Report of the work undertaken by the supervisory authorities within the 101 Task Force

28 March 2023

Table of contents

DISCLAIMER

The EDPB created the 101 Task Force to promote cooperation and effective exchange of information between the Supervisory Authorities on this specific subject-matter, in accordance with Article 70(1)(u) GDPR. The positions presented in this document result from the coordination of the Supervisory Authorities taking part in the task force with a view to handling the “101 complaints” received from NOYB regarding the tools “Google Analytics” and “Facebook Business Tools”. They reflect the common denominator agreed by the Supervisory Authorities in their interpretation of the applicable provisions of the GDPR. The positions do not prejudge the analysis that will have to be made by the Supervisory Authorities of each complaint and each tool concerned. In particular, it must be taken into account that the circumstances may change over time, for example, in case the aforementioned tools change from a technical point of view or in case the legal framework changes. The positions of the Supervisory Authorities expressed in this report do not represent the position of the EDPB.

1 BACKGROUND

1. On 17 August 2020, a total of 101 complaints were lodged with the European Supervisory Authorities (hereinafter: "SAs") by NOYB regarding transfers of personal data to the USA. The complaints revolve around the implementation of the tools "Google Analytics" and "Facebook Business Tools" (hereinafter: "tools") on a website and the subsequent processing[1] of personal data that may follow because of such implementation.

2. During the Plenary meeting of the European Data Protection Board (EDPB) on 2 September 2020, it was decided that a task force shall be established in order to ensure a consistent approach to handle the complaints ("101 task force", SAs participating in the "101 task force" are hereinafter referred to as "TF members").

3. The TF members focused their analysis on the subsequent processing that should comply with the requirements of the GDPR and that may be subject to cooperation. Following several meetings of the TF members to coordinate their actions, the following points were noted:

2 ASSESSMENT

2.1 Transfers of personal data

4. In general, before assessing the lawfulness of transfers of personal data within the meaning of Chapter V of the GDPR, controllers must ensure that all other provisions of the Regulation are complied with[2]. For example, if a certain tool is being used for collection of personal data on a website without a legal basis within the meaning of Article 6(1) GDPR, the data processing is unlawful, even if there were no issues with the requirements of Chapter V GDPR.

5. However, due to the subject matter of the present complaints, the following assessment will be limited to issues related to Chapter V of the GDPR.

6. The TF members agreed that there was no compliance with Chapter V of the GDPR if the transfer was based on the invalidated EU-US adequacy decision after 16 July 2020[3]. Furthermore, there was an agreement that concluding standard data protection clauses pursuant to Article 46 (2)(c) GDPR with retroactive effect, as brought forward by an entity in a complaint case, is not permissible[4].

7. Where standard data protection clauses were concluded, and supplementary measures implemented as appropriate safeguards, the TF members recall that such measures must address the specific deficiencies identified by the ECJ in its judgement from 16 July 2020[5] in the assessment of the situation in the third country[6] in order to ensure that this legislation will not impinge on the safeguards adduced.

---

[1] The term "subsequent processing" refers to the processing operations which take place after storing or gaining access to information stored in the terminal equipment of a user in accordance with Article 5(3) Directive 2002/58/EC (for example, the placement or reading of cookies).
[2] EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, version 2.0, paragraph 5.
[3] ECJ C-311/18 (Schrems II), paragraph 201.
[4] According to the wording of Article 44 and Article 46 (1) GDPR, the appropriate safeguards must be in place before the transfer of personal data.
[5] ECJ C-311/18 (Schrems II).
[6] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 75.

8. In this context, the TF members agreed that encryption by the data importer was not a suitable measure if the data importer, as provider of the tool, has legal obligations to provide the cryptographic keys[7]. In addition, there was an agreement that anonymization functions, such as the anonymization of the IP address, are not a suitable measure where the anonymization takes place only after all the data has been transferred to the third country to the importer[8].

9. Furthermore, in cases where a processor acts as data exporter on behalf of the controller (the website operator), the controller is also responsible and could be liable under Chapter V of the GDPR, and also has to ensure that the processor provides for sufficient guarantees under Article 28 GDPR[9].

2.2 Principle of accountability

10. In cases where website operators are regarded as controller, they must carefully examine whether the respective tool can be used in compliance with data protection requirements[10]. The European Court of Justice (ECJ) interprets the accountability principle as requiring every data controller to be able to demonstrate that appropriate measures have been taken to safeguard the right to data protection, in order to prevent any breaches of the provisions of the GDPR.[11]

11. If such evidence cannot be provided (and tools are integrated on a website without a prior compliance check), in particular in case of joint-controllership, this may result in a breach of the principle of accountability. Following a case by case analysis, in particular where the controller is not in a position to provide sufficient elements to demonstrate how transfers take place, this could lead to a breach of Article 5(2) and Article 24(1) GDPR in accordance with the accountability principle stipulated in these Articles.

12. The TF members emphasise that not only the website operators (as controllers), but also the respective provider of tools who process personal data must ensure continuous compliance with the GDPR, either because the provider of the tool is, at least concerning certain processing operations, regarded as controller or, where the provider is qualified as a processor, due to the assistance obligations specified in Article 28 GDPR.

2.3 Allocation of roles

13. As the decision of a website operator to integrate and use third-party tools (such as social media plugins or analytics tools,) regularly results in the processing of personal data of the website visitors, this could entail liability for the website operator, even if the liability may be limited to certain processing operations[12].

14. In the context of the present cases, the TF members agreed that the decision of a website operator to use a specific tool for specific purposes (for example, analyzing the behavior of the website visitor) is

[7] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 81.
[8] As it cannot be ruled out that access to the data will take place between the transfer to the third country and anonymization.
[9] EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, version 2.0, paragraph 19.
[10] In addition, the requirements of Article 5(3) of Directive 2002/58/EC (ePrivacy Directive) may be applicable. This is the case when information is stored or accessed to in the terminal equipment of a user (for example, the placement or reading of cookies). For more information, the EDPB recommends its Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR as well as its Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications.
[11] ECJ C-129/21 (Proximus), paragraph 81.
[12] ECJ C-40/17 (Fashion ID), paragraph 74.

regarded as determining the "purposes and means" pursuant to Article 4(7) GDPR. Save for those cases in which the SA's analysis provides otherwise, those website operators are hence to be regarded as controllers for the processing of personal data of the website visitors that takes place within the context of the use of the tools on those websites. The degree of liability for the processing operations, however, must be determined on the basis of a case-by-case analysis, taking into account the different functions and options the respective tool provides.

15. Concerning such case-by-case analysis, the TF members recall that the allocation of roles is the result of a thorough analysis of objective factors, including the factual elements or circumstances of the case[13]. In particular, the conclusion of agreements pursuant to Article 28 or Article 26 GDPR between website operators and providers does not limit the assessment and qualification retained by SAs.

3 OUTCOME OF THE COMPLAINTS

16. This common assessment has enabled several SAs to adopt consistent decisions in the present "101 complaints"[14].

17. Notably, SAs have ordered website operators to comply with the requirements of Chapter V of the GDPR, and if necessary, to stop the transfer at stake. Part of these decisions have been adopted in the framework of the One-Stop-Shop mechanism, in cooperation with all concerned SAs. In some cases, website operators have stopped using the tools at stake before any decisions by the SAs, which, in practice, resulted in decisions without any suspension order.

18. Furthermore, additional guidance and practical recommendations have been provided by Several Authorities to follow up on the consequences of these decisions with regards to alternative solutions.

19. Further decisions are expected in due time regarding the remaining complaints for which decisions have not been adopted yet.

[13] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.1, cf. paragraph 12.
[14] At this point of time, the following SAs have already issued decisions in the context of the present complaints: AT, DK, EE, ES, FI, FR, HU, IT. Furthermore, the TF members note that the EDPS has also issued a decision in relation to "Google Analytics" in the complaint case 2020-1013 against the European Parliament.