Computer & Communications Industry Association

Tech Advocacy Since 1972

CCIA response to EDPB consultation on processor / controller

Update of the Article 29 Working Party's opinion on the concepts of controller and processor (Opinion 1/2010, WP 169)

The concepts of data controller and its interaction with the concept of data processor play a crucial role in the application of the General Data Protection Regulation 2016/679 (GDPR). The European Data Protection Board has decided to review the existing opinion of the Article 29 Working Party from 2010 on the concepts of controller and processor in the light of the GDPR. One step in this process is to arrange a meeting with different European stakeholders in order to get their view on which issues that need to be covered and which aspects that are problematic. This event will take place in Brussels on 25 March 2019 and an invitation will be sent out separately. The survey seeks to gather views of sectoral organisations (trade associations) across various industries in order to prepare the discussions at the event.

Please try to keep your replies as brief as possible – more in depth discussions will be held at the event on 25 March. Please also **do not** include any personal data in your reply.

Please reply to this survey **by no later than the 15th March 2019.**

About the contributor

[…]

1. Looking back at Opinion 1/2010

a) How useful has Opinion 1/2010 been to you in applying the controller and processor concepts in practice?

	Very useful
X	Useful
	Not useful

a.1) If not useful, give up to three reasons why.

1000 character(s) maximum

While the guidelines have been useful in some instances, there are significant discussions and interpretations on the qualification and allocations of roles and responsibilities between contracting parties. Much discussion revolves around the determination of the means of processing, and the new guidelines should reinforce the nuanced approach of the existing Opinion.

b) Please indicate three aspects of Opinion 1/2010 which could be improved to increase its relevance.

1000 character(s) maximum

1) Further clarification on the boundaries of the concept of “joint controllership”, particularly in light of the Wirtschaftsakademie case. While the existing guidelines confine the concept of joint controllership to situations where controllers share the same purpose of processing, the Wirtschaftsakademie CJEU opinion implies that joint controllership can be extended to situations where two controllers do not share the same purpose of processing.

2) Building on the existing Opinion, reinforce the message that the determination of the means of processing should not, alone, qualify a contracting party as controller. Possible ways forward include prioritization of the purpose determination element, further details on the definition of 'essential' means in light of modern processing realities, etc.

c) Regarding the examples provided, please indicate:

c.1) Up to three examples you would like to see improved in the current opinion;

1000 character(s) maximum

1) The guidelines should build up on the existing opinion and reinforce the fact that the “determination of means” should not automatically, and on its own, qualify a service provider as controller. Public cloud service providers design and implement a range of security measures for the benefits of their clients. In fact, clients will almost in all cases rely on the advice of their cloud infrastructure expertise in secure hosting. These measures should not mean that they become controllers.

2) The role of “controller” of telecommunication providers should remain and be reinforced whenever they are providing telecommunications services.

c.2) Up to three examples of elements you would like to see addressed in the current opinion

1000 character(s) maximum

1) A clarification on what kind of operations a processor can undertake without becoming a controller would be helpful. In many cases, processors have to undertake certain operations for service maintenance and continuity, such as basic analyses of the efficiency of cloud systems to adjust workflow and dedicated infrastructures. These could be interpreted as a determination of the purpose of processing.

c.3) Up to three examples you would like to see improved in the current opinion;
1000 character(s) maximum

See response to 1.c.1.

d) Are there any specific issues, arising from your experience, regarding:
(i) the concepts of controller and processor;
(ii) the relationship between joint controllers; and
(iii) the relationship between controllers and processors
which you think should be addressed or clarified in the updated guidelines? If so, please enumerate them here:

1000 character(s) maximum

(i) It would be helpful to clarify that service providers which simply provide support and maintenance services and may gain occasional access to personal data do not qualify as processors, and that a processing agreement under Article 28 is not needed.

(ii) A list of best practices of issues which joint controllers should address in their contract would also be helpful. While Article 28 provides an exhaustive list of items which a controller-processor contract should address, Article 26 remains generally more elusive.

(iii) It would be helpful to clarify the level of specificity of technical and organizational measures, including the choosing of sub-processors, which should feature in a controller-processor contract. We invite the EDPB to be mindful of the confidentiality and security concerns that over-detailed information would raise for the processor and any other controllers to which the processor provides services. In addition, the EDPB should clarify that the data transfers between the controller and the processor do not require an additional legal basis under Article 6.

2) GDPR changes and challenges

a) What do you perceive as the main changes of the GDPR in relation to the concepts of controller and processor (including third party / recipient) and their role in ensuring compliance with the

GDPR's objectives? Please indicate up to three perceived main changes of the GDPR in relation to the concepts/roles of controller and processor.

1000 character(s) maximum

Main challenges are:

- Direct liability of the processor towards data subjects;
- Short notice for any data breach notification;
- Audits of processors conducted by controllers.

b) Please indicate briefly the three main issues you have encountered so far when applying the new or enhanced provisions of the GDPR in relation to the concepts/roles of controller / processor / joint controllership but also on liability implications.

For example, you may wish to outline any issues you have experienced in the following areas:

1. The allocation of responsibility between joint controllers for the performance of obligations (e.g. breach notification) and compliance with data subject rights (e.g. access requests) under the GDPR, and arrangements / agreements entered into for this purpose (as per Article 26);
2. The allocation of responsibility between controllers and processors, and contracts between controllers and processors (as per Article 28);
3. Subcontracting by processors and issues arising in relation to this (Article 28);
4. Liability issues between joint controllers or between controllers and processors (Article 82).

If possible, please provide specific (anonymised) examples.

1000 character(s) maximum

GDPR does not specify whether the controller or processor is responsible for ensuring compliance with the Article 28 requirements. Contractual negotiations would be much more straightforward if the responsibilities of each party were clear.

Pre-contractual discussions also highlight uncertainty around the choosing and acceptance of sub-processors. We invite the EDPB to clarify that the controller's right to object to the use of a sub-processor under Article 28(2) should not oblige the processor to provide, or continue providing, the service if it is technically or financially disproportionate for the processor.

See also responses to earlier and subsequent questions.

c) Given that, in a change from Directive 95/46/EC, processors now have obligations under the GDPR (rather than obligations arising purely under contract with a controller) what, if any, difficulties have you encountered with respect to the possible overlap of controller and processor obligations, for example in determining which party is responsible for compliance?

1000 character(s) maximum

The mandatory audit requirement can be very challenging for large-scale processors, particularly for those operating cloud infrastructure services. Where hundreds of controllers use the same cloud service provider, allowing a specific controller to exercise his right of audit cannot only be impractical, but it may also not be desirable from a security perspective. We invite the EDPB to acknowledge these difficulties and concerns arising from Article 28(3)(h).

It would also be helpful to clarify that, when a processor does inform the controller about the infringing character of a given processing instruction, the processor is exempt from liability should the controller ignore or decide not to alter said instruction.

d) Do other stakeholders you interact with generally share the same views when it comes to applying the concepts and related provisions under the GDPR? Please provide (anonymised) examples of where you have experienced a divergence of views – for example, in relation to the respective roles and responsibilities of joint controllers or of controllers and processors in the context of vendor management.

1000 character(s) maximum

Stakeholders have different interpretations of the concepts of GDPR, including:

(a) at which point a processor becomes a controller considering today's Internet architecture and processing relationship;

(b) how detailed should the technical and organizational measures be under Article 28;

(c) how detailed should the information related to subcontractors be;

(d) the relationship of an Article 28 agreement with the main contract (does an annex to the main contract suffice? Should it be a separate contract? Etc.);

(e) whether a legal basis for data transfers between controllers and processors is needed (for transfers both within and outside the EU)

3) Future Challenges

Technology does not stand still. Please briefly indicate three future scenarios where you consider that applying the current concepts of controller / processor / joint controllership / third party / recipient may be complex (e.g. smart cities, block chain, artificial intelligence)?

1000 character(s) maximum