Baker McKenzie.

Hot Topics

Data & Technology
Europe

September 2020

Guidelines on the concepts of controller, processor and joint controller and on content of data processing agreements

The European Data Protection Board ("EDPB") has published draft guidelines on the concepts of controller and processor in the GDPR ("Guidelines"). They replace the previous guidelines on the concepts of controllers and processors which the Art. 29 Working Party, i.e. basically the EDPB's predecessor, had published in 2010. The Guidelines are open for public consultation until October 19, 2020, after which the final version will be issued.

In its comprehensive Guidelines (45 pages), the EDPB not only provides guidance on the concepts of controllers, processors and joint controllers, but also long-anticipated guidance on data processing agreements pursuant to Art. 28 GDPR. We have summarized the key aspects of the Guidelines below:

Summary:

- The criteria leading to the qualification as a controller or a processor have remained unchanged considering the guidelines of the Art. 29 Working Party on controller and processor under the previous EU Data Protection Directive.
- For data processing agreements, it shall not be sufficient to recap the obligations in Art. 28 GDPR. Rather, the data processing agreement shall specify the obligations and the procedures between the controller and the processor to comply with those obligations. We, therefore, recommend reviewing any existing data processing agreements as well as templates and determining whether they should be updated in light of the Guidelines (at least once the Guidelines are final).
- The EDPB provides further guidance on the criteria leading to a joint controllership, in particular: (a) the fact that one of the parties does not have access to personal data processed is not sufficient to exclude joint controllership, (b) joint responsibility does not necessarily imply equal responsibility of the various operators involved, and (c) joint controllership does not necessarily mean that entities need to have the same purpose, but that purposes which are closely linked or complementary may be sufficient.
- The Guidelines indicate that situations that so far have been qualified as a controller to processor relationship may now be qualified as joint controller relationships. Companies should consider whether certain controller-processor set-ups should be re-qualified and implemented as joint controller relationships, in particular in light of existing case law by the Court of Justice of the European Union relating to certain website tools and sharing of website user data and other explicit examples provided by the EDPB in the Guidelines.

Our Expertise
Data & Technology

In detail:

1. Concepts of controller, joint controller and processor

As a general observation, the EDPB states that the concepts of controller and processor have not changed and that the criteria for how to attribute the different roles remain the same. They reiterate that the legal status must be determined by its actual activities, rather than the formal designation, e.g. in a contract. The EDPB states that the qualification as a controller or processor has to be assessed with regard to each specific data processing activity and explicitly confirms that the same entity may act at the same time as a controller for certain processing operations and as a processor for others. This may be helpful for determining the role of headquarters of a group of companies which often store HR data as processors for their group companies, but also act as controllers for certain global HR management activities.

2. Concept of controller

With regard to controllers, the EDPB clarifies in particular the following:

- If a company appoints a specific person responsible for compliance with data protection rules, this person will not be the controller, but acts on behalf of the company and the company will ultimately be responsible in case of violations.
- With regard to the part of the controller definition concerning "purposes and means", the EDPB reiterates that the decisions on the purpose must always be done by the controller, whereas regarding the determination of the means, a distinction can be made between essential and non-essential means. Examples of essential means, which are reserved to the controller, are the type of personal data which are processed, the duration of the processing, the categories of recipients and categories of data subjects. Non-essential means shall be practical aspects of the implementation, such as the choice for a particular type of hard- or software. This may be relevant for service providers that provide standardized tools.
- The EDPB states that *"it is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller"*. Thus, even if an entity does not have access to the personal data, such entity may still qualify as controller if it decides on the purposes and essential means of their processing.

3. Concept of joint controller

With regard to joint controllers, the most significant aspects of the Guidelines are in our opinion the following:

- According to the EDPB, joint participation cannot only take the form of common decisions taken by two or more entities. It can also result from converging decisions which have a tangible impact on determining the purposes and means of processing, where the processing would not be possible without both parties' participation in the sense that the processing by each party is inextricably linked.

- By citing various decisions of the Court of Justice of the European Union regarding joint controllers, the EDPB states inter alia that (a) the fact that one of the parties does not have access to personal data processed is not sufficient to exclude joint controllership, (b) joint responsibility does not necessarily imply equal responsibility of the various operators involved, and (c) joint controllership does not necessarily mean that entities need to have the same purpose, but that purposes which are closely linked or complementary may be sufficient.
- A key question in this context is the differentiation between processor and controller. The EDPB emphasizes that the use of a system or infrastructure by two or more parties will not in all cases lead to joint controllership, in particular if the provider of the system or infrastructure does not pursue any own purposes (with the exception of being paid for the services rendered). However, for any platforms and standardized tools it must be assessed carefully whether the parties may qualify as joint controllers.

4. Concept of processor

With regard to processors the Guidelines include, inter alia, the following:

- According to the EDPB one of the basic conditions for qualifying as a processor is being a separate entity in relation to the controller, i.e., a department within a company cannot generally be a processor to another department within the same entity. Since the EDPB requires a separate entity, although not addressed expressly in the Guidelines, this implies that a branch and the head office do not have to conclude a data processing agreement if one of them processes personal data for the other, since they are the same legal entity.
- The EDPB states that the lawfulness of the processing according to Art. 6 and, if relevant, Art. 9 GDPR, will be derived from the controller's activity.

5. Data processing agreements

Before the EDPB comments on each of the requirements set out by Art. 28 GDPR regarding the content of a data processing agreement, the EDPB makes some general statements:

- In contrast to the data protection law pre-GDPR, the GDPR imposes direct obligations on processors, e.g. Art. 30 (2), 33 (2) GDPR. Both, controller and processor shall be responsible for having an appropriate data processing agreement in place. It emphasizes that processors can also be subject to administrative fines under the GDPR.
- Regarding any amendments to the data processing agreement, the EDPB is of the opinion that they must be notified to and approved by the controller - the mere publication of these modifications on the processor's website is not compliant with Art. 28 GDPR. In our opinion this leaves room to argue that mechanisms according to which the controller's failure to object within a set time period (which, for example, is under certain circumstances permissible under German, English, Polish and Italian contract law) can be interpreted as an approval.

- The EDPB states that data processing agreements should not merely restate the provisions of the GDPR. Additional details, e.g. on a procedure to give instructions or to report a security breach should - according to the EDPB - be set out in Annexes.

Regarding the individual requirements set out in Art. 28 (3) GDPR, the Guidelines state, inter alia, the following:

- The EDPB recommends documenting technical and organizational measures in the data processing agreement or other legally binding instrument. This recommendation is not surprising for some EU countries (in Germany and Italy, the pre-GDPR privacy laws and guidance from national privacy authorities already required to set out the technical and organizational measures in the data processing agreement between the controller and the processor) and it has been best practice to document the technical and organizational measures in writing. According to the EDPB, the data processing agreement should also include an obligation on the processor to obtain the controller's approval before making changes and a regular review of the security measures.
- Regarding the engagement of subprocessors, the EDPB recommends that the data processing agreement should set out a process for changing a subprocessor, in particular by actively informing the controller of any changes. Furthermore, the EDPB provides guidance on how to obtain the approval of the controller for the new subprocessor.

6. Joint controller's arrangements

According to the EDPB:

- The joint controller arrangement should specify the allocation of responsibilities between the controllers and cover other general data protection obligations, such as compliance with general data protection principles, requirement for a legal basis, security measures, and data breach notification obligation.
- The joint controller arrangement shall be made in the form of a binding document such as a contract or other legal binding act.
- Each joint controller has the duty to ensure that it has a legal basis for the processing.

Hot Topics

For further questions don't hesitate to contact our specialists:

Dr. Michaela Nebel
Frankfurt
michaela.nebel@bakermckenzie.com

Julia Kaufmann, LL.M.
Munich
julia.kaufmann@bakermckenzie.com

Francesca Rubina Gaudino
Milan
francesca.gaudino@bakermckenzie.com

Magdalena Kogut-Czarkowska
Warsaw
Magdalena.Kogut-Czarkowska@bakermckenzie.com

Benjamin Slinn
London
Benjamin.Slinn@bakermckenzie.com

Joanna de Fonseka
London
Joanna.deFonseka@bakermckenzie.com

Dr. Lukas Feiler
Vienna
Lukas.Feiler@bakermckenzie.com

Elisabeth Dehareng
Brussels
Elisabeth.Dehareng@bakermckenzie.com

Prof. Dr. Michael Schmidl, LL.M
Munich
michael.schmidl@bakermckenzie.com

Dr. Holger Lutz, LL.M
Frankfurt
holger.lutz@bakermckenzie.com

Florian Tannen
Munich
florian.tannen@bakermckenzie.coma

Baker & McKenzie - Partnerschaft von Rechtsanwälten und Steuerberatern mbB

Berlin
Friedrichstrasse 88/Unter den Linden
10117 Berlin
Tel.: +49 30 2 20 02 81 0
Fax: +49 30 2 20 02 81 199

Frankfurt am Main
Bethmannstrasse 50-54
60311 Frankfurt / Main
Tel.: +49 69 2 99 08 0
Fax: +49 69 2 99 08 108

Dusseldorf
Neuer Zollhof 2
40221 Dusseldorf
Tel.: +49 211 3 11 16 0
Fax: +49 211 3 11 16 199

Munich
Theatinerstrasse 23
80333 Munich
Tel.: +49 89 5 52 38 0
Fax: +49 89 5 52 38 199

www.bakermckenzie.com

Get Connected: