Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CIPL response to the EDPB public consultation on Guidelines 8/2022 on identifying a controller or processor's lead supervisory authority

Centre for Information Policy Leadership (CIPL)

1 December 2022

The Centre for Information Policy Leadership[1] (CIPL) welcomes the opportunity to comment on the European Data Protection Board's (EDPB) proposed amendments to Guidelines 08/2022 on identifying a controller or processor's lead supervisory authority, namely paragraphs 29-34 and points ii. and iii. under 2.d. of the Annex related to joint controllership.

CIPL believes that a fully functioning cooperation mechanism among data protection authorities (DPAs), based on the concept of a one-stop-shop (OSS) and a lead DPA, is an essential prerequisite for the consistent and effective implementation of the GDPR. Clarifying the meaning of the relevant GDPR concepts and their implementation is crucial in this context. The OSS was originally designed to reduce legal uncertainty and ease the administrative burdens of companies resulting from divergent rules and practices of different DPAs across the member states. Any guidelines on the OSS or elements that impact the OSS should be designed to support these objectives and to strengthen harmonisation further.

The 2017 Guidelines on identifying a controller or processor's lead supervisory authority[2], still created by the Article 29 Data Protection Working Party (WP29) and adopted by the EDBP, state that: "... to benefit from the one-stop-shop principle, the joint controllers should designate (among the establishments where decisions are taken) which establishment of the joint controllers will have the power to implement decisions about the processing with respect to all joint controllers."[3] With this, the designated establishment would be considered the main establishment for the processing carried out by the joint controllership, and the joint controllership could benefit from the OSS.

In contrast, the proposed language, especially in paragraphs 32 to 34 of Guidelines 8/2022, appears to reject the notion of the main establishment in a joint controller context and, by extension, access to the OSS. **The changes are not substantiated with guidance on why these amendments are being proposed, and it does not take the importance of the joint controller agreement into account. Lastly, the changes lack clarity on how DPAs will cooperate in a joint-controller cross-border processing context.**

In particular, CIPL would like to raise the following concerns:

I. PROPOSED AMENDMENTS IGNORE THE NATURE OF ARTICLE 26 GDPR

The understanding of what constitutes joint controllership is quite broad, and parties within often very complex joint controllership arrangements will not have the same level of responsibility over all parts of the processing activity. Article 26(1) GDPR consequently mandates that controllers in a joint

[1] CIPL is a global privacy and data policy think and do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 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.

[2] Article 29 Working Party Guidelines for identifying a controller or processor's lead supervisory authority (WP244 rev.01), endorsed by the European Data Protection Board on 25 May 2018.

[3] Ibid, p.7.

controllership proactively set out their respective responsibilities to ensure transparency, particularly also vis-a-vis the individuals whose data is being processed.[4] The joint controller agreement must reflect the actual division of tasks and responsibilities and is binding on each of the joint controllers. For a DPA to ignore the agreement and instead potentially assume full responsibility for each (joint) controller for all parts of the processing would, in fact, negate Article 26 GDPR.

Instead, the Guidelines should clarify that supervisory authorities must take joint controller agreements into account on a case-by-case basis. Annex 2d should include the joint controllership agreement and continue to allow for identification of an LSA for the joint controllership.[5]

II. THE PROPOSED CHANGES FURTHER WEAKEN THE ONE-STOP-SHOP MECHANISM

The proposed changes have the potential to undermine the integrity and cohesiveness of the GDPR's one-stop-shop (OSS) mechanism by creating a risk that multiple supervisory authorities will take enforcement action in respect of the same cross-border processing activity, leading to potentially contradictory applications of the GDPR in different EU Member States.

While the GDPR does not explicitly mention a common main establishment for joint controllers, the aim of the GDPR has been to create further harmonisation in the interpretation and application of data protection law to support a single market of data. [6]

The proposed changes to the Guidelines move away from this in several ways:

- Creates a risk that two or more supervisory authorities will claim to be competent as LSA over the same cross-border processing activity, which would lead to competing investigations of the same processing activity and conflicting outcomes.
- Results in legal uncertainty for joint controllers where DPAs can disregard the joint controllership agreement, ultimately complicating compliance with the GDPR and undermining effective business operations.
- Produces uncertainty for data subjects over which supervisory authority is responsible for investigating their complaint in the case of cross-border processing, negatively impacting a high level of protection of data subject rights.

In line with the CJEU case law, which states particularly in relation to cross-border processing that: "The competence of the lead supervisory authority <…> constitutes the rule whereas the competence

[4] Diverging levels of responsibility between joint controllers have been confirmed in the *Wirtschaftsakademie* case C-210/16, where the CJEU stated: "The existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case", para 43.

[5] Annex I flowchart in European Data Protection Board, Guidelines 07/2022 on the concepts of controller and processor in the GDPR, p. 51 provides a good example.

[6] This is also supported by CJEU case law which highlights the need to ensure consistent application of the GDPR. For example, in Case C-645/19, the Court notes that: "Regulation 2016/679 seeks <…> to ensure consistent and homogeneous application of the rules for the protection of the freedoms and fundamental rights of natural persons with regard to the processing of personal data throughout the European Union and to remove obstacles to flows of personal data within the Union."

of the other supervisory authorities concerned for the adoption of such a decision, even provisionally, constitutes the exception."[7] The EDPB should encourage clear joint-controller arrangements and, as noted by the WP29 in their original guidance, joint controllers should benefit from the OSS based on the joint controllership agreement to avoid re-introducing inconsistent interpretation and enforcement of the GDPR.

CIPL also encourages the EDPB to provide more guidance regarding the cooperation of supervisory authorities in cases involving joint controllers and cross-border processing without undermining the effectiveness of a one-stop-shop mechanism, effective compliance with the GDPR and protection of data subject rights. The EDPB could employ a similar approach to identifying lead and concerned supervisory authorities as noted in Annex 2b of the Guidelines (cases involving a controller and a processor). Instead of potentially having multiple LSA, the LSA could be identified based on the roles and responsibilities set in the joint controllership agreement. In comparison, other SA (non-lead) would be considered a concerned supervisory authority. This approach would reduce conflicts between supervisory authorities and, at the same time, ensure that the relevant SA still has a role in the process.

***

In the context of Guidelines 8/2022, the EDPB should:

- Ensure that arrangements between joint controllers, as noted in Art 26 GDPR, are taken into account when assessing whether the controller in question is responsible for the specific GDPR obligation at issue and whether the local DPA is actually in charge of assessing this specific part of the processing.

- Clarify and ensure that proposed changes to the Guidelines 8/2022 do not undermine the effectiveness of the one-stop-shop mechanism by potentially creating a situation where multiple supervisory authorities take a decision with respect to the same cross-border activity.

We look forward to providing additional input as the Guidelines are finalised.

***

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@HuntonAK.com, Markus Heyder, mheyder@HuntonAK.com, Natascha Gerlach, ngerlach@HuntonAK.com or Lukas Adomavicius, ladomavicius@HuntonAK.com.

[7] Case C-645/19, *Facebook Ireland and others v Gegevensbeschermingsautoriteit,* para 63.