David Rosenthal

Partner, VISCHER AG, Zurich, Switzerland
Lecturer Federal Institute of Technology Zurich, Switzerland
Lecturer University of Basel Law School, Basel, Switzerland

drosenthal@vischer.com

www.rosenthal.ch / www.vischer.com

Winterthur, October 17, 2020

Att. **European Data Protection Board (EDPB)**

Comments on "Guidelines 07/2020 on the concepts of controller and processor in the GDPR"

Dear Sirs:

I am working as a privacy practitioner and scholar in Switzerland, I am the secretary of the Swiss association of in-house data protection officers (www.vud.ch), and I have published one of the main commentaries on the Swiss Data Protection Act. Some references as to my qualifications, if you are interested: https://www.vischer.com/en/team/references/david-rosenthal/

Among my publications is also an extensive piece on the topic of controller, processor and joint-controller with dozens of practical examples. I published because I was repeatedly asked to give practitioners in Switzerland much needed practical guidance on this issue. The outcome was an in-depth analysis that goes probably deeper than most you have seen. You may, therefore, find it practical for finalizing your guidance. One of the concepts I developed is referred to also below, and I propose it as an alternative to your "inextricably linked" criterion. Unfortunately, the paper, it is in German. You can download it here: http://www.rosenthal.ch/downloads/Rosenthal-ControllerProcessor.pdf

Note that the topic of controller and processor is of particular interest in Switzerland because the revised Swiss Data Protection Act has adopted the same definition of controller and processor as has the GDPR.

I will not comment on the entire guideline, but just want to point out three areas you may want to provide clarification:

- *First*, a party will automatically become a controller by *either* determining the purpose *or* the essential means. Even if a party only determines the purpose of a particular processing activity and the other only over the (other) essential aspects of the same processing activity, the fact that they both exercise control over the same processing activity will result them being responsible for the data processing activity – and, thus, being joint controllers. This was clear under the old WP29 guideline, and it is what you describe in para. 53 as decisions that "complement" each other.

  Example: A client instructs a lawyer to make various submissions in the client's name with particular purpose, but leaves the details to the lawyer. Hence, the client determines the

purpose, and the lawyer the means (e.g., which type of personal data to include). The submissions are *one* data processing activity for which both the lawyer and the client are joint controllers.[1] Their decisions are undoubtedly inextricably linked.

Counterexample: The management of the lawyer's own files (which contains personal data received from the client and other sources) is a data processing activity for which the lawyer is a sole controller, even though him acting under a mandate of the client. It serves the purpose of the lawyer being able to provide his service, and thus the lawyer determines the purpose and essential means.

In your draft you are not clear about this distinction. In para. 34 you suggest that a party who only decides over the purpose but not the means or vice versa will not be considered a controller. At least this is how this paragraph is being interpreted in various publications[2]. What you probably intend to say: If a party is a controller, it remains responsible for the entire data processing activity, and can't leave it to the processor. However, the sentence "It must also make decisions about the means of the processing" leaves no room for a situation in which one joint controller determines the purpose and the other the essential means.

Of course, you can always argue that by determining the purpose you, to a certain extent, influence the essential means, but that's doesn't change the underlying principle of the GDPR being drafted to ensure that anybody who determines a relevant aspect of a data processing activity shall become responsible for such determination.

- *Second*, you are in my view too complicated in para. 53 by requiring that in the case of joint-controllers their converging decisions have to have "a tangible impact on the determination of the purposes and means of the processing". Your criterion of an "inextricably link" between the two decisions raises many questions in practical use and will be very difficult to apply.

  A much easier approach would be to ask whether they the decisions of the various parties (or to be joint controllers) concern the *same* logical data processing activity. In my paper, I explain why a telecom provider and its customer are two separate controllers with regard to the *same* transmission of personal data. As per your "inextricably linked" test, they would be joint controllers, which you probably agree would be the wrong result. If you instead ask whether their data processing activity is the same, you will conclude that both of them control *different* processing activities because they take place *at different logical levels*, with each controlling the purposes and means of the data processing taking place at their respective level (the network level vs. the customer's transmission level), even though the transmitted data is the same. You may find it interesting to introduce this concept, as it is much easier to apply in practice and solves the deficiencies of your "inextricably linked" criterion.

  I note that the criterion of "inextricably linked" is problematic also for the reason that your draft guidance suggests that a mutual benefit related to a particular data processing activity can be sufficient. In todays world, the interests in a data processing activities are very often inextricably linked with each other. If you want to stick to this criterion, please make clear that

---

1 You avoid this result in your example

2 See, e.g., https://datenrecht.ch/verantwortliche-und-auftragsverarbeiter-zu-den-leitlinien-des-edsa-entwurf-zum-controller-und-processor/

a mutual benefit in a particular data processing activity is clearly not sufficient for the two parties involved in it (for entirely reasons) become *joint* controllers.

- *Third*, your statement in para. 34 that "the party acting as a processor can never determine the purpose of the processing" can also be misunderstood that even if the processor does – de facto – determine the essential means it will not become controller. This is how this sentence is being interpreted, and such statement would be clearly wrong.

  You should clarify that if a controller merely determines the purpose, but leaves determining the essential means to the processor, and if such processor *does* determine the essential means, it becomes a (joint-)controller – even if it does not determine the purpose. This is a logical consequence of the underlying principle that whoever determines an essential aspect of a data processing activity becomes (jointly) responsible for it.

  Think of a party who determines only the purposes of a data processing activity but not the essential means and would, therefore, not be considered the controller for lack of deciding over both (see above). It would result in a responsibility vacuum because the processor instructed to carry out the processing would not be responsible either, because he would not be considered a controller. In such a situation, the processor determining the essential means would automatically become a joint controller, with the result that it becomes responsible for the data processing activity. This is the intended result. Hence, the processor lacking sufficient instructions should either not process data until it has received adequate instructions or get in the driver seat itself.

  This is comparable to the situation in which the processor misappropriates personal data of the controller and uses it for its own purposes: For such unauthorized processing of personal data the processor becomes a controller of its own – and can be held responsible for it under the GDPR.

Happy to provide more input on these aspects, if you wish.

Best regards,

David Rosenthal