Recommendation no. 04/2015 of 13 May 2015

Re: Own-initiative recommendation relating to 1) Facebook, 2) Internet and/or Facebook users as well as 3) users and providers of Facebook services, particularly plug-ins[1] (CO-AR-2015-003)

The Commission for the Protection of Privacy (hereafter "the Privacy Commission");

Having regard to the Act of 8 December 1992 *on the protection of privacy relating to the processing of personal data* (hereafter Privacy Act), particularly article 30;

Having regard to the Facebook Group's attendance of the meeting of 29 April 2015;

Having regard to the report by Mr Willem Debeuckelaere and Mr Stefan Verschuere;

Issues the following recommendation on 13 May 2015:

[1] This is an unofficial English translation of the recommendation, the Dutch and French versions of the text being authentic.

1. Introduction

1. This is a recommendation by the Commission for the Protection of Privacy, the Privacy Commission for short. With a recommendation the Privacy Commission addresses all stakeholders concerned who in one way or another use or are the object of processing operations of personal data. The present recommendation does not constitute a decision. The Privacy Commission is nevertheless of the opinion that its recommendations and the arguments it invokes are sufficiently clear and substantiated in order to constitute a set of rules safeguarding the observation of the law.

2. More particularly the Privacy Commission wishes to ensure the protection of citizens, data subjects. It addresses controllers, agents or processors, those who offer services and products, as well as the data subjects themselves. Consequently, this is a targeted recommendation which has been divided into three distinct recommendations addressing different target groups:
1. The Facebook Group itself;
2. Internet users in general, both non-users and users of Facebook;
3. Those who in one way or another use and offer Facebook services or products on web pages, including plug-ins.

3. This first recommendation deals with the obvious issues. With regard to Facebook it focuses on preliminary issues such as applicable law and competent jurisdiction, the duty to cooperate consisting of whether or not effectively responding to queries by the Privacy Commission, and the first findings relating to tracking, among others by plug-ins and cookies.

4. In a second recommendation the Privacy Commission intends to deal with the remaining issues. This second recommendation will be issued later this year.

5. These recommendations may be complemented, modified and adapted, particularly when:
- *rebus sic stantibus* or the factual situation is modified;
- this is required as a result of advancing insight;
- this is justified by modifications of Facebook's "terms of use" and practices and services;
- this is supported by experiences and advice from Facebook users and service providers;
- this is proffered in European cooperation, particularly in the context of the Article 29 Working Party[2].

[2] The Article 29 Working Party is an independent European task force dealing with issues relating to the protection of personal data and privacy. It represents the privacy commissions or data protection authorities of the European Union's 28 Member States. The Privacy Commission is therefore also a part of it. Apart from the EU Member States, the European Data Protection Supervisor is also part of the Article 29 Working Party.

And whenever it appears useful and advisable the Privacy Commission can adapt these recommendations.

2. History

6. On 27 November 2014 Facebook announced a global revision of its Statement of Rights and Responsibilities, Data Policy and Cookie Policy (hereafter "new terms of use") as of 1 January 2015[3]. On 25 December 2014 Facebook postponed the entry into force of these new terms of use to 30 January 2015, as of which date the terms have entered into force.

7. As a result of these new terms of use the Privacy Commission has received multiple queries from concerned Facebook users, the media, Belgian Federal Parliament, as well as the Secretary of State competent for Privacy, among others. Taking into account the above, the Privacy Commission decided to proceed with an investigation of these new terms of use, in order to find out what the scope of this modification is for Belgian users, and also to examine compatibility with the Privacy Act. To do so, the Privacy Commission also appealed to the technical expertise of researchers of the KULeuven and the VUB, two Belgian universities which had already investigated into Facebook, among others, in the context of the SPION and EMSOC research projects. For an overview of the issues relating to the content of the new terms of use, the Privacy Commission refers to the latest versions of the report by KULeuven/VUB[4]. As regards tracking through social plug-ins, reference is made to chapter 8 (pages 52-62) of the abovementioned report as well as to the technical report in its Annex 1 "Facebook tracking through social plug-ins" (which can be consulted on https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf). Their technical findings have also been summarised on a separate web page (as "Frequently Asked Questions"): https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/.

8. The Privacy Commission is also part of a contact group together with the data protection authorities from Hamburg, the Netherlands, Spain and France.

3. Procedure

A) Correspondence

9. Following the abovementioned investigation the Privacy Commission and Facebook Belgium SPRL corresponded between 16 January 2015 and 15 April 2015.

[3] https://www.facebook.com/legal/terms

[4] https://www.law.kuleuven.be/icri/en/news/item/icri-cir-advises-belgian-privacy-commission-in-facebook-investigation

10. On 16 January 2015 the Privacy Commission wrote to Facebook Belgium SPRL indicating that it wished to investigate the scope of the new terms of use for Belgian users, and examine the compatibility of this modification with the Privacy Act. For this purpose it sent Facebook a questionnaire, requesting a reply within 20 days, and the postponement of the modification of the terms of use in the meantime. At present, Facebook has still not provided an adequate reply to this questionnaire.

11. On 2 February 2015 Facebook replied to this letter stating that Facebook Ireland must be considered as controller and that the latter is the point of contact for the investigation. The request for postponement was not discussed.

12. On 9 February 2015 the Privacy Commission replied to this letter that pursuant to article 3bis, paragraph 1, 1° of the Privacy Act, Belgian privacy legislation applies to Facebook's activities in Belgium. Furthermore, Facebook was served notice of default regarding the entry into force of the new terms of use, and was requested once again to reply to the questions from the letter of 16 January 2015.

13. Facebook subsequently replied to this letter on 20 February 2015, providing information about Facebook's overarching structure, the identity of the company it considers as controller for the processing of Belgian user data, as well as an explanation of its position on applicable law.

14. On 25 February 2015 the Privacy Commission responded to this letter with regard to applicable law and the Privacy Commission's competence, and serving notice of default regarding two issues, i.e. the urgent request to provide information (see letter of 16 January 2015) and the termination of internet user tracking (through so-called 'social plug-ins').

15. In its letter of 2 March 2015 Facebook provided an answer regarding these social plug-ins.

16. On 3 March 2015 the Privacy Commission addressed an additional letter to Facebook relating to the processing of sensitive personal data by Facebook and the use of this data for advertising purposes.

17. Facebook replied on 6 March 2015 that no personal data were processed by Facebook Belgium.

18. The Privacy Commission then wrote to Facebook on 20 March 2015 stating that it had still not received an answer to the questions from the letter of 16 January 2015, and that otherwise Facebook had not refuted the other elements mentioned by the Privacy Commission. Also, Facebook continued to deny the application of the Belgian Privacy Act and the Privacy Commission's

competence. The Privacy Commission therefore reserved all rights and invited Facebook to a hearing on 29 April 2015 in the context of a recommendation pursuant to article 31 of the Privacy Act.

19. On 31 March 2015 the Privacy Commission wrote to Facebook to provide more information about the hearing planned on 29 April 2015.

20. Facebook replied to the Privacy Commission's letter of 20 March 2015 with a letter of 2 April 2015, in which Facebook stated that it had already answered the Privacy Commission's questions and that it had replied to the questions from the Privacy Commission's letter of 16 January 2015.

21. The Privacy Commission replied to this on 15 April 2015, stating that Facebook had never provided a relevant answer. Moreover, the answers to the Privacy Commission's letter of 16 January 2015 are not relevant, since they do not provide an answer to the questions addressed to the entire Facebook Group, for which Facebook Belgium SPRL acts as an establishment on Belgian territory. Consequently, Facebook was requested once again to answer the questions in the letter of 16 January 2015. Not complying with this request constitutes a violation of article 17, § 4 and article 32 of the Privacy Act[5].

B) Privacy Commission Hearing of 29 April 2015

22. Facebook was heard at the Privacy Commission meeting of 29 April 2015. To prepare the meeting a preliminary investigation report was sent to Privacy Commission members and Facebook. During the meeting Facebook representatives were heard and they could bring forward their findings about the KULeuven/VUB report. The KULeuven/VUB researchers also gave a presentation on their findings regarding social plug-ins (also see marginals 57 and following).

4. Role of Facebook Inc., Facebook Ireland and Facebook Belgium SPRL

23. Facebook exclusively recognizes the Irish Privacy Commission's competence and therefore contests the competence of other Member States' data protection authorities. Moreover, Facebook holds that only Irish national data protection law can be applied to all European users of its social network. Facebook argues that not Facebook Inc. – established in the United States – but Facebook Ireland should be considered as controller for the processing of European users' data.

24. The Privacy Commission dismisses Facebook's arguments for the reasons below.

[5] Punishable pursuant to article 39, 7°, 8° and 13° of the Privacy Act.

A) Facebook Inc. as controller

25. Facebook has a business model based on revenue from targeted advertising[6]. These advertisements target Facebook users' individual interests, age, gender, locations and profile. Facebook enables advertisers to select specific target groups, and target advertisements to a very large extent, regardless of where users are, either on the Facebook website or on any other arbitrary website using Facebook's advertising services[7].

26. Facebook's annual financial report for the American Securities and Exchange Commission (SEC)[8] shows that Facebook mentions its worldwide turnover as the turnover of Facebook Inc. With regard to the power of decision-making Facebook states in the same report that this lies with the CEO, and that therefore there is a structure with one single reporting unit and one single operational unit.

27. In its general terms and conditions, however, Facebook Inc. states that all users outside the United States of America and Canada conclude an agreement with Facebook Ireland Limited. Facebook states that Facebook Ireland is the controller for the processing of these users' data. Moreover, Facebook claims that Facebook Inc. acts as processor for Facebook Ireland, with Facebook Inc. processing personal data for which Facebook Ireland is controller, including the personal data of Belgian users. These processing operations by Facebook Inc. are also said to relate to the storage and hosting of user data for which Facebook Ireland is responsible[9]. Facebook Ireland is a full subsidiary of Facebook Inc. and had been included as such in the list of Facebook Inc. subsidiaries[10].

28. According to Facebook, Facebook Inc. has only one establishment in the EU, viz. Facebook Ireland. Consequently, Facebook is of the opinion that Irish law is applicable to the processing of personal data of all European users. Facebook states that article 4 (1) a of Privacy Directive 95/46/EC should be interpreted in such a way that if a controller has an establishment in a European Member State (Ireland in this case) this implies that only the law of that Member State may be

---

[6] See Facebook Inc. Form 10-K for the American SEC, filed on 29 Januari 2015, relating to the period until 31 December 2014, Part 1, Item 1: "We generate the substantial majority of our revenue from selling advertising placements to marketeers. Our ads let marketeers reach people on Facebook based on a variety of factors including age, gender, location and interests."

[7] Facebook provided the following information about its business model to the Privacy Commission: "Facebook's underlying business model is based on advertising. … Equally, advertisers prefer to present adverts that are relevant to their audience, because users respond more positively to relevant adverts, and there is less waste in their marketing efforts. To do this we use a variety of information about our users use of Facebook services in order to gauge which adverts will be of relevance."

[8] See Facebook Inc. Form 10-K for the American SEC, filed on 29 January 2015, relating to the period until 31 December 2014, p. 67: "Our chief operating decision-maker is our Chief Executive Officer who makes resource allocation decisions and assesses performance based on financial information presented on a consolidated basis. There are no segment managers who are held accountable by the chief operating decision maker, or anyone else, for operations, operating results, and planning for levels or components below the consolidated level unit. Accordingly, we have determined that we have a single reportable segment and operating unit structure. ‴

[9] Facebook's letter of 20 February 2015 to the Privacy Commission.

[10] See Facebook Form 10-K, exhibit 21.1, List of subsidiaries.

applied. According to Facebook supervisory authorities in other Member States must not impose restrictions on the services Facebook Ireland provides, because the free movement of data within the European Union is a fundamental principle of the internal market[11].

29. In Facebook's annual financial report to the SEC the Privacy Commission observed that Facebook Inc. speaks of one single operational business unit, viz. Facebook Inc. in the United States of America, and states that the power of decision-making for all transactions lies exclusively with the CEO, and not with another person. Facebook also confirmed that Facebook Inc. is responsible for storing all user data collected. However, according to the Privacy Commission Facebook Ireland does not appear to be able to take independent decisions when it comes to determining the purpose and the resources relating to the processing of the personal data of Belgian citizens. The examples[12] mentioned by Facebook Ireland of decisions allegedly showing its capacity of controller, rather indicate an advisory role towards Facebook Inc. Incidentally, Facebook's new terms of use were introduced at the same time all over the world, and there was no different privacy policy for European citizens. To the contrary, nowhere does this privacy policy mention the technical term 'personal data' which is used in European legislation, but mentions 'data' and 'personal information', which according to Facebook is only a name or an e-mail address that can be used to contact the data subject or find out his/her identity.

30. First and foremost it is therefore Facebook Inc. that determined which information was to be provided to data subjects relating to the new terms of use. Moreover, by introducing the new terms of use Facebook Inc. set out which personal data are processed for which purposes and how long it is kept. All these elements show that Facebook Inc. determines the essential elements of the data processing and must therefore be considered as the only controller[13].

31. Furthermore, even if one assumed that Facebook Ireland could be considered as a controller, in no way does this influence the (in)applicability of Belgian privacy legislation (see c) infra), since the application of national privacy law does not take into account the distinction between controller and processor, but examines whether the data are processed in the context of effective and actual activities of a permanent establishment of the controller on Belgian territory[14].

---

[11] Facebook's letter of 20 February 2015 to the Privacy Commission.

[12] Ibidem.

[13] In this context see the Article 29 WP's opinion on applicable law on http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf, as well as the sentence of the Berlin Kammergericht of January 2014, in which the Court stated that all decisions about data processing by Facebook are in fact taken in the United States and that Facebook Ireland can consequently not be considered as a controller (KG Berlin 5 Zivilsenat, 24/01/2014, 5 U 42/12, preambles 135-137).

[14] See Lokke MOEREL, Swift revisited-when do the directive and the proposed regulation apply?, in "Data Protection anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014), pages 159-172.

B) The role of Facebook Belgium SPRL

32. Facebook Belgium SPRL was established as the limited-liability company Facebook Belgium SPRL[15]. In Facebook Belgium's annual financial statement Facebook Inc. is mentioned as the 'entreprise mère consolidante[16]' ('consolidating parent company'). Pursuant to the company object established in the deed of incorporation, Facebook Belgium's activities include the following:

- The limited-liability company cannot only perform activities *"pour son propre compte"* ("for its own account") but also *"pour compte de tiers"* ("on behalf of third parties"), for example for Facebook Inc.

- *"toute activité se rapportant au domaine des affaires publiques et du lobbying, et spécialement des systèmes d'influence, les stratégies de communication d'influence, l'identification des interlocuteurs clés (tels que décideurs, relais, alliés), la création d'alliances et de partenariats, la prise de contacts avec le Gouvernement, le Parlement, les administrations, les institutions européennes et internationales, l'établissement de propositions d'aménagements réglementaires ou législatifs (tels que les amendements), ainsi que l'élaboration d'argumentaires et d'outils de communication";*
  ("any activity relating to the field of public affairs and lobbying, and particularly influencing systems, influencing communication strategies, identification of key contacts (such as decision-makers, intermediaries, allies), the creation of alliances and partnerships, contacts with the Government, Parliament, administrations, European and international institutions, drawing up proposals for regulatory or legislative changes (such as amendments), as well as elaborating sales pitches and communication tools") (unofficial translation);

33. These activities obviously aim at serving and promoting the commercial interests and activities of Facebook and the entire Facebook Group regarding to their social network and advertising activities:

- First of all this is admitted explicitly in Facebook Belgium SPRL's 2013 financial statement (p. 29): *"L'activité principale de la société en 2013 a consisté à apporter du soutien en matière de "*public policy" *au Groupe Facebook*." ("The company's main activity in 2013 consisted of providing support in the field of public policy") (unofficial translation).

- Secondly, Facebook Belgium SPRL reported to the press that this establishment was especially going to take on lobbying and that this lobbying would target the European privacy legislation

[15] In this context please refer to the deed of incorporation of Facebook Belgium SPRL in the annexes to the Belgian Official Journal of 24 June 2011: http://www.ejustice.just.fgov.be/cgi_tsv/tsv_rech.pl?language=nl&btw=0836948464&liste=Liste

[16] See Facebook Belgium's 2013 financial statement, p. 22.

under reform[17]. Considering the date of incorporation of Facebook Belgium SPRL (31 May 2011) and the date on which the European Commission published its proposals for the reform of European privacy legislation (25 January 2012), that seems very plausible indeed.

- Thirdly a "Public Policy Manager" job vacancy at Facebook Belgium confirms that this company has the object of supporting, representing and advising the entire Facebook Group[18]:

  - *"Monitor legislation and regulatory matters affecting Facebook and advise company with respect to policy challenges"*: obviously not legislation and matters are intended affecting Facebook Belgium SPRL, but Facebook Inc. and the entire Facebook Group.
  - *"Represent Facebook in meetings with government officials and elected members"* : obviously this does not mean represent Facebook Belgium SPRL but Facebook Inc. and the entire Facebook Group.
  - *"Develop public policy positions with other team members at Facebook":* obviously this is about developing a public policy for Facebook Inc. and the entire Facebook Group, among others in cooperation with or probably even following the instructions of public policy employees of Facebook Inc.
  - *"Advise Facebook team**s** on public policy matters to guide development of products, services and policies"*: according to Facebook Belgium SPRL's financial statements there were only 4 employees in 2013[19]. Consequently, it is very unlikely that the teams referred to here are (exclusively) teams at Facebook Belgium SPRL. This is more than likely about advising teams within the entire Facebook Group.

- Fourthly the managers of Facebook Belgium SPRL are top-ranking managers of Facebook Inc.:
  - T.U. (from the incorporation on 31 May 2011 to 19 October 2012): between September 2008 and July 2013 he was General Counsel of Facebook Inc. and therefore of the entire Facebook Group. He lives in California.
  - C.H. (from the incorporation on 31 May 2011 to 19 October 2012): she was Vice President of Finance of Facebook Inc. until October 2012, i.e. number 2 of the Finance Department of the Facebook Group. At the time she played an important role in Facebook's IPO. She lives in California.
  - D.K. (from October 2012 until today): he is Deputy General Counsel and Vice President of Facebook Inc. and therefore of the Facebook Group. He lives in California.

---

[17] http://facebookblog.nl/nieuws/facebook-opent-kantoor-in-belgie: "Facebook Belgium, as the company is called in Belgium, will be able to lobby even more from the Brussels office. The lobbying will especially target the privacy legislation the European Union is currently working on […] What this privacy legislation will look like exactly is still unknown, but Facebook hopes to contribute with its office in Belgium."

[18] https://nl-nl.facebook.com/careers/department?dept=grad&req=a0IA000000G2RSIMA3

[19] During the hearing a Facebook representative explained that there are 5 employees in the meantime, including *'a couple of people who are marketing specialists who market Facebook advertisement products'*.

- D.S. (between October 2012 and April 2014): at the time he was Chief Accounting Officer of Facebook Inc. and therefore of the Facebook Group. He lives in California.
- J.A. (from April 2014 until today): he is the successor of D.S. as the Chief Accounting Officer of Facebook Inc.

The above shows that Facebook Belgium SPRL is managed from Facebook Inc. and, furthermore, by top-ranking persons at Facebook Inc.

- Fifthly, the 2013 financial statement of Facebook Belgium SPRL even mentions that one of the main risks and insecurities this company faces consists of *"des problèmes liés à la protection de la vie privée pouvant impliquer une réduction du nombre d'utilisateurs"* ("problems related to the protection of privacy which could involve a decrease in the number of users") (p. 29) (unofficial translation). It is thus admitted that Facebook Belgium SPRL is impacted by the privacy issues of the social network. This obviously refers to the number of users of the social network of the entire Facebook Group.

34. According to Facebook, Facebook Belgium SPRL is a processor for Facebook Ireland. Both companies are said to have concluded a cooperation agreement to this end[20]. As shown above under A) Facebook Ireland cannot be considered as the only controller, and only Facebook Inc. can be qualified as such. Below under C) the Privacy Commission will clarify that Facebook Belgium SPRL constitutes a permenant establishment of Facebook Inc. on Belgian territory.

5. Applicable law and the Belgian Privacy Commission's competence

35. As shown below, it is undeniable that the Privacy Commission has the competence – granted to it by the Privacy Act and Directive 95/46/EC – to take measures against the processing of personal data by Facebook which are the object of this recommendation, since the Privacy Act is the applicable law in the light of article 4, § 1, a) of Directive 95/46/EC and the Judgment of 13 May 2014 of the European Court of Justice (CJEU) in the case *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-131/12).

36. Even if the applicability of the Privacy Act was contested based on the application of article 4, § 1, a) of Directive 95/46/EC and article 3bis, paragraph 1, 1° of the Privacy Act, the Privacy Act would nevertheless remain applicable taking into account article 4, § 1, c) of the Directive, which is examined in the alternative.

[20] Facebook's letter of 20 February 2015 to the Privacy Commission.

A) The application of article 4, § 1, a) of Privacy Directive 95/46/EC and article 3bis, paragraph 1, 1° of the Privacy Act

37. The Privacy Commission has decided to analyse the rules on applicable national law established by article 4, §1, a) of Directive 95/46/EC because this facilitates the analysis of the examination which took place in the CJEU Judgment of 13 May 2014. Although the Privacy Commission does not analyse article 3bis, 1st paragraph, 1°[21] itself (which transposes article 4, §1, a) of Directive 95/46/EC into Belgian law), it would nevertheless like to draw attention to the fact that the reasoning in the analysis of article 4, §1, a) of the Directive below, also applies to this article and must therefore also be understood as such.

38. Article 4, § 1 of the Directive stipulates: *"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;".

39. Article 2, d) of the Directive defines the "controller" as "*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law*".

40. As mentioned above, the question of whether Facebook Ireland can be considered as controller in the light of the Directive does not have to be examined here because it does not influence the applicability of Belgian law and the competence of the Belgian Privacy Commission, taking into account the interpretation the CJEU gives to article 4, § 1, a) in its Judgment of 13 May 2014, which applies in full considering that it deals with questions that are similar to those in this recommendation. The question of whether the controller is established in the European Union or not, is not relevant in this context.

41. Apart from Facebook Ireland, Facebook Inc. also has establishments in other EU Member States. To the knowledge of the Belgian Privacy Commission this is the case in the Netherlands, Germany, Spain, France and Belgium. These establishments are not presented as controllers for those

[21] Art. 3bis, paragraph 1: "1° to the processing of personal data carried out in the context of the effective and actual activities of any controller permanently established on Belgian territory or in a place where Belgian law applies by virtue of international public law".

countries, and this is not contested. Supporting activities are mostly involved, more particularly advertising activities, the purchase of commercial space, lobbying activities etc.

42. As shown by the articles of association published in the Belgian Official Journal, one of Facebook Belgium SPRL's objects is to perform for its own account or on behalf of third parties "*toute activité se rapportant au domaine des affaires publiques et du lobbying, et spécialement : l'analyse des systèmes d'influence, les stratégies de communication d'influence, l'identification des interlocuteurs clés (tels que les décideurs, relais, alliés), la création d'alliances et de partenaires, la prise de contact avec le Gouvernement, le Parlement, les administrations, les institutions européennes et internationales, l'établissement de propositions d'aménagements réglementaires ou législatifs (tels que les amendements) ainsi que l'élaboration d'argumentaires et d'outils de communication* ; (…)" ("any activity relating to the field of public affairs and lobbying, and particularly influencing systems, influencing communication strategies, identification of key contacts (such as decision-makers, intermediaries, allies), the creation of alliances and partnerships, contacts with the Government, Parliament, administrations, European and international institutions, drawing up proposals for regulatory or legislative changes (such as amendments), as well as elaborating sales pitches and communication tools; (…)") (unofficial translation). "*Elle peut accomplir d'une manière générale toutes opérations industrielles et commerciales*[22]*, financières et civiles, mobilières et immobilières ayant un rapport direct ou indirect avec son objet et pouvant en faciliter directement ou indirectement, entièrement ou partiellement, la réalisation. Elle peut s'intéresser par voie d'association, d'apport, de fusion, d'intervention financière ou autrement dans toutes sociétés, associations ou entreprises dont l'objet est analogue ou connexe au sien ou susceptible de favoriser le développement de son entreprise ou de constituer pour elle une source de débouchés*" (Broadly speaking it can perform all industrial and commercial, financial and civil, moveable and immoveable operations which are directly or indirectly related to its object and which could directly or indirectly, partially or entirely facilitate its achievement. Through association, merger, financial interventions or otherwise it can show an interest in any company, association or enterprise with an object that is analogous or related to its own object, or which might promote the development of its enterprise or constitute a source of business opportunities for it.") Moreover, the 2013 financial statement of Facebook Belgium SPRL explicitly mentions the fact that "*l'activité principale de la société en 2013 a consisté à apporter du soutien en matière de « public policy » au Groupe Facebook* » ("the company's main activity in 2013 consisted of providing support to the Facebook Group in the field of public policy") (unofficial translation).

43. By choosing the wording of article 4, 1 a) of the Directive as it is known today, the European legislator deliberately decided that – in the case in which a controllers has multiple establishments

[22] Underlined by the Privacy Commission.

within the European Union – the different national legislations regarding privacy protection apply to the processing of personal data of inhabitants of the Member States involved, so that actual and efficient protection is guaranteed in those Member States.

44. Preamble 19 of the Directive confirms this: "*Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities*".

45. Even if there were doubts about whether the law of a Member State in which there is an establishment of a controller must be applied because it is difficult to know in which way the nature of the activities of that establishment could or could not influence the applicability of national law, in its Judgment of 13 May 2014 the CJEU provided complete clarity with its interpretation in this context: the Court was of the opinion that a Member State's national data protection law is applicable if the activities of an establishment, incorporated in that Member State, are inextricably connected to the activities of the controller, and this regardless of the question of whether the establishment performs data processing activities or not.

46. The Court builds this argument as follows:

"*52. Nevertheless, as the Spanish Government and the Commission in particular have pointed out, Article 4(1)(a) of Directive 95/46 does not require the processing of personal data in question to be carried out 'by' the establishment concerned itself, but only that it be carried out 'in the context of the activities' of the establishment.*

53. Furthermore, in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively (see, by analogy, Case C-324/09 L'Oréal and Others EU:C:2011:474, paragraphs 62 and 63).

54. It is to be noted in this context that it is clear in particular from recitals 18 to 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope.

55. In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an

establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.
56. In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed."

47. And concludes:
"*60. It follows from the foregoing that the answer to Question 1(a) is that Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State."*

48. Pursuant to this reasoning of the Court in its judgment – a reasoning which, incidentally, is valid regardless of whether the controller is established in a third country or in the EU - and considering the activities[23] of Facebook Belgium SPRL, which are inextricably connected to the activities of the controller, there is not a shadow of doubt on the applicability of the Belgian privacy legislation and the competence of the Belgian Privacy Commission.

49. Moreover, the interpretation of the CJEU clearly advocates the effective protection of the fundamental right to privacy for data subjects by their own national data protection law, which is why the corresponding missions that national data protection authorities have been entrusted with are actually guaranteed and ensured. Therefore, it is self-evident that multiple national laws in this context apply to Facebook's new terms of use and to possibly resulting difficulties for all European citizens.

50. Apart from this manifest wish of the Court, attention must also be drawn to the fundamental right enshrined in article 13 of the European Convention on Human Rights: "*Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.*" This is a public duty which was made concrete by the Belgian legislator by granting

[23] See marginals 32-33.

competence to courts and tribunals, as well as to the Privacy Commission (article 30, § 1 of the Privacy Act).

51. Considering the above, there is no doubt that the Privacy Commission is competent and that Belgian privacy law applies, since Facebook processes data as described in this recommendation and has an establishment in Belgium, the activities of which are inextricably linked to its activities. Facebook consequently has to take all measures in order for Belgian data protection law to be applied and abided by on Belgian territory.

B) In the alternative: the application of article 4, § 1, c) of Privacy Directive 95/46/EC and article 3*bis*, paragraph 1, 2° of the Privacy Act

52. Even if the data processing operations subject to this recommendation could not be considered as being carried out in the context of the activities of Facebook Belgium in the meaning of the interpretation by the Court of Justice in its Judgment of 13 May 2014, *quod non*, article 4, § 1, c) of the Directive would still apply to the data processing operations carried out by Facebook on Belgian territory.

53. Article 4, § 1, c) of the Directive provides: *"Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:*

c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."

54. At first sight, this article can appear not to apply because there are several Facebook establishments on European Union territory. This is not the case, however: in order for this article not to be applicable, the different establishments would have to be considered as controllers. Yet as shown, this is not the case since the real controller, viz. Facebook Inc., is not established on European Union territory, but does use automated means for the purposes of processing personal data on this territory, using cookies for example[24].

[24] The Privacy Commission also refers to opinions of the Article 29 Working Party: no. 8/2010 of 16 December 2010 *on applicable law*, no. 8/2014 *on the Recent Developments on the Internet of Things* and the Working Document *on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites*, adopted on 30 May 2002.

55. As mentioned earlier it has not been shown that Facebook Ireland can be considered as controller in the meaning of the Directive, at least not in respect of the Belgian users of the Facebook network.

56. That said, even if article 4, § 1, a) of the Directive was not applicable, the Belgian Privacy legislation would still apply and the Privacy Commission would be competent for the processing operations carried out by Facebook Inc. involving Belgian users' personal data, taking into account article 4, § 1, c) of the Directive.

6. Tracking by means of social plug-ins[25]

A) Background and technical description

57. One of the main concerns for the public, the media as well as policy makers following the introduction of Facebook's modified terms of use, is that Facebook would track the surfing behaviour of both users and non-users of Facebook on external websites, so outside the domain of the social network site. "Tracking" in this context is understood to mean collect information about internet users' surfing behaviour on different websites. These tracking practices by Facebook are said to be carried out through plug-ins for integration, offered by Facebook to external website owners.

58. Social plug-ins are website components designed to share contents from an external source with Facebook's social network and enable a certain personalisation of an external website. Examples of social plug-ins are the "Like" button and the "Share" button. Owners of external websites who add such a social plug-in to their website integrate a part of Facebook into their website, as it were.[26] In other words the way in which these social plug-ins are usually implemented on external websites forces the user's browsers to collect content (such as images or scripts) from the Facebook servers, which discloses information to Facebook about the websites visited by the user through cookies (so-called "third-party tracking").

59. Social plug-ins are extremely popular because website owners attract more visitors when their content is shared on Facebook's social network. The "Like" button, Facebook's most popular plug-in, can be found on 32% of the top 10,000 of most visited websites[27], including more or less all categories of websites, including health and government websites. The Privacy Commission also

---

[25] Please refer to the technical report "Facebook tracking through social plug-ins" (which can be consulted on https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf). The technical findings have also been summarized on a separate web page (as "Frequently Asked Questions"): https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/.

[26] More information about Facebook's social plug-ins can be found, for example, on https://www.facebook.com/help/social-plugins.

[27] According to the Quantcast ranking: http://trends.builtwith.com/widgets/Facebook-Like

ordered an investigation into the top 100 of websites most visited by Belgian Internet users by means of a web crawler[28]. The results of this investigation confirmed the widespread use of social plug-ins.

60. Thanks to the widespread use of social plug-ins Facebook can track the surfing behaviour of its users on a large number of websites. Moreover, it has to be noted that Facebook is thus in a unique position, since it can easily links its users' surfing behaviour to their real identity, social network interactions and sensitive data such as medical information and religious, sexual and political preferences. This implies that tracking by Facebook is more intrusive compared to most of the other cases of so-called "third-party tracking".

61. Taking into account the concerns surrounding Facebook's tracking practices through social plug-ins and earlier findings in this context in the KULeuven/VUB research report, the Privacy Commission requested a further investigation into this matter. This resulted in a technical research report entitled "Facebook Tracking Through Social Plug-ins" (which can be consulted on https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf), which was added as an annex to the first research report "From social media service to advertising network. A critical analysis of Facebook's Revised Policies and Terms". The Privacy Commission's recommendation is based on the results of these reports, the main technical findings of which it has summarised below.

62. Facebook's tracking practices through social plug-ins are different depending on circumstances. That is why the technical findings have been divided according to data subjects, i.e. users and non-users of Facebook on the one hand, and the different scenarios on the other hand (logged in, logged out, deactivated or opted-out).

B) Main findings with regard to Facebook users

63. Relating to Facebook users, Facebook uses cookies for various purposes[29]. In principle[30] Facebook also reserves the right to use all the data it receives for different purposes, advertising purposes for example.

- *Users who have logged in*

[28] The results of this investigation showed that 35 out of 100 examined websites contained social plug-ins from Facebook.
[29] https://www.facebook.com/help/cookies/: including verification, security and site integrity, advertiing, insights and measurements, localisation, on-site functions and services, performance, statistics and research.
[30] The data policy includes: '*We use the information we have to improve our advertising and measurement systems […]*' (see https://www.facebook.com/about/privacy/update#what-kinds-of-information-do-we-collect)

64. When a user has logged in to Facebook and visits a web page with a social plug-in Facebook receives up to 11 cookies together with the URL of the page visited. The cookies received include the 4 following unique identifier cookies:

- c_user (contains the user's Facebook ID);
- datr (contains a unique browser ID);
- fr (contains the encrypted Facebook ID and browser ID[31]); and
- lu (contains the last user's encrypted ID).

65. These findings confirm that for users who have logged in, Facebook tracks surfing behaviour through social plug-ins outside the domain of Facebook's social network.

- *Users who have logged out*

66. If a user has logged out from Facebook and visits a web page with a social plug-in, Facebook receives a total of 4 cookies together with, among others, the URL of the page visited. The cookies received include the "fr" and "datr" unique identifier cookies.

67. These findings confirm that for users who have logged out, Facebook tracks surfing behaviour through social plug-ins outside the domain of Facebook's social network.

- *Deactivated users*[32]

68. If a user has deactivated his account and visits a web page with a social plug-in, Facebook receives a total of 4 cookies together with, among others, the URL of the page visited. The cookies received include the "fr" and "datr" unique identifier cookies.

69. These findings confirm that for deactivated users, Facebook tracks surfing behaviour through social plug-ins outside the domain of Facebook's social network.

- *Users who have opted-out*

70. If a user has opted out of targeted Facebook advertisements using the opt-out mechanism of the European Interactive Digital Advertising Alliance (www.youronlinechoices.eu)[33] proposed by

---

[31] According to Facebook's statement in the Audit Report of the Irish data protection report the "fr" cookie is used for advertising purposes
(see https://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf).

[32] These are users who have temporarily deactivated their account, but who have not permanently removed it. Their profile is invisible to others on Facebook and invisible in search results. Users who have deactivated their account can always restore their entire profile by reactivating their account. For more information please refer to https://www.facebook.com/help/214376678584711.

Facebook and visits a web page with a social plug-in, Facebook receives the "c_user", "datr", "lu" en "fr" unique identifier cookies together with, among others, the URL of the page visited. One of these cookies, viz. the "fr" cookie, is used exactly for advertising purposes according to Facebook's statement in the Irish data protection authority's Audit Report.

71. These findings confirm that for users who have opted out from targeted advertisements, Facebook tracks surfing behaviour through social plug-ins outside the domain of Facebook's social network.

C) Main findings with regard to non-users of Facebook

72. Facebook places a unique identifier "datr" cookie (which contains a unique browser ID) with a 2-year life when a non-user takes one of the following actions:

- the user visits a web page that is part of the facebook.com domain[34];
- the users visits certain websites in which Facebook Connect or social plug-ins have been integrated, although Facebook acts as a third party in this context;[35]
- the user opts out of tracking in the context of targeted advertisements by Facebook (among others) on the European Interactive Digital Advertising Alliance website (www.youronlinechoices.eu).

73. When the data subject (browser) then visits a web page with Facebook's social plug-ins, Facebook generally receives this unique identifier cookie again and again, together with, among others, the URL of the web page visited.

74. These findings confirm that for non-users of Facebook, Facebook is able to track surfing behaviour through social plug-ins outside the domain of Facebook's social network.

D) Legal analysis: the Privacy Act and the Act on Electronic Communication[36]

- *Privacy Act*

75. Pursuant to the Privacy Act, when Facebook receives information through cookies in the context of social plug-ins, this constitutes the "processing of personal data" in the meaning of article 1, § 1

---

[33] https://www.facebook.com/about/ads/
[34] In other words, this does not have to be Facebook's main page, but e.g. a Facebook fan page, a shop's Facebook page, a Facebook event page (party, jumble sale, …).
[35] This involves a limited number of websites. Facebook declared that this is an unintentional practice and that i twill investigate the matter further.
[36] Act of 13 June 2005 on electronic communication.

and § 2 of the Privacy Act.[37] Facebook's argument that in certain cases there is no tracking because the data collected are anonymized or destroyed after some time, is therefore irrelevant here, since initially – purely by collecting cookies and website data through plug-ins – personal data were processed.

76. Pursuant to article 5 of the Privacy Act processing personal data is only authorised if there is a legitimate basis. To collect data through social plug-ins Facebook can in fact only invoke (a) the data subject's consent or (b) the fact that the processing is necessary for the performance of a contract to which the data subject is a party.

77. In order to justify the processing operations concerned, it is difficult For Facebook to invoke the necessity to perform these operations to guarantee the performance of the contract (particularly the contractual provisions described in the terms of use) to which the data subjects are a party:

- As regards non-users of the social network: there can never have been any contract with provisions applying to them;
- As regards users: the possibility they are given (even though its conditions can be criticised – see infra) by Facebook to block or refuse the use of the cookies is sufficient to ascertain the non-necessary nature of this use for the performance of the contract for signing up to Facebook.[38]

78. Consequently, Facebook must first of all invoke article 5, a) of the Privacy Act to justify the processing operations concerned, regardless of other legal bases which are invoked or not, and be able to demonstrate that the requirements of this provision have actually been met.

79. The above implies that **data subjects must always give their unambiguous and specific prior consent before Facebook can place or receive the cookie in the context of social plug-ins.**

---

[37] Article 1, §1 and §2: "§1. For the purposes of this Act"personal data" meansany information relating to an identified or identifiable natural person, hereinafter the "data subject"; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or morefactors specific to his physical, physiological, mental, economic, cultural or social identity.
§ 2. '"Processing" means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by means of transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data."
In its letter of 2 March 2015, Facebook implicitly yet unjustly indicates that collecting information about an end user does not involve "personal data" because this does not identify an individual but a browser (Facebook's letter of 2 March 2015, p. 6 ("*If the person visited Facebook, but did not log in, the person would have received our "datr" cookie, which contains an alphanumeric string that uniquely identifies a browser — not a particular Facebook user*")

[38] In its letter of 2 March 2015 Facebook alleges that placing the "datr" cookie is necessary to guarantee the security and integrity of its services. The argument that placing and receiving cookies is also strictly necessary to ensure Facebook users' security, lacks both a legal and a factual basis. First of all it is possible to guarantee user security in a less intrusive way. Moreover, it would be child's play for a potential attacker to simply block and/or remove cookies when launching the attack. Even if this argument on security was accepted, this would obviously not constitute a basis to use the cookies for other purposes. Such use for other purposes would therefore also explicitly have to excluded as such in the terms of use.

80. In order to be lawful, the data subject's consent must be (1) freely given; (2) informed; (3) specific and (4) unambiguous. [39]

- *Freely given*

81. The data subject must be given the possibility to exercise a "real choice". In other words, there must not be any "*risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.*"[40] In this case there are two factors compromising "freely given" consent. The first factor relates to Facebook's dominant position on the market of social networks. One of the most important reasons to register on Facebook is exactly because "everybody is already on Facebook". Secondly, individuals' possibilities not to grant consent are limited considerably. It is not possible, for example, to only grant consent for Facebook's basic functions (e.g. sharing information with your friends), without also granting consent to the processing of your data for commercial profiling. This practice conflicts with the Article 29 Working Party's guidelines in its opinion on consent:
"Considering the importance that some social networks have acquired, some categories of users (such as teenagers) will accept the receipt of behavioural advertising in order to avoid the risk of being partially excluded from social interactions. The user should be put in a position to give free and specific consent to receiving behavioural advertising, independently of his access to the social network service. A pop-up box could be used to offer the user such a possibility."[41]

- *Specific*

82. As the Article 29 Working Party also emphasises in its opinion on consent:
"Considering that the application can run without it being necessary that any data is transferred to the developer of the application, the WP encourages granularity while obtaining the consent of the user, i.e. obtaining separate consent from the user for the transmission of his data to the developer for these various purposes. Different mechanisms, such as pop-up boxes, could be used to offer the user the possibility to select the use of data to which he agrees (transfer to the developer; added value services; behavioural advertising; transfer to third parties; etc)."

- *Informed*

83. In order to be sufficiently informed, the data subject must at least receive the information described in article 9 of the Privacy Act. Moreover, the European Court of Justice has already

[39] Article 29 Working Party, Opinion 15/2011 *on the definition of consent*, WP 187, 25 November 2011.
[40] Article 29 Working Party, Opinion 15/2011 *on the definition of consent*, p. 12
[41] Article 29 Working Party, Opinion 15/2011 *on the definition of consent*, p. 18.

sentenced that purely offering a hyperlink (which does not oblige users to read the entire text) is insufficient.[42]

- *Unambiguous*

84. "Unambiguous" means that data subjects' actions can only be considered as the expression of their agreement that personal data relating to them will be processed. Setting which have been pre-configured in such a way that information is disclosed unnecessarily without users' active involvement, do not result in "unambiguous" consent. As underlined by the Article 29 Working Party, an opt-out mechanism is *"not an adequate mechanism to obtain average users' informed consent"*, particularly relating to behavioural advertising.[43] In other words: Facebook's opt-out approach relating to profiling does not meet the conditions for lawful consent.[44]

85. Finally, pursuant to article 4, § 1, 3° of the Privacy Act, the data processed must be adequate, relevant and not excessive. This means that the data of the processing operation must be limited to what is strictly necessary in order to achieve the specific purpose(s).

86. The present recommendation does not aim to give an extensive description of Facebook's purposes as indicated in their general terms of use and to which we would like to refer the reader[45], As explained above, these terms of use do not only apply to users because Facebook's processing operations, and consequently the purposes it aims to achieve, are not limited to the users of the social network.

87. The collection personal data of non-users of Facebook, who did not register for their service and were consequently not informed of the collection of data pursuant to article 9 of the Privacy Act (cfr. supra), cannot be considered as relevant to a social network service provider in any case.

88. As to Facebook users, even if they have subscribed to the terms of service, it must also be noted that it is excessive for Facebook to systematically collect data about websites which are not part of its domain but which contain social plug-ins it developed, even if the member did not interact with these social plug-ins and simply viewed the page they are on.

---

[42] CJEU, 5 July 2012, *Content Services Ltd v Bundesarbeitskammer*, C-49/11. See E. Wauters, E. Lievens en P. Valcke, "A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: 'Rights & obligations in a social media environment", EMSOC D1.2.4, 19 December 2013, available on http://emsoc.be/wp-content/uploads/2013/12/D-1.2.4-A-legal-analysis-of-Terms-of-Use-of-Social-Networking-Sites-including-a-practical-legal-guide-for-users_Rights-obligations-in-a-social-media-environment6.pdf.

[43] Article 29 Working Party, Opinion 2/2010 *on online behavioural advertising*, WP 171, 22 June 2010, p. 15.

[44] Also see the following letter by the Article 29 Working Party: "Letter from the Article 29 Working Party addressed to Online Behavioural Advertising (OBA) Industry regarding the self-regulatory Framework", 23 Augustus 2011, available on http://ec.europa.eu/justice/data-protection/article29/documentation/otherdocument/files/2011/20110803_letter_to_oba_annexes.pdf.

[45] See footnote 2.

In principle this reasoning remains valid, whether or not the member has logged in to Facebook when consulting these websites. It is valid all the more so for "deactivated" users and users who opted-out of targeted Facebook advertisements. Only if the collection of data is strictly necessary for an explicitly requested service (e.g. personalisation) systematic collection can be justified. But for such purposes "session cookies" can be used: they serve a specific purpose and their life must end when the user "logs out" of the social network platform or when the browser window is closed.[46]

89. The Privacy Commission therefore only wishes to stress vigorously that it is important for controllers to ensure that they observe the rule of article 4, § 1, 3° of the Privacy Act.

- *Act on Electronic Communication*

90. As in its own-initiative recommendation no. 01/2015 of 4 February 2015 on the use of cookies[47], the Privacy Commission would also like to draw attention to the legislative framework on electronic communication, in the sense that some of its provisions provide a specific framework for the consent of Internet service users.

91. The preambles of Directive 2002/58/EC of 12 July 2002 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[48] indicate that the provisions of this Directive clearly reflect the rules of Directive 95/46/EC and stipulate particularly that *"by supplementing Directive 95/46/EC, this Directive is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons."*[49] Preamble 17 specifically states that "*For the purposes of this Directive, consent of a user or subscriber (…) should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC.*" This reference is important to the extent that it ensures the effectiveness of the protective privacy rules provided for by Directive 2002/58/EC.

92. The Act of 13 June 2005 on electronic communication, which transposes Directive 2002/58/EC into Belgian law, explicitly refers to the Privacy Act in its article 129[50].

---

[46] Article 29 Working Party, Opinion 04/2012 on Cookie Consent Exemption, WP 194, 7 June 2012, pages 9-10.

[47] http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2015_0.pdf

[48] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[49] See preamble 12 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 (Directive on privacy and electronic communications).

[50] Unofficial English translation: "Storing information or gaining access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that: 1° pursuant to the conditions established by the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, the subscriber or user concerned is provided with clear and precise information about the purposes of the processing and his rights based on the Act of 8 December 1992; 2° the subscriber or end user has given his consent after having been informed pursuant to the provisions mentioned in 1°. The

93. Because the Act of 13 June 2005, contrary to the Privacy Act, is not subject to a criminal sanction and is intended to protect users of an electronic communication service open to the public (see article 2, 12° of the Act of 13 June 2005) against the processing of personal data relating to them by such a service, it is important to guarantee the competence of the Belgian supervisory authority. The latter must be able to examine whether the rules of the Privacy Act for the processing of personal data are actually observed by the controller – such as the rule established by article 5 to which the Act of 13 June 2005 refers concerning user consent[51] - and if necessary, resort to the application of article 39, 2° of the Privacy Act providing for a criminal sanction in case of violations of the legal provisions in this context.

94. The above implies that data subjects must always give their unambiguous and specific prior consent before Facebook can place or receive the cookie in the context of social plug-ins.

95. As for *non-users* of Facebook, according to the Article 29 Working Party this means that social network site such as Facebook cannot invoke one of the grounds for exemption from article 5(3) of e-Privacy Directive 2002/58/EC (article 129 of the Act on Electronic Communication).

96. As for Facebook *users*, the Article 29 Working Party makes an additional *distinction based on whether or not the user has logged in* to Facebook:
"To address this use case, it is important to distinguish users who "logged-in" through their browser in a particular social network account, from "non-logged-in" users who are either simply not a member of that specific social network or who have "disconnected" from their social network account. Since by definition social plug-ins are destined to members of a particular social network, they are not of any use for non members, and therefore do not match CRITERION B.[52] *This can be extended to actual members of a social network who have explicitly "logged-out" of the platform, and as such do not expect to be "connected" to the social network anymore. Consent from non-members and "logged-out" members is thus needed before third party cookies can be used by social plug-ins. On the other hand, many "logged in" users expect to be able to use and access social plug-ins on third party websites . In this particular case, the cookie is strictly necessary for a functionality explicitly requested by the user and CRITERION B applies. Such cookies are session cookies: to*

---

first paragraph does not apply to the technical registration of information or of access to the information stored on a subscriber's or end user's terminal equipment for the sole purpose of transmitting a communication over an electronic communication network or providing a service explicitly requested by the subscriber or the end user if this is strictly necessary for this purpose. Consent in the meaning of paragraph 1 or the application of paragraph 2 does not imply that the controller is exempt from the obligations of the Act of 8 December 1992 on the protection of privacy relating to the processing of personal data that are not imposed by the present article. The controller shall enable subscribers or end users free of charge to withdraw their consent in a simple manner."

[51] See marginals 81 and following relating to consent.

[52] "CRITERION B" refers to the exception of article 129 of the Act on Electronic Communication when a cookies is strictly necessary for *"a service explicitly requested by the subscriber or end user"*.

serve their particular purpose, their lifespan should end when the user "logs-out" of his social network platform or if the browser is closed. Social networks that wish to use cookies for additional purposes (or a longer lifespan) beyond CRITERION B have ample opportunity to inform and gain consent from their members on the social network platform itself."[53]

97. There are already several tools limiting the unnecessary collection of data by Facebook. The "Social Share Privacy" tool, for example, enables webmasters to disable social plug-ins until visitors express their wish to use them or not.[54].

98. The "Social Share Privacy" tool works as follows: a standard grey image of a plug-in is shown. It is not until the user clicks this image that the "real" plug-in is loaded (and that the information is transmitted to the OSN provider). With a second mouse click the user can use the plug-in.[55] The French Commission for the Protection of Personal Data (CNIL) has approved this method as a way to obtain valid consent.[56]

99. As controller **Facebook is responsible for collecting and receiving cookies and related information,** regardless of any additional responsibilities of webmasters. More particularly, Facebook must design and offer its plug-ins in such a way that webmasters can integrate these components without unnecessarily providing data to Facebook.

100. The Privacy Commission would like to recall that the principles relating to fundamental rights are applicable regardless of technical implementations. From this point of view and in the light of both Directive 95/46/EC and Recommendation 01/2015 on cookies, the Privacy Commission underlines that the principles in the present recommendation are general principles for all tracking information, regardless of which technical tool is used (such as cookies, plug-ins, add-ons, …) or where it is stored (local disk, websites visited, social networks, …).

FOR THOSE REASONS,

---

[53] See the Article 29 Working Party, opinion no. 04/2012 *on Cookie Consent Exemption*, p. 9-10. Also see Article 29 Working Party, Opinion no. 2/2010 *on online behavioural advertising*, p. 13: *"It follows from the literal wording of Article 5.(3) that: i) consent must be obtained before the cookie is placed and/or information stored in the user's terminal equipment is collected, which is usually referred to as prior consent and ii) informed consent can only be obtained if prior information about the sending and purposes of the cookie has been given to the user. In this context, it is important to take into account that for consent to be valid whatever the circumstances in which it is given, it must be freely given, specific and constitute an informed indication of the data subject's wishes. Consent must be obtained before the personal data are collected, as a necessary measure to ensure that data subjects can fully appreciate that they are consenting and what they are consenting to. Furthermore, consent must be revocable."*

[54] More information can be found on http://panzi.github.io/SocialSharePrivacy/.

[55] More information can be found on http://panzi.github.io/SocialSharePrivacy/.

[56] See "*Solutions pour les boutons sociaux*" ("Solutions for social buttons"), Commission nationale de l'informatique et des libertés (CNIL), available in French on http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/outils-et-codes-sources/les-boutons-sociaux

The Commission for the Protection of Privacy,
Based on the competence it has been granted and on the law of Belgium and the European Union
Recommends:

To Facebook

- Facebook must provide full transparency about the use of cookies. For each cookie separately, Facebook must specify its content (such as unique identifiers, language settings, etc.) and its purpose (such as advertising, security etc.). These descriptions must always be kept up-to-date and be offered to users of Facebook services in an readily accessible way.
- Facebook must refrain from systematically placing long-life and unique identifier cookies with non-users of Facebook, as well as from collecting and using data by means of social plug-ins unless it obtains the data subjects' unambiguous and specific consent through an opt-in and to the extent that this is strictly necessary for legitimate purposes. Both deactivated users and users who have logged out must be treated like non-users in this context.
- Facebook must refrain from collecting and using the data of Facebook users by means of cookies and social plug-ins, except when (and only to the extent that) this is strictly necessary for a service explicitly requested by the user or unless it obtains the data subjects' unambiguous and specific consent through an opt-in since working with an opt-out does not result in unambiguous consent.
- Facebook must limit its range of integration possibilities for social plug-ins to privacy-friendly versions meeting data protection requirements. More particularly, for the design of social plug-ins the Privacy Commission recommends that:
    - The mere presence of a social plug-in on an external website does not lead to the transmission of data to Facebook. By way of example the Privacy Commission refers to the concept of the "Social Share Privacy" tool, where data are not sent to the involved social network until users have signified unambiguously by means of a mouse click that they want to use the social network button. Other solutions, such as the integration of a URL/link offered by Facebook as an integration possibility until March 2015, are nevertheless not excluded.
    - If loading (non-personalised) content from Facebook servers is required, no cookies are sent to Facebook.
    - If personalisation is necessary, only session cookies are used.
    - The transmission of cookies used by Facebook in the context of security (such as the "datr" cookie) is limited to logging in to Facebook or to pages that are part of the facebook.com domain (but not on web pages of third parties with social plug-ins).

- Facebook must adapt its user interface in such a way that it obtains its users' unambiguous and specific consent through an opt-in for any further collection and use of information obtained by means of cookies, particularly for advertising purposes.

To Website Owners

- Relating to website owners or webmasters who wish to use the social plug-ins offered by Facebook, the Privacy Commission refers to its own-initiative recommendation on the use of cookies,[57] in which it stipulates that owners must properly inform visitors of their website and obtain the latter's specific consent for cookies and other meta files of which they may not control re-use. In this context, the Privacy Commission refers to social networks, among others, and recommends that social network buttons are not activated until users have given their specific consent. The current integration possibilities of social plug-ins offered by Facebook, however, do not meet these criteria yet. For the time being, the Privacy Commission therefore recommends to use tools such as "Social Share Privacy" (http://panzi.github.io/SocialSharePrivacy/) as a way to obtain user consent. By using a tool such as "Social Share Privacy", third-party plug-ins do not connect to third-party servers (and consequently data are not sent to third parties) until users have clicked on the social plug-in.

To End Users

- Internet users who wish to protect themselves against tracking by Facebook through social plug-ins are advised to use browser add-ons that block tracking. Examples of such browser add-ons are:
    - Privacy Badger (https://www.eff.org/privacybadger)
    - Ghostery (https://www.ghostery.com)
    - Disconnect (https://disconnect.me/disconnect)
- Internet users can also protect themselves by using the incognito or "private navigation" mode offered as a functionality in recent versions of most frequently-used browsers (Internet Explorer, Firefox, Chrome, Safari, etc.). This functionality forces the browser to delete traces of surfing behaviour (cookies, history, etc.) after the window is closed and thus protects Internet users from being tracked by Facebook or others[58].

[57] http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2015_0.pdf

[58] There are also special privacy-protecting browsers, e.g. Epic Privacy Browser (www.epicbrowser.com).

- Facebook users can opt-out of tracking in the context of targeted Facebook advertisements on the European Interactive Digital Advertising Alliance website (www.youronlinechoices.eu). It must be noted, however, that Facebook currently continues to collect the same information about visits of users to external websites, even after they have opted out from targeted advertisements. Nevertheless, Facebook has promised to no longer use this information for advertising purposes. Users who wish to protect themselves against the collection of this information are therefore advised to also use their browser's incognito mode or use one of the abovementioned add-ons.

For the Acting Administrator, absent

(sgd.) An Machtens
Acting Head of the ORM Department.

The President,

(sgd.) Willem Debeuckelaere