MyData-TRUST S.A.
Boulevard Initialis 7, Bte 3
7000 Mons (BELGIUM)
www.mydata-trust.com

December 02nd , 2022

Comments on Guidelines 08/2022 on Identifying a controller or processor's lead supervisory authority.

Comments from:

MyData-TRUST

When DATA PROTECTION Meets Life Sciences

MyData-TRUST provides DATA PROTECTION services in the LIFE SCIENCE sector (such as privacy risk assessments, external DPO as a service, etc.). Active since 2017, it is registered under Belgian Laws. Its Multi-Disciplinary Team relies on Data Privacy Lawyers, IT Security Specialists and Clinical Experts. Our clients include among others Pharmaceutical, Biotech and Medical Device companies, Contract Research Organisations (CROs), Healthcare providers and associations.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

Key messages

MyData-TRUST (hereinafter referred as "**MD-T**" or "**we**") welcomes the clarifications brought by the Guidelines 08/2022 on identifying a controller or processor's lead supervisory authority ("**Guidelines**"). In particular, the clarifications on the object and the criteria of the certification but also on the obligations up to the exporter when relying on such transfer tool.

However, the application of the solution as proposed without any other clarification **does not ensure the benefits of the one-stop shop mechanism** for data subjects and organisations.

Introduction and general considerations

- Recital (124) GDPR: "Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection";

- Recital (125): "The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged";

- EDPB Guideline WP244 for identifying a controller or processor's lead supervisory authority on the 25 May 2018.

- Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority on October 10, 2022. updated version of the previous guidelines WP244 rev.01 adopted by the Working Party 29 and endorsed by the EDPB on 25 May 2018) for a targeted public consultation.

Specific comments

- In paragraph 31, The EDPB asserts that the compliance measures and related obligations that joint controllers must take into account when determining their respective responsibilities, in addition to those specifically referred to in Article 26(1) of the GDPR, include, among other things, organizing contacts with data subjects and **supervisory authorities**. Paragraph 32 states that the distribution of competences between the joint controllers **does not bind** the supervisory authorities either on the qualification of joint controller or on the designation of the contact point for data subjects. These paragraphs leave some **questions open and lack clarity**. If the joint controllers cannot contractually decide who will be the lead authority for their processing, the supervisory authorities should take into account the distribution of responsibilities as defined in the contract. **for example**, in case of a data breach, the joint controllers have agreed that the notification of the authority is the responsibility of the joint controller A, this distribution of responsibilities should exempt the joint controller B from notifying his superior authority who is also the lead supervisory authority. Note that notification to both could lead to a control of both.

- According to points **ii. and iii**. The lead authority in case of joint controllers is the

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

supervisory authority of the respective place of establishment of each joint controller. This results in two or more lead supervisory authorities for a single processing operation. This solution may cause difficulties in practice. **Let's imagine** the case where one of the joint controllers is located in the European Union and the other one outside the Union. In this specific case, we could say that there is only one lead authority, the one located in the Union, but the joint controller outside the Union may have a **national supervisory authority** that imposes on him, **for example**, an obligation to notify in the event of a data breach. This authority could declare itself competent for a data breach and if at the same time the supervisory authority located in Europe is seized of the same breach, this could lead to a double decision for the same processing.

- **Another example**: if the joint controllers are located in Europe and therefore each has a lead supervisory authority. **Let's imagine** that the joint controllers have not clearly identified the responsibilities or are equally responsible for each other and decide to carry out a high-risk processing operation. **Each of the joint controllers will therefore have to seek authorization from its lead supervisory authority and this may lead to contradictory decisions between the different lead supervisory authorities**. There are no details to analyze this situation.

- Having two lead supervisory authorities does not help much in a joint controllers relationship. Especially in case of **complaints** from data subject. **Let's imagine** joint controllers located in Europe. For a joint processing, a data subject having been informed of the joint controllership decides to file a complaint with each of the lead supervisory authorities according to the place of main establishment of each of the joint controllers (**France and Italy for example**). Each of the supervisory authorities being the lead authority for this processing, is competent to judge the complaint. We can think in this situation of the **cooperation mechanism** between the supervisory authorities provided for in **Article 60** of the **GDPR**, but it should be noted that if we stick to a strict interpretation of this article, this cooperation mechanism **will not apply** to the joint controllers of the processing because it applies between a lead authority and the authorities concerned. We are in a situation where there are **several** lead supervisory authorities for the same data processing. The question therefore arises as to **which**

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

authority will assume the role of lead supervisory authority? The question of **collaboration** between the lead supervisory authorities can also be raised. **It would be wise to know how the primary supervisors should communicate about who will start the investigation when a complaint has been filed and who will ultimately take the lead, but also how to respond if one authority acts more quickly without collaborating with the other.** In this situation, each of the lead supervisory authorities will be competent and no cooperation mechanism will apply, which may result in different decisions or two decisions for the same processing.

MD-T suggests

If the lead authority in case of joint controllers is the supervisory authority of each joint controller according to the respective **main** place of establishment, **MD-T suggests** the EDPB to **clarify** the following points

- That in case of joint controllers, the lead supervisory authorities will have to stick to the contractual arrangements between the different parties. That is to say, if all the tasks (notification, complaint, etc.) that are under the scope of competence of the lead supervisory authority are contractually delegated to a joint controller, the joint controllers will have to stick to and collaborate only with the corresponding lead supervisory authority. With this solution, it will be clear which lead supervisory authority is competent for a given issue. For example, in case of a data breach, if contractually the responsibility for notification is assigned to one of the joint controllers, the notification should only be made to the lead authority corresponding to this joint controller.

- To put an **obligation of collaboration** between the lead supervisory authorities. It is difficult to envisage two or more lead authorities for the same processing without a cooperation mechanism established between these authorities. The risk of conflict and especially of contradictory decisions is high. This cooperation must be accompanied by the points on which these authorities must agree to determine their respective competences. It would also be important to have a criterion on which the authorities can base themselves to determine which of them will be the lead of the other leads, a sort of **"lead of the leads".**

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

MD-T suggested another solution. The EDPB could leave it up to the joint controllers to decide contractually who will be the lead supervisory authority for their processing. While knowing that both control authorities are lead authorities, the parties can contractually decide who will be the lead authority of the lead authorities. **The lead of the leads** as mentioned above. This solution could be accompanied by an obligation of collaboration between the lead authorities. It should also be made clear that the assessment will be made on the basis of the facts and not on the basis of contractual provisions. That is, the parties must not contractually indicate a situation that does not reflect reality. The regulatory authorities will still be able to rely on a factual analysis to determine their jurisdiction.

Conclusion

We greatly welcome the EDPB's initiative, but the proposed solution deserves clarification. The benefits of the one-stop shop mechanism for both data subjects and organizations are: cost reduction, time saving and avoiding the risk of different data protection authorities taking different approaches to cross-border data processing activities. But the application of the solution as proposed without clarification does not guarantee any of the advantages of the one-stop shop mechanism. Therefore, clarification remains necessary, if not indispensable, for the application of this solution.

MD-T is committed to sharing its expertise in the field and we remain at your disposal if you need more information or clarification.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.

Contains confidential information protected by MyData-TRUST. All rights reserved. Disclosure not allowed.