Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

19 October 2020

Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Guidelines 7/2020 on the Concepts of Controller and Processor in the GDPR of 2 September 2020

On 2 September 2020, the European Data Protection Board (EDPB) issued its Draft Guidelines 7/2020 on the concepts of controller and processor in the GDPR (Guidelines).[1] The EDPB invited public comments on this document by 19 October 2020. The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to submit the comments and recommendations below as input for the final Guidelines.[3]

Comments

CIPL welcomes the EDPB's initiative to further explore the concepts of controller and processor in the GDPR as these are key building blocks of EU data protection law. The definition of controller or processor under the GDPR is of paramount importance for the rights of individuals and triggers different obligations and rights for the entities themselves.

CIPL welcomes the Guidelines' consistent interpretation of the concepts of controller and processor with the 2010 guidelines. This allows companies to continue operating in their current roles without significant disruption. CIPL also welcomes the inclusion of several examples as well as a flow chart. CIPL believes, however, that the interpretation currently proposed in the Guidelines may in some instances appear overly narrow, extend beyond the strict language of the GDPR, and is not aligned with current market practices. In particular, the Guidelines do not sufficiently take into account the following points:

- **The state of technology and business practices**—The Guidelines should account for the developments in technology, growing diversity of data uses and emergence of new business models that trigger more complex and dynamic relationships between organisations. This is the case in particular in the development, deployment and use of technologies, such as artificial intelligence (AI) and blockchain,[4] where the concepts of controller and processor may be challenging to transpose, especially when personal data is used to train an algorithmic model.

[1] Draft Guidelines 07/2020 on the concepts of controller and processor in the GDPR, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 85 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[3] These comments also include remarks that are relevant to the EDPB Draft Guidelines 8/2020 on the targeting of social medial users.

[4] The recommendations issued in the study commissioned by the Parliament on Blockchain and the GDPR are particularly useful in this respect (https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

- **The emergence of the data economy**—The Guidelines do not sufficiently reflect the increasing data sharing practices of all organisations (including public entities). The Guidelines focus mainly on controller to processor and joint controller relationships and overlook the independent controller to independent controller relationship where most data sharing occurs and will continue to increase. The COVID-19 crisis has highlighted the huge value of responsible data sharing between private and public actors to address the crisis. CIPL recommends the EDPB and the Data Protection Authorities (DPAs) work with organisations to develop a framework for accountable data sharing that complies with the GDPR.[5] This will provide a trustworthy framework to share data and contribute to the building of the EU data economy.

- **The need for flexible and future-proof Guidelines**—By the time the Guidelines are updated, more technological developments will have happened and new business models, actors and data uses in new contexts will have emerged. Therefore, CIPL recommends that the Guidelines preferably rely on rebuttable criteria (or rebuttable presumptions) that may lead to classification as a controller, processor, joint or independent controllers, rather than making firm and definitive classifications. CIPL highlights that these classifications bear consequences for organisations that will have to reflect them in their contractual terms with clients or to flow down some of these obligations to processors or sub-processors. As a consequence, any criterion should not be assessed in isolation, but in relation to its specific processing context, together with other criteria. This approach will better accommodate the variety and complexity of current and future data uses and business relationships.

- **The changing nature of organisations' roles**—The Guidelines must acknowledge that the same parties may have different roles in respect of the same pool of personal data in the context of different processing operations. An organization may receive data from a controller and may act as its processor with respect of certain processing operations but may also act as a controller with respect to the same data but for different processing operations. A (joint) controller might also decide to use the data for another/additional purpose besides the joint purposes.[6] Using the same data both for a joint purpose and for another purpose should be acceptable provided that there is an appropriate legal basis for both uses. This may be the case, for example, were a payment service provider processes transactions (authorisation, clearing, settlement activities) as a processor and relies on the same data to match a qualifying transaction to a loyalty offer, acting as a joint controller in the context of a card-linked loyalty scheme that a cardholder has subscribed to.

- **The reality of commercial relationships–**The Guidelines should refrain from requiring excessive formalism in all situations. It may not actually be feasible that the data processing terms be always negotiated by both parties. Some companies may decide to purchase a product or service based

[5] See CIPL's response to the EU Commission consultation on GDPR evaluation and the data economy. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_eu_commission_consultation_on_gdpr_evaluation__28_april_2020_.pdf

[6] 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.

on conditions and terms offered for a given price (and may not be in a position to enter into lengthy and costly negotiations on contractual terms), as long as these terms comply with the requirements of the GDPR. This may be the case for smaller companies or SMEs who simply do not have the resources to do so, but also for any company choosing not to allocate resources when the service or product they purchase is not essential to their core business activities. CIPL stresses that an overly legalistic approach may put controllers (and in particular SMEs and smaller organisations) in difficult situations while not bringing added value to the protection of individuals.

- **Joint controllership should not be a "by-default" solution**—As per the case law of the CJEU, joint controllership requires a real and decisive influence on the processing by the organisation. The scope of joint controllership should not extend beyond these specific and strictly defined situations to apply to any situation where several organisations access the same databases or systems processing personal data. This would run the risk of leading to a mesh of actors and responsibilities that complicates collaborative business models and is built on the wrong assumption that increasing the number of responsible parties would increase the protection of individuals.

- **The existence of the third-party concept in the GDPR**–Article 4(10) GDPR as well as recitals 47 and 69 recognize the concept of a third party that is neither a controller nor a processor but a natural or legal person, public authority, agency or body with an interest in the processing. The Guidelines should seek to preserve that concept and avoid an overly broad interpretation of the concepts of controller and processor that would simply eliminate its existence.

- **The important role of certifications and codes of conducts**—Organisations tend to spend a significant amount of time properly identifying their roles under the GDPR, responding to due diligence privacy questionnaires, negotiating data processing agreements and requesting increased supply chain transparency based on their own interpretations of the GDPR. CIPL believes that the upcoming certifications and codes of conduct will help simplify and streamline the relationships between different actors of the ecosystem for better efficiency. CIPL underlines that the current ISO 27701 certification classifies the role of the organisation as controller or processor and would welcome a consistent approach with this internationally recognised standard.

1. Definition of Controller and Processor

Terminology–The Guidelines refer to several criteria to characterise controllership, such as "decision making," "actually exerting influence" and "complete autonomy." These correspond to different situations in practice and are based on specific contexts. For instance, having influence is different from having complete autonomy and may lead to different classifications. The Guidelines also imply controllers must be processing data for their own purposes. However, determination of purpose by an organisation does not necessarily equate to processing for this same organisation's own purpose. At the same time, in some situations, the controller may not always have "complete autonomy" to determine the purposes of the processing, but only exerts determinative influence on the purposes of processing. The Guidelines should therefore recognize that there may be varying manners in how decisions are being made on the data processing and that this may not be a determinative criterion for controllership *per se*. For instance, a payment network acting as a processor may issue certain mandatory requirements related to the data processing (e.g., a requirement to keep card details up-to-date), which may be seen as "defining purposes." However, in this case, the purposes are defined for the benefit of the broader financial ecosystem (banks and cardholders) rather than the network itself.

Functional role versus legal classification—Paragraph 12 of the Guidelines provide that the concepts of controller and processor are *functional* concepts, aiming to allocate responsibilities according to the actual roles of the parties, rather according to their formal designation in a contract. CIPL underlines that the notion of *functional* concept also implies that the role of a party may change over time if the nature of its processing responsibilities change. A party that is initially a processor may become a controller or a joint controller. It also means that one party can also be simultaneously involved in processing operations of a different nature, thus being at the same time controller and processor for each of the different operations. For instance, if an organization uses an HR tool for talent acquisition and management and enables its subsidiaries to use such tool, such use may create controller to processor relationship or a joint controllership, depending on the circumstances. At the same time, the organization may decide (based on an appropriate legal basis) to use the entire pool of data collected from its subsidiaries to create a program enhancing diversity and inclusion across the group. The subsidiaries initially acting as controllers do not have access to the entire pool of data and do not decide on the purposes and means of such processing. These situations are also frequent in the context if AI where an organization acts as a processor on the instructions of a controller to design and build an AI application for specific purposes. Subsequently, based on the appropriate legal basis and subject to appropriate data sharing arrangements, the processor becomes a controller that is accountable for processing the data set for an AI project encompassing additional data sets.

Consequences of controllership—Paragraph 14 of the Guidelines interprets the notion of controller broadly to ensure accountability and the effective and comprehensive protection of personal data. While CIPL agrees that the controller plays a pivotal role in protecting the rights of individuals, an overly broad interpretation would reflect neither the GDPR categories of processor and third-party nor the state of current market practices and could create confusion, particularly where one controller is located outside of the EEA. In addition to creating rights for individuals, the classification of controller also conveys rights on the controller, such as the possibility to claim a legal basis for the processing of that data. Depending on the relevant legal basis, the controller can also process personal data even against the data subject's will (compliance with a legal obligation, legitimate interest, public interest, vital interest, defense of a legal claim). Individuals may also find it more difficult to exercise their rights with a controller with whom they have no direct relationship, not only as a result of increased difficulty in objecting to processing, but also because of the complexity in claiming compensation. For example, the company with whom the individual has a direct relationship may defend against the claim on the basis that the secondary controller is responsible and that the company is "not in any way responsible for the event giving rise to the damage," or the individual may face difficulty in establishing a tort claim against a secondary controller, particularly if that controller is based in another jurisdiction.

Legal obligation to provide data and controllership—Paragraph 22 of the Guidelines seems to link the legal obligation to retain or provide data and controllership. CIPL notes that in certain situations (for instance criminal or tax law), a processor may be legally compelled to disclose data to the authorities that it processes on behalf of a controller. Although processors generally try to have the request directed to the controller itself, this may not always be possible under applicable law. When the processor is left with no choice but to provide the data as per applicable law (and sometimes not authorised to inform the controller), it should not become a controller for all the processing activities as a result and bear all corresponding obligations, but rather should only assume responsibility with respect to the disclosure. CIPL recommends the EDPB provide for a specific exception in this case.

Core and ancillary data processing purpose—CIPL highlights that it is paramount that the Guidelines keep a "functional aim" to classify the parties as controller or processor according to their actual role in defining the purposes and means of the processing of personal data. This would avoid having controllership apply to situations where it was not originally intended to apply in particular where the processing of personal data is just a side-effect of an entity's primary activity. The Guidelines should stress that there needs to be an inherent relationship between the determined purpose and the personal data that is being processed to avoid that every activity meets the requirement of controllership under Article 4(7). For instance, a waste collection company will have to process personal data when collecting and then destroying or storing waste, but by pursuing the purpose of waste collection it does not as such pursue a purpose as controller under Article 4(7) GDPR. Similarly, a company that refurbishes used processing hardware to resell it routinely wipes all storage in that hardware as part of the refurbishing process does not as such pursue a purpose as controller under Article 4(7) GDPR. Even a processor pursues a purpose with the processing of personal data, namely to make a profit charging for the processing services, but does not as such fall under Article 4(7).

Choice of processor - standardized services—Paragraph 28 of the Guidelines provides that a processor may offer a standardized service and expects the controller to "actively approve the way the processing is carried out and to be able to request changes if necessary." CIPL highlights that standardized services cannot generally be customized and controllers may actually not have the necessary technical expertise or market power to request changes. The Guidelines should clarify that if a controller accepts the service without the possibility of making the changes, it does not turn the processor into a controller.

Processor's changes to the services–Paragraph 28 of the Guidelines provides that "the processor cannot at a later stage change the essential elements of the processing without the approval of the controller." This statement should be nuanced to account for instances in which the processor modifies a product or service to improve it over time by adding new features, for example. The Guidelines should also recognize that contracts generally provide that the processor cannot unilaterally decide to change the essential elements of its service and mandate prior notice and/or authorisation from the controller, including the possibility for the controller to terminate the contract. CIPL recommends that the concept of "essential elements of the processing" be directly linked to the changes of the service that would require an amendment to the contract.

Essential versus non-essential means—Paragraph 38 of the Guidelines provides examples of decisions made on essential means[7] that would help identify a controller (such as, for instance, type of personal data, duration of the processing, categories of recipients, categories of data subjects) versus decisions

[7] The Guidelines appear to conflate "purposes" with "essential means." For example, a decision on whose personal data are being processed (i.e., to whom the service is being offered - B2B or B2C, consumers or employees) is essential for determining the purpose of the service rather than defining the means of the processing.

made on non-essential means that would help identify a processor (such as choice for a particular type of hard- or software or detailed security measures). This distinction may not reflect the reality of the operations of large scale service providers. In reality, most hosting providers will offer standard security measures and the controller will have little influence over them. Security measures and retention periods are often off the shelf elements of a service and are made clear to the controller before choosing to use the service. Yet the controller ultimately decides to use that system and that decision includes relying on all the standardized aspects of that system that the controller deems appropriate for the purposes of the processing, the nature of the personal and more generally the risks of the processing.[8] Financial service providers, for example, may need to define or specify data elements needed for the service in order to comply with financial standards. Enterprise communication services (phones, email, videoconferencing, text messaging, etc.) are also standardized due to underlying technical standards and many required data fields are pre-set and offer very little room for customization. The organisation who decides to use these services for internal communication and communication with customers, will still have to be regarded as a controller. The same reasoning applies to online advertising products and tools that allow for customization of marketing efforts based on audience segments from email lists. These products are standardised in many ways and it is the targeter who decides who must be shown what ads, on the basis of matched email addresses (i.e. with no other profiling criteria being used by the social media provider). The targeter (not the social media provider) determines the purpose and "essential means" of the processing. CIPL recommends clarifying that there is a level of flexibility in determining what are essential versus non-essential means.

Information about the means of processing–Paragraph 39 of the Guidelines provides that the controller needs to be fully informed about the means that are used for the processing in order to make an informed decision in this regard. However, CIPL notes that providing full transparency may reveal a processor's commercially sensitive information as well as weaken its security. This could affect not only this particular controller but also other clients as well as the data processor itself. CIPL recommends that the level of detail on the means of processing to be disclosed by the processor be balanced with these other crucial considerations. CIPL underlines also the important role that certifications and codes of conduct may play in this context by providing assurances to the controller that the processor meets certain standards without having to review itself the means used by the processor.

Lack of access to processed data–Paragraph 42 of the Guidelines provides that an organisation may be classified as a controller without actually accessing the data being processed. CIPL highlights that likewise in the supply chain some processors never have access to the controller's data and do not consider themselves as processors under the GDPR. CIPL would welcome clarification on these situations.

Variety of processor activities–Paragraph 73 of the Guidelines provides 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. In order to reflect certain nuances of the role of a data processor in practice, CIPL would also recommend adding that a controller might also decide to separately instruct two distinct processors to

[8] Providers of SaaS products often predetermine the types of personal data that they can process by specifying for instance, that the product is not aimed at processing special categories of data, such as health data. Such specifications should not turn the SaaS provider into a data controller.

share data among each other.

Processor becoming a controller—Paragraph 79 of the Guidelines provides that a processor that goes beyond the instructions of the controller and starts to determine its own purposes and means of processing will be considered to be a controller and could be subject to sanctions. CIPL believes that the Guidelines should make clear that the requirement for the processor to process data "on instructions" from the controller be interpreted broadly. In addition, the Guidelines should distinguish between: (a) processing that is outside of the controller's instructions, but does not constitute determination of purposes and means, and does not turn the processor into a controller, such as for instance upgrading infrastructure to improve reliability, resilience or security of the service; (b) processing that amounts to determining the purpose and means, but that is done in compliance with the GDPR, in respect of which the processor becomes a controller; and (c) processing that amounts to determining the process and means, in respect of which the processor becomes a controller, but that is not done in compliance with the GDPR, such as reusing a direct marketing list provided by another company for their own purposes.

Law firms–The example on page 12 of the Guidelines recognises that when hired to represent a company in a dispute, law firms act as data controllers because they act with a significant degree of independence when deciding what information to use and how to use it. This example may not capture the variety of processing operations that law firms may perform in practice. There may be specific cases where a law firm may act as a data processor if it is retained to perform specific tasks involving the processing of personal data on behalf of the company.

Cloud service provider–The example on page 27 of the Guidelines may not capture all the processing operations of the cloud service provider in practice. It provides that personal data should be processed for the client's purposes only. But the service provider may also process certain personal data for example, to anonymise data for analytics purposes, to perform cognitive and predictive analytics, to assess the efficiency of the service provider's delivery automation data or to improve its services). In addition, depending on customised features of the specific service and its level of standardisation, the obligation to respect the client's specific instructions regarding storage periods or deletion of data may not be achievable in practice. This example should therefore be nuanced and adapted to take into account the level of standardisation of the service.

Summary of CIPL Recommendations:

- Acknowledge that there are several ways decisions are made on the processing of data and such decisions may not be determinative criteria of controllership *per se*

- Acknowledge that the same organisations may have different roles

- Refrain from an overly broad and extensive interpretation of controllership

- Provide that a processor under a legal obligation to provide data does not become a controller

- Recognize that there needs to be an inherent relationship between the determined purpose and the personal data processed to trigger controllership

- Clarify that if a controller accepts the service without the possibility of making the changes, it does not turn the processor into a controller

- Link the concept of "essential elements of the processing" to the changes of the service that would require an amendment to the contract

- Clarify that there is a level of flexibility in determining what essential versus non-essential means

- Balance the level of detail on the means of processing to be disclosed by the processor with security and trade secret considerations

- Provide clarification on the status of organisations that do not have access to the processed data

- Clearly identify the situations where a processor acting outside of the instructions of the controller can become a controller

- Provide more nuanced examples that take into account the variety of situations

2. Definition of Joint Controller

Converging decisions and joint controllership—Paragraph 53 of the Guidelines provides that joint controller situations should be distinguished from controller to processor situations where the latter does not process the data for its own purposes but carries out the processing on behalf of the controller. It underlines that "converging decisions" by two entities that "complement each other" and have a "tangible impact" on the determination of the purposes and means of the processing may be an indicator of joint controllership. CIPL underlines that all or part of these elements are inherent to any commercial relationship. As a matter of fact, a controller and processor working together will more likely than not have common/converging business interests and a close relationship that will have an impact on the way the processing is carried out. As a result, the processor may be routinely involved in determining the means of the processing. However, the processor does not pursue any purpose(s) of its own in relation to the processing activity, but is merely acting on the instructions of the controller and being paid for services rendered. In addition, if data processing purposes are broadly qualified as "commercial purposes," almost every organisation entering into a commercial relationship would erroneously be deemed a joint controller. It is obvious that when two or more organisations enter into a relationship, their purposes are by definition commercial as well as compatible/complementary. This does not, however determine the (joint) controllership or a processor's role. For example, in the situation where a controller uses a data lake platform and relies on the recommendations of the provider to implement the platform in its data landscape and to adjust privacy by design settings, the platform is engaged in a collaborative relation but it would not become a joint controller. In order to make a determination as to whether several controllers are joint or independent controllers or processors, it is indispensable that the definition of the data processing purposes under the control of each organisation is specific. CIPL calls for better clarity in distinguishing joint controllership from controller/processor and independent controller relationships. The "converging decision" and "commercial purposes" criteria are far from being a decisive factor of joint controllership, but rather an indication.

Inseparability of the parties—Similarly, paragraph 53 of the Guidelines provides that in joint controllership situations, the processing would not be possible without both parties' participation, i.e., the processing by each party is "inseparable" from the other party's processing activity. CIPL believes this criterion is potentially unlimited and therefore unreliable. There are numerous scenarios where two independent controllers work together in an inseparable and inextricable manner (whether they process the same data set or whether the processing of one controller is indispensable to the processing of the other controller) and do not become joint controllers but remain separate controllers. For instance, when the individual joins two independent controllers, e.g., by enabling controller A to pull data from controller B through an Application Programming Interface (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). The 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 individual's choice to combine the controllers in this way, while the controllers simply have enabled interoperability. A similar situation may arise when a user uses a music streaming service B that can be used through B's app or a third party app. C offers an app with an improved user interface enabling users to access and manage content from any music streaming service. The user sets up C's application in such a way that he/she can now navigate and play B's content through that application. B and C continue to be independent controllers in this scenario. Another example of the inadaptability of this criterion is where a merchant uses payment services offered by a service provider acting as an independent data controller that is subject to specific financial regulations. The processing of data for purposes of completion of the payment would not be possible without both parties' inseparable participation in the payment chain, while not making them joint controllers. CIPL requests therefore that this criterion be removed in the Guidelines.

Pursuing a purpose versus determining a purpose—Paragraph 60 of the Guidelines provides that if the entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity, it is acting as a processor rather than as a joint controller. The Guidelines seems to conflate however "determination of purpose" with "pursuing its own purpose." In some instances, service providers design services that include defining the data elements that need to be collected as part of the service and the purposes for which the data is intended to be used. In addition, a processor generally pursues the same purpose as the controller by definition, because the processor works on the instruction of the controller (but does not determine the purpose). The concept of "pursuing a purpose of its own" is therefore imprecise and confusing as processors are always pursuing their own purpose because, at bottom, their "own purpose" is to pursue the purpose of the controller. This does mean however that such entity becomes a joint controller. The relevant criteria is more about "determination of purpose" rather than "pursuit of purpose."

Use of systems and tools developed by one entity—Paragraph 63 of the Guidelines provide that "the use of an already existing technical system does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context." Paragraph 65 of the Guidelines provides that "the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of processing by the those entities." This assertion seem very broad and could make it difficult to distinguish between joint controllership and controller/processor relationship whenever off the shelf products, platforms or standardised tools are used. CIPL suggests deleting these sentences.

Travel agency–The examples on pages 20 and 21 regarding travel agencies provide that they act as independent controllers or joint controllers. These examples address cases where the customers (i.e., natural persons) of the travel agency make a reservation on their own behalf through them but do not capture the case where an employer is booking business travel and/or hotels on behalf of its employees via a travel agent. In this last case, it is the business customer who provides the travel agencies with the instructions on how to use the data of their employees (e.g., travel date, preferred flight times, destination). Therefore, these examples should be nuanced and adapted to take into account different scenarios.

Examples of joint-controllership—In general, the examples given in the Guidelines in different contexts seem inconsistent – similar configurations of relationships in the examples in controller, joint controller and processor sections sometimes result in different classifications. CIPL would suggest using one example built around a more complex system of multiple actors and different stages to illustrate further. The example of multiple parties with independently determined purposes and means provided in Paragraph 70 remains rather static in comparison to the dynamic and fluid data processing arrangements that are common in many sectors.

Joint-Controllership in the targeting of social media users (TSM) draft guidelines—The TSM guidelines would have the effect of turning advertisers into data controllers for all parts of running an ad campaign. This would even include processing activities on which advertisers do not exert active control, or do not have decisive influence in defining the means or purpose (such as for instance reporting insights about ad campaign performance). In most cases, in practice, advertisers also have no or only very limited influence as to how a personalized advertising is run on another party's infrastructure. The fact that an advertiser provides the content of an advertisement and might be able to give broad and abstract indications with respect to the large group of potential users of which a fraction might form an audience for the actual advertisement should not be sufficient to trigger joint controllership. The analysis may be different if the actual audience is determined by the advertiser and the advertiser has a decisive influence over the underlying processing. Mere causality between the definition of a targeting criteria and the activity of the advertiser (e.g., the assumption that targeting criteria would not be defined if a social media provider was not planning to offer personalized advertising at some point) is not sufficient for the assumption of joint controllership either. This broad interpretation would lead to joint controllership in all cases where an organisation is processing personal data also for the purpose of potentially offering a service at a later stage. In practice, this broad interpretation of joint controllership could lead to a retroactive analysis because the social media provider might have defined possible targeting criteria long before entering into a contractual relationship with the advertiser. CIPL believes that the broad interpretation of joint controllership would not better protect the rights of individuals since either the advertiser and/or the social media provider will already be independent controllers with the corresponding accountability obligations. CIPL recommends the TSM guidelines take a more balanced approach of the classification of joint controllership that relies on practical control over how data is used. In other words, advertisers would only become joint controllers for processing activities in which they actively participate and on which they actually exercise substantive influence.

Summary of CIPL Recommendations:

- Provide that the “converging decision” and “commercial purposes” criteria may be an indication only of joint controllership

- Remove the criteria of inseparability of the organisations’ activities to characterise joint controllership

- Replace the concept of “pursuing a purpose of its own” by “determination of purpose”

- Remove the use of an existing technical system developed by another entity as possible criterion for joint controllership

- Provide examples involving multiple parties with independently determined purposes and means to better illustrate the reality of dynamic organisations’ processing arrangements

- Take a more balanced approach in the TSM guidelines to restrict classification of joint controllership to processing activities in which advertisers actively participate and on which they actually exercise substantive influence

3. Relationship between Controller, Processor and Joint Controller

Application of GDPR obligations to processors—Paragraph 91 of the Guidelines provide that “Article 28(3) GDPR imposes direct obligations upon processors.” CIPL requests the Guidelines to clarify that obligations on the processors in article 28 GDPR are in fact subject to a “contract or other legal act.” They are not intended to be statutory obligations in their own right. If it were the case, there would be no need for a contract setting out such terms.

Organisations' autonomy in decision making—The Guidelines should acknowledge that the controller may decide between a variety of possibilities in terms of how and where to process data. This could go as far as deciding to fully outsource the processing of data and to accept a standardized service without the possibility of customizing it if the controller considers this to be within its business interests. This may be because the cost of a customizable service is higher than a standard one, or because the controller does not have the technical expertise to perform the processing itself and must rely on an expert. In addition, the Guidelines should provide that the parties are free to agree to commercial terms allocating liability between the controller and processor however they deem appropriate in order to reflect a reasonable balance of risk and reward between the parties as well as marketplace norms, while at all times making sure that the rights and freedoms of data subjects are not diminished.

Modifications to the data processing agreement—Paragraphs 107 and 125 of the Guidelines provide that any modification to the data processing agreement must be approved by the controller. The mere publication of a modification on the processor's website to the data processing agreement is not compliant with article 28. CIPL believes that this statement extends beyond the pure remit of data protection law and encroaches on the controller's and processor's contractual freedom.[9] The question as to how a data processing agreement can be amended by the parties is a matter for governing contract law only. In other words, where a controller has agreed through the contract (or other legal act) that the processor may update or modify the processing agreement, then it should be possible for the processor to publish changes to it, including updating the list of sub-processors. These changes need to be properly notified and identified to the controller, e.g., via an internal portal or other similar channels. Similarly, the processor remains bound by the obligation to ensure that the data processing agreement includes the provisions required by Article 28(3). Any change to the agreement in such a way that it no longer meets these provisions would be directly in breach of the GDPR. In addition, the parties should be free to agree contractually that the controller's silence means approval of the proposed changes. This may be necessary in situations where the controller works with many processors or where many changes routinely occur. This would not in any manner relieve the processor from complying with the general instructions under the agreement (in addition, of course, to the GDPR obligations directly applicable to the processor). CIPL recommends that the Guidelines do not seek to override the provisions of the contract freely chosen by the parties. The absolute requirement to obtain the approval of the data controller for each and every single change of the data processing agreement creates unnecessary administrative burdens in particular where processing operations convey low risks. The way to amend a data processing agreement should remain a part of the controller's assessment of the level of risk of these changes and how they impact the data controller's obligations.

Instructions of the controller to the processor—Paragraph 111 of the Guidelines recommends that the data processing agreement set out the controller's obligation "to provide and document, in writing, any instruction bearing on the processing of data by the processor." CIPL believes the Guidelines should avoid using the term "in writing." This may be misinterpreted as meaning that the instructions would have to be put in a human readable text or in the form of words where that may not always be the case. In fact, instructions may be provided through diverse interactions such as configuration of the service, choosing

[9] As a matter of fact, the Rome I Regulation sets out the general principle that the parties to a contract have the freedom to choose the governing law of their contract. This means that the validity of the data processing agreement and any amendments to the agreement have to be assessed in light of the governing law of the contract.

certain settings or the use of technical signals by using a user interface or API calls to instruct the processor to process data in a certain way. These instructions are properly documented through a digital log entry or similar means. In addition, because a commercial and contractual relationship is dynamic and internal and external circumstances continuously evolve, the contract cannot foresee all the possible future circumstances (some of which will be unexpected) that may arise in the performance of the service.

Security measures—Paragraphs 123 and 124 of the Guidelines provide that the processor must obtain the controller's approval of its proposed security measures, including when the processor makes changes to the security measures. While intense controller oversight on the processor's security measures may be relevant and possible in some specific circumstances, CIPL underlines that this recommendation is not generally in line with current market practices and may be unworkable in most controller/processor relationships. Service providers generally have a pre-defined set of security measures in place that rely on the state of the art and globally recognized information security management certifications (such as ISO 27001 and SOC 2 for instance). Controllers usually rely on these external assurances to select their processors and therefore implicitly are approving the security measures mandated by these standards. Controllers also acknowledge that, as part of these certifications, processors are subject to regular internal and third party audits. As a consequence, these security programs cannot be modified on a case-by-case basis for multiple clients. Likewise, it is impossible to obtain approval from controllers each and every time the security controls need to be adjusted. Maintaining compliance with the security standard is the processor's own responsibility that requires on-going activity to review policies and controls, to perform audits and to implement remedies as needed. Continuous improvement is a key requirement for these certifications. Having to obtain the controller's approval before policies and controls can be adopted or amended to improve the processor's security management program is unrealistic, may weaken the overall robustness of the controller security's program, and may also undermine the enforceability of the processor's insurance policies. In practice, a processor may make updates (e.g., to ensure security measures reflect the state of the art) that are actually within the controller's expectations. Such changes may not always require the controller's approval, in particular if they do not cause any material non programmed disruption to the controller's business operation. CIPL believes that the controller should be involved only in situations where the changes would have the effect of lowering the security protections of the processing or would significantly affect the protection of the individuals' personal data. CIPL stresses also that the Guidelines as drafted may put controllers in difficult situations (and even more so SMEs and smaller organisations) as it is unlikely that processors investing heavily in maintaining these certifications will have the capacity to be immediately responsive to client demands regarding approval of changes to security measures.

Assistance of the processor to the controller–Paragraphs 127 to 130 provide that the agreement should contain details as to how the processor is helping the controller to meet its obligations under articles 32 and 36 GDPR. CIPL underlines that while the GDPR imposes a duty to assist, it does not expressly require that the data processing agreement spells out, in detail, how such assistance will be provided. It is not uncommon for data processing agreements to simply say that reasonable assistance will be provided, without going into detail. In addition, as acknowledged by the Guidelines, because each request is specific, the level of assistance may vary greatly and the means of such assistance are assessed on a case by case basis (the assistance could just consist of providing technical assistance). CIPL believes this approach is overly prescriptive. It should be possible for the data processing agreement to focus only on the general obligation for the processor to provide the reasonable assistance and not necessarily describe the details of this assistance. The assistance could also consist of other and separate arrangements between the controller and the processor. The parties should be entitled to arrive at their own commercial arrangement with respect to any possible compensation for the assistance provided.

Notification of a data breach—Paragraph 133 of the Guidelines provides that the data processing agreement should mention a specific time frame (e.g., number of hours) for the processor to notify the controller of a data breach. CIPL believes that controllers and processors should remain free to apply the legal standard of the GDPR which provides for an obligation for the processor to notify the controller "without undue delay." Each data breach may have different sources, causes and consequences that will require flexibility in handling the crisis and informing the controller to best mitigate the impact of the data breach on individuals.[10] In addition, in line with the WP 29 guidelines on personal data breach notifications,[11] CIPL recommends that the Guidelines restate that the controller's timeline for notification of the breach to the DPA and to the individuals begins upon the controller becoming aware of the breach, and the controller would not be considered to be aware of the breach until the processor has notified the controller. Therefore, the follow-on logic is that the time taken by the processor to notify the controller would not be factored into the time permitted for the controller to notify the DPA and individuals, as the case may be.

Deletion of personal data by the processor—Paragraphs 136 to 139 of the Guidelines assume that it is always for the processor to undertake a specific action to delete the personal data. CIPL recommends the Guidelines acknowledge that deletion of personal data by the processor may not be feasible in instances where products or services are self-serve. In these instances, the controller retains full control on the personal data, including its deletion. The Guidelines should provide that processors would also meet their obligations of deletion by giving access to a technological tool to the controller allowing for data deletion at the end of the contract. The Guidelines should also recognise that deletion shall be achieved by anonymising the data or by returning all the data to the controller or to another processor designated by the controller.

Information provided to the controller to help demonstrate compliance–Paragraph 140 of the Guidelines provides the processor should disclose all information to the controller on how the processing activity is carried out. This statement goes beyond Article 28(3) (h) GDPR which only requires the provision of all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR. CIPL also suggests that in this context, the Guidelines also mention the possibility for the processor to provide the audit report related to an existing certification—like ISO or SOC 2. This is a frequent market practice as controllers are not able to audit or inspect all their processors, especially when they are thousands of miles away. As a consequence, CIPL recommends that the Guidelines mention that an audit report can help demonstrate compliance and serves as a means for the processor to fulfil its obligation to assist the controller.

[10] See **Comments by the Centre for Information Policy Leadership on the Article 29 Working Party's "Guidelines on Personal Data Breach Notification under Regulation 2016/679" adopted on 3 October 2017.**

[11] See **Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018.**

Instructions infringing data protection law - Paragraphs 142 to 145 of the Guidelines provide that in accordance with article 28(3) GDPR, the processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR. Because of the possible wide ranging effect of this provision, CIPL recommends the Guidelines make it clear that the processor is not as such required to continuously monitor laws applicable to the controller and to provide legal advice. The information to be provided by the processor should be limited to what is reasonable for a service provider in its position to be aware of. In addition, Paragraph 145 of the Guidelines provides that the parties may decide to spell out that a processor's notice of infringing instruction could lead to contract termination. CIPL recommends to provide instead that a processor's notice of infringing instruction may trigger the right for the processor to suspend the services and/or to request indemnification from the controller.

Sub-processors—Paragraph 152 of the Guidelines provides that the controller may provide a general authorisation to the use of sub-processors in the contract. The contract would include a list of sub-processors in an annex thereto, together with criteria to guide the processor's choice. Again, CIPL believes this goes far beyond GDPR requirements. In addition, sub-processors may change from time to time and this cannot trigger per se the need to execute a contractual amendment. The requirement to include a list of sub-processors in the contract should be restricted to contracts whereby controllers are providing a specific authorisation to the use of a particular processor. Where the controller provides a general authorisation, the criteria and guide for the choice of a sub-processor (e.g., guarantees in terms of technical and organisational measures, expert knowledge, reliability and resources) should suffice. Alternatively, a list could be available to the controller even if the list itself is not replicated directly in the contract.

Respective accountability of joint controllers—Paragraph 164 of the Guidelines provides 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 seems to suggest that in a joint controller relationship, each controller would have to police the other controller's further use of data. The duty of the controller to oversee the practices of its joint controller would be required as a matter of accountability. CIPL warns against imposing unrealistic burden on (joint) controllers. Each controller is already independently legally bound by the obligations of the GDPR under the oversight of the DPAs. If for instance A and B share data as part of a joint controller relationship for purpose 1 and A decides to further process the data for purpose 2 because it considers there is a compatible purpose, B cannot verify the use of the data by A for purpose 2 as A is then an independent controller acting on its own purpose. It would add no value to impose an additional due diligence obligation from one independent organisation on another independent organisation and runs the risk of blurring the frontier between the joint controller relationship and the controller to processor relationship (where the controller has such oversight obligation on the processor in particular to verify compliance with the controller's instructions).

Obligations towards individuals—Paragraph 187 of the Guidelines recommends that joint controllers communicate to the other controllers in charge or to the designated contact point, the requests received in order to be effectively handled to avoid imposing an excessive burden on individuals. To enable controllers to address in the most efficient manner a wide variety of situations, CIPL suggests the Guidelines confirm that this would include having a joint controller connect the individual to the contact point via email or other similar channels where one controller is in a better position and has the technical means to fulfil the data subject rights.

Summary of CIPL Recommendations:

- Clarify that obligations on the processors in article 28 GDPR are not intended to be statutory obligations
- Recognise organisation's autonomy in deciding how the data processing should be performed and in negotiating the commercial and contractual terms as long as it complies with the GDPR
- Recognise that instructions of the controller to the processor can be provided and document in several formats to account for a variety of situations and evolving circumstances
- Provide that the processor must obtain the controller's approval of changes to the security measures only when these changes would have the effect of lowering the security protections of the processing or would otherwise significantly affect the protection of the individuals' personal data
- Provide flexibility in how the data processing agreement describes the obligation for the processor to provide reasonable assistance to the controller, inlcuding the possibility to enter into separate agreements, and provide for a possible compensation
- Clarify that controllers and processors should remain free to apply the "without undue delay" legal standard of the GDPR for breach notification purposes
- Provide that the obligation to delete data may be discharged by giving access to a technological tool to the controller allowing for data deletion, by anonymising the data, or by returning all the data to the controller or to another processor designated by the controller
- Clarify that an audit report can help demonstrate compliance and serves as a possible means for the processor to fulfil its obligation to assist the controller
- Clarify the boundaries of the processor's obligation to inform the controller of an infringing instruction and provide more options to the parties to define the consequences of such infringing instruction
- Restrict the requirement to include a list of sub-processors in the contract to cases where controllers are providing a specific (and not general) authorisation to the use of a particular processor
- Remove the obligation for a joint controller to oversee the further processing of data by the other joint controller
- Acknowledge that to address an individual's requests, a joint controller may connect the individual to the contact point via email or other similar channels

CIPL is grateful for the opportunity to provide recommendations on the EDPB's Guidelines on the concepts of controller and processor. If you would like to discuss these recommendations or require additional information, contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, or Nathalie Laneret, nlaneret@huntonAK.com.