Deliberation of the restricted committee No. SAN-2021-024 of 31 December 2021 concerning FACEBOOK IRELAND LIMITED

***Courtesy translation**: in the event of any inconsistencies between the French version and this English courtesy translation, please note that the French version shall prevail and have legal validity.*

Since the translation is currently being finalized, a new updated version may be put online in the next few days.

The Commission Nationale de l'Informatique et des libertés (CNIL - French Data Protection Authority), meeting in its restricted committee consisting of Mr Alexandre Linden, Chair, Philippe-Pierre Cabourdin, Vice-Chair, and Mesdames Christine Maugüe and Anne Debet and Mr Alain Dru, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data;

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular articles 20 *et seq.*;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 concerning adoption of CNIL's internal regulations; Having regard to Decision No. 2021-044C of 6 April 2021 of the Chair of the Commission to instruct the secretary-general to carry out or to have a third party carry out an assignment to verify the processing accessible from the domain "facebook.com" or concerning personal data collected from that domain;

Having regard to the Decision of the Chair of the Commission nationale de l'informatique et des libertés appointing a Rapporteur before the restricted committee, of 26 July 2021;

Having regard to the report of Ms Valérie Peugeot, Rapporteur commissioner, notified to FACEBOOK IRELAND LIMITED on 1st September 2021;

Having regard to the written observations made by the counsel of FACEBOOK IRELAND LIMITED on 8 October 2021;

Having regard to the Rapporteur's response to these observations notified to FACEBOOK IRELAND LIMITED on 28 October 2021;

Having regard to the new written observations made by the counsel of FACEBOOK IRELAND LIMITED, received on 21 November 2021;

Having regard to the letter sent by FACEBOOK IRELAND LIMITED to the chairman of the restricted committee and to the Rapporteur on 6 December 2021;

Having regard to the oral observations made at the restricted committee session;

Having regard to the other exhibits;

The following were present at the restricted committee session on 2 December 2021:
- Ms Valérie Peugeot, Commissioner, her report having been heard;

In the capacity of representatives of FACEBOOK IRELAND LIMITED:
- […];

FACEBOOK IRELAND LIMITED having addressed the session last;

The restricted committee has adopted the following decision:

I. Facts and proceedings

1. Founded in 2004 and with its head office in the United States (Menlo Park, California), FACEBOOK INC., known as META PLATFORMS, INC. since 28 October 2021, has developed a social network (hereinafter "the Facebook social network"), available on the web and on mobile applications, which allows users who have created an account to share their experiences and socialise. It currently brings together over 2.5 billion active users per month in the world.

2. META PLATFORMS, INC. has dozens of offices located in about thirty countries and has more than 35,000 employees worldwide. It has its own advertising department and since its creation, it has notably acquired the Instagram photo sharing service (2012) as well as the instant messaging service WhatsApp (2014). In 2020, it generated revenue of nearly 86 billion dollars and a net profit of more than 29 billion dollars. 98% of this revenue is generated by the income from advertising used in connection with its products and services.

3. FACEBOOK IRELAND LIMITED (hereinafter "FIL"), located at 4 Grand Canal Square, Grand Canal Harbour in Dublin, Ireland, has been presenting itself as the head office of the Facebook Group for its activities in the European region since 2008. A subsidiary of META PLATFORMS, INC. it employs approximately […] employees. In 2019, it generated revenue of over [...] euros and a net profit of over [...] euros.

4. FACEBOOK FRANCE, located at 6 rue Ménars, Paris (75002), is the establishment of META PLATFORMS, INC. in France. A subsidiary of META PLATFORMS, INC., it employs […] employees. In 2019, it generated revenue of over [...] euros and a net profit of [...] euros.

5. On 8 April 2021, following four referrals filed between October 2020 and March 2021, a CNIL delegation carried out an online check on the website "facebook.com" pursuant to Decision No. 2021-044C of 6 April 2021 of the Chair of the Commission Nationale de l'Informatique et des Libertés (hereinafter "the CNIL" or "the Commission").

6. The purpose of this mission was to verify compliance by the company with the provisions of amended Act No. 78-17 of 6 January 1978 on information technology, data files and liberties (hereinafter "the French Data Protection Act" or "Act of 6 January 1978"), in connection with processing consisting of operations to read and/or write information in the terminal of users residing in France during their visit to the website "facebook.com".

7. On 16 April 2021, the delegation sent two questionnaires to FACEBOOK FRANCE and FIL, asking them in particular to specify the purposes of the operations to read and/or write carried out from the website "facebook.com" in the terminal of users residing in France, and to confirm that FIL was indeed the data controller for these operations. The companies were also invited to clarify their organisation, activities and links between each other.

8. These companies replied to these questionnaires respectively on 21 May and 11 June 2021, confirming in particular that FIL was acting as *"data controller for the processing of personal data used in the context of the provision of the Facebook service to users in the European region, including for the operations to write and read cookies on the website "facebook.com""*.

9. On 26 July 2021, on the basis of Article 22 of the Act of 6 January 1978, the Chair of the Commission appointed Ms Valérie Peugeot as Rapporteur for the purpose of investigating these elements.

10. On 1st September 2021, at the end of her investigation, the Rapporteur issued to FIL a report detailing the breach of the French Data Protection Act which she considered to be constituted in this particular case with regard to freedom of consent, since the company did not make available to users located in France, on the website "facebook.com", a means of refusing operations to read and/or write information in their terminals with the same degree of simplicity as the means provided to accept their use. Also attached to the report was an invitation to attend the restricted committee session held on 2 December 2021.

11. This report proposed to the restricted committee handing down an administrative fine against FIL, along with an injunction to ensure the compliance of the processing consisting of operations to read and/or write information carried out, on the website "facebook.com", on the terminal of users residing in France with the provisions of Article 82 of the French Data Protection Act, combined with a periodic penalty payment. The report also proposed that this decision be made public and that the company no longer be identifiable by name upon expiry of a period of two years following its publication.

12. By letter of 6 September 2021, the company requested an additional deadline from the chairman of the restricted committee in which to submit its observations in response to the Rapporteur's report, which was granted on 9 September, on the basis of Article 40(4) of Decree No. 2019-536 of 29 May 2019 implementing the French Data Protection Act (hereinafter "the Decree of 19 May 2019").

13. On 8 October 2021, the company submitted observations in response to the Rapporteur's report.

14. On 18 October 2021, the Rapporteur asked the chairman of the restricted committee for an additional deadline in which to reply to the company's observations, which was granted on 21 October, of which the company was informed on the same day.

15. On 28 October 2021, the Rapporteur replied to the company's observations.

16. On 29 October 2021, the company asked the chairman of the restricted committee for an extension of the deadline in which to submit its observations on the Rapporteur's reply, which was granted on 4 November.

17. On 21 November 2021, the company submitted further observations in response to those of the Rapporteur.

18. On 29 November 2021, the company requested that the data expressly identified in its submissions as falling under business secrecy should not be disclosed to the public at the restricted committee session, which the chairman of the restricted committee allowed by a letter dated 30 November 2021.

19. The company and the Rapporteur presented oral observations at the restricted committee session, which took place on 2 December 2021.

20. On 6 December 2021, the company sent the chairman of the restricted committee and the Rapporteur additional information reporting on an update being rolled out on the website "facebook.com".

II. Reasons for the decision

A. On the competence of the CNIL

1. On the material competence of the CNIL and the non-applicability of the "one-stop-shop" mechanism provided for by the GDPR

21. The provisions of 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 - as amended by Directive 2006/24/EC of 15 March 2006 and by Directive 2009/136/CE of 25 November 2009 (hereinafter referred to as the ePrivacy Directive) - relating to the storage of or access to information already stored on the terminal equipment of a subscriber or user, have been transposed into national law in Article 82 of the French Data Protection Act, in Chapter IV "*Rights and Obligations for Processing in the Electronic Communications Sector*" of this Act.

22. Under Article 16 of the French Data Protection Act, "*the restricted committee shall take measures and impose sanctions against data controllers or processors who do not comply with the obligations arising [...] from this law"*. According to Article 20(III) of the same Act, "*where the data controller or its processor fails to comply with the obligations arising* […] *from this Act, the chair of the CNIL* […] *may refer the matter to the restricted committee"*.

23. The Rapporteur considers that the CNIL is materially competent in accordance with these provisions to monitor and, where appropriate, sanction the operations of access to or deposit of information carried out by the company on the terminals of users of the Facebook social network residing in France and, more specifically, the fact that the company fails to recognise the freedom of consent of Internet users by not providing them with a means of refusing operations to read and/or write information in their terminal that has the same degree of simplicity as the means provided for accepting their use.

24. The company disputes this competence on the grounds that the alleged breach does not fall within the scope of the ePrivacy Directive.

25. It argues that, unlike the companies Google and Amazon, sanctioned by the restricted committee in December 2020 for a breach of the prohibition on placing cookies on users' computers without having first obtained their consent (CNIL decisions, restricted committee, 7 December 2020, SAN-2020-012 and SAN-2020-013), it is only being criticised, in respect of these proceedings, for having breached the rule according to which it must be as easy for users to refuse the deposit of cookies as to consent to this.

26. However, according to the company, this rule does not result, as such, from any applicable statutory or regulatory provision and is a creation of the CNIL, formalised in the deliberations of 17 September 2020 No. 2020-091 adopting guidelines on the application of Article 82 of the amended Act of 6 January 1978, to operations to read and/or write in a user's terminal (in particular "cookies and other tracers") and No. 2020-092 adopting a recommendation proposing practical procedures for ensuring compliance in the event of use of "cookies and other tracers" (hereinafter the "Guidelines and Recommendation of 17 September 2020").

27. The company considers that, assuming that this rule actually exists, it could not materially fall within the scope of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "Regulation" or the "GDPR"), as the CNIL partially acknowledged in a communication dated 2 April 2021 posted on its website indicating that "*the mere presence of a "Settings" button in addition to the "Accept all" button tends, in practice, to deter refusal and therefore does not allow compliance with the requirements laid down by the GDPR.*"

28. The company concludes that it would be appropriate to apply the "one-stop-shop" mechanism provided for in Chapter VII of the Regulation to these proceedings. Under this mechanism, since FIL, which is the data controller in question, is established in Ireland and its head office is located in that country, the supervisory authority competent to hear the facts alleged against it would not be the CNIL but the Irish data protection authority, the Data Protection Commission (hereinafter "the DPC").

29. **First**, the restricted committee states that a distinction should be made between, on the one hand, operations consisting of depositing and reading cookies in a user's terminal and, on the other hand, the subsequent use made of the data generated by these cookies, for example for profiling purposes, referred to as "subsequent processing" (also known as "further processing").

30. It points out that each of these two successive stages is subject to different legal rules: whilst reading and/or writing operations are governed by special rules, as laid down in Article 5(3) of the ePrivacy Directive, subsequent processing falls within the scope of the GDPR and, as such, may be subject to the "one-stop shop" mechanism in the event that this involves cross-border processing.

31. It points out that it is apparent from the above provisions that the French legislator has instructed the CNIL to ensure compliance with the provisions of the ePrivacy Directive transposed into Article 82 of the French Data Protection Act, by entrusting it in particular with the power to sanction any breach of this article. It points out that this competence was notably recognised by the French State Council in its decision *Association des agences-conseils en communication* of 19 June 2020 concerning CNIL deliberation No. 2019-093 adopting guidelines on the application of

Article 82 of the amended Act of 6 January 1978 to operations to read and/or right in a user's terminal. The French State Council in fact noted that "*Article 20 of this act entrusts [the] Chair [of the CNIL] with the power to take corrective measures in the event of non-compliance with the obligations resulting from Regulation (EU) 2016/279 or its own provisions, as well as the possibility of referring matters to the restricted committee with a view to the imposition of sanctions likely to be imposed*" (French State Council, 19 June 2020, application 434684, paragraph 3).

32. In this particular case, the restricted committee notes that these proceedings only concern the reading and/or writing operations carried out on the terminal of users located in France using the Facebook social network, the material findings made by the delegation during the online control of 8 April 2021 having concerned only these operations, without making any reference to the subsequent processing carried out on the basis of the data collected via these cookies.

33. **Secondly**, the restricted committee states that under the rules providing for the relationship between the ePrivacy Directive and the GDPR, Article 1(2) of that Directive provides that *"the provisions of this Directive particularise and complement Directive 95/46/EC"* of the European Parliament and of the Council of 24 October 1995 on the protection of personal data [hereinafter "Directive 95/46/EC"], it being stated that, since the entry into force of the Regulation, references to Directive 95/46/EC are to be construed as references to the GDPR, in accordance with Article 94 of the GDPR.

34. Similarly, it follows from recital 173 of the GDPR that this legislation expressly provides that it should not apply to the processing of personal data *"subject to specific obligations with the same objective [of protection of fundamental rights and freedoms] set out in Directive 2002/58/EC of the European Parliament and of the Council, including the obligations on the controller and the rights of natural persons".*

35. The restricted committee points out that this relationship was confirmed by the Court of Justice of the European Union (hereinafter referred to as the CJEU) in its *Planet49* decision of 1st October 2019 (CJEU, 1st October 2019, C-673/17, paragraph 42).

36. It also points out that the ePrivacy Directive, for the specific obligations it entails, provides for its own mechanism for the implementation and control of its application by leaving to Member States, through its Article 15a, the task of specifying, within the framework of their national law, the system of sanctions that they wish to implement to guarantee its effectiveness.

37. It notes in this particular case that the rule laid down in Article 5(3) of the ePrivacy Directive, according to which reading and/or writing operations must systematically form the subject of the user's prior consent, after the provision of information, constitutes a specific obligation, since it prohibits a party involved from relying on the bases of lawfulness mentioned in Article 6 of the GDPR in order to be able to lawfully proceed with these operations of reading and/or writing on the terminal. It follows that breach of this rule falls within the specific control and sanction system provided for by the ePrivacy Directive and not that provided for by the GDPR.

38. The restricted committee also notes that the EDPB, in its Opinion 5/2019 of 12 March 2019 on the interplay between the ePrivacy Directive and the GDPR, expressly excluded the application of the "one-stop shop" mechanism to facts that are materially covered by the ePrivacy Directive in these terms: "*Following Chapter VII of the GDPR, the cooperation and consistency mechanisms available to data protection authorities under the GDPR concern the monitoring of the application*

of GDPR provisions. The GDPR mechanisms do not apply to the enforcement of the provisions contained in the ePrivacy Directive as such" (EDPB, Opinion 5/2019, 12 March 2019, paragraph 80).

39. It also notes that the CJEU, in a *Facebook Belgium* judgment handed down on 15 June 2021, supported the aforementioned EDPB Opinion 5/2019, while agreeing, on this point, with the opinion of its Advocate General Bobek, who had considered that "*In order to decide whether or not a case does in fact fall within the scope of the GDPR ratione materiae, a national court, including any referring court, ought to enquire about the exact source of the legal obligation incumbent on an economic operator that is said to have been infringed by the latter. If the source of that obligation is not the GDPR, then the procedures set out by that instrument, related to the substantive scope of that instrument, are logically not applicable either"* (CJEU, Opinion of Advocate General Bobek, 13 January 2021, *Facebook Belgium,* C-645/19, paragraphs 37 and 38).

40. In this particular case, the restricted committee notes that, in these proceedings, the precise source of the legal obligation being monitored is solely based on the specific obligation laid down in Article 5(3) of the ePrivacy Directive, transposed into French Act in Article 82 of the French Data Protection Act.

41. **Thirdly**, with regard to the scope to be given to this specific obligation, the restricted committee points out that operations to read and/or write in the user's terminal must systematically form the subject of the user's "*prior consent*". It points out that pursuant to Article 2(f) of the ePrivacy Directive, consent corresponds to the "*data subject's consent*" in Directive 95/46/EC. However, to the extent that, as already mentioned, since the entry into force of the Regulation, references made to Directive 95/46/EC are to be construed as references to the GDPR, it follows that the "*consent*" provided for in Article 5(3) of the ePrivacy Directive, as transposed into Article 82 of the French Data Protection Act, must now be construed within the meaning of the GDPR.

42. In this respect, the restricted committee notes that consent within the meaning of the GDPR imposes more requirements in this area than provided for in Article 2(h) of Directive 95/46/EC. In particular, under these new requirements, Article 4(11) of the GDPR requires that consent is now unambiguous, which implies that it is given by a "*clear affirmative action*", and recital 42 of the GDPR reinforces the fact that it must be given freely, specifying that the person must now have a "*genuine or free choice*" when consenting.

43. With regard to operations to read and/or write information, this reinforcing of the fact that consent must be given freely implies that the methods that are offered to the user to express their choice are such that they do not encourage them to accept cookies more than they encourage them to refuse cookies.

44. The restricted committee notes that CNIL communication of 2 April 2021, posted on its website and criticised by the company, should be construed in this sense. In fact, by writing that "*the mere presence of a "Settings" button in addition to the "Accept all" button tends, in practice, to deter refusal and therefore does not allow compliance with the requirements laid down by the GDPR*", the CNIL had only intended to highlight the enhancement of requirements relating to collecting the user's consent before any operation to read and/or write information in their terminal brought about by the entry into force of the GDPR.

45. The restricted committee nevertheless points out that while the GDPR does indeed support the conditions of consent, compliance with the specific provisions resulting from the ePrivacy

Directive requiring such consent, now enhanced, from the user before any operation to read and/or write information in their terminal, continues to fall within the scope of the maxim *specialia generalibus derogant*, the specific rule laid down in Article 5(3) of the ePrivacy Directive and, consequently, of the specific monitoring and sanction mechanism provided for in Article 15a of that Directive.

46. Thus, a simple reference to the GDPR made by the provisions of the ePrivacy Directive on the definition of consent, is not sufficient to entail the applicability of the "one-stop-shop" mechanism to the facts of the case in point.

47. **Fourthly**, the restricted committee observes that it would in any case be materially impossible, as the law currently stands, to apply the "one-stop-shop" mechanism to facts falling within the scope of the ePrivacy Directive and that this position is also the subject of consensus at European level.

48. In fact, Member States, which are free to determine the competent national authority for determining violations of national provisions adopted pursuant to the ePrivacy Directive, may have assigned this competence to an authority other than their national data protection authority established by the GDPR, in this case, to their telecommunications regulatory authority. Therefore, to the extent that these latter authorities are not part of the EDPB, while this committee plays an essential role in the consistency mechanism implemented in Chapter VII of the GDPR, it is in fact impossible to apply the "one-stop-shop" to practices likely to be sanctioned by national supervisory authorities not sitting in this Board.

49. The restricted committee also points out that other national data protection authorities have also already imposed sanctions for failures relating to operations to read and/or write information in users' terminals. The Spanish authority has thus issued several sanction decisions against various data controllers in application exclusively of the national provisions transposing the ePrivacy Directive, in this case Article 22(2) of the Spanish Act 34/2002 of 11 July on Information Society and Electronic Commerce Services, without implementing the cooperation procedure established by the GDPR.

50. Finally, the restricted committee notes that the question of the possible application of the "one-stop-shop" mechanism to processing activities today governed by the current ePrivacy Directive, is currently the subject of numerous discussions in the preparation of the draft ePrivacy Regulation which has been under negotiation for over four years at European level. The very existence of these debates confirms that, as is, the "one-stop-shop" mechanism provided for by the GDPR is not applicable to the matters governed by the current ePrivacy Directive.

51. It follows from the above that the "one-stop-shop" mechanism provided for by the GDPR is not applicable to these proceedings and that the CNIL is competent to monitor and initiate a sanction procedure against the processing implemented by the company, consisting of operations to read and/or write information, carried out from the website "facebook.com", in the terminal of users residing in France, falling within the scope of the ePrivacy Directive, provided that this processing relates to its territorial jurisdiction.

2. On the territorial jurisdiction of the CNIL

52. The rule of territorial application of the requirements laid down in Article 82 of the French Data Protection Act is set out in Article 3(I) of this Act, which states: *"without prejudice, with regard to processing falling within the scope of Regulation (EU) 2016/679 of 27 April 2016, the criteria*

laid down in Article 3 of that Regulation, all the provisions of this Act shall apply to the processing of personal data carried out as part of the activities of an establishment of a data controller […] *on French territory, regardless of whether or not the processing takes place in France".*

53. The Rapporteur considers that the CNIL is territorially competent in application of these provisions since the processing subject of these proceedings, consisting of operations to access and/or deposit information on the terminals of users residing in France when using the Facebook social network, in particular for advertising purposes, is carried out in the "*context of the activities*" of FACEBOOK FRANCE, which constitutes "*the establishment*" on French territory of the Facebook Group.

54. The company argues that to the extent that the rules of jurisdiction and the cooperation procedures defined by the GDPR should be applied, the CNIL would not have territorial jurisdiction to hear this case since the "real headquarters" of the Facebook Group in Europe, i.e., the place of its central administration within the meaning of Article 56 of the GDPR, is located in Ireland.

55. **The restricted committee** notes that, in order to determine whether the CNIL has competence to monitor FIL's compliance with the requirements provided for in Article 82 of the French Data Protection Act in the context of the processing in question, it is necessary to examine in this particular case whether the two criteria for the territorial application of the French Data Protection Act, as provided for in Article 3(I) are met: namely, first, whether Facebook has an "*establishment on French territory*" and second, whether the processing in question is carried out "*in the context of the activities of that establishment*".

56. The restricted committee points out in this regard that the ePrivacy Directive does not itself explicitly lay down the rule for the territorial application of the various transposition laws adopted by each Member State. However, this Directive states that its provisions "*particularise and complement Directive 95/46/EC*", which had provided, at the time, in its Article 4 that "*Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable*".

57. While this rule for determining the national law applicable within the European Union is no longer necessary for application of the GDPR rules, which has replaced Directive 95/46/EC and applies uniformly throughout the territory of the European Union, the restricted committee notes that the French legislator has maintained these two criteria relating to territorial application for the specific rules contained in the French Data Protection Act, in particular those transposing the ePrivacy Directive. It follows, as will be developed *below*, that the case law of the CJEU on the application of Article 4 of Directive 95/46/EC remains relevant in order to clarify the scope to be given to these two criteria.

58. **Firstly**, on the existence of a Facebook establishment on French territory, the restricted committee points out that, consistently, the CJEU has considered that the concept "*in the context of the activities of an establishment*" cannot be interpreted restrictively in data protection law, and that in order to establish whether a data controller has an "*establishment*", both the degree of stability of the arrangements and the effective exercise of activities in a Member State must be interpreted

in the light of the specific nature of the economic activities and the provision of services concerned (see in particular, CJEU,1 October 2015, *Weltimmo*, C-230/14, paragraphs 25 to 31).

59. In particular, the Court stated that "*the concept of "establishment", within the meaning of Directive 95/46, extends to any real and effective activity - even a minimal one - exercised through stable arrangements"* (idem, paragraph 31), the criterion of stability of the arrangements being assessed in through the presence of *"the necessary equipment for provision of the specific services concerned"* (idem, paragraph 30). The Court also considered that a company, an autonomous legal entity, from the same group as the data controller, may constitute an establishment of the data controller within the meaning of these provisions (CJEU, 13 May 2014, *Google Spain*, C-131/12, paragraph 48).

60. In this case, FACEBOOK FRANCE, registered in France since 3 February 2011, is the registered office of the French subsidiary of META PLATFORMS, INC. It has premises located in Paris and employs approximately […] people. It is specified in this company's articles of association, updated and filed with the registry of the Paris Commercial Court on 9 July 2020, that its business includes "*any activity relating, directly or indirectly, to the purchase, sale or intermediation of advertising spaces on the Facebook Online Social Network Platform or any other platform operated by the Facebook group, or any other commercial agreement, in its broadest sense, relating to online advertising space and in particular, without this list being exhaustive, the offer to buy, sell or provide online advertising space, the negotiation of contracts concerning online advertising space, the implementation of marketing strategies relating to offers for the sale of advertising space and any other advertising service that may be provided to advertisers, advertising agencies or any other third party*".

61. As regards the links of this company with FIL, the restricted committee notes that they are both subsidiaries of the group's parent company, META PLATFORMS, INC., and that they are in particular linked to each other by a contract for the resale of advertising space and by a service contract, in force since 1st July 2018.

62. In this respect, the restricted committee notes that while, in its reply of 21 May 2021, FACEBOOK FRANCE stated that *"as a matter of principle, FIL is the contracting company for advertisers and partners in France wishing to use Facebook's advertising products and services "[...] for the creation, submission or distribution of advertisements or any other activity or any other commercial or sponsored content" [...]",* it also states very clearly that its role consists *of "the provision of local support to advertisers and partners in France and the placing of orders and invoicing of certain customers".*

63. In particular, the restricted committee notes that under the service agreement, FACEBOOK FRANCE provides, on a non-exclusive basis, a number of services to FIL, including general, administrative, human resources, accounting, legal, policy, marketing and partnership management services.

64. Therefore, in view of the nature of these services, the restricted committee considers that FACEBOOK FRANCE must be regarded as FIL's establishment in France.

65. **Secondly**, on the existence of processing carried out "*in the context of the activities*" of FACEBOOK FRANCE, the restricted committee states that in its decisions *Wirtschaftsakademie* (CJEU, Grand Chamber, 5 June 2018, *Wirtschaftsakademie*, C-210/16, paragraphs 56 to 60) and *Facebook Belgium* (CJEU, Grand Chamber, 15 June 2021, *Facebook Belgium,* C-645/19,

paragraphs 92 to 95), which are in line with the *Google Spain* case law of 13 May 2014 relating to the activities of the Google search engine in Spain (CJEU, Grand Chamber, 13 May 2014, *Google Spain*, C-131/12, paragraph 55), the Court of Justice held that the processing consisting of the collection of personal data via cookies stored on the terminals of users visiting, in Germany and Belgium, pages hosted on the Facebook social network were respectively carried out *"in the context of the activities"* of FACEBOOK GERMANY and FACEBOOK BELGIUM, German and Belgian establishments of the Facebook group, insofar as these establishments are intended to promote and sell, in their respective countries, advertising space offered by this social network which serves to make the service offered by Facebook profitable.

66. Thus, in the *Facebook Belgium* judgment, the Court of Justice observed that "*first, a social network such as Facebook generates a substantial proportion of its income from, inter alia, the advertising that is disseminated on that social network, and that the activity carried out by the establishment located in Belgium is intended to ensure, within Belgium, even if it is only a secondary function, the promotion and sale of advertising spots which serve to make Facebook services profitable. Second, the activity primarily carried out by Facebook Belgium, which consists in engaging with the EU institutions and constituting a point of contact for those institutions, seeks, inter alia, to determine the personal data processing policy of Facebook Ireland. In those circumstances, the activities of the establishment of the Facebook group located in Belgium must be considered to be inextricably linked to the processing of personal data at issue in the main proceedings, with respect to which Facebook Ireland is the controller within the European Union*." (paragraphs 94-95).

67. Even though these three judgments concerned more specifically the subsequent processing activities carried out using the cookies stored in the users' terminals - which had justified the application of Directive 95/46/EC for the *Google Spain* and *Wirtschaftsakademie* cases and of the GDPR for the *Facebook Belgium case* -, this case law remains relevant in order to clarify the scope to be given to the concept of processing *"in the context of the activities"* of an establishment, the French legislator having used this case law when transposing the ePrivacy Directive, in order to justify the territorial jurisdiction of the CNIL with regard to the processing activities covered by this Directive.

68. In this particular case, the restricted committee notes that the analyses carried out in Germany and Belgium by the German and Belgian data protection authorities with regard to FACEBOOK GERMANY and FACEBOOK BELGIUM, and confirmed by the CJEU, can be reproduced in France by the CNIL with regard to FACEBOOK FRANCE.

69. In fact, it is apparent from FACEBOOK FRANCE's response of 21 May 2021 that its activities consist of providing "*advertising support services to advertisers and partners in France on behalf of FIL*". More specifically, "*it informs advertisers and partners in France about how they can use Facebook advertising services offered by FIL. By way of illustration, FB France provides advice on how to use the tools and functionalities of Facebook products to optimize advertising budgets or improve the quality of advertising campaigns*". And lastly, "*since 1st July 2018, [it] has also been interacting with certain advertisers and partners in France, with regard to placing their orders and invoicing related to the resale of advertising space for their benefit*".

70. Consequently, the restricted committee considers that the processing in question - consisting of operations to access or deposit information on the terminal of users residing in France when using the Facebook social network, in particular for advertising purposes - is carried out "*in the context of the activities of FACEBOOK FRANCE*", a company which is "*Facebook's establishment on French territory*" and contributes, as such, to the promotion and marketing of Facebook products

and their advertising solutions in France. Since the two criteria provided for in Article 3(I) of the French Data Protection Act are met, the processing is subject to French law.

71. The restricted committee points out that the application of French law only concerns the reading and/or writing operations carried out on French territory (Article 4 of Directive 95/46/EC further stated that the law of the Member State applies only to the activities of the establishment "*on the territory of the Member State*").

72. And lastly, it notes that this is a consistent position on its part, since the intervention of the *Google Spain* case law in 2014 (see in particular the CNIL decisions, restricted committee, 27 April 2017, SAN-2017-006; CNIL, restricted committee, 19 December 2018, SAN-2018-011; CNIL, restricted committee, 7 December 2021, SAN-2020-012 and CNIL, restricted committee, 7 December 2021, SAN-2020-013).

73. It follows from the foregoing that French law is applicable and that the CNIL is materially and territorially competent to exercise its powers, including the power to take a sanction measure concerning the processing in question which falls within the scope of the ePrivacy Directive.

B. On the ground for complaint alleging the unlawfulness of these sanction proceedings

74. The company complains of not having received prior formal notice, as did the sixty parties involved having formed the subject of this corrective measure between May and July 2021 for similar offences, and invokes the resulting infringement of the principle of equality in the eyes of the law.

75. It argues that this principle is also not fully taken into account due to the severity of the corrective measures proposed by the Rapporteur in comparison with recent restricted committee decisions pronounced against major stakeholders for non-compliance with the provisions of Article 82 of the French Data Protection Act (see CNIL decisions, restricted committee, 18 November 2020, SAN-2020-009, *Carrefour Banque*; 7 December 2020, SAN-2020-012, *Amazon* and SAN-2020-013, *Google*; 27 July 2021, SAN-2021-013, *Le Figaro*).

76. Firstly, with regard to the lack of prior formal notice, the restricted committee points out that, pursuant to Article 20(III) of the French Data Protection Act, directing a case towards a sanction procedure is the sole responsibility of the Chair of the CNIL, so that the restricted committee does not have to hand down a decision on the principle of referral of the matter to it.

77. It also states that it is apparent from these provisions that the Chair of the CNIL is not required to send a prior formal notice to a data controller before initiating a sanction procedure against them. It adds that the possibility of directly initiating a sanction procedure was confirmed by the French State Council (see, in particular, French State Council, 4 Nov. 2020, application no. 433311, paragraph 3).

78. Moreover, the restricted committee notes that a prior formal notice was even less justified in this particular case since the company had already, following a prior formal notice, formed the subject of a sanction by the restricted committee for breaches relating to cookies in 2017. The company therefore needed to be both particularly vigilant with regard to fulfilment of its obligations in terms of cookies and also attentive to changes in the regulations in this area, in particular following the enhancing of the conditions of consent following the entry into force of the GDPR.

79. And lastly, the restricted committee notes that the CNIL particularly issued communications about these changes, in particular by defining an action plan relating to cookies, the terms of which were detailed in 2019 in a press release posted on its website on 28 June 2019. In that press release, the CNIL stated in particular that it would allow data controllers a "transitional period", to give them the time necessary to bring their reading and/or writing operations into compliance with the new requirements following the entry into force of the GDPR and which would be enshrined in the new recommendation that was to be drafted. It had already pointed out that it would be carrying out checks on compliance with this future recommendation within six months of its final adoption. Extended once, this adaptation period expired on 1st April 2021.

80. Secondly, as regards the amount of the fine proposed by the Rapporteur, this does not affect the lawfulness of the procedure.

81. Consequently, the restricted committee considers that the ground for complaint alleging the unlawfulness of the procedure must be dismissed.

C. On the breach of cookie obligations

82. According to Article 82 of the French Data Protection Act which transposes into French law the provisions of Article 5(3) of the ePrivacy Directive, "*any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless it has been previously informed by the data controller or its representative:*

1. Of the purpose of any action aimed at electronically accessing information already stored in their electronic communications terminal equipment, or writing information to this equipment;

2. Of how he or she can object to it.

Such access or writing may only take place provided that the subscriber or user has expressed, after receiving such information, his or her consent (...)".

83. Pursuant to Article 2(f) of the ePrivacy Directive, consent corresponds to the "*data subject's consent*" in Directive 95/46/EC. According to Article 94 of the GDPR, "*references to the repealed Directive shall be construed as references to the [GDPR]*".

84. Under Article 4(11) of the GDPR, in order to be validly collected, consent must be "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

85. The scope of this article is clarified by Recital 42 of the GDPR, according to which "*consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment*".

86. In this case, the delegation established in connection with the online control of 8 April 2021 that, when a user visits the social network Facebook, a pop-up window entitled *"Accept Facebook cookies in this browser"* appears and that, at the bottom of this window, there are two buttons entitled *"Manage data settings"* and *"Accept all"*. It was also found that, at this stage, no cookie was placed on the user's terminal and that the user was required to click on one of these two buttons in order to be able to continue browsing the social network.

87. Thus, when the user clicks the *"Accept all"* button at the bottom of this first window and gives their consent to the reading and/or writing of information on their terminal, the window disappears, allowing them to continue browsing on the social network.

88. When the user clicks on the *"Manage Data Settings"* button, a new pop-up window appears, containing the two main purposes pursued by cookies subject to consent - personalised ads by Facebook and personalised ads by third parties - and next to which there are sliding buttons, disabled by default.

89. The delegation found that when the user scrolls this second window, leaves the two sliding buttons disabled, then clicks on the *"Accept cookies"* button at the bottom of this window, this window disappears, allowing them to continue browsing on the social network without having any advertising cookies placed on their terminal.

90. In light of these findings, the Rapporteur considers that the company had committed a breach of Article 82 of the French Data Protection Act, as clarified by the enhanced requirements in terms of consent laid down by the GDPR, since it does not make available to users residing in France, on the website "facebook.com", a method of freely consenting by refusing operations to read and/or write information on their terminal having the same degree of simplicity as the method envisaged for accepting their use. The Rapporteur also considers that the information provided to the user does not allow them to clearly understand that they can refuse cookies.

91. By way of clarification, she also notes that, according to its Guidelines 5/2020 on consent within the meaning of Regulation (EU) 2016/679, adopted on 4 May 2020, the EDPB had pointed out that "*the element "free" implies real choice and control for data subjects*" (§13).

92. Similarly, in the context of its Deliberation No. 2020-092 of 17 September 2020 adopting a recommendation proposing practical arrangements for compliance in the event of use of "cookies and other tracers", the Commission considered, in view of the above-mentioned applicable legislation, that "*the controller must offer users both the means of accepting and of refusing reading and/or writing operations with the same degree of simplicity*".

93. The company argues that neither the ePrivacy Directive nor its transposition into French law in Article 82 of the French Data Protection Act provides for the rule according to which it must be as easy to refuse cookies as it is to accept them. It adds that this rule is also not provided for by the GDPR, Article 7(3) of which introduces only an obligation relating to withdrawal of consent, which does not extend to the initial refusal to consent to cookies.

94. It argues that the CNIL Guidelines and Recommendation of 17 September 2020 are not mandatory and do not in any event refer to any binding provision of the GDPR or of the ePrivacy Directive when they refer to this rule which, in these two instruments of the CNIL, is, furthermore, mentioned under titles relating to refusal of consent and not to freedom of consent.

95. And lastly, it argues that its click path complies with the applicable rules since it does indeed provide, from the first window, information relating to cookies settings, and that a distracted user who has reached the second window allowing these settings, and who clicks on the *"Accept cookies"* button at the bottom of this second window, would not have any advertising cookie placed on their terminal.

96. **Firstly**, as regards the methods of refusal, the restricted committee refers to the provisions mentioned in paragraphs 41 to 43 and paragraphs 82 *et seq.* of this deliberation. It considers that, in order to guarantee freedom of consent, it should, in the case in point, be as easy to refuse cookies as to accept them. It points out that the EDPB clarifies this point in its Guidelines on Consent adopted on 4 May 2020 by stating that "*the element "free" implies real choice and control for data subjects*".

97. By applying this requirement of freedom of consent to cookies, it considers that making the opt-out mechanism more complex than the method allowing them to accept cookies, for example, by relegating to a second window the button allowing them to refuse cookies, amounts in actual fact, in general terms, in the context of browsing on the Internet, to altering users' freedom of choice by encouraging them to favour acceptance of these cookies rather than their refusal.

98. It notes that this conclusion is in particular corroborated by a university study entitled *"Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*" conducted in 2020 based on different cookie banners offered to a panel of users. In this study, researchers from Cambridge University and MIT showed that 93.1% of Internet users, faced with cookie banners, stop at the first level and that only a small minority of them go to the second level to customise their settings or reject cookies. This study also showed that the fact of relegating the opt-out button to the second level increased the rate of consent to cookies, on average, by 23.1 percentage points.

99. It also points out that, in order to take into account the changes brought about by entry into force of the GDPR and in particular to clarify the scope to be given to the rule challenged in these proceedings, the CNIL amended its Deliberation No. 2013-378 of 5 December 2013, adopting a recommendation on cookies and other tracers (hereinafter "the Recommendation of 5 December 2013").

100. This amendment was firstly translated by the adoption of Deliberation No. 2019-093 of 4 July 2019 adopting guidelines relating to the application of Article 82 of the amended Act of 6 January 1978 to the operations of reading and/or writing on a user's terminal (in particular, to cookies and other tracers) (hereinafter "the Guidelines of 4 July 2019"), which had already provided in Article 2, "*that it must be as easy to refuse or withdraw consent as to give it*", followed by the Guidelines and the Recommendation of 17 September 2020, which repealed the Guidelines of 4 July 2019 and the Recommendation of 5 December 2013.

101. The restricted committee points out that the two instruments adopted in 2020 aim to interpret the legislative provisions and to inform the parties concerned about the implementation of concrete measures to ensure compliance with these provisions, so that they implement these measures or measures having equivalent effect, without however providing for new statutory obligations. It notes that the Guidelines of 17 September 2020 state that *"are primarily intended to recall and explain the law applicable to the reading and/or writing of information* […] *in the subscriber's or user's electronic communications terminal equipment, including the use of cookies*."

102. It notes that Article 2 of the Guidelines of 17 September 2020 and Article 2.4 of the Recommendation of 17 September 2020 are very clear, the latter stating that *"the data controller must offer users both the possibility of accepting and refusing reading and/or writing operations with the same degree of simplicity*."

103. It points out that while, in the interests of providing further information, these clarifications feature in these two instruments under headings which refer to content rather than legal origin (*"Procedures for refusing"* for the Recommendation of 17 September 2020; *"Refusing and withdrawing consent"* for the Guidelines of 17 September 2020), it is indeed the requirement of freedom of consent laid down by the GDPR which implies, with regard to the deposit of cookies, that the methods offered to the user to make this choice are such that they do not encourage them to accept cookies any more than they encourage them to refuse cookies.

104. The restricted committee also notes that the French State Council had already had the opportunity to rule on this issue in its decision *Association des agences-conseils en communication,* in which it examined the Guidelines of 4 July 2019. It thus ruled that: "*the CNIL, which, in stating that it should be "as easy to refuse or withdraw consent as to give it", limited itself to characterising the conditions of the user's refusal, without defining specific technical methods for expressing such a refusal, did not vitiate its deliberation with any disregard of the rules applicable in this matter*" (French State Council, 19 June 2020, No. 434684, T., paragraph 15).

105. It notes that this paragraph must be read in the light of the conclusions of the Public Rapporteur on this judgment, who stated: "*As the CNIL points out, the contested guidelines do not impose any technical procedure for collecting this refusal. They merely demand, in general and rightly, that it is no more complicated to refuse than to accept*" (French State Council, conclusions of the Public Rapporteur on judgment No. 434684, p. 17).

106. And lastly, it points out that in the Guidelines and in the Recommendation of 17 September 2020, the CNIL does not necessarily require the insertion of a "*Reject all*" button, but draws attention to the importance of putting in place a simple alternative allowing the user to refuse cookies just as easily to accept them, by giving examples of wording and methods that can be used by organisations so that the freedom of consent of users is truly respected.

107. Thus, under the Recommendation of 17 September 2020, the CNIL proposes: *"For example, at the point of the first level of information, users may have the choice between two buttons shown at the same level and in the same format, which propose "Accept all" and "Reject all", "Allow" and "Do not allow", or "Consent" and "Do not consent", or any other equivalent and sufficiently clear wording. The Commission considers that this method is a simple and clear way for the user to express their refusal as easily as their consent. The expression of refusal to consent may, however, arise from other types of actions than that consisting of clicking on one of the buttons described above. In any event, the Commission points out that the methods allowing users to consent or refuse must be presented in a clear and comprehensible manner. In particular, where refusal can be expressed by merely closing the consent window or by the lack of interaction with that window for a certain period of time, this option must be clearly indicated to users on that window. In fact, failing this, the user might fail to understand that these actions mean that no reading or writing operation subject to consent can lawfully take place. Appropriate design and information should enable them to understand the options available to them".*

108. **In this particular case,** the restricted committee points out that, as evidenced by the findings made during the online check of 8 April 2021, when a user residing in France visits the website facebook.com, they can agree to the deposit of advertising cookies in a single action, by clicking on the button entitled "*Accept cookies*" appearing on the first window.

109. It notes that, in order to refuse these cookies however, the user will have to complete no fewer than three actions: first, click on the *"Manage data settings"* button located above the *"Accept*

cookies" button in the first window, second, scroll down the entire content of the second window, in particular to establish that the two sliding buttons allowing the deposit of advertising cookies are disabled by default, and finally, click on the *"Accept all"* button located at the bottom of this second window.

110. In this case and as it has already mentioned, the restricted committee considers that the fact, for the company, of making the mechanism for rejecting cookies more complex than the mechanism for accepting cookies, amounts, in reality, to discouraging users from refusing cookies and encouraging them to favour the *"Accept cookies"* button. In fact, an Internet user is generally led to visit many sites. Browsing on the Internet is characterised by its speed and fluidity. Having to click on *"Manage data settings"* and having to understand the set-up of the page making it possible to reject cookies, is likely to discourage the user, who would nevertheless like to refuse the storage of cookies. It is not disputed that in this case, the company offers a choice between acceptance or refusal of cookies, but the methods by which this refusal can be expressed, in the context of browsing on the Internet, skews the expression of choice in favour of consent, in such a way as to alter freedom of choice.

111. **Secondly**, with regard to the information provided, the restricted committee points out that under Article 82 of the French Data Protection Act, the user must be informed, before consenting to cookies, of "*the means at their disposal to oppose it*", that is to say, to refuse them, and that the information provided must be *"clear and comprehensive"*. It points out that these provisions should be read in the light of recital 66 of amending ePrivacy Directive 2009/136/EC, which provides that "*the methods of providing information and offering the right to refuse should be as user-friendly as possible*".

112. It points out that, in the context of its Recommendation of 17 September 2020, the Commission had taken care to clarify that this requirement for "*clear and comprehensive*" information should be construed in such a way that "*the information accompanying each actionable element allowing for expressing consent or refusal is readily understandable and does not require a concentration or interpretation effort on the part of the user. For example, it is recommended to ensure that it is not written in such a way that a quick or less attentive reading could lead to the impression that the selected option produces the opposite of what users thought they chose*".

113. In this particular case, it points out that it is apparent from the online control of 8 April 2021 that, having reached the website "facebook.com", the user must, in order to refuse the deposit of advertising cookies, first click on the *"Manage Data Settings"* button on the first window, scroll down the entire second window, leaving the two sliding buttons disabled so as not to accept cookies, then click on the *"Accept cookies"* button at the bottom of this second window.

114. While, as the company argues in defence, the restricted committee recognises that a distracted user who clicks on the *"Accept cookies"* button at the bottom of the second window would not see any advertising cookies placed in their terminal if the sliding buttons enabling the deposit of these cookies are disabled by default, it notes that it is particularly counter-intuitive to have to click on a button entitled *"Accept cookies"* to actually refuse the deposit of cookies.

115. The restricted committee considers that these methods instead encourage the user to believe that it is, ultimately, not possible to continue browsing having refused the deposit of advertising cookies, since the entire process of rejecting cookies is based on information referring to the acceptance of cookies.

116. It notes that this impression can only be strengthened by the unclear nature of the *"Manage Data Settings"* button offered on the first window, which does not clearly mention the existence of means to reject cookies.

117. It considers that the fact that, ultimately, cookies are not stored, does not affect the confusion generated by this contradictory click path which may give the user the impression that it is not possible to refuse the deposit of cookies and that they have no means of control in this regard.

118. In view of these elements, the restricted committee considers that the information provided to users residing in France visiting the page "facebook.com", as well as the methods of obtaining consent offered to them by the company on this website, do not comply with the provisions of Article 82 of the French Data Protection Act as clarified by the enhanced consent requirements laid down by the GDPR.

III. On the issue of corrective measures and publicity

119. Article 20 of amended Act No. 78-17 of 6 January 1978 provides that:

"When the data controller or its processor does not comply with the obligations resulting from the aforementioned Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 or from this Act, the chair of the Commission nationale de l'informatique et des libertés (French Data Protection Authority) may also, where applicable after having sent it the warning provided for in I of this article or, where applicable, in addition to an order provided for in II, refer the matter to the restricted committee of the Commission with a view to pronouncing, after an adversarial proceeding, any one or more of the following measures: […]
2. An injunction to make the processing compliant with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this Act or to comply with the requests made by the data subject to exercise their rights, which may be accompanied, except in cases where the processing is implemented by the State, with a penalty fine not exceeding 100,000 euros per day of delay from the date fixed by the restricted committee; […]
7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. […] *In determining the amount of the fine, the restricted committee shall take into account the criteria specified in the same Article 83*".

Article 83 of the GDPR, as referred to in Article 20(III) of the French Data Protection Act, provides that *"Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive"*, before specifying the elements to be taken into account when deciding whether to impose an administrative fine and when deciding on the amount of that fine.

A. On the issue of an administrative fine and its amount

120. The company firstly argues that the Rapporteur's demonstration of the gravity of the non-compliance and the number of data subjects in support of her proposal for a sanction is insufficient.

121. It also argues that the Rapporteur's developments relating to the scope of the breach and the financial benefits gained as a result of the breach are ineffective, since the sliding buttons on the second window are disabled by default, so that a distracted user who clicks on the *"Accept cookies"* button located at the bottom of this second window would not see any cookie placed in their terminal.

122. The restricted committee points out, in general terms, that Article 20(III) of the French Data Protection Act gives it authority to impose various penalties, including administrative fines, the maximum amount of which may be equal to 2% of the data controller's total worldwide annual turnover in the previous financial year. Determination of the amount of these fines is assessed in light of the criteria specified in Article 83 of the GDPR, to which this article refers.

123. **Firstly**, with regard to the imposition of an administrative fine, the restricted committee considers that it is firstly appropriate to apply the criterion provided for in Article 83(2)(a) of the GDPR relating to the gravity of the infringement taking into account the nature, scope of the processing as well as the number of data subjects affected.

124. It notes, first of all, that by failing to comply with the requirements of Article 82 of the French Data Protection Act, the company does not allow users residing in France visiting the website "facebook.com" to refuse cookies as easily as to accept cookies. By depriving them of this real freedom of choice, the company strongly encourages users to consent to the storage of advertising cookies.

125. The restricted committee points out the scope of the Facebook social network and the inescapable place it occupies in France, since it dominates by far the social media market, as noted by the French competition regulator, the Autorité de la concurrence, in its Opinion No. 18-A-03 of 6 March 2018. It also notes the "network effects" generated by this dominant position, highlighted by the German competition regulator in a decision of 6 February 2019.

126. It points out that this failure is all the more harmful to data subjects since, in parallel with its traditional function of maintaining and developing interpersonal relationships, this social network also occupies an increasingly larger role in areas as diverse as access to information, public debate or even civil security via the Facebook safety check feature in the event of a natural disaster or an attack, which are of some significance in a democratic society.

127. It also points out that the tracking of data subjects, which begins with the collection of information related to the user account and continues throughout the user's browsing on Facebook, for an advertising purpose clearly recognised by the data controller, does not stop at the borders of the social network.

128. It is not disputed that Facebook makes available to many third-party sites a set of tracking tools - such as social plugins, login buttons or the Facebook Pixel - that will continue to collect the data of users visiting these third-party sites in order to cross-reference them with data already collected within the social network in order to increase the value of these data. A 2019 study revealed the presence of these Facebook tracking tools on 44% of the 65,000 most visited sites in the world, so the indirect scope of processing is considerable.

129. And lastly, as regards the number of data subjects affected by the processing at issue, the restricted committee points out that, according to the volume figures provided by the company itself, the

social network accounts for approximately […] of monthly users in France, which corresponds to […] % of the population.

130. Secondly, the restricted committee considers that it is appropriate to apply the criterion set out in Article 83(2)(k) of the GDPR related to financial benefits gained from the infringement.

131. In this respect, it notes that insofar as Facebook follows a business model known as "target content matching", operating both in the collection of data, their exploitation and the operational implementation of advertisements posted in banners deployed within the social network, the performance of its business model is primarily based on targeting tools and in particular cookies, which make it possible to distinguish and reach the identified user in order to offer them advertising content adapted to their interests and profile.

132. In this particular case, the restricted committee considers that the breach in question provides the company with undeniable financial benefits, since the fact of opting for a path that makes the storage of cookies easier than the refusal of cookies, increases the proportion of users with whom advertising cookies are likely to be stored, and therefore also increases the volume of advertising revenues generated by the profiling to which these cookies contribute.

133. With regard to this point, it is apparent from the financial information of FACEBOOK INC., communicated by FIL, that the former draws almost 98% of its gross revenues from the online advertising segment and that it operates a worldwide operating margin of approximately 40% on this segment. Even if all of these revenues are not directly linked to cookies, the restricted committee points out that this segment is primarily based on the targeting of Internet users, to which cookies directly contribute by making it possible to distinguish and reach the identified user with a view to showing them advertising content corresponding to their interests and to their profile.

134. In this particular case, while it is not aware of the amount of profit made by the Facebook group from the collection and analysis of cookies on the French market via the revenues generated by targeted advertising aimed at French Internet users, the restricted committee notes that a proportional approximation based on the figures at its disposal, in particular, the average revenues generated by a European user for the online advertising segment and the number of users residing in France, would suggest that France is contributing to the net income of FACEBOOK INC., the parent company of the Facebook group, today called META PLATFORMS, INC., for an amount of between EUR 550 and 660 million.

135. **Secondly**, with regard to determination of the amount of the fine, the restricted committee points out that, pursuant to the provisions of Article 20(III) of the French Data Protection Act, FIL incurs a financial penalty of up to 2% of its turnover, which was EUR […] in 2019.

136. Therefore, in view of the company's liability, its financial capacities and the relevant criteria of Article 83(2) of the Regulation, referred to above, the restricted committee considers that a fine of EUR 60 million against the company appears to be justified.

B. Concerning the issue of an injunction combined with a periodic penalty payment

137. In its submissions of 8 October 2021, the company indicated that an update of its cookie consent collection interface was in the process of being rolled out in the European region, including in France, without however, producing any supporting documents. It stated that *"this update for the European region does not introduce any additional purposes for cookies, nor does it add any new cookies"* and that it is aiming to *"improve the ergonomics of the interface"*.

138. On 6 December 2021, the company provided screenshots reflecting the nature of this update.

139. **Firstly**, the restricted committee found that this update changes, notably, the content of the buttons in the first window, *"Manage Data Settings"* and *"Accept all"*, which are now entitled respectively *"Other options"* and *"Allow all cookies"* and that in the second window, the old *"Allow cookies"* button is now entitled *"Allow essential cookies only"* and that next to this, the company has introduced a second button entitled *"Allow all cookies"*.

140. The restricted committee notes that, in accordance with the explanations already mentioned during the session and repeated by the company in the letter accompanying these screenshots, this update only concerns *"users logged on to the website www.facebook.com"*, which informal checks enabled it to effectively establish.

141. Moreover, and above all, the restricted committee notes that this update still does not put in place any means making it as easy to reject cookies as it is to accept cookies.

142. Consequently, since the interface resulting from this update still does not comply with the provisions of Article 82 of the French Data Protection Act, as clarified by the enhanced consent requirements laid down by the GDPR, the restricted committee considers it necessary to issue an injunction in order for the company to comply with the obligations applicable in this respect.

143. **Secondly**, the restricted committee states out that a periodic penalty payment is a financial penalty per day of delay to be paid by the data controller in the event of non-compliance with the injunction at the end of the stipulated time limit. Its imposition may therefore sometimes be necessary to ensure compliance of the data controller within a certain period of time.

144. The restricted committee adds that for the purpose of preserving its comminatory function, its amount must be both proportionate to the seriousness of the breaches committed and adapted to the financial capacity of the data controller. It further notes that for determination of this amount, account should also be taken of the fact that the breach to which the injunction relates, indirectly contributes to the profits generated by the data controller.

145. In the light of these elements, the restricted committee considers justified the imposition of a periodic penalty payment amounting to EUR 100,000 per day of delay, payable at the end of a three-month period.

C. On publication of the decision

146. The company asks the restricted committee to not make its decision public.

147. The restricted committee however, considers that publication of this decision is justified in the light of the seriousness of the breach in question, the scope of the processing and the number of data subjects concerned.

148. It also points out that this measure will alert French users of the Facebook social network residing in France of the characterisation of the breach of Article 82 of the French Data Protection Act in its various aspects, and inform them of the persistence of the breach on the day of this deliberation and the injunction against the company to remedy it.

149. Finally, it considers that this measure is not disproportionate since the decision will no longer identify the company by name upon expiry of a period of two years following its publication.

FOR THESE REASONS

The CNIL's restricted committee, after having deliberated, decides to:

- **impose an administrative fine of sixty million euros (€60,000,000) on FACEBOOK IRELAND LIMITED for breach of Article 82 of the French Data Protection Act;**
- **issue an injunction against FACEBOOK IRELAND LIMITED** to modify, on the website "facebook.com", the methods of obtaining the consent of users located in France to read and/or write information in their terminals, offering them a means of rejecting these operations presenting simplicity equivalent to the mechanism provided for their acceptance, in order to guarantee the freedom of their consent;
- **associate the injunction with a periodic penalty payment of one hundred thousand euros (EUR 100,000) per day of delay at the end of a period of three months** following notification of this decision, with proof of compliance to be sent to the restricted committee within this period;
- **make its deliberation public, on CNIL's website and on the Légifrance website,** the deliberation no longer identifying the company by name upon expiry of a period of two years following its publication.
- **send its deliberation to FACEBOOK FRANCE with a view to its execution.**

The Chairman

Alexandre Linden

This decision may be appealed before the French Council of State within four months of its notification.