SVENSKT NÄRINGSLIV
SWEDISH ENTERPRISE

European Data Protection Board

Stockholm 19 October 2020

Public consultation reply: Guidelines 07/2020 on the concepts of controller and processor in the GDPR

The European Data Protection Board **(EDPB)** has published "Guidelines 07/2020 on the concepts of controller and processor in the GDPR – version for public consultation" ("**guidelines**"). In connection with its publication, EDPB has requested comments on the guidelines.

The Confederation of Swedish Enterprise has, with the participation of senior specialist Martin Brinnen at the law firm Kahn Pedersen, compiled the comments below.

1. General comments

1.1.1. Welcome and long-awaited guidance

Assessing the division of controllership in wider cooperation with several actors involved may be one of the most complex issues facing the GDPR. The rules are relatively short and do not provide much guidance. The case-law of the Court of Justice of the European Union **(CJEU)** may provide some additional guidance but in some cases has made the already complex assessments even more complex.

Against this background, the guidelines are a welcome and long-awaited piece of work. Consistently, the guidelines also maintain a very high legal quality and deal with virtually all essential issues, many times at a very detailed level.

1.1.2 Make guidelines more practical

The guidelines deal with issues that often require very complex assessments of the practitioner. However, with the design and scope of the guidelines, it is difficult to see how an undertaking, without special expert assistance, will be able to make the necessary assessments. This applies not least to small and micro-companies that rarely have access to expert assistance. The guidelines should therefore be complemented by more practical guidance.

In this context, it should be noted that the guidelines cover 48 pages with many in-depth footnotes and are generally of such detail that they are more similar to a legislative commentary addressed to experts than a guide for companies and others applying the rules. This is reflected not least in the light of the fact that the guidelines are formulated on the basis of the concepts of the regulation and not from the questions faced by the practical practitioner. There is, of course, a great need for such guidance, but they do not cover the

Confederation of Swedish Enterprise
Address: SE-114 82 Stockholm Visitors: Storgatan 19 Phone: +46 (0)8 553 430 00
www.swedishenterprise.se

need for guidance from the many companies that do not have access to expert assistance or time to read and familiarise themselves with the guidelines.

Having said that, it is welcome that the guidelines contain a number of examples and a final flowchart. We see that there is room for several such practical elements. In addition, the guidelines can be supplemented with, among other things, graphic presentations, checklists, proposals for contract texts. Several and more descriptive headings can also help you read the guidelines.

Furthermore, it should be noted that the guidelines have no explicit target group (cf. p. 1). However, it is clear that the aim is to provide guidance to those who are to apply the provisions in practical situations and not only to the supervisory authorities.

1.1.3 The guidelines can contribute to a more coherent interpretation of the GDPR

We also see that the guidelines may have an important role to play in contributing to a more uniform interpretation and application of the GDPR by national regulatory authorities. However, there is a risk that consistency will be lost if each national regulatory authority in its own way simplifies and summaries the guidelines in order to make them more practical. For this reason, too, it may therefore be appropriate to align the EDPB guidelines with the practical practitioners, thereby ensuring a uniform interpretation and perception of the responsibilities and obligations under the GDPR.

2 The structure of the guidelines

2.1.2 Use more examples and index them

Examples are a very good tool for explaining complex statements of principle made in the guidance. The many examples in the guidelines are therefore a good complement to the texts. For this reason, it is appropriate to have several examples and with an index of examples and/or some form of classification that will help the practitioner to find the situation that he or she has to assess and thus find the right section to read in the guidelines. See compilation of the examples in Article 29 Working group, Opinion 03/2013 on purpose limitation WP 203, Annex 3.

Many of the examples mentioned in Article 29 Working Group, Opinion 1/2010 on the concepts of "controller" and "processor" WP 169, are missing from the guidelines. It is appropriate that as many of these as possible should be included in the guidelines and supplemented by further examples.

It may also be useful to include examples in Part II on e.g. contract texts relating to processor agreements and agreements between joint controllers.

2.1.2 Describe more clearly how the guidelines differ from previous guidance

The guidelines replace previous guidance of the Article 29 Working Party (p. 4). At the same time, the EDPB notes that the concepts of controller and processors have not changed (p. 11). Many companies have used the previous guidance and it may therefore be appropriate to clearly indicate how the guidelines contain new interpretations of the concepts or other changes.

2.1.3 Identify the simple cases

The so-called risk-based approach on which the GDPR is based should not only be reflected in identifying particularly privacy-sensitive processing that requires specific considerations. It should also be used to identify the less privacy-sensitive processings for which responsibilities and obligations are more limited. Such a method should also be reflected in EDPB guidelines.

It is likely that the vast majority of the situations in which companies and other organisations have to assess controllership are relatively simple. It is therefore appropriate that the guidelines should initially describe such simple cases. The guidelines in their current form are largely focused on complex assessments in specific situations, which of course is good because it is in these cases guidance is of paramount importance. However, in order not to have all companies and organisations to devote unnecessary time to these situations, it is advisable to identify and account initially (or in an annex) the simple cases.

In such an initial part (or annexed), it is appropriate to structure the guidance on the basis of common practical situations rather than structuring the text on the provisions of the GDPR. This means that many people can find the answers to their questions more quickly or confirmation that they have thought right.

2.1.4 Clarify how companies should act in unclear situations

Given the complexity of assessing the personal data controller, many companies may find themselves in situations where it is unclear what role the company has in the processing of personal data, even after consulting the guidelines. In addition to the general recommendation to always make an assessment and document it, it may be appropriate to take external assistance, e.g. from the supervisory authorities. However, the issue of controllership is rarely in itself one that requires prior consultation with supervisory authorities under Article 36 of the GDPR.

Against this background, it is appropriate that the guidelines contain recommendations on what companies should do in such unclear situations when assessing personal liability.

3 Data Controller (section 2)

3.1 General comments

3.1.1 Explain how the concepts should be interpreted based on the purpose of the GDPR

According to the guidelines (p.14), the concept of controller, as also pointed out by the CJEU, must be interpreted on the basis of the underlying purpose of the GDPR and the right to the protection of personal data. It is therefore welcome that the guidelines are complemented by a detailed explanation of how such an interpretation may affect the meaning of the concepts, especially in unclear and complex cases.

3.1.2 Improve guidance on how to delimit ”processing"

Central to the identification of both data controllers and processors is the concept of "processing". As noted in the guidelines, the definition in Article 4(2) includes a wide array of

operations ranging from collection, storage and consultation to use, dissemination or otherwise making available and destruction. In practice, this means that all imaginable action of personal data constitutes processing" (our underline). In addition, according to the definition, a processing may include "any operation or set of operations".

The definition thus provides very little guidance on how a processing is separated from another processing. The processing of personal data in a cooperation between several companies may be divided into several smaller processing operations for which each company can be considered to determine the purpose and means.

Conversely, a number of a set of operations can be considered to constitute a single processing (processing chain), either with one or more common purposes, which may entail a common personal responsibility, or with separate purposes (which may be similar) which probably means that the companies involved are independent controllers – each for 'their' processing.

It is therefore desirable for the guidelines to give a clear account of how the EDPB sees the concept of 'processing' and how the different concepts used in the guidelines relate to each other. Concepts used in the guidelines include "specific processing activity"(p. 48), "specific data processing activity" (p. 24), "a single processing operation" (p. 40), "a set of operations" (p. 40), " the entirety of processing at issue"(p. 40), "a stage particular in the processing" (p. 40) and "chain of processing" (p 55).

An example of how some of these concepts are used is paragraph 40. *"As a result, the concept of a controller can be linked either to* a single processing *operation or to* a set *of operations. In practice, this may mean that the control exercised by a particular entity may extend to* the *entirety of processing* at issue but may also be limited *to* a particular stage in *the processing"* our underlinings.

A graphic illustration can be an appropriate tool for describing the relationships between processing (a operation or a set of operations) and purpose (see below), at least at an overall level.

3.1.3 Improve guidance on what constitutes a purpose

Just as a processing may be difficult to delimit from another processing, the appropriate demarcation of one purpose compared to another purpose may cause problems for the practitioner.

Article 5(1)(b) of the General Data Protection Regulation requires personal data to be collected for 'specific, explicit and legitimate ”purposes'. It should be noted that the Article 29 Group considered that the target description could be adapted to the context (see "Examples 1-4: How purposes are specified needs to be adapted to the context" in Annex 3 to Opinion 03/2013 on purpose limitation WP 203). In the same opinion, the Article 29 Group also considered that a purpose could be broken down into several sub-purposes (se "Example 11: Breaking down more general purposes into 'sub-purposes'" in Annex 3 to Opinion 03/2013 on purpose limitation WP 203).

It should therefore be possible, for example, to specify several sub-purposes and thus to allocate personal data responsibilities to several actors depending on who has an impact on

the purpose and the funds for each sub-purpose. It is also possible to influence the distribution of personal data responsibility through a relatively broad-based purpose.

There is therefore a great deal of flexibility in the way purposes are to be described, which leads to difficulties not only for the person who is to draw up a statement of purpose which meets the requirement referred to in Article 5(1)(b) but also for the person determining the personal responsibility.

The difficulties in determining controllership on the basis of the purpose are highlighted in the three examples listed on page 14, "Payroll administration", "Bank payments" and "Accountants". All actors in these examples are engaged by the customer, Employer A, and perform services at the customer's request, which is the person who provides the actors with the personal data. In all three cases, it is possible to formulate a purpose for the operators whereby they process personal data in order to perform each service. In the example of the bank, the purpose is stated as "performing banking activity" and the example of the auditor states the purpose as "auditing". What distinguishes them from the case of the payroll administrator? Neither the bank nor the auditor has a particular chance of deciding which personal data are to be processed, as this is largely due to the nature of the mandate and to some extent by the legislation applicable to their activities. One possible alternative explanation in these two examples is that the bank and the auditor have such roles that their personal data responsibilities result indirectly from legislation that applies to their activities. The purposes can then be said to be indirectly determined by the legislation (cf. p. 25).

In those circumstances, it is appropriate that the guidelines contain guidance on how to define and delimit the purpose, in particular in relation to another purpose.

3.2 Controllership by law

3.2.1 When the controller by law is not the entity who determines the purpose and means

The guidelines (p. 21) state the following concerning the possibility of specifying by law the criteria for controllership. "This presupposes that the legislator has designated as controller the entity that has a genuine ability to exercise control". It may be appropriate to clarify, in this connection, what is not the case, i.e. when the entity designated by law as a controller has no practical and legal means to influence the purposes and means of processing.

3.2.2 Explain the controllership of companies engaged by authorities for activities of general interest

A not uncommon situation is that authorities carrying out an activity for which "processing is necessary for the performance of a task carried out in the public interest" (Art. 6.1(e) of the General Data Protection Regulation) are using private companies as providers, e.g. to provide medical care or care for the elderly. Although these companies generally carry their own personal data responsibilities, uncertainties may arise in communication with the contracting authority, e.g. requiring feedback via an IT system provided by the Authority. It may be appropriate to explain how controllership should be allocated in such a situation through an example in the guidelines.

3.3 Control stemming from factual influence

3.3.1 Clarify the presumption of employer's controllership

The guidelines (p. 25) state that "In practice, certain processing activities can be considered as naturally attached to the role or activities of an entity ultimately entailing responsibilities from a data protection point of view".". Examples include employers. It should be made clear that this is a rebuttable presumption and that the starting point is the right of decision over the purposes and means set out in the facts and not that the role as such is decisive (cf. p. 26).

3.3.2 Explain the role of telecommunications service providers and other similar providers

Questions often arise about the role of telecommunications and other similar service providers in the area of personal data liability. The fact that they do not normally assume the role of controllers was previously demonstrated by the Data Protection Directive (recital 47 of the Data Protection Directive 95/46/EC, see also example 1 of Article 29 Working Group, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169). Instead, the questions have concerned whether such providers are data processors for their customers and whether it is therefore necessary to establish data processing agreements, or whether they are also not data processors (so-called third party under the GDPR).

As a general rule, providers of telecommunications services and other similar services should not be controllers or processors when they transmit information only on behalf of their customers even if information contains personal data. One reason given for such an interpretation is that suppliers are prohibited by law (with certain exceptions) from taking part of the content of the information. However, this argument can be used for an assessment that many other suppliers, such as those who only store information for their customers, are also not processors.

For this reason, it is appropriate for the guidelines to clarify the role of telecommunications and similar service providers when it comes to the controllership.

4 Joint controllership (section 3)

4.1.1 Too broad interpretation of CJEU's practice?

In the guidelines (p. 53), the EDPB has attempted to explain in general terms the CJEU practice of joint controllership. It is difficult to assess, but it appears that the EDPB is going further in its attempt to carve out a general rule than can be gleaned from CJEU practice. It is not excluded that, in the three cases of joint controllership assessed by the Court, the statements made by the Court of Justice have been justified by ensuring that the persons concerned 'the effective and comprehensive protection' (see, for example, C-40/17 p. 70) were justified under the special conditions available in the three cases.

It is, of course, welcome that the EDPB sets out its interpretation of CJEU's practices and makes an attempt to create a more comprehensible definition of joint controllership. However, an increased scope for shared personal data responsibility creates ambiguities for all those involved. That not only makes it difficult for companies to understand and limit their responsibilities – especially in situations like the one that were featured in the Fashion ID

case. In addition, identifying the data subject or persons responsible for the processing of their personal data may cause difficulties for data subjects.

Against this background, the EDPB should consider whether the description of joint controllership in so-called converting decisions is too wide and possibly limit the situations in which a common controllership may arise. For example, there may be a requirement that there be a clear common intention on the part of the parties involved.

5 Data processors (section 4)

5.1.1 Clearify that it does not constitute an infringement of Article 28(10) when a processor performs own processing under agreements in contracts

Article 28.10 of the GDPR states that "... if a processor infringes this Regulation by determining the purposes and means of processing ...". The guidelines (p. 79, 114 and 146) refer to the provision.

A common situation in cloud services contracts, for example, is that the provider – who mainly acts as a data processor for its customers – reserves the right to process personal data for certain purposes for its own purposes. Such an agreement usually involves the transfer of personal data from an independent data controller to another independent data controller. The customer who discloses the personal data must assess how such disclosure is compatible with the General Data Protection Regulation

It should therefore be clarified in the Guidelines that such processing by the processor does not constitute an infringement of the GDPR and that in such cases the processor does not process personal data contrary to the instructions of the controller.

5.1.2 Improve guidance on how data controllers can verify that data processors provide "sufficient guarantees" under Article 28(1)

The GDPR places a great deal of responsibility on a company that is to hire a data processor. According to Article 28.1, "the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."." This involves complex assessments, especially if it is a larger supplier. In addition, the assessment of sufficient guarantees must be made not only when hiring the assistant but also on a regular basis (p. 97).

The guidelines (p. 93) state that this obligation usually "will require an exchange of relevant documentation(e.g. privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external audits, recognized international certifications, like ISO 27000 series)." However, it does not specify how the checks are to be carried out on those documents or the rest of the verification.

Against this background, guidance on how to carry out this review in a practical manner is to be welcomed.

5.1.3 Clarify what is included in the "sufficient guarantees" referred to in Article 28(1)

The guidelines (p. 93) state that "The guarantees "provided" by the processor are actually those that the processor is able to demonstrate to the satisfaction of the controller, as those are the only ones that can effectively be taken into account by the controller when assessing compliance with its bonds. "We're going

It is appropriate to clarify in the Guidelines how this obligation relates to risks arising from transfers to third countries, in particular the risk of personal data processor being forced, under foreign law and in breach of the GDPR, to disclose personal data to third-country authorities. Does Article 28(1) mean that the processor must be able to provide sufficient guarantees that disclosure to foreign authorities does not take place in breach of the Data Protection Regulation?

6 The relationship between controllers and processors

6.1.1 Difficulties in negotiating processer agreements with large suppliers

It is often difficult to negotiate assistant agreements with major suppliers who are required to act as data processors, especially if the customer is a smaller company. In addition, the conditions of the suppliers are often very extensive and complicated, which makes it difficult to ensure that the supplier meets all the requirements to be imposed on a data processor.

The guidelines (p. 107) state "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 bonds. 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."

It is appropriate that the guidelines contain recommendations on how a smaller company should deal with situations where they have to negotiate with large suppliers providing standardised assistance agreements. Furthermore, it may be appropriate to explain what the consequences will be if, in such a situation, the assistance agreements do not comply with the requirements of the General Data Protection Regulation.

7 Missing part

7.1.1 Further guidance on the relationship between two independent controllers is lacking

The guidelines contain guidance in Part II on the relationship between the controller and the data processor and between the joint controller. On the other hand, there is no guidance for the transfer of personal data between two or more independent controllers. This includes guidance on the conditions under which such transfers are to be considered as complying with the requirements of the GDPR, e.g. what the principle of legality and the principle of purpose limitation mean for the assessments of data controllers in the disclosure or receipt of personal data. Furthermore, it is necessary to clarify the form of duty of inquiry applicable

to the assessment of the planned further processing of the recipient controller and the assessment of the previous processing carried out by the disclosure controller.

***