Internal EDPB Document 2/2019 on Proposals for Common Strategic Priorities for Supervision and Guidance

Adopted on 4 June 2019

IMPORTANT NOTE:

This document was originally written for internal use among EDPB members. At its Plenary meeting of 14 June 2022, the EDPB has decided, in the interests of transparency, to make this document available to the public by publishing it on its website. This document contains proposals from one of the EDPB Expert subgroup in relation of the Coordinated Enforcement Framework (CEF). In the meantime, the EDPB adopted a document dedicated to this CEF and decided on the CEF topic for 2022. Therefore, some of the information in this document may no longer be up to date.

This document contains redactions as the publication of this information would undermine the commercial interests of a natural or legal person.

Table of contents

The European Data Protection Board

Having regard to Article 70 (1) (e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 3 and Article 22 of its Rules of Procedure as amended on 23 November 2018,

HAS ADOPTED THE FOLLOWING INTERNAL DOCUMENT

1 INTRODUCTION

1. One of the mandates of the Social Media Expert Subgroup (hereinafter "SOCM ESG") is to propose strategic priorities for supervision and guidance. As stated in the Workplan of the SOCM ESG, while providers of social media may have a lead supervisory authority within the "one stop shop" GDPR mechanism, the supervision of other actors, which are associated with, related to or interlinked with social media platforms, is often the responsibility of other supervisory authorities. The SOCM ESG's mandate also recognises that the regulation of the processing of personal data that takes place in the context of social media may be rendered more effective if supervisory authorities agree upon common strategic supervision priorities.

2. Pursuant to its mandate, the SOCM ESG has identified strategic priorities for supervision on the basis of trends in data subject complaints, technological trends, findings or milestones in national investigations concerning social media and related actors. This internal document identifying proposals for common strategic priorities for supervision and guidance is therefore complementary to and recognises the role of competent supervisory authorities (including lead supervisory authorities) in their enforcement activities under the GDPR. The SOCM ESG recognises that these strategic priorities are best tackled in conjunction with other Subgroups, in particular to ensure efficient use of resources and avoid overlap between Subgroups.

3. The present internal document identifies common strategic priorities and recommendations in relation to these priorities (i.e. the Recommendations). Most Recommendations include cooperation with between Subgroups including cooperation with the SOCM ESG. In respect of these Recommendations, it is therefore proposed that the SOCM ESG cooperates with the other Subgroups identified as the strategic priorities either within existing Workplans or in respect of a standalone work items in the future.

4. Where issues are proposed for consideration by other Subgroups, it is recognised that it is entirely a matter for each Subgroup how it wishes to address the relevant issue. For example, where issues have been referred to the Enforcement Expert Subgroup (hereinafter "ENF ESG"), it may be that this issue may form part of the coordinated enforcement framework (hereinafter "CEF"), which is currently under consideration in that context.

2 PROPOSALS FOR COMMON STRATEGIC PRIORITIES

5. The following strategic priorities have been identified by the SOCM ESG:

    a. Adtech

    b. Third-party Apps/APIs

    c. Data brokers

    d. Data subject's right to object to direct marketing

    e. Processing of personal data of non-members of social media services

    f. Interplay between the ePrivacy Directive and the GDPR.

6. In respect of each strategic priority, a number of possible recommendations are identified for potential next steps (the Recommendations). While each recommendation could be beneficial, one recommendation is identified in particular in relation to each identified strategic priority (i.e. the recommendation that carried the broadest support within the SOCM ESG).

2.1 Adtech

7. The adtech sector encompasses a vast array of actors including advertisers, publishers, ad networks, ad exchanges, demand-side and supply-side platforms, data management platforms. It has emerged as a separate eco-system within the online environment which permeates all social networking services as well as extending further to almost all categories of internet activity. Some of the key questions which arise in relation to the regulation of the adtech sector from a data protection law perspective are:

    a. Data subjects' perceived loss of control of their personal data once collected and its consequences including the exercise of data subject rights;

    b. Lawful bases of personal data processing in the context of the adtech industry;

    c. Further processing of personal data collected for specific purposes;

    d. Processing of special categories of personal data;

    e. Employment of data protection by design and default; and

    f. Standard of technical and organisation measures employed in relation to personal data processed in the adtech ecosystem.

8. When considering this topic, the [redacted] Framework should also be considered, as it is one to which many in the adtech sector align themselves.

9. Recommendation 1

It is recommended that the [redacted] industry bodies/ appropriate parties are engaged with via an EDPB stakeholder group with the aim of increasing compliance and reducing complaints. It is recommended that the EDPB stakeholder group could include members from the SOCM ESG, the Technology Expert Subgroup (hereinafter "TECH ESG"), the ENF ESG and the Compliance, e-Government and Health Expert Subgroup. This paper and therefore this recommendation of participation in a potential EDPB Adtech stakeholder group has been mentioned at recent meetings of the aforementioned Subgroups.

10. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 1 may be:

    a. Develop (additional) guidance: the TECH ESG might develop further guidance addressing this issue, for example by:

        i. Updating Opinion 2/2010 on online behavioural advertising;[1]

        ii. Updating Opinion 2/2013 on obtaining consent for cookies;[2]

        iii. Assessing and/or reviewing the [redacted] Framework.

    b. The ENF ESG could also consider this issue further as part of the CEF.

2.2 Third Party Apps/APIs

11. Many major online platforms, including (but not limited to) social networks such as [redacted], enable third parties to develop apps on those platforms which can process users' personal data. The third parties involved may include actors within the online advertising sector as mentioned under "Adtech". Compliance with data protection law by online platforms and third party app developers requires fresh scrutiny under the GDPR, due to the potential risks to individuals in terms of transparency, lawful basis, consent and other key data protection principles such as purpose limitation, data minimisation and security of processing. Third-party apps/APIs are also broader in scope than the facilities major social media platforms offer developers, encompassing much of the online and particularly the mobile eco-systems. Given the state of the art of technological development and the ways in which users currently interact with online services, we believe there are clear risks posed to individuals and that SAs should ensure that actors in this space are appropriately complying with data protection obligations.

[1] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf
[2] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

12. Recommendation 2

It is recommended that this issue be further developed as part of SOCM ESG's Work Item 3 "Governance of social media platforms", which is planned for later in 2019. SOCM ESG also proposes to engage with the ENF ESG (e.g. in order identify case studies), the TECH ESG (e.g. regarding measures to limit misuse) and Key Provisions Expert Subgroup (e.g. as regards possible arrangements among controllers), as appropriate.

13. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 2 may be:

    a. Develop (additional) guidance: the TECH ESG or Key Provisions Expert Subgroup (hereinafter "KEYPRO ESG") might also further address this matter, for example by:

        i. Updating Opinion 5/2009 on online social networking;[3] and/or

        ii. Updating Opinion 02/2013 on apps on smart devices.[4]

    b. The ENF ESG could also consider this issue further as part of the CEF.

2.3 Data Brokers

14. Data brokers collect personal data and resell or share that information with other stakeholders. In other words, they aggregate data collected from a wide variety of sources. They subsequently transfer the aggregated data to third parties, i.e. their clients, for a variety of purposes, including targeting of data subject (advertisement, improvement of customer experience), and fight against fraud for example.

15. Generally speaking, there are two situations: in the first one, the data broker acts as an intermediary between its clients who are seeking to monetise their databases on the one hand, and those that are seeking to enrich their databases on the other. Here, the broker acts on behalf of and in the name of its clients. In the second case, the data broker centralises, aggregates and enriches the data on his own account, and sells this enriched data to other stakeholders.

16. Sources of personal data might include the following: (i) database formed as part of the relationship between a company and its customers (classic customer files, loyalty programs, etc.), (ii) data derived from the data subject's navigation activity (cookies, fingerprint and other tracers), (iii) the use of mobile applications, and (iv) the data relating to purchases made online.

17. There are many issues that have been identified regarding this type of processing, of which transparency is one. Indeed, it is common practice for data controllers to collect the consent for the transmission of the personal data by simply including the "partners", without even providing information on the purpose of the processing or the identity of the recipients. In addition, certain data brokers may not inform data subjects on their role as data controllers or

[3] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf
[4] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

on their rights. In this sense, the EDPB should provide guidelines on the precise information that data brokers need to provide to data subjects and possible best practices for doing so.[5]

18. Another issue which should be tackled by the EDPB is one of the legal basis. First of all, when the legal basis is consent (for instance because the processing involves the implementation of a tracking device for advertisement purposes), it may be that the clients of the data brokers have no way of proving that the data subject has consented to the re-use of their data by the data brokers and their transmission to them. In addition, the lack of specificity of consent due to the above-mentioned lack of transparency, may deprive the partners' processing of a legal basis, which would render the re-use of the data purchased from the data broker unlawful. Furthermore, it appears that many data brokers seek to rely on legitimate interests for their processing. It is proposed that the EDPB provide practical examples and concrete guidelines on the circumstances in which legitimate interest would be a valid legal basis. Indeed, the opacity of the online advertising industry, the difficulty for the data subject to identify the data controllers processing their data, and the lack of true control that they may exercise (including the ability to exercise the unconditional right to opt-out of direct marketing (article 21 (2)), may mean that legitimate interest may not be employed as a lawful basis for the relevant processing.

19. **Recommendation 3**

It is recommended that the ENF ESG could consider this issue in the context of the CEF.

20. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 3 may be:

    a. Develop (additional) guidance: Subgroups such as the TECH ESG or KEYPRO ESG could further progress this issue (e.g. in the context of the update of the opinion on legitimate interest and/or future work items of the TECH ESG).

    b. The SOCM ESG could also refer to the role of data brokers in the context of SOCM ESG's Work Item 1 and/or 3.

2.4 Data subject's right to object to direct marketing (Art. 21(3) GDPR)

21. Articles 21(2) of the GDPR provides that where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Article 21 (3) also states that where the data subject objects to processing for direct marketing purposes, the personal data shall no longer

[5] It is indeed important to remind data brokers that article 14 of the GDPR requires that they inform the data subject within a month before starting processing the data on their own account. It may also be necessary to remind data controllers that as stated in article 13 of the GDPR, they need to inform the data subject before transmitting the data to data brokers. In this sense, the EDPB could recommend concrete solutions, such as presenting the data subject with the boxes: one for consenting to the collection of the data processed and the profiling by the data controller, and the second one for the processing to be carried out by partners, including data brokers. A hyperlink could also be provided with an updated listing the names of data brokers who are the recipients as well as data controllers of the data.

be processed for such purposes. Article 21(5) provides that in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

22. It appears that the right to object is absolute and that once the data subject has exercised this right, the controller needs to stop the processing of personal data for direct marketing purposes. There are however a few questions relating the right of objection for direct marketing purposes which would benefit from a harmonised approach at the European level.

23. First of all, the concept of "direct marketing" is not clearly defined in the GDPR and may, in some situations, be difficult to delineate precisely. For instance, in the context of social media, the scope of the definition of "direct marketing" may be a little difficult to identify. Indeed, some social media providers offer advertisers tools (such as the use of "Lookalike Audiences" by Facebook) which enable an advertiser to target people who are similar to their existing customers. In this situation, it is not clear whether the existing customers are being "directly marketed" to or not, as they are not receiving any targeted advertisement themselves but at the same time, their personal data is being processed for the purposes of targeting other data subjects. Speaking more broadly, it should be clarified whether or not targeted display ads are included within the scope of direct marketing. It would be beneficial to all stakeholders to clearly determine the scope of direct marketing, insofar as the GDPR does not provide a clear definition of this concept.

24. Secondly, the GDPR is not clear whether the controller needs to delete the data as well once the data subject objects to the processing for direct marketing purposes. One might consider that the controller only needs to stop the processing of the data for this purpose and to ensure that their preference not to receive direct marketing solicitations is complied with. This is a question which could be addressed at European level.

25. Another point which should be addressed at the European level is the question of tracking techniques, including cookie-based technologies, social plugins and tracking pixels that are stored on the terminal equipment of the data subject. The EDPB is aware of the review of the ePrivacy Directive (2002/58/EC), which requires the collection of consent for most online marketing messages or marketing calls, and online tracking methods including the use of cookies or apps or other software. Indeed, article 5(3) of the ePrivacy Directive requires prior informed consent for storage or for access to information stored on a user's terminal equipment. The EDPB could also clarify that in addition to the right of objection which is absolute for the processing for direct marketing purposes, the data subject should be able to withdraw his or her consent as easily and without any justification. The EDPB could also recall that in respect of personal data which the right to erasure is exercised in accordance with article 17(1)(b) GDPR, the controller is obliged to erase such personal data "without undue delay".

26. Furthermore, the EDPB could clarify when the right to object to the processing for direct marketing under article 21 of the GDPR is exercisable in respect of direct marketing. It is worth noting that according to article 21, the data subject can object to the processing at any time. Some Member States even consider that the right to object can be exercised before the processing takes place. A harmonized approach on this point is also recommended at the European level.

27. Finally, processing of personal data for marketing purposes often involves a significant number of stakeholders (partners, data brokers, data processors...), who may, under article 26 of the

GDPR, be categorised as joint controllers. Data subjects should be able to exercise their right of objection to any of the data controller who must then put in place processes to reflect the will of the data subject to the next "link" in the chain.

28. **Recommendation 4**

> It is recommended that SOCM ESG could provide assistance to KEYPRO ESG in the development of guidance on this issue, specifically in the context in the proposed guidance in respect of data subject rights, which is scheduled for 2019.

29. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 4 may be:

    a. SOCM ESG could also consider dealing with this issue as part of SOCM ESG's Work Item 1 or 3;

    b. ENF ESG could also consider this issue further as part of the CEF.

2.5 Processing of personal data of non-members of social networking services

30. Certain social media providers also process the personal data of people who are not members of the social networking service, for example, by tracking their browsing behaviour across multiple websites or by collecting such information through mobile applications. Collection of personal data of non-members may be achieved using technical tools (such as cookies) and browser information and other tools developed by social media providers. In this context, the existence of a legal basis for the processing of non-member personal data should be examined.

2.5.1 General risks regarding the processing of personal data of "non-members"

31. The general risk of the processing of personal data of social media users is already being addressed by the SOCM ESG in the context of Work item 1 (the targeting of social media users) which identifies inter alia the following risks: risks related to privacy and protection of personal data, discrimination, manipulation, the interference of political discourse and democratic electoral process and chilling effects on freedom of expression and the restraint of access to information.

32. In regard to "non-members" these risks are increased by a lack of transparency. The reasonable expectations of the individual without a specific social media account do not include the systematic targeting and profiling of their person.

2.5.2 Standard of protection for "non-members"

33. In its decision of June 5, 2018 (file number C-210/16), the Court of Justice of the European Union ruled that a "fan page administrator's responsibility for the processing of the personal data of (non-members) appears to be even greater, as the mere consultation of the homepage by visitors automatically starts the processing of their personal data." This emphasises the high level of protection that is needed regarding the persons whose personal data are processed by the social networking services without having an account on the relevant platform. Because of the non-transparent practices in this field, there are a high number of data subjects who are not in a position to anticipate and assess the processing of their personal data. This

corresponds with the general risk regarding the processing of personal data of "non-members".

2.5.3 Third party apps as multipliers

34. The described risks are usually multiplied by the use of third party apps and the combination of the data collected of the social network service and the data processed by the operators of the third party apps. Through the processing of personal data across different applications a profiling and systematic monitoring could be established. As different actors in this ecosystem of data processing in the social media and advertisement sector share the data of many individuals and evaluate and score these individuals in order to make decisions and assessments about them, these risks are also relevant for "non-members".

2.5.4 Unlawfulness of the processing and supervision of joint controllers

35. With regard to Work Item 1 of the SOCM ESG concerning the targeting of social media users and the definition of joint controllers under Article 26 GDPR, this issue may stretch beyond controllers or processors of social media services. According to Article 26 GDPR specific operators of a fan page or other comparable types of social media accounts can be held responsible for the processing of personal data of "non-members" of these platforms. Therefore, supervisory authorities should raise the awareness of this common responsibility. The first step which could be taken are informal or formal investigations and the German Conference of the Independent Data Protection Authorities of the Federal State and the Länder (DSK) has provided an example in form of a questionnaire in its "DSK decision regarding Facebook Fan Pages".[6]

36. Recommendation 5

> It is recommended that SOCM ESG address this Issue as part of SOCM ESG's Work Item 3 "Governance of social media platforms", which is planned for later in 2019. In this context and in developing Work item 3, the SOCM ESG plans to, at the appropriate time, seek the input from both the TECH ESG and KEYPRO ESG.

37. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 5 may be:

    a. Develop guidance: the SOCM ESG or another Subgroup (such as the TECH ESG or KEYPRO ESG) could progress this issue, for example by updating Opinion 4/2012 on Consent Exemption,[7] 2/2010 on Online Behavioural Advertising[8] and 5/2009 on Online Social Networking.[9]

    b. Develop additional guidance: the SOCM ESG could further progress this topic.

    c. ENF ESG could also consider this issue further as part of the CEF.

[6] https://datenschutz-hamburg.de/assets/pdf/DSK-decision_regarding_Facebook_Fan_Pages.pdf
[7] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf
[8] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf
[9] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf

2.6 Interplay between the ePrivacy Directive and the GDPR

38. There are processing activities which trigger the material scope of both the GDPR and the ePrivacy Directive. For example, the gaining of access to information stored in an end-user's device may also give rise to the processing of personal data. If that is the case, both Article 5(3) of the ePrivacy Directive and the GDPR shall apply.[10]

39. The aim of the ePrivacy Directive is to particularise and complement the provisions of the GDPR.[11] As a "lex specialis", the ePrivacy Directive takes precedence over the (more general) provisions of the GDPR insofar as the matter is specifically addressed by the ePrivacy Directive.[12]

40. While the interaction between the ePrivacy Directive and Directive 95/46 has already been addressed in previous WP29 guidance, questions have emerged regarding the competence of supervisory authorities to exercise their powers under the GDPR in cases where both the GDPR and national implementations of the ePrivacy Directive are applicable.

41. The ePrivacy Directive allows Member States to assign supervisory competences to national regulatory authorities other than data protection authorities. It does not, however, stipulate that the supervision of its provisions shall be the exclusive competence of such a national regulatory authority,[13] and, as stated above, this is a matter for national Member State law. The question may be asked to what extent data protection authorities should consider the provisions of the ePrivacy Directive when exercising their powers under the GDPR (e.g., when assessing the lawfulness of processing). Closely related is the question of whether the applicability of ePrivacy rules imposes any limits on the handling of cases in the context of the cooperation and consistency mechanisms of Chapter VII, and if so, to what extent. Further clarification may also be necessary regarding the extent to which a set of processing operations can be governed by provisions of the ePrivacy Directive and the GDPR (e.g. in terms of lawfulness of processing including consent, principles relating to the processing of personal data, transparency, etc).

42. Recommendation 6

No further immediate action recommended given the outcome of the Art. 64(2) GDPR opinion launched by the Belgian DPA on this topic. Additional guidance may be provided in the context of other work items, as appropriate (e.g. C-ITS).

[10] See e.g. Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 9 ("*If as a result of placing and retrieving information through the cookie or similar device, the information collected can be considered personal data then, in addition to Article 5(3), Directive 95/46/EC will also apply*.").

[11] Article 1(2) of Directive 2002/58 as amended by Directive 2006/24/EC and Directive 2009/136/EC in light of article 94(2) of the GDPR.

[12] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171, p. 10. See also recital (173) GDPR ("*This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à- vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council (2), including the obligations on the controller and the rights of natural persons. […]*")

[13] On the contrary, the ePrivacy Directive explicitly recognises that multiple authorities may be competent for its supervision and enforcement. See article 15a of Directive 2002/58 as amended by Directive 2006/24/EC and Directive 2009/136/EC.

43. Other supervision activities, guidance or other actions which may be taken contingent on and, where appropriate, in addition to, Recommendation 6 may be:

    a. The ENF ESG could also consider this issue further as part of the CEF.

For the European Data Protection Board

The Chair

(Andrea Jelinek)