COCIR feedback to the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR [1]

COCIR welcomes the updated guidance provided by the European Data Protection Board on the concepts of controller and processor in the GDPR.

These concepts of controller and processor are central to the correct application of the GDPR, and essential in determining the roles and responsibilities applicable for different entities within the processing of personal data.

Given the variety and complexity of data processing activities such determination can be challenging, with the consequences thereof having strong legal, financial or other implications. Between business partners there can be different legal interpretations, or even other elements at play (commercial interests, risk appetite, market dominance,...), that will further affect the outcome of the discussions on determining the relevant roles and responsibilities.

Therefore it is paramount that the guidance creates as much clarity as possible for all processors and controllers in order to find strong consensus and, even more importantly, to ensure full compliance with the requirements of the GDPR that provide a high level of data protection for citizens in Europe.

1. COCIR would like to caution against making explicit recommendations or be overly prescriptive in some areas as this can suggest measures or actions that go beyond the legal text of the GDPR.

2. COCIR would like to recommend for the various sections the use of more complex or high-level examples that move beyond single transaction-like processing activities that are not that realistic or relevant when it comes to the determination of controller and processor.

3. COCIR believes the document may be helpful by having a more elaborate and dedicated section on group companies.

4. COCIR commends the EDPB for making use of flowcharts that facilitate the understanding and determination of roles and related responsibilities, as is the case in Annex I. It would however be good to more closely link/align this with the rest of the guidance document, for instance by referring to specific paragraphs.

Below we list more specific comments regarding the guidance document which we hope the EDPB will take into full consideration.

COCIR remains available to provide further clarification or assistance to the EDPB where needed.

[1] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en

#	Comment
PART I – CONCEPTS	
1. General observations	
12	We agree that controller and processor are functional concepts and that these can not be forced upon parties solely on the basis of a legal contract. It would however be good to clarify that these concepts do need to be concretely specified within the context of a data processing agreement between controller and processor.
2. Definition of controller	
22	It would be good to clarify that this is not the case for all legal provisions, and more importantly, that even if there would be control stemming from implicit competence that this does not necessarily imply the entity becomes controller for all related processing activities.
25	It is stated that one of the tests to determine 'control' is factual influence stemming from traditional roles/professional expertise that implies a certain responsibility. 1. Employer-employee relationship has been included as an example It is not uncommon, except for obligations stemming directly from law (such as tax, social security, etc.), that a multinational group of companies take a centralized approach to processing of employee data, thereby determining the purposes as well as means of processing. In those cases, would we still consider the local entity to be the controller? If not, would we consider the local entity to at least be a joint controller by virtue of the fact that it is the legal employing entity? It would be good to clarify the other criteria that must be taken into account when making this determination. 2. Interaction with customers Does the logic elucidated in para 25 also extend to other relationships such as between a company and its customers, especially in the context of data processing for purposes covered under a contract (such as a service contract)? In that case, is the company entering into the contract to provide service to a customer always considered to be a sole controller, even when another company (such as a parent entity) makes factual decisions about the kind of service that ought to be provided, the personal data elements that are needed to provide the service, etc.? What other elements must be considered in this assessment? It might be good to consider additional examples
38	Example: Hosting services Many hosting providers offer a range of packages that may be diversified on the basis of minimum security levels or other more specific technical and organisational security measures. The customer (employer in the stated example) will choose the service package that best fits his/her needs and may therefore not explicitly provide instructions on all possible measures. The current formulation of the example might be incorrectly understood as suggesting instructions that go beyond the requirements of GDPR Article 28.
3. Definition of joint controllers	
66	Example: clinical trials The example ignores the complexity of the roles within a clinical trial setup and may therefore lead to the incorrect application of the concepts of controller, processor and joint controllers.
4. Definition of processor	

75	The term 'external organisation' is confusing, as it is here referring to companies within a group being external organisations to each other. 'External entity' would make more sense.
5. Definition of third party/recipient	
87	Particularly within the context of a group of companies it would be good to clarify that "controller" can be understood as *either* being a controller in its own right *or* as a joint-controller.
87	Example: Company groups Typo: Company Z becomes Company ZZ throughout the example
PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES	
1. Relationship between controller and processor	
110	The controller is responsible for compliance with the GDPR. There can be various reaons why the controller may want to impose more stringent measures on a processor, even if only minor risks arise. Hence, the text should not suggest that this is not possible nor allowed. Next to that, it is not always the case that the controller has a deeper understanding of the risks that the processing entails. This may vary case-by-case. Therefore it would be better to rephrase or remove the related sentences to this.
112	This paragraph should not suggest there to be other requirements mandatory that go beyond the legal text of the GDPR.
115	There can be several options on how to document the instructions, but the document should refrain from explicit recommendations. The process and procedures can vary strongly based on the nature and type of processing activities. Specific recommendations could lead to misconceptions of the actual legal requirements and/or diverging views between controllers and processors.
122-124	Art. 28.3(c) specifies that the contract should stipulate that the processor takes all measures required pursuant to Art. 32. Even where both parties would agree to more detailed references to the security measures, once again the obligation for instance on the processor to obtain the controller's approval before making any changes as suggested is not a legal requirement nor is it relevant for all processing activities. Also the contract may not be the best suited means to document or instruct security measures.
130	The guidance should restrict itself indicating that more concrete details should be specified between controller and processor, but that these do not necessarily be overly prescriptive. The contract may also not be the most appropriate instrument to cover this for the range of processing ativities, to inform or update practical or technical procedures and templates, or to effectively reach responsible persons within the organisations.
133	According the legal requirements this should happen without undue delay. Although an agreed timeframe could be considered useful in some cases, it should not be generally recommended nor should it be by default specified in the contract.
2. Consequences of joint controllership	
161-164	New requirements are created in addition to those already defined in Art. 26 GDPR. The fact that GDPR says "in particular" (in art. 26) is because it wants to leave the determination to the parties. The role of the EDPB is to ensure consistency, not to generate new requirements. It would be best to propose to remove points 161-164 or at least to make clear that any additional distribution of responsibilities between the parties (in the joint controller arrangement) are not mandatory. It should be up to the parties to decide whether or not to cover such extra distribution of responsibilities in the joint controller arrangement.

173	This paragraph again suggests establishing new requirements for joint-controller arrangements.

About COCIR

COCIR is the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries.

Founded in 1959, COCIR is a non-profit association headquartered in Brussels (Belgium) with a China Desk based in Beijing since 2007. COCIR is unique as it brings together the healthcare, IT and telecommunications industries. www.cocir.org