Internal EDPB Document 04/2021 on criteria of territorial competence of supervisory authorities to enforce Article 5(3) of the ePrivacy Directive

Adopted on 18 June 2021

The European Data Protection Board

HAS ADOPTED THE FOLLOWING INTERNAL DOCUMENT

1 BACKGROUND

1. A number of recent decisions adopted by some supervisory authorities ("SAs") competent for the enforcement of Article 5(3) of the ePrivacy Directive[1] show that the territorial application of this directive may differ across SAs, in particular when a controller / service provider has establishments in several member states.
2. The aim of this document is to establish a common interpretation of the territorial competence of SAs responsible for enforcing Article 5(3) of the ePrivacy Directive, whatever the choices made by each Member State when transposing the ePrivacy Directive. This point is not specifically covered in the Opinion on the Interplay between the ePrivacy Directive and GDPR[2]. However, uncertainty on such a fundamental question would risk jeopardizing decisions adopted by the SAs across the European Union.

2 DISCUSSION

3. Article 17(1) of the ePrivacy Directive provides that "*Member States shall bring into force the provisions necessary to comply with this Directive*" and Article 15(1) provides that "*Member States shall lay down the rules on penalties, including criminal sanctions where appropriate, applicable to infringements of the national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented*". It follows from these provisions that it is thus up to each Member State to take the necessary measures to ensure that the objectives set by the ePrivacy Directive are achieved.
4. However, the ePrivacy Directive remains silent regarding its territorial application. Consequently, the case-law of the CJEU on the territorial application of the repealed directive 95/46/EC gives an indication of how the territorial application should be organised. Indeed, in the case *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, 5 June 2018, the Court stated that the supervisory authority of a Member State was entitled to exercise its powers against an establishment of an undertaking situated in its territory and in the course of whose activities the processing is carried out, even if the establishment responsible for the collection and processing of data was situated in another Member State[3].

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC.

[2] EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019.

[3] The Court ruled that *" Articles 4 and 28 of Directive 95/46 must be interpreted as meaning that, where an undertaking established outside the European Union has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State."*

5. If the data controller/service provider has no establishment in a Member State, the national law of this Member State may provide other criteria than establishment to enforce its national law in respect of this controller/service provider.
6. It stems from these elements that each competent SA is entitled to enforce its national law transposing the ePrivacy Directive, as far as it concerns users located in its territorial jurisdiction. It also implies that no legislation transposing the ePrivacy Directive may prevent the SA of another Member State to enforce the ePrivacy Directive in accordance with its national provision, with respect to users located in its territorial jurisdiction[4]. Otherwise, this would not be consistent with the objective of protecting the fundamental rights and freedoms of data subjects, as set by Article 1(1) of the ePrivacy Directive.
7. Ultimately, it would mean that the fine imposed on a controller/service provider would depend on the national legislation of one single Member State. Considering that maximum sanctions for an infringement of the ePrivacy Directive vary significantly across Member States (with some legislations providing for smaller fines), it would mean that, in certain cases, fines might not be a deterrent ensuring an effective protection of European users' data and this could reactivate, at the same time, a risk of forum shopping[5].
8. This does not prevent the SAs to initiate a spontaneous cross border dialogue with the objective to create harmonised conditions regarding ePrivacy matters, as provided by Article 15a (4) of the ePrivacy Directive.

3 CONCLUSION

9. Consequently, when the processing is regulated exclusively by the national law provisions transposing Article 5(3) of the ePrivacy Directive, the EDPB considers that SAs competent for the enforcement of Article 5(3) of the ePrivacy Directive are entitled to exercise the powers conferred on them by their national law, whenever:

- **the controller/service provider is established in their territorial jurisdiction;**

It should be noted that in the case at stake, the processing in question was carried out "in the context of the activities" of the establishment in question.

[4] In its opinion in the case *Wirtschaftsakademie Schleswig-Holstein*, the Advocate General stated:
"*95. The fact that, by contrast with the situation in the case which gave rise to the judgment of 13 May 2014, Google Spain and Google, (56) the Facebook group has a European head office, in Ireland, does not mean that the interpretation of Article 4(1)(a) of Directive 95/46 which the Court adopted in that judgment cannot be applied in the present case. In that judgment, the Court voiced the intention that the processing of personal data should not escape the obligations and guarantees laid down by Directive 95/46. It has been suggested in the present proceedings that the problem of such circumvention does not arise here, because the controller is established in a Member State, namely Ireland. According to that logic, Article 4(1)(a) of Directive 95/46 should be interpreted as requiring that controller to have regard to the legislation of only one Member State and to answer to only one supervisory authority, that is to say, Irish legislation and the Irish authority. Such an interpretation, however, is contrary to the wording of Article 4(1)(a) of Directive 95/46 as well as to the origins of that provision.*
96. Such an interpretation, however, is contrary to the wording of Article 4(1)(a) of Directive 95/46 as well as to the origins of that provision. Indeed, as the Belgian Government rightly observed at the hearing, the directive does not introduce a one-stop-shop mechanism or a country-of-origin principle […] The result, arrived at in Directive 95/46, reflects the wishes of the Member States to preserve their national powers of enforcement. By not adopting the country-of-origin principle, the EU legislature enabled each Member State to apply its own national legislation and thus made the application of multiple national legislations possible.

[5] Article 15 a (1) of the ePrivacy Directive states *" The penalties provided for must be effective, proportionate and dissuasive and may be applied to cover the period of any breach, even where the breach has subsequently been rectified."*

- **the processing is carried out in the context of the activities of an establishment located in their territorial jurisdiction, even when exclusive responsibility for collecting and processing belongs, for the entire territory of the European Union, to an establishment situated in another Member State;**
- **in the absence of controller/service provider or establishment in their territorial jurisdiction, the national law provides another criterion for its enforcement.**

10. **In any event, the measures taken:**
    - **should not concern users located in a territorial jurisdiction for which the SA is not competent;**
    - **should not prevent another competent SA to enforce the ePrivacy Directive in respect of its territorial jurisdiction.**

For the European Data Protection Board

The Chair

(Andrea Jelinek)