity that actually exerts influence on the purposes and means of the processing is the controller´*. We would suggest amending this to avoid the suggestion that any level of influence will amount to controllership.

Notably, it is established elsewhere that such influence must be 'decisive' or 'determinative': this wording could be incorporated here for consistency and clarity.

Regarding Paragraph 34 we suggest including more explanation regarding whether the choice to use a service is sufficient to determine the purpose and/or means of processing, esp. where the service itself is standardized.

Paragraph 38 states that *´[e]xamples of essential means are the type of personal data which are processed, the duration of the processing , the categories of recipients and the categories of data subjects´*. It is important to note, however, that processors will often set up a standardized system that only allows for limited customization by the controller, yet the controller still ultimately decides to use that system and that decision includes relying on all the standardized aspects of that system. Prior to use, the system does not process any personal data, so the controller sets this all in motion when signing up and starting to use it. For a lot of (IT) Services, it is not up to the customer to decide which category of personal data is being processed, as this may be inherent to the technology used (e.g. communication through the internet needs IP addresses to be routed) and the service selected.

We therefore ask the Board to add more clarity as to the extent of the actual influence required to give rise to a Controller-Processor relationship. Is the selection of the particular service sufficient for the determination of purpose and means? E.g. the provider describes in the service description what data will be used (and the customer cannot chose or change it) and the tools used (´means´) are also not for the customer to alter, affect or select.

Enterprise email services are a useful example in this regard as well: they are standardized in many ways (and a lot of that standardization comes from underlying technical standards) with many required data fields and pre-set very little room for customization, but the enterprise who decides to start to use that email services for internal communication and communication with customers, will still have to be regarded as a controller.

Paragraph 16 separates the requirement ´the purposes and means´ from the requirement ´of the processing of personal data´, whereas these are not separate building blocks but instead one building block, i.e. ´the purposes of the processing of personal data´. The consequence of treating these requirements as separate are elaborated in paragraph 40. By failing to emphasize that there needs to be an inherent relation between the determined purpose and the personal data

that is being processed the guidelines may be interpreted as meaning that every processing of processing will meet the requirement under Art. 4(7) GDPR. A (general) waste collection company knows that it will inevitably process personal data when collecting and then destroying or storing waste, but pursuing the purpose of waste collection it does not pursue a purpose under Art. 4(7) GDPR. The same is true for a company that refurbishes used processing hardware to resell it and routinely wipes all storage in that hardware as part of the refurbishing process. A scientist collecting digital copies of scientific articles published by named authors, will know that she collects and processes personal data but, pursuing the purpose of scientific research will not turn the scientist into a controller. Even a processor pursues a purpose with the processing of personal data, namely to make a profit charging for the processing services. By not appropriately addressing the requirement for the relationship between the purpose and the personal data, an approach in which any purpose of processing could qualify as a ´controller purpose´ would therefore turn entities into controllers for whom that designation is simply inappropriate, and it would deprive the controller designation of its functional aim emphasized in the guidelines, i.e. to allocate responsibilities according to the actual role of a party.

The Guidelines state that regardless of the wording of a contract, liability should depend on the de facto exercise of the controller´s influence, p. 12, Paragraphs 27-28. This would be rather difficult to implement in practice. The de facto influence and control cannot always be reflected in a contract in detail because f.i. of the balance of power between parties. Furthermore, the actual data protection perspective is also not easy to determine and is not clearly objective. A clear legal assignment of roles by means of unambiguous criteria indicating when a party has control with respect to the processing of the personal data would create more legal certainty here.

The data controller must decide on both the purposes and the means of processing and must not be satisfied with determining the purposes alone. Accordingly, a processor should never determine the purposes, p. 13, Paragraph 34. The distinction between means and purposes seems somewhat artificial and is not easy to make in practice. However, the distinction between essential and non-essential means is even more complicated, as it is difficult to determine this clearly. The more unclear such a concept is, the more the negotiating power of the parties is ultimately important, so that in cases of doubt it is not the solution desired under data protection law that dominates, but the law of the party with the greater negotiating power. However, this

should not be relevant for the determination of roles as under data protection law the control over the personal data in question should be the determining and relevant factor.

According to the Guidelines, the status of data controller can refer to a totality of data processing operations, but also to individual processing operations, p. 15, Paragraph 40. The distinction between ´data processing´ and ´individual processing operation´ is difficult to make in practice, but by extending liability it leads to an extension of liability and possible sanctions. It may be better to clarify which processing is relevant and also to clarify that for subsequent processing activities the parties can have different roles depending on whether they determine the purpose and means of that processing activity.

With regard to Paragraph 42 [Market Research] the given example remains unclear. We therefore suggest including further elaborations. Under realistic considerations, XYZ ´owns´ the data, hence controls what services customers can buy from them to perform on XYZ's own data. Also XYZ would likely not allow ABC to review neither their methodology as this is their trade secret, nor would they share the actual customer data. Also XYZ's right to the data may not include the right to provide ABC access. It seems odd that ABC is responsible if something happens to data sets that ABC does not have access to. It seems rather incidental that something has happened while XYZ is performing a service. Also ABC as a controller would add another party with rights to the data and thus increase the risk for the data subjects.

3. Scope and Notion of Joint Controllership

As with the interpretation of 'controller' more generally, an overbroad interpretation of 'joint controllership' could create uncertainty and fail to reflect the breadth of nuance within the state of technology and practice.

This is notably the case where the Board underlines that converging decisions by two entities may be an indicator of joint controllership. Indeed, a co controller and processor working together will more likely than not have common business interests that will have an impact on the way the processing is carried out. This does not necessarily indicate that decisions on the purposes of processing are made jointly.

Likewise, the criterion that ´the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable´ is overly broad and

could be unreliable. There are numerous scenarios where the data subject joins two independent controllers, e.g. by enabling controller A to pull data from controller B through an API to deliver an augmented service. E.g. an app provided by A that allows a user to combine and play content from multiple streaming services. Those streaming services B make the API available and the processing by A and B is inextricably linked to provide the service. That in itself, however, is not sufficient to turn A and B into joint controllers, given that it was the data subject that chose to combine the controllers in this way, while the controllers simply have enabled interoperability.

Paragraph 37 states that ´Decisions on the purpose of the processing are clearly always for the controller to make´. In practice, a processor may also consult and advise the controller on how to achieve a certain objective. The Board's Guidelines should acknowledge that this is sometimes the case and that this does not turn the processor into a (joint) controller, when the ultimate decision power to go ahead with a processing operation lies with the controller.

In Paragraph 67, the Board states that joint controllership must be assessed on a case-by-case analysis. We would suggest that the Board further clarify that certain criteria for joint controllership need to be fulfilled cumulatively, rather than in isolation.

Among the examples of situations where no joint controllership arises, we would suggest adding the following: A data subject joining independent controllers. For instance: User A uses a music streaming service B that can be used through B's app or third party apps. C offers an app with an improved user interface enabling users to access and manage content from any music streaming service. A sets up C's application in such a way that he can now navigate and play B's content through that application. B and C continue to be independent controllers in this scenario.

A joint controllership on the means of data processing does not require that each controller decides on the means to the same extent in every situation. It may well be that one controller provides the means for all other controllers. Whoever makes use of this would then also make a decision on the means of data processing, p. 20, Paragraph 62. The question here is what this means f.i. for cloud computing and other business in IT or online services. Is cloud computing or the mere provision of cloud infrastructure then joint responsibility? It could be difficult in practice to formulate this correctly in a contract, as the negotiating power of the cloud providers generally offers little opportunity for individual formulation.

4. Overly prescriptive indications on the relationship among joint controllers

In seeking to clarify the obligations placed on joint controllers, these guidelines appear to go beyond the language and intent of the GDPR.

The Board lays out that the contract between joint controllers *´should cover other controller obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities´*. This is overly prescriptive. Each controller is already, separately, subject to these obligations under GDPR. Joint controllers are not required by GDPR to specify those again amongst each other. These Guidelines would also go beyond the GDPR by requiring the designation of a point of contact for data subjects in this contract, which is optional under the wording of Article 26.

The Board notes that *´[e]ach joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data´*. This approach is overly restrictive: when controller A collects data for purpose 1 and then shares this data with controller B, then that constitutes an independent processing event for which controllers A & B may jointly have determined a new purpose 2. So the original purpose 1 becomes irrelevant for the processing by the joint controllers.

A controller might also decide to use the data for another/additional purpose. For example, in the Fashion ID case, the CJEU concluded that a joint controllership existed between the parties *´in respect of the operations involving the collection and disclosure by transmission of the personal data of visitors to its website´,* but that this joint controllership did not cover any processing before or after that stage. Furthermore, besides the joint purposes, the receiving controller might have additional purposes for the data processing. This should be acceptable provided that there is an appropriate legal basis for it.

In Paragraph 79, the Board states that Acting on behalf of´ means that the processor may not carry out processing for its own purpose(s). However, it should be clarified that everything that is

necessary for the processor to provide the service to the specific contractual partner in a faultless, safe, high-quality and sustainable manner is part of the processing on behalf of the controller.

With regard to Paragraph 81 [General IT Support] we suggest including further elaborations about general IT support that does not include ´vast amount of personal data´, where contact to personal data is rather incidental and not relevant to the task at hand, which for many devices would be the standard (e.g. review of error-logs that may or may not contain machine identifiers that belongs to a machine that may or may not be assigned to a human).

Also in Paragraph 81 [IT-consultant fixing a software bug], it appears that the 2 examples should be swapped. In general IT support it is more likely that access to personal data will be purely incidental, where specialized software support has a good chance of requiring access to production data. In practice, the two given examples cannot be separated. Often the manufacturer provides a maintenance/support service, which is fulfilled in 90% of the cases with the provision of patches and updates, but in case of occurring errors an access to the system cannot be excluded. The examples would lead to a differentiation within a value proposition; in both cases a processing of personal data is not the focus of the performance but the functionality of the system. The processing of the data can simply not be excluded in the process of delivering the service.

5. Definition of a Processor

While guidance around the definition of a processor is undoubtedly impacted by the interpretation of 'controller', these guidelines could also be further improved to better reflect certain nuances around the role of a processor in practice.

In Paragraph 73, the Board states that *´The processing activity entrusted to the processor may be limited to a very specific task or context or may be more general and extended´*. We would suggest adding that a controller might also decide to join multiple processors by instructing two separate processors to share data among each other.

In Paragraph 77, the Board states that *´in practice that means that all imaginable processing of data constitutes processing´*. While we acknowledge the GDPR's broad definition of processing, we would suggest the above is arguably even more expansive, especially if taken out of the context of that section of the guidelines. E.g. it would mean that a postman processes personal data by

handling a package containing personal data. We would therefore suggest deleting that sentence.

Also, the given example of a Cloud service provider is specific in ways which may be unexpectedly problematic in practice. Notably: it states that personal data should be processed for the municipality's purposes only; while this is intuitively correct, it is possible that on occasion a case might arise where the service provider may or must be a controller of certain personal data in some capacity. In addition, the following sentence about ensuring the municipality's specific instructions are invariably accepted may be too restrictive.

6. Controller/Processor Relationship

In seeking to clarify elements of the relationship between controllers and processors, these guidelines at times appear to exceed the requirements of the statute, and do not take into account certain practicalities arising from the current state of technology.

In Paragraph 91, the Board states that *´the EDPB considers that Article 28(3) GDPR imposes direct obligations upon processors, including the duty to assist the controller in ensuring compliance´*. This does not align with the clear intent of the legislators: the GDPR makes those obligations subject to a ´contract or other legal act´. They are not intended to be statutory obligations in their own right, or there would be no need for a contract setting out such terms. With regard to the controller's own obligations, such as ensuring the rights of data subjects, reporting of data breaches, etc., a processor can only support the controller in those areas. As a result, the controller must be able to fulfill its obligations even if a processor is used. This does, however, not include a free support from the processor.

In Paragraph 107, the Board states 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. The mere publication of these modifications on the processor's website is not compliant with Article 28´*. We would like to underline that the Rome I Regulation sets out the general principle that parties to a contract have the freedom to choose the governing law of their contract. Therefore, the validity of the data protection agreement and any amendments to the agreement are a matter for the governing law of the contract. It is not appropriate for the Guidelines to seek to override the requirements of the governing law. In any case, the processor has a direct obligation to ensure that the data protection agreement includes the provisions

required by Article 28(3) and if the processor sought to change the agreement in such a way that it no longer met the requirements of Article 28(3), it would be directly in breach of the GDPR.

In Paragraph 111 the Guidelines advise that the contract shall set out the controller's obligation *´to provide and document, in writing any instruction bearing on the processing of data by the processor´*. The Guidelines should avoid using the term ´in writing´, since it may be misinterpreted as meaning that the instructions need to be put in a human readable text or in the form of words. That will often not be the case. The controller may use technical signals to issue instructions, e.g. by using a user interface or API calls to instruct the processor to process data in a certain way. Those instructions will be documented through a digital log entry or similar.

Paragraph 115 is perhaps drafted too narrowly to reflect how controllers often give instructions in practice. Many processors make user interfaces available that enable the controllers to issue instructions by choosing certain settings or other interactions with the interface.

In Paragraph 123, the Board mentions *´an obligation on the processor to obtain the controller's approval before making changes´*. We suggest taking into consideration that in practice, a processor may make updates from time to time (e.g. to ensure their security measures reflect the state of the art). A clarification should be included in the Guidelines that the example does not include changes provided that there is no deterioration in the level of protection (e.g. replacement of security personnel by video cameras, or replacement of virus scanner A by virus scanner B, etc.). Such updates may be within the controller's expectations and may not always require the controller's approval, provided that they do not result in the degradation of the overall security of the service.

Paragraph 137 may be unduly restrictive in practice. It states that *´the controller can decide at the beginning whether personal data shall be deleted or returned by specifying it in the contract, through a written communication to be timely sent to the processor. The contract or other legal act should reflect the possibility for the data controller to change the choice made before the end of the provision of services related to the processing´*. We would suggest deleting the latter sentence: it suggests a requirement that may not always be possible to meet in practice, the lack of which does not preclude the controller from being able to make an informed choice.

With regard to Paragraph 140 a clarification would be welcomed on how many details have to be given. For security reasons, security measures should not be disclosed in too much detail,

especially in mass business - unfortunately there is still no certification possibility for these purposes - but a reference to a certification possibility could be added here, with which the processor can provide proof.

In Paragraph 141 (and 147) a clarification on sub-processors is necessary; e.g. no approval requirement for e.g. change of telecommunications provider, postal service provider, maintenance services that do not provide the agreed main service.

Regarding Paragraph 147-157 a clarification is needed regarding the connection to the examples in Paragraph 81: when would a maintenance partner of a machine used for the main service as a sub-processor require approval? Can a call centre only change its telephone system or maintenance partner if all call centre customers agree beforehand, because it cannot be ruled out that telephone numbers from maintenance/support orders can be taken note of? This does seem rather impractical so the Guidelines should take these circumstances into account. We suggest amending the Guidelines in this regard and include a clarification.