Bonn, Bucharest, Dublin, Lisbon, Madrid, Milan, Paris, The Hague, Vienna, Warsaw

CEDPO comments on

Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 1.0)

The Confederation of Data Protection Organisations welcomes the revision of WP 169 on the concepts of "controller" and "processor". The paper offers practical guidance on the differentiation between the concepts by including many examples from common business processes delegated to third parties. Furthermore, the remarks on the contractual clauses between controllers and processors clearly distinguish between mandatory and optional clauses giving the parties the opportunity to reflect their individual requirements.

In light of the above, CEDPO wants to share the following observations with the EDPB:

A. General remarks

I. Joint controllership

A ‘broad’ interpretation of joint controllership is incorrect and harmful. Joint controllership situations should be exceptional because it is a reality that the parties rarely determine jointly

specific purposes and means of the processing and liability should be allocated to a party due to actions that are actually under its actual control and, thus, which could be agreed contractually.

- **Compatible purposes are not joint purposes.** It is obvious that by the mere fact of the existence of an agreement, of any nature, they are converging decisions, because otherwise, there is no agreement. In particular, in any commercial agreement, these decisions are precisely converging because either party finds its own commercial interest addressed. This does not mean that they have the same processing purposes but that the contractual arrangements make commercial sense for each of them for compatible reasons. And the existence of these compatible commercial purposes happens in any agreement between a controller and a processor, separate controllers and joint controllers. Therefore, the existence of converging decisions or commercial purposes is absolutely inappropriate to determine a joint controllership situation.

- **Specific purposes rather than "commercial purposes".** In particular, a lack of specificity of the processing purposes and a lack of attention to the actual control on the personal data for these specific purposes would lead to a harmful proliferation of artificial "joint controllership" situations which, in addition to being incorrect, neither benefits the actual protection of the individuals nor the development of trade.

- In particular, it should be recognized that the determination of the purposes of the data processing is the key element to identify who is acting as controller and should be specific. A broad definition of purposes, e.g. "commercial purposes" lead to a situation where every company (being it separate or joint controllers or controllers and processors) entering in an agreement would be qualified as joint controllers. Being specific in identifying the specific purposes of the processing is key to clarify roles of all the actors involved.

II. Controllership

- **Natural persons acting as controllers.** Guidance on the status of a controller usually takes into account the legal entity controllers. Aligning natural persons controllers with

legal persons controllers - as intended by the GDPR - needs further clarifications and clarifying examples from supervisory authorities in order to foster a better application of the law. Therefore, CEDPO would welcome concrete guidance as to what extent the natural persons controllers should be bind to their obligations as a controller, especially regarding the data subject rights (e.g. providing within the contact details the address of their establishment, which is also their home address), keeping the records of processing activities according to Art. 30 GDPR (paragraph 5 of Art. 30 provides derogations for an 'enterprise' or an 'organisation' employing fewer than 250 persons which might lead to misinterpretation by natural persons controllers), implementing organisational measures to ensure a level of security when processing personal data (especially concerning organisational measures such as staff training for family members) etc.

- **Actual control on the data.** In order to be considered as controller, a real level of control need to be exercised over the data by the entity concerned. This is supported by the jurisprudence of the CJEU which argues that real and decisive influence needs to be exercised on the processing to qualify as controller. This will also help ensure that joint controllership is not identified artificially. On the one hand, the lack of physical control of the data per se does not automatically exclude any controllership situation. On the other hand, the level of actual influence of how the data are processed and how the rights of the data subjects are addressed does not have (as it should) have an impact on evaluation of a controllership situation.
  In a recent case, a DPA has considered an association that has created a mechanism of notice and choice that is actually implemented voluntarily by its members a joint controller. This is unacceptable, in particular, because the members are the only ones collecting the data and determining their own processing purposes. This kind of reasoning will undermine, among others, any efforts towards Codes of Conduct or GDPR certifications.

- **Data subject requests.** For the data subject to have a single point of contact where his/her request will actually be addressed is the best way to ensure effective protection. In any event, if the reason to have a single point of contact in one controller is only because the other alleged "joint" controller is actually unable to access the data or identify the data subject (because the data are anonymous or pseudonymised) or to address the request itself (e.g., data cannot be deleted because it does not have

access to the data or is technically impossible) may be a solid indication that this second controller is actually not a joint controller for the same processing purposes.

III. Controller-processor relationship

- **Processing contracts are not and should not be a detailed instruction manual. What is essential for the parties is what is described.** A contract is not a manual of instructions of any service: the level of detail regarding the description of the service and the processor's duties will depend on different factors: how critic this service is for the data controller, how customised or not the service is, the contract duration and its price, the sensitivity of the data processed, the likelihood and seriousness of the risks associated to the processing of this data, who is in charge of the access control, etc.

  What is an "essential" means of processing is dependent on whether the relevant duty is key for the controller's compliance programme and/or what is key for the processor to assume the agreed levels of service (and KPIs) and, for both parties, to determine the price: this is what will determine that the contract is more specific in one aspect or another and that will vary in each contract (specific security measures in place, how to answer an access request or prohibition to do so, specific retention periods, etc.).
  The goal of the specificity in any contract is to facilitate the enforcement of a contractual duty and to control the degree of operational flexibility that any contract, in particular, long-term contracts, must have.

  Both parties shall be able to determine the level of detail of the processing services according to a risk-based approach and bear the consequences of the lack of specificity, all of which shall be construed according to the rules of contract law and not the GDPR.

- **Controllers cannot unilaterally change a contract.** One of the main reasons that should guide a controller to outsource a service involving the processing of personal data are the technical and security capabilities of the data processor. These capabilities are linked to a specific price and are not (and cannot be) determined by the controller unilaterally or changed at the request of the data controller without a previous

assessment of the technical and economic viability of the change at hand for the processor and the corresponding price adjustment.

- **Controllers' decision regarding data return and deletion.** In order for the processor be able to ensure that the data are returned or deleted is implemented according to the controller's choice, timely and within the scope of the agreed price, the parties should be able to agree when the controller must make a choice regarding the return / deletion (in any occasions, this could be made at the end of the agreement) and, if no choice is made by the controller by the agreed date, what should happen by default.

- **Sub-processors.** It should be possible for processors to notify controllers by updating a list of sub-processors via an internal portal, as the Article 29 Party did in the past regarding SCC for cloud computing services, or any other channel that ensures the controller's actual knowledge. Further, the requirement to include a list of sub-processors should be restricted to specific authorisations; in case of general authorisations, the controller's criteria to guide the processor's choice of sub-processors should suffice (e.g., member or not of the same corporate group, holder of a specific ISO or service license, adherence to a specific Code of Conduct, presence in a specific region, etc.).

- **Imbalanced controller-processor relationships.** CEDPO acknowledges that 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. Though, more practical guidance is needed - especially for small controllers – to what extent predefined and non-negotiable contractual clauses and technical-organizational measures by processors with a dominant position in the market will not undermine the status of a controllers-processor relationship. It would be beneficial, if the EDPB would provide main rules for dealing with dominant processors.

- **Controllers and processors assuming different roles.** The EDPB should clarify that in a contractual relationship, from a factual/practical perspective, the parties may have several qualities concerning a data processing (for example on one processing they may be joint controllers and on another processing they might be controller and

processor on the same contract), depending on the legal basis of the processing and the objective to be achieved with the processing.

B. Specific remarks on the Guidelines

PART I – CONCEPTS

2. DEFINITION OF CONTROLLER

2.1.4 “Purposes and means”

From a practical perspective, the differentiation between essential and non-essential means appropriately addresses the fact that processors usually build their own standardised infrastructure, therefore determining certain means of data processing. The example of the hosting services, where employer A hires hosting service H to store encrypted data on H’s servers, though might lead to an extensive interpretation of a “processor” according to Art. 28 GDPR. On the one hand, the example does not distinguish between a processing, where the processor has access to the decrypting key(s) and a processing, where there is no potential access to personal data due to state-of-the-art encryption using strong encryption keys, often referred as to a “black box” service.

On the other hand, the Article 29 Working Party itself was pointing to the fact, published in WP 136[1], that *[…]”Putting in place the appropriate state-of-the-art technical and organizational measures to protect the data against identification may make the difference to consider that the persons are not identifiable […].* CEDPO would welcome further clarification, in which cases a processing of encrypted data shall fall under Art. 28 GDPR.

4 DEFINITION OF PROCESSOR

When assessing, whether a third-party should be considered a data processor, Guidelines 07/2020 provide useful practical examples. They also address controversial processing activities such as troubleshooting of software or general IT support. In practice, controllers and processers often take different positions on the question, if such services require a data protection agreement according to Art. 28 GDPR. The EDPB stresses, that one of the questions

[1] Opinion 4/2007 on the concept of personal data (WP 136), p. 17.

which should be asked during the assessment, is, if the service provider actually has been instructed to process personal data. In many cases, contracts including software troubleshooting and IT service and support in general do not specifically address the processing of personal data. Processing such data is most likely a side effect of the instructions of the controller.

Guidelines 07/2020 therefore conclude in one of the examples that if an IT-consultant is *not* hired to process personal data, and Company ABC determines that any access to personal data will be purely *incidental* and therefore *very limited* in practice, an agreement according to Art. 28 GDPR is *not* required. For a better understanding between the scenario of a general IT support with access to a vast amount of data and software troubleshooting, even though both do not have the main objective of processing personal data, it would be helpful from the EDPB to clarify, i. how a systematic access to personal data has to be interpreted and ii. to what extent the amount of personal data accessible to processor can be taken into account.

PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES

1. RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR

1.3 Content of the contract or other legal act

1.3.8 The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR).

Guidelines 07/2020 stipulate the obligation of the contracting parties to include in the controller-processor agreement details on how often and how the flow of information between the processor and the controller should take place so that the controller is fully informed as to the details of the processing. Such agreements usually do not include clauses concerning technical details of flows of information. They usually cover important aspects of a processing, such

as changes to technical organisation measures or to sub-processors, giving the controller the opportunity to gain knowledge on core aspects of the data processing. It should be determined on a case-by-case basis, how general notification obligations between the parties are being followed through technical or organizational measures. Such rather practical considerations – which may change over time – shall *not* be a mandatory part of a data protection agreement. Besides, Art. 28 (3) GDPR already contains sufficient information to be included in a contract in order to facilitate a better understanding of the processing operations at the processor. Describing the general functioning of a system for example forms rather part of precontractual descriptions of a service of the service provider or the related SLA and therefore should be considered when choosing the appropriate data processor. Information on recipients of data should only be provided when relevant to the controller, especially concerning subcontractors. Third-party recipients for data from the data processor with no relevance to the service offered to controllers, cannot be considered mandatory information in this case.

1.6 Sub-processors

The concept of sub-processing is applicable in most cases of a controller-processor scenario. There are contractual templates available which exclude certain processing activities from the chain of subcontracting such as telecommunication service providers, external cleaning personnel or IT-service providers. It would be helpful if the EDPB would address this issue in the revised Guidelines. Criteria for a sub-processor could be the *intended processing* of personal data as well as the provision of services *with relevance* to the services offered by the processor towards and on behalf of its clients. In practice, there are often additional processors engaged which provide general services or support to the processor without to be considered as sub-processor in the sense of the GDPR. It makes a difference whether the sub-processes are to be used as general services or are explicit directed to the main services which are subject of the agreement between the controller and the processor. Excluding certain third parties from the chain of sub-processors shall not exempt the processor from agreeing on appropriate safeguards with the third party.

Concerning the involvement of sub-processors Article 28(2) GDPR stipulates that the processor shall not engage another processor without prior specific or general written authorisation of the controller. It remains unclear from Guidelines 07/2020 whether such authorization can also be provided in electronic form as foreseen in Art. 28 (9) GDPR when entering into a

contract or the other legal act referred to in paragraphs 3 and 4. CEDPO would welcome a clarification.

2. CONSEQUENCES OF JOINT CONTROLLERSHIP

2.3 Obligations towards data protection authorities

When stipulating an agreement as joint controllers, the parties should, inter alia, include a point of contact when communicating with data protection authorities. A single point of contact facilitates interacting with supervisory authorities and is considered beneficial for both sides. Paragraph 189 of Guidelines 07/2020 states though that *"data protection authorities are not bound by the terms if the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point.*" The parties of a joint controller relationship establish a single point of contact for good reasons. In many cases a controller is appointed as single point of contact which plays a pivotal role within the common undertaking, therefore having sufficient knowledge to respond to investigations from a supervisory authority. Giving the authorities the opportunity to choose any controller from the joint operations while ignoring the contractual stipulations will most likely will result in unnecessary administrative burden within the joint controller at the cost of the data subject. CEDPO would therefore welcome the clarification that supervisory authorities *should* follow contractual stipulations concerning a point of contact, whereas each party is still subject to the investigative powers according to Art. 58 GDPR.

23/10/2020

Contact information

Email: info@cedpo.eu / Website: www.cedpo.eu