Litigation Chamber

Decision on the merits 37/2020 of 14 July 2020

This decision was annulled by the judgment 2020/AR/1111 of the Court of appeal of 30 June 2021

Case no.: DOS-2019-03780

Subject: X v Google (delinking, right to be forgotten)

The Litigation Chamber of the Belgian Data Protection Authority, composed of Hielke Hijmans, chairman, along with Yves Poullet and Christophe Boeraeve, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter the 'GDPR';

Having regard to the Belgian Data Protection Authority Act of 3 December 2017, hereinafter the 'DPAA';

Having regard to the by-laws approved by the House of Representatives on 20 December 2018 and published in the Belgian Official Gazette on 15 January 2019;

Having regard to the documents submitted in this case;

Has issued the following decision concerning:

- plaintiff 'X', represented by Carine Doutrelepont;
- the data controller: Google Belgium SA, Chaussée d'Etterbeek 180, 1040 Brussels, represented by Louis-Dorsan Jolly and Gerrit Vandendriessche.

1. Facts and procedure

1. Plaintiff, a resident of Belgium, filed a complaint signed on 12 August 2019 against Google Belgium SA, a Belgian company, regarding the removal of a series of search listings numbered from 1 to 12, each of the twelve URLs being listed in the complaint. The complaint was declared admissible by the Litigation Chamber's front office on 14 August 2019.

2. In essence, plaintiff opposes Google's refusal of his delisting requests submitted via the online form for requests to delete personal data. According to him, a web search of his first and last name returns content from Belgian print news outlets that is damaging to his honour and his reputation.

3. More specifically, he criticises two categories of content indexed by Google. The first is content depicting plaintiff as 'affiliated with the Y party' (a Belgian political party), despite the fact that this constitutes, according to plaintiff, processing of a special category of personal data within the meaning of article 9 of the GDPR – not covered by the exceptions provided for in the GDPR – and that, furthermore, it is inaccurate.

4. The second is content mentioning a harassment complaint against plaintiff, which was dismissed in 2010 when the body tasked with examining it, ARISTA,[1] held that it was without merit, and as such, plaintiff contends that the information in question is no longer current.

5. For the first category of content, numbered 1 through 8, Google replied that it was unable to access search listing 2[2] ('Google therefore asks that a screenshot of all of the content of the page in question be sent to allow it to study the request in further detail.'); that search listing 7 was deleted or the page could not be displayed; and that it had decided to not block search listings 1, 3, 4, 5, and 8[3] or search listing 6.[4]

6. As for the second category of content, numbered 9 through 12, Google also decided not to block it.[5]

[1] SPMT-ARISTA is an external workplace protection and prevention service, which since 1 January 2020 is named cohezio (see https://www.cohezio.be/fr, consulted 20 February 2020).

[2] Google therefore asks that a screenshot of all of the content of the page in question be sent to allow it to study the request in further detail.

[3] As to the reasons given: 'After weighing the interests and rights associated with the content in question, including factors such as the content's relevance to your working life, Google has decided not to block it.'

[4] The following justification was given: 'After weighing the interests and rights associated with the content in question, including factors such as the obvious relevance of the content, Google has decided not to block it.'

[5] The following justification was given: 'After weighing the interests and rights associated content in question, including factors such as your role in public life, Google has decided not to block it.'

7. On 30 August 2019, the Litigation Chamber decided, pursuant to article 95, paragraph 1, point 1 and article 98 of the DPAA, that the complaint was admissible for a decision on the merits. The parties were asked to provide written submissions. Google's submitted its written submissions on 30 September 2019. On 15 October 2019, plaintiff asked the clerks' office of the Litigation Chamber, in the absence of any clear provisions in the DPAA, to decide whether it was possible to join Google Ireland Ltd and Google LLC to the proceedings. On 21 October 2019, plaintiff was informed that, without prejudice to the decision that would ultimately be made on this point, he was authorised to include this request in his written submissions, which would also allow opposing counsel to express its position regarding to this matter. That same day, plaintiff submitted its written submissions in response, which did not include a request for other parties to be joined into the proceedings. On 12 November 2019, Google filed its final written submissions.

8. Several times, and most recently in a letter dated 21 November 2019, Google requested an oral hearing. The parties were asked by the Litigation Chamber to attend a hearing. Article 93 of the DPAA authorises the Litigation Chamber to hold oral hearings with the parties involved in a complaint. On this basis, and in light of the parties' written submissions, the Litigation Chamber also requested that Google LLC participate in the scheduled hearing to put forward any arguments it deemed necessary. A hearing was held on 6 May 2020 in the presence of Google Belgium SA and plaintiff, represented by his counsel, Carine Doutrelepont. Google LLC did not respond to the Litigation Chamber's request and was not present. Google Belgium SA, when asked about this point, explained that the request had been received by Google LLC, but that in California, nothing was being signed manually due to the COVID-19 epidemic. However, the Litigation Chamber wrote Google LLC by ordinary post, and Google LLC responds using the same means of communication by which it is contacted. Nevertheless, Google was aware of the Litigation Chamber's email address, and could have used it to reply. Owing to the COVID-19 epidemic, the hearing was held by remote videoconference.

9. The parties were sent the hearing minutes on 11 May 2020. On 13 May 2020, plaintiff informed the Litigation Chamber that he had no observations. On 22 May 2020, Google Belgium SA submitted its remarks on the minutes from the May 6 hearing using the 'track changes' feature.

10. On 4 June 2020, the Litigation Chamber sent an email to Google Belgium SA informing it of the amount of the proposed fine to be imposed on it and the reasons for which the GDPR breaches that had been committed justified that amount. Google Belgium SA was asked, in the same email, to submit arguments in its defence regarding the proposed amount of the fine. The Litigation Chamber received these arguments by email on 24 June 2020.

11. On 9 June 2020, the Litigation Chamber sent an informal voluntary information request under article 61 of the GDPR using the system for mutual assistance between data protection authorities,

asking for a response within two weeks. Data protection authorities in Spain, Portugal, Hungary, Slovakia, Germany (Hamburg and Baden-Württemberg), France, Italy, and Ireland submitted comments within this time period.

2. Structure of the decision

12. In this decision, the Litigation Chamber examines the issue of the delisting of content displayed by a search engine when searches are performed on a natural person. This issue has been covered in leading cases from the Court of Justice of the European Union (hereinafter the 'CJEU' or the 'Court of Justice'), including the *Google Spain*[6], *Google v CNIL*[7], and *GC et al. v CNIL*[8] rulings. The Belgian Court of Cassation has also issued rulings on delisting and the right to be forgotten.[9]

13. For the Litigation Chamber, this is an opportunity to adopt a general stance and set out certain fundamental principles regarding delisting, on the basis of CJEU case law in this area and regarding other points related to the scope of its authority (in particular the CJEU's *Wirtschaftsakademie* ruling).[10]

14. In this decision, the Litigation Chamber first evaluates the jurisdiction of the Belgian Data Protection Authority (DPA) in cases subject to article 55.1 and recital 122 of the GDPR, demonstrating that the 'one-stop-shop mechanism' described in the GDPR does not apply to the instant case (Section 3).

15. Second, after concluding that it does in fact have jurisdiction, the Litigation Chamber turns to the notion of the 'data controller' within the meaning of article 4(7) of the GDPR, with the aim of deciding whether Google Belgium SA – the respondent in this case – can be considered to be the data controller and/or to have its activities inextricably linked to those of the data controller (Google LLC), and whether the DPA is entitled to exercise its authority over Google Belgium (Section 4).

16. Third, it determines the territorial scope of the delisting, in light of the *Google/CNIL* judgment (Section 5).

---

[6] CJEU, 13 May 2014, C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

[7] CJEU, 24 September 2019, C-507/17, Google LLC v Commission nationale de l'informatique et des libertés (CNIL).

[8] CJEU, 24 September 2019, C-136/17, GC et al. v Commission nationale de l'informatique et des libertés (CNIL).

[9] See, for instance, the Belgian Court of Cassation ruling of 29 April 2016.

[10] CJEU, 5 June 2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH.

17. Fourth, the Litigation Chamber examines plaintiff's delisting requests regarding his alleged political affiliations and the harassment complaint (Section 6).

18. Fifth, the Litigation Chamber finds that certain facts brought to its attention in this case constitute a violation of the GDPR (Section 7) and orders the corrective measures to be taken.

3. The jurisdiction of the DPA and the inapplicability of the 'one-stop-shop mechanism'

19. The jurisdiction of the DPA is defined and regulated by Chapter VI of the GDPR.

20. Article 55.1 of the GDPR provides that each supervisory authority has the authority to conduct matters relating to its powers and responsibilities 'within the territory of its own Member State'. Recital 122 of the GDPR states that this should cover, inter alia, 'processing in the context of the activities of an establishment of the controller or processor' within this territory, as well as 'processing affecting data subjects' within this territory.

21. Territorial jurisdiction is a major principle of the GDPR, which must be understood in light of article 3, paragraph 1 of the GDPR regarding the territorial scope of the GDPR. The territorial jurisdiction of the supervisory authority is a jurisdictional rule rooted in the principle of public international law holding that countries have the authority to dictate the law within the boundaries of their territory. This principle of the GDPR is to be considered alongside the purpose (*ratio legis*) of the GDPR to ensure effective, comprehensive protection of data subjects' basic rights. Territorial jurisdiction can include the activities of a local subsidiary of a company based in a third country.[11]

22. Territorial jurisdiction also applies when processing is performed by a data controller not established in the European Union, as provided for in and in accordance with the requirements of article 3.2 of the GDPR. This has been confirmed by the European Data Protection Board (EDPB).[12]

23. However, an exception to this foundational principle of the GDPR is provided for in article 56.1 and article 60, which covers cooperation between the lead supervisory authority and the other supervisory

[11] THE EU GENERAL DATA PROTECTION REGULATION (GDPR), A Commentary, Edited by Kuner, Bygrave and Docksey, OUP 2020, pp. 903, 906-908. See also points 34 and 53 of the *Google Spain* ruling.

[12] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – for public consultation, adopted 12 November 2019, available on www.edpb.europa.eu.

authorities concerned (the 'one-stop-shop' mechanism). Whenever cross-border data processing takes place within the European Union, the lead supervisory authority guides cooperation. The scope of this exception is limited to 'cross-border processing' as defined in article 4(23) of the GDPR – that is, processing that takes place in several of a data controller's establishments in more than one Member State, or processing that substantially affects data subjects in more than one Member State (or is likely to affect them). In this case, the complaint was filed against Google Belgium SA, a subsidiary of Google LLC (United States). This Belgian entity, a subsidiary of Google for the purposes of company law, is the respondent. Google Belgium SA, however, contends that Google LLC (United States) is the sole data controller.

24. The Litigation Chamber notes that even were Google LLC (and not Google Belgium SA) the data controller – an argument that the Litigation Chamber does not agree with[13] – the DPA would nevertheless have jurisdiction over a complaint filed by a Belgian national. Processing of personal data by a data controller's entity located outside of the European Economic Area is not covered by articles 56.1 and 60 of the GDPR. Google, an American company, has a 'main establishment' in the European Union – specifically, in Ireland, via Google Ireland Ltd. Were the processing in question in this case to take place within the context of the activities of this main establishment, it would be covered by article 56.1 of the GDPR and the 'one-stop-shop' system of cooperation, with the Irish data protection authority acting as lead supervisory authority.

25. At the hearing, the division of responsibilities within the Google group was discussed, as the Litigation Chamber had said it would be in its invitation to attend the hearing. In this invitation, the Chamber clearly expressed its desire to be informed of the roles and responsibilities of the 'Google' group's establishments, including whether a 'main establishment' (within the meaning of article 4(16) of the GDPR) exists.[14]

26. Google Belgium SA acknowledged that Google Ireland Ltd was Google's main establishment within the meaning of article 4(16) of the GDPR, i.e. Google LLC's 'place of central administration' in the European Union. While the role of Google Ireland is mentioned in these proceedings, the Litigation Chamber has determined that the data processing in this case does not fall within the activities of Google Ireland Ltd.

27. First, at the hearing, Google Belgium SA contended that the reference to Google Ireland Ltd was not within the scope of this case. According to Google Belgium SA, plaintiff's written submissions did not

[13] See below, points 32-53.

[14] The request contained the following passage: 'Without prejudice to any arguments they might wish to make before the Litigation Chamber, the parties are each invited, within the context of this case, to inform the Chamber of the activities, roles, and responsibilities of Google LLC and Google Belgium SA, as well as whether Google has a "main establishment" (within the meaning of article 4(16) of the GDPR) within the European Economic Area.'

include any reference to Google Ireland and the issue was between Google Belgium SA and Google LLC – and therefore, Google Ireland Ltd could not be a party to the case. In these proceedings, the parties did not debate the issue of 'Google Ireland versus Google Belgium', with the debate revolving solely around Google Belgium SA and Google LLC. Consequently, for procedural reasons, Google felt that the Litigation Chamber should not express an opinion on the role of Google Ireland Ltd. The Litigation Chamber feels it bears repeating, however, that it had expressly asked the parties to say whether Google has a 'main establishment' in the European Economic Area,[15] and it was determined at the hearing that Google Ireland Ltd was in fact the main establishment.

28. Second, at oral argument, Google Belgium SA insisted on the fact that Google Ireland Ltd's activities as data controller concern matters not related to search engine indexing. Such processing concerns 'user data', e.g. when an individual uses Google's search engine, his or her search history may be used by Google to provide tailored search results. In this case, Google Ireland Ltd would be the data controller. For Google's search engine and the processing corresponding to the three steps needed for the operation of the search engine (crawling, indexing, and selection of search results) at issue in the proceedings, Google Ireland Ltd is not the data controller. This division of roles is explained by the fact that Google Ireland Ltd acts as the liaison for EU residents but is not involved in the creation and operation of the search engine, for which Google LLC is exclusively responsible.

29. Thus, the position defended by Google Belgium SA at the hearing that Google Ireland Ltd is the data controller when, for example, a user's search history is processed to tailor the results displayed to him or her by the search engine, potentially contradicts Google Belgium SA's other argument that Google LLC is, in fact, the sole data controller within the context of the operation of the search engine and the three phases mentioned above (crawling, indexing, and selecting results).

30. Consequently, the data processing (i.e. the delisting) in this case does not fall within the scope of Google Ireland Ltd's activities. In sum, in this case, the Irish supervisory authority cannot be the lead supervisory authority within the meaning of articles 56 and 60 of GDPR, meaning that the 'one-stop-shop mechanism' does not apply and the Litigation Chamber's jurisdiction can be seen from the perspective of the principle of territoriality set out in article 55.1 of the GDPR.

31. This conclusion is corroborated by the position Google LLC assumed in a letter to the Irish supervisory authority on 23 June 2020, in which Google LLC explained that it would not be opposed to allowing a supervisory authority exercise local jurisdiction over data processing that fall within the scope of

[15] See above, note 14.

Google LLC's responsibility.[16] Google LLC's stance, however, does not mean that a system of cooperation cannot apply.[17]

4. Regarding the data controller

32. The aim of this section is to determine whether Google Belgium SA – the respondent in this case – can be considered as the data controller for the purposes of plaintiff's delisting requests, i.e. the entity that determines the purposes and means of processing and/or whose activities are inextricably tied to those of the data controller – in this case, Google LLC.

33. At this stage, the Litigation Chamber raises a preliminary point on the territorial scope of the GDPR. Article 3 of the GDPR covers two distinct scenarios regarding its territorial applicability:
    a. the first scenario concerns the applicability of the GDPR to the processing of personal data in the context of the activities of an establishment of a data controller in the Union, regardless of whether the processing itself takes place in the Union or not (article 3.1);[18]
    b. the second scenario concerns the applicability of the GDPR to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union (article 3.2).

34. The Litigation Chamber notes that these two paragraphs must be read side by side. This is because a purely textual reading might result in the creation of a legal vacuum for processing carried out by a data controller with an establishment within the Union that is not performed within the context of the activities of the European establishment, and is instead covered by the activities of a data controller established in a non-EEA country.

35. In the instant case, it cannot be contested that the data subject (plaintiff) is a European Union resident (in this case, a Belgian resident). Google LLC has several establishments in the European Union, and article 3.2 therefore does not apply. Accordingly, the territorial scope is determined by article 3.1 of

[16] The Litigation Chamber has included this letter in the case file.

[17] See below, point 89.

[18] Pursuant to the decision of the EEA Joint Committee of 6 July 2018, effective 20 July 2018, the territorial scope of the GDPR extends to the 3 states of the European Economic Area (EEA) – namely, Iceland, Norway, and Lichtenstein. Although the Joint Committee decision is not relevant to the instant case, this decision does refer to the EEA on several occasions.

the GDPR. Indeed, were neither of these provisions to apply, the effective and complete protection of data subjects required by the Court of Justice of the European Union[19] could not be ensured.

36. In addition, the Litigation Chamber feels it bears emphasising that, because the GDPR and Court of Justice case law require effective and complete protection of data subjects, article 3.1 should be considered as generally applicable, if only because effective supervision becomes complex if the processing of personal data is performed by an establishment outside the European Union. For example, it can be difficult for a supervisory authority to exercise the investigative or corrective powers provided for in article 58 of the GDPR over an establishment not located within the European Union.

4.1 The position of the data controller and the *Google Spain* ruling

37. In essence, Google Belgium SA contends that the complaint against it is inadmissible, since the sole data controller for Google's online search engine is the American company Google LLC, not Google Belgium SA. In support of this argument, respondent cites the Court of Justice's *Google Spain* ruling[20].

38. In that ruling, the Court of Justice held that an establishment such as Google Spain satisfied the criteria set out in article 4(1)(a) of Directive 95/46/EC,[21] finding that in essence, the activities of the search engine operator (then Google Inc., now Google LLC) and its establishment located in the Member State in question were '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'.[22]

39. In the same case, the Court also found (as Google Belgium SA itself claims) that the 'operator of the search engine' is the data controller for the processing conducted in the context of its activities, which 'can be distinguished from and is additional to that carried out by publishers of websites'.[23]

40. The aim of this judgment is to 'ensure, through a broad definition of the concept of "controller", effective and complete protection of data subjects'.[24] Google Belgium SA contends that the *Google Spain* ruling shows that Google LLC is the sole data controller. This argument is unconvincing. The

---

[19] CJEU, 13 May 2014, C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Point 58.

[20] CJEU, 13 May 2014, C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEU L281/31.

[22] CJEU, 13 May 2014, C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, point 56.

[23] *Ibid*, points 32 to 38.

[24] *Ibid*, point 34.

Court of Justice did not clearly distinguish the responsibilities of the American company from those of its European establishment; to the contrary, it held that the activities of the two entities were inextricably linked. Even were such a theoretical distinction between the responsibilities of the parent company and its subsidiary to be convincing, Google Belgium SA would still be a valid respondent, precisely *because* of these inextricable ties and the necessity for effective and complete protection of data subjects.

41. In addition, Google Belgium SA argued at the hearing that its processing was covered by article 3.1 of the GDPR, which provides that 'this Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not', and so the aforementioned Court of Justice ruling can be applied; incidentally, the Court of Justice later did just that in its *Google/CNIL* ruling on the scope of the delisting that can be imposed on Google.[25]

42. The Litigation Chamber notes that this argument ostensibly implies Google Belgium SA's admission that the processing is being conducted within the context of the activities of one of the data controller's establishments in the European Union, in this case Google Belgium SA. Put another way, this argument would – as the Court found in the *Google/CNIL* ruling – 'result in the processing of personal data […] escaping the obligations and guarantees laid down by Directive 95/46 and [the GDPR]'. Such an interpretation would, in other words, effectively jeopardise the effectiveness of the GDPR.

43. The Litigation Chamber does, of course, recognise that this case law on the principle of the 'inextricable link' arose from the application of Directive 95/46/EC, the provisions of which regarding territorial jurisdiction are distinct from those of the GDPR. Be that as it may, in its *Google/CNIL* ruling, the Court confirmed its will to apply its case law in this area to the GDPR. The Litigation Chamber cites the following paragraphs:

> '50 | In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Union are inextricably linked […]. 51 | That being so, the fact that the search engine is operated by an undertaking that has its seat in a third State cannot result in the processing of personal data carried out for the purposes of the operation of that search engine in the context of the advertising and commercial activity of an establishment of the controller on the territory of a Member State escaping the obligations and guarantees laid down by Directive 95/46 **and Regulation 2016/679** […].'

[25] CJEU, 24 September 2019, C-507/17, Google LLC v Commission nationale de l'informatique et des libertés (CNIL), points 48 to 52.

Furthermore, it is clearly established and acknowledged that the GDPR's drafters intended to achieve improved, more effective protection of data subjects.

4.2. The Role of Google's establishments.

44. In his written submissions in response, plaintiff contends that Google Belgium SA is a subsidiary of Google LLC with its head office in Brussels; that it targets residents of Belgium; that most of its activities are in the area of digital marketing; and that the activities of Google Belgium SA and Google LLC are inextricably linked within the meaning of the aforementioned *Google Spain* ruling.

45. Google Belgium SA makes no argument to the contrary. Neither does it contest that Google Belgium SA truly and effectively conducts activities in Belgium.

46. At the hearing, Google Belgium SA was asked about the roles of Google's different establishments. It confirmed that it plays no role with regard to the data processed during three phases of operation of Google's search engine – i.e. crawling, indexing, and the selection of results based on the user's search request. It stated that Google LLC is the only data controller in that respect. In essence, at the hearing, Google Belgium SA explained that it was a Belgian subsidiary of Google and that as a result, European and Belgian law apply. Google Belgium SA is therefore of the opinion that Google LLC is bound by the GDPR under article 3.1 GDPR, and that as such, it is not required to choose a representative pursuant to articles 3.2 and 27 of the GDPR.

47. Google Belgium SA explained that it was limited to offering consulting services related to its marketing of services from other Google entities on the Belgian market. Delisting requests are directly and exclusively handled by Google LLC via online forms filled in by data subjects with no involvement from Google Belgium SA. Google Belgium explained that when it is contacted by data subjects requesting to have content delisted, it systematically refers them to the online forms that are sent (and addressed) to Google LLC. On the basis of the country and language chosen by the data subject via the form, employees from Google LLC's initial response team are selected to provide a response if there are any questions. When the content in question requires further evaluation, an 'escalation' process is implemented, and, in this case, a Belgian person working for Google LLC in the United States (who is not an employee of Google Belgium SA) would be contacted. The review performed by this Google employee would be based on information from public sources and on his or her thorough understanding of the particularities of the country of which he or she is a citizen.

48. The Litigation Chamber concludes that, on the basis of the foregoing information, when the *Google Spain* ruling is applied to this case, the GDPR does in fact apply to Google LLC pursuant to article 3.1 of the GDPR, and the subsidiary Google Belgium SA is in fact an establishment requiring the application of the GDPR pursuant to article 3.1 thereof. In light of this, the Litigation Chamber cites the *Google/CNIL* ruling,[26] in which the Court underscored the fact that it is of little importance whether the processing itself takes place within the European Union.

49. While it is true that Google Belgium SA does not, strictly speaking, determine the purposes or means of the processing (these being determined by Google LLC), Google Belgium SA is a subsidiary of Google LLC, and Google Belgium SA's own position logically requires us to infer that its activities trigger the application of article 3.1 of the GDPR. Stated another way, the processing in question is performed within the context of Google's establishment in Belgium. Yet another interpretation would involve the application of article 3.2 of the GDPR and the requirement that Google select a representative in the European Union pursuant to article 27 of the GDPR. Google has not announced plans to do so, nor is it necessary, given Google Belgium SA's role.

50. The Litigation Chamber points out that this interpretation is supported by the *Google Spain* ruling, although the circumstances of the case were not identical. In that case, the Court held – pursuant to Directive 95/46 – '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.'[27]

51. What's more, as its activities are inextricably linked to those of Google LLC, this Belgian subsidiary – given the role it plays and itself describes – can be treated in the same way as a data controller for processing conducted within the context of the operation of Google's search engine and responses to delisting requests in Belgium.

52. In sum, the Litigation Chamber has determined that Google Belgium SA should be treated as data controller on the basis of the particulars of this case and the case law developed under the Court of Justice's *Google Spain* ruling.

---

[26] CJEU, 24 September 2019, C-507/17, Google LLC v Commission nationale de l'informatique et des libertés (CNIL), point 48.

[27] CJEU, 13 May 2014, C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, point 60.

53. In any case, even were it not possible to consider Google Belgium SA as the data controller, the Litigation Chamber would have jurisdiction over Google Belgium SA because of its presence in Belgium, as the following section shows.

4.3 The DPA's jurisdiction over Google Belgium

54. The Litigation Chamber will first examine the application of the Court of Justice's *Wirtschaftsakademie* ruling[28] of 5 June 2018 regarding Directive 95/46, in which the Court found that supervisory authorities have jurisdiction over an establishment of the data controller *even if that establishment is not a joint data controller*. It will then be shown that this ruling applies to the instant case.[29]

55. In the *Wirtschaftsakademie* ruling, the Court held that the German supervisory authority, in order to ensure compliance with data protection regulations in Germany, had the authority, with regard to Facebook Germany, to utilise the full scope of the authority vested in it under its national legislation transposing article 28(3) of Directive 95/46 (recitals no. 50 et seq.). Yet in that same case, the Court also clearly held that '*Facebook Inc. and, for the European Union, Facebook Ireland* must be regarded as primarily determining the purposes and means of processing the personal data of users of Facebook and persons visiting the fan pages hosted on Facebook, and therefore fall within the concept of "controller" within the meaning of Article 2(d) of Directive 95/46.'[30] [Emphasis added by the Litigation Chamber] In other words, Facebook Germany was not the data controller (or joint data controller) for the processing at issue.

56. The Court determined that this authority belonged to the German supervisory authority after verifying that the two conditions set out in article 4(1)(a) of Directive 95/46 were met:

> 'to determine whether, in circumstances such as those of the main proceedings, a supervisory authority is entitled to exercise the powers conferred on it by national law against an establishment situated in the territory of its own Member State, it must be ascertained whether the two conditions laid down by Article 4(1)(a) of Directive 95/46 are satisfied, in other words, whether there is an "establishment of the controller" within the meaning of that provision and whether the processing is carried out "in the context of the activities" of the establishment, also within the meaning of that provision.'[31]

---

[28] CJEU, 5 June 2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH.

[29] See below, points 64 et seq.

[30] CJEU, 5 June 2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, point 30.

[31] *Ibid*, point 53.

57. The Court found that the first condition was met, writing, 'It is common ground that Facebook Inc., as controller jointly responsible with Facebook Ireland for processing personal data, has a permanent establishment in Germany, namely Facebook Germany, situated in Hamburg, and that Facebook Germany effectively and genuinely exercises activities in that Member State.'[32]

58. *Mutatis mutandis*, this is also the case for Google Belgium SA[33], which effectively and genuinely exercises activities in Belgium.

59. As for the second condition, to ensure effective and complete protection for data subjects under the aforementioned *Google Spain* ruling, the Court held that the activities of Facebook's establishment located in Germany were inextricably linked to those of the joint data controllers Facebook Inc. and Facebook Ireland.[34]

60. Once more, *mutatis mutandis*, this is also the case for Google Belgium SA, which has itself confirmed this to be the case, as it does not contest plaintiff's claim in this respect.[35]

61. On this basis, the Court concluded in the *Wirtschaftsakademie* ruling that German law applied by virtue of article 4(1)(a) of Directive 95/46, and that the German' supervisory authority, pursuant to article 28(1) thereof, had jurisdiction to apply German data protection law, and therefore that it could act, towards Facebook's German establishment, with the full authority vested in it under the German legislation transposing article 28(3) of Directive 95/46.[36]

62. The Court further held that 'the circumstance […] that the strategic decisions on the collection and processing of personal data relating to persons resident in EU territory are taken by a parent company established in a third country, such as Facebook Inc. in the present case, is not capable of calling in question the competence of the supervisory authority operating under the law of a Member State with respect to an establishment in the territory of that State belonging to the controller responsible for the processing of that data.'[37]

63. The entry into force of the GDPR does not affect the relevance of this ruling – indeed, it even strengthens it, at least within the context of the instant case. Article 3.1 of the GDPR is seen as the

---

[32] *Ibid*, point 55.

[33] See above, points 44-47.

[34] CJEU, 5 June 2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, points 56 to 60.

[35] See above, points 44-47, and in particular point 45.

[36] CJEU, 5 June 2018, C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, points 61 to 62.

[37] *Ibid*, point 63.

successor to article 4(1)(a) of Directive 95/46.[38] Incidentally, in the *Google/CNIL* ruling, these two provisions are mentioned together.[39]

64. The Litigation Chamber has determined that for the three reasons set out below, the *Wirtschaftsakademie* ruling should, in order to ensure the effective application of the GDPR, be applied to the instant case, and that it therefore has jurisdiction to exercise its authority over Google Belgium SA for complaints filed against this entity with the DPA.

65. **First: The data controller is located outside the European Economic Area.** *Mutatis mutandis*, and, more importantly, for the purpose of ensuring effective and complete protection of data subjects in situations such as this one, in which the data controller is located outside the European Economic Area (in this case, Google LLC), the *Wirtschaftsakademie* ruling should be applied to the framework created by the GDPR. The new rules defined in the GDPR do not contradict the principles established by the Court in this case: the GDPR harmonises the powers and responsibilities of supervisory authorities (see articles 57 and 58), the jurisdiction of which remains subject to the principle of territoriality (see article 55.1 of the GDPR).

66. To the contrary, the GDPR aimed to increase the effectiveness of data protection regulations and offer better protection for data subjects. Yet although the Court held that even when a data controller is established in a Member State, the supervisory authority of another Member State with an establishment that is not a joint data controller still has jurisdiction over such an establishment, this line of reasoning is all the more applicable when the data controller is established in the European Union.

67. **Second: the data controller is not required to appoint a representative because it is established within the European Union.** In light of the roles played by Google Belgium SA[40] and Google LLC, Google LLC is a data controller subject to article 3.1 of the GDPR. Google LLC therefore was not required to appoint a representative pursuant to article 27 of the GDPR. Recital no. 80 of the GDPR provides that:

> 'The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its

[38] THE EU GENERAL DATA PROTECTION REGULATION (GDPR), A Commentary, Edited by Kuner, Bygrave and Docksey, OUP 2020, p. 77.

[39] CJEU, 24 September 2019, C-507/17, Google LLC v Commission nationale de l'informatique et des libertés (CNIL), point 48.

[40] See above, points 44-47.

tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.'

68. Article 27.4 of the GDPR provides that, 'The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.'

69. The fact that the European Parliament did not find it necessary, when adopting article 3.1 of the GDPR, to require a data controller in a situation such as the one in which Google LLC found itself in *Google Spain* to appoint a representative[41] shows that it did not feel that the presence of one of the data controller's establishments in the Union within the meaning of article 3.1 of the GDPR constituted a sufficient territorial link with the European Union to ensure adequate compliance with the GDPR. It is implicit, but undeniable, that an establishment within the meaning of this provision could not be less responsible for the application of the GDPR than a representative within the meaning of article 27 of the GDPR.

70. Quite the opposite, in fact, as the *Wirtschaftsakademie* ruling fits cleanly into this line of reasoning: to ensure effective compliance with the GDPR with regard to data subjects, this ruling must also be applied to an establishment run by a data controller within the European Union (such as Google Belgium SA), whenever the controller, which is subject to the GDPR under article 3.1 thereof, has not been able to appoint a representative pursuant to article 27 of the GDPR. Not allowing supervisory authorities to disregard the self-made legal, social, and operational divisions put in place by a non-EEA controller, and requiring them to overlook fact that an EEA establishment is carrying out an activity inextricably linked to that controller's activities, would unduly restrict the territorial jurisdiction of those authorities by systematically forcing them to exercise their jurisdiction extraterritorially in spite of the clear existence of such a link, which constitutes a strong territorial foothold. In such circumstances, the requirement to apply extraterritorial jurisdiction, in light of the legal and procedural limitations thereof, would directly undermine the effectiveness of the GDPR. This might raise the very question of how, in fact, a supervisory authority would be able to exercise the authority vested in it under articles 58 and 83 of the GDPR in an effective way.

71. **Third: Google being a multinational entity, it is not possible to clearly identify the data controller.** The two arguments above are strengthened by the fact that Google LLC's and Google

[41] A ruling that the Parliament was clearly aware of during the adoption of the GDPR: the ruling is from 13 May 2014 and the GDPR was adopted nearly 2 years later on 27 April 2016.

Belgium SA's communications with data subjects lack clarity in terms of the identification of the data controller. It is therefore all the more necessary to apply the *Wirtschaftsakademie* ruling to the instant case to ensure the effectiveness of the GDPR.

72. Google Belgium SA, in its final written submissions, argued that plaintiff 'sent the initial delisting request to Google LLC (exhibit B.1 and B.2) using the standard form that it makes available (exhibit A.3)'. He did not directly contact Google Belgium SA. The French-language data deletion request form refers, to a certain extent, to Google LLC, particularly concerning the use of the information submitted via the form, information used to identify the data subject, and 'copyright' information.

73. Yet the start of the form simply refers to 'Google', as does the last sentence placed next to a tick box stating, 'I understand that Google will not be able to process my request […]'. Regarding this first reference (at the start of the form), Google Belgium SA explained at the hearing that the intent was to be 'down-to-earth' towards its users, and that references to Google LLC were present in the important legal parts of the form.

74. French-language responses from Google also refer to 'Google' and 'The Google Team'.

75. Regarding the possibility to contest Google's delisting decision, the response form states only the following: 'If you do not agree with our decision, you have the right to take the issue up with the data protection authority in your country. In this case, we advise you to include the reference number for your request […] and a copy of the confirmation you received after submitting the request form. If Google is the webmaster of the website, you can attempt to contact the owner or the author of the page and send him or her your deletion request directly.'

76. Neither the form, nor Google (LLC)'s responses explicitly name a data controller. In light of the foregoing, the Litigation chamber has determined that the delisting process therefore fosters a certain sense of ambiguity for data subjects regarding the identity of the data controller.

77. On this point, during the hearing, Google Belgium SA expressed its surprise that data subjects would still have doubts regarding the identity of the controller for search result delisting, in the light of the aforementioned *Google Spain* ruling, which identifies Google Inc. as the sole data controller. Google, however, fails to understand that this settled case law has not eliminated doubt in the minds of data subjects and their legal counsel as to the controller's identity.

78. On this matter, the Litigation Chamber has determined that this does not in any way relieve the data controller of its obligation to inform the data subject, pursuant to articles 12.1 and 12.2 of the GDPR, in a transparent, intelligible, and easily accessible form, using clear and plain language, to support the

exercise of the data subject's rights (regarding this topic, see above, point 168). Accordingly, the data controller must provide precise information as required by articles 13 and 14 of the GDPR.

79. In conclusion, this ambiguity concerning the respective roles and responsibilities of Google LLC and Google Belgium SA, which may legitimately lead to doubts in the minds of the data subjects as to whether the entity they are contacting is (or is not) the data controller, constitutes a third reason justifying the application of the *Wirtschaftsakademie* ruling to the instant case, such that the Litigation Chamber has jurisdiction to take action in response to a complaint submitted by a data subject against Google Belgium SA alone.

80. **Conclusion.** On the basis of the foregoing, the Litigation Chamber has determined that plaintiff was entitled to direct his complaint regarding the delisting of content from Google's search engine against Google Belgium SA alone. In the Litigation Chamber's view, it is of little importance whether the processing of the data is actually performed outside of the European Union by Google LLC employees.

5. The territorial scope of delisting

81. In the instant case, plaintiff has asked for the content to be delisted worldwide due to the fact that he is at the head of a large company.

82. In the event of a delisting request sent by a data subject to the supervisory authority in the country where his or her centre of interests is located – which is plaintiff's case here – the Litigation Chamber is of the opinion that that local supervisory authority is best placed to decide on the matter.

In another area of the law – the international jurisdiction of national courts over civil or commercial disputes – the Court of Justice held as follows in its *eDate Advertising*[42] ruling of 25 October 2011:

[42] CJEU, 25 October 2011, C-509/09 and C-161/10, eDate Advertising GmbH et al. v X and Société MGN LIMITED. The judgment was delivered under Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, now replaced by Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (albeit with no impact on the reasoning of this decision).

> '48 | The connecting criteria referred to in paragraph 42 of the present judgment must therefore be adapted in such a way that a person who has suffered an infringement of a personality right by means of the internet may bring an action in one forum in respect of all of the damage caused, depending on the place in which the damage caused in the European Union by that infringement occurred. Given that the impact which material placed online is liable to have on an individual's personality rights might best be assessed by the court of the place where the alleged victim has his centre of interests, the attribution of jurisdiction to that court corresponds to the objective of the sound administration of justice, referred to in paragraph 40 above.
>
> '49. The place where a person has the centre of his interests corresponds in general to his habitual residence. However, a person may also have the centre of his interests in a Member State in which he does not habitually reside, in so far as other factors, such as the pursuit of a professional activity, may establish the existence of a particularly close link with that State.' [Emphasis added by the Litigation Chamber]

83. *Mutatis mutandis*, this holding is also relevant to the instant case. Not only is plaintiff's habitual residence in Belgium, but his career is also in Belgium.[43] The Data Protection Authority is therefore best placed to assess the impact of the content on his rights.

84. Regarding plaintiff's request for a worldwide delisting owing to the fact that he is at the head of a large company, the Litigation Chamber has first determined that plaintiff does not sufficiently show, using concrete proof, that his interests are also harmed in other Member States or non-EU countries (which does not exclude the fact that his interests in Belgium might be harmed *from* these countries).

85. In addition, the Court of Justice held in its *Google/CNIL* ruling that article 17 of the GDPR (on which the right to delist content is based) cannot require Google to delist content worldwide on every version of its search engine. In addition, under Belgian law, neither the Data Protection Authority Act of 3 December 2017 (see article 4 in particular) nor the Personal Data Processing Protection Act of 30 July 2018, which together define the scope of the Litigation Chamber's authority, grant the Chamber the right to impose worldwide delisting. The Litigation Chamber therefore cannot accept plaintiff's request for a worldwide delisting.

86. Next, the Litigation Chamber verifies the arguments in favour of delisting at a European scale. In its aforementioned Google/CNIL ruling, the Court wrote the following:

[43] See below, points 100-108.

'67 | However, it should be pointed out that the interest of the public in accessing information may, even within the Union, vary from one Member State to another, meaning that the result of weighing up that interest, on the one hand, and a data subject's rights to privacy and the protection of personal data, on the other, is not necessarily the same for all the Member States, especially since, under Article 9 of Directive 95/46 and Article 85 of Regulation 2016/679, it is for the Member States, in particular as regards processing undertaken solely for journalistic purposes or for the purpose of artistic or literary expression, to provide for the exemptions and derogations necessary to reconcile those rights with, inter alia, the freedom of information.

68 | It follows from, inter alia, Articles 56 and 60 of Regulation 2016/679 that, for cross-border processing as defined in Article 4(23) of that regulation, and subject to Article 56(2) thereof, the various national supervisory authorities concerned must cooperate, in accordance with the procedure laid down in those provisions, in order to reach a consensus and a single decision which is binding on all those authorities and with which the controller must ensure compliance as regards processing activities in the context of all its establishments in the Union. Moreover, Article 61(1) of Regulation 2016/679 obliges the supervisory authorities, in particular, to provide each other with relevant information and mutual assistance in order to implement and to apply that regulation in a consistent manner throughout the Union, and Article 63 of that regulation specifies that it is for this purpose that provision has been made for the consistency mechanism set out in Articles 64 and 65 thereof. Lastly, the urgency procedure provided for in Article 66 of Regulation 2016/679 permits the immediate adoption, in exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, of provisional measures intended to produce legal effects on its own territory with a specified period of validity which is not to exceed three months.

69 | That regulatory framework thus provides the national supervisory authorities with the instruments and mechanisms necessary to reconcile a data subject's rights to privacy and the protection of personal data with the interest of the whole public throughout the Member States in accessing the information in question and, accordingly, to be able to adopt, where appropriate, a de-referencing decision which covers all searches conducted from the territory of the Union on the basis of that data subject's name.' [Emphasis added by the Litigation Chamber]

87. This passage from the Court of Justice's case law emphasises that the aim of consulting other supervisory authorities is to take into account the *public interest* in other Member States to access information, whenever a decision is to be made as to the delisting of content for *all* Google's European

domain names (google.be, google.fr, google.de, etc.) and European residents. In the case of a more limited delisting, on the other hand – only Google's top-level Belgian domain name (.be) and geo-blocking of Belgian users, for instance – residents of other Member States would not be prevented from accessing the information.[44]

88. In this regard, two possibilities for international cooperation exist under the GDPR: either mandatory cooperation under articles 56.1 and 60 of the GDPR (authority of a lead supervisory authority and one-stop shop), or voluntary cooperation under article 61 of the GDPR, limited to supervisory authorities providing each other with relevant information.

89. Because the Litigation Chamber has found that the one-stop-shop mechanism does not apply to the instant case,[45] the Litigation Chamber, if it intends to order content to be delisted for all (or multiple) Google domain names corresponding to country codes within the European Economic Area, in addition to geo-blocking for all (or some) European resident users, must consult with (all or some of, depending on the case) of its fellow supervisory authorities pursuant to article 61 of the GDPR. In this case, pursuant to the *Google/CNIL* ruling (particularly point 69 thereof), the Litigation Chamber informally contacted other European supervisory authorities pursuant to article 61 of the GDPR to ascertain whether the delisting would disproportionately infringe on free access to information for internet users in other Member States. When this process was completed, the following result emerged: with the exception of one German supervisory authority (Hamburg), the supervisory authorities that responded showed support for the Litigation Chamber's intended course of action, including delisting for the entire European Economic Area.

90. The Litigation Chamber has determined that delisting cannot be effective if it does not also apply to searches performed outside of Belgium. In a borderless Europe, it would be futile to order that the delisting apply only to searches performed from Belgian IP addresses.

91. Regarding the geographical scope of the delisting, the Litigation Chamber has determined – in accordance with the *Google/CNIL* ruling – that the delisting should be effective throughout the European Union (and the countries of the European Economic Area). First, the Chamber has determined that searches from outside Belgium (physically or using a proxy server to access other versions of the search engine) might potentially have a serious impact on plaintiff's data protection rights. Indeed, it is perfectly conceivable that, within the context of his work life, plaintiff will have contacts in other European countries (countries that share a border with Belgium, for instance), and

[44] Other possibilities do exist, of course, in which, for instance, cooperation with only two authorities might suffice, such as if delisting was ordered for only two other Google country extensions, .fr and .lu, combined with geo-blocking of residents of these two countries, which would require contacting only the authorities of these two countries.

[45] See above, points 19-31.

that these contacts will then look for information on plaintiff using versions of Google other than the Belgian one (.be). In light of this, delisting in Belgium alone would not be effective.

6. Regarding the requests for delisting

92. The delisting requests sent to Google by plaintiff must be viewed in light of the criteria and rules established by the Court of Justice in its *Google Spain* ruling, the Article 29 Working Party Guidelines on that ruling[46] (hereinafter the 'Article 29 Working Party Guidelines'), as well as the *GC et al. v CNIL* ruling of 24 September 2019[47] and the European Data Protection Board's 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR'[48] (hereinafter the 'EDPB Guidelines') to ensure the proper balance between the rights of data subjects and the freedom of expression and right to information of internet users.

93. As a preliminary observation, it should be noted that while an invasion of privacy caused by a listing may be compounded by the central role of search engines in accessing information online, delisting may, likewise and for the same reasons, have an impact on the freedom of information of internet users.

94. In its *GC et al. v CNIL* ruling, the Court of Justice held as follows:

> '66 | In any event, when the operator of a search engine receives a request for de-referencing, he must ascertain, having regard to the reasons of substantial public interest referred to in Article 8(4) of Directive 95/46 or Article 9(2)(g) of Regulation 2016/679 and in compliance with the conditions laid down in those provisions, whether the inclusion of the link to the web page in question in the list displayed following a search on the basis of the data subject's name is necessary for exercising the right of freedom of information of internet users potentially interested in accessing that web page by means of such a search, a right protected by Article 11 of the Charter. While the data subject's rights protected by Articles 7 and 8 of the Charter override, as a general rule, the freedom of information of internet users, that balance may, however, depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life […].

[46] Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc. v Agencia española de protección de datos (AEPD) and Mario Costeja González', C-131/12, adopted on 26 November 2014 by the 'Article 29 Working Party'.

[47] CJEU, 24 September 2019, C-507/17, Google LLC v Commission nationale de l'informatique et des libertés (CNIL).

[48] Version 2.0, after consultation, adopted on 7 July 2020, available on www.edpb.europa.eu.

> 67 | Furthermore, where the processing relates to the special categories of data mentioned in Article 8(1) and (5) of Directive 95/46 or Article 9(1) and Article 10 of Regulation 2016/679, the interference with the data subject's fundamental rights to privacy and protection of personal data is, as observed in paragraph 44 above, liable to be particularly serious because of the sensitivity of those data.'[49]

95. In that same ruling, regarding information on criminal proceedings, the Court held as follows:

> 'It is thus for the operator of a search engine to assess, in the context of a request for de-referencing relating to links to web pages on which information is published relating to criminal proceedings brought against the data subject, *concerning an earlier stage of the proceedings and no longer corresponding to the current situation*, whether, in the light of all the circumstances of the case, such as, in particular, the *nature and seriousness of the offence* in question, the *progress and the outcome of the proceedings*, the *time elapsed*, the *part played by the data subject in public life and his past conduct*, *the public's interest at the time of the request, the content and form of the publication and the consequences of publication for the data subject*, he or she has a right to the information in question no longer, in the present state of things, being linked with his or her name by a list of results displayed following a search carried out on the basis of that name.'[50]

96. The Article 29 Working Group also explains that:

> 'The overall purpose of these criteria is to assess whether the information contained in a search result is relevant or not according to the interest of the general public in having access to the information. Relevance is also closely related to the data's age. Depending on the facts of the case, information that was published a long time ago, e.g. 15 years ago, might be less relevant that information that was published 1 year ago. The DPA's [sic] will assess relevance in accordance with the factors set out below.
>
> a. Does the data relate to the working life of the data subject? An initial distinction between private and professional life has to be made by DPAs when they examine de-listing request. Data protection – and privacy law more widely – are primarily concerned with ensuring respect for the individual's fundamental right to privacy (and to data protection).'[51]

---

[49] CJEU, 24 September 2019, C-136/17, GC et al. v Commission nationale de l'informatique et des libertés (CNIL).

[50] CJEU, 24 September 2019, C-136/17, GC et al. v Commission nationale de l'informatique et des libertés (CNIL).

[51] Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and Inc. v Agencia española de protección de datos (AEPD) and Mario Costeja González', C-131/12, adopted on 26 November 2014 by the 'Article 29 Working Party'.

97. In his complaint, plaintiff lists eight search listings and URLS, numbered from 1 through 8, in which plaintiff is depicted as 'affiliated with the Y party'. They are listed in exhibit 1 of his written submissions. The remaining content, numbered from 9 through 12, is associated with results pertaining to a 'complaint for harassment'. They are also listed in exhibit 1 of his written submissions. In essence, in support of his claim, plaintiff argues that the listed content is inaccurate and/or obsolete and contains sensitive data that was unlawfully released to the public. He does not challenge the lawfulness of the publication of the content pointed to by the search listings.

98. Before analysing the disputed search listings one by one,[52] the Litigation Chamber will first evaluate whether plaintiff plays a role in public life[53] and whether the search listings contain one or more of the specific categories of data referred to in article 9 of the GDPR regarding plaintiff.[54]

6.1. The role played by plaintiff in public life

99. Among the criteria that must be factored into our analysis,[55] the role played by the data subject in public life is a decisive one. In the EDPB Guidelines, the EDPB, citing the Court of Justice, states the following:

> 'The Court also considered that the rights of the data subjects will prevail, in general, on the interest of Internet users in accessing information through the search engine provider. However, it identified several factors that may influence such determination. Among them include: the nature of the information or its sensitivity, and especially the interest of Internet users in accessing information, an interest that can vary depending on the role played by the interested party in public life. […]'*[56]*

100. The Article 29 Working Party Guidelines state the following on pages 13-14:

> 'What constitutes "a role in public life"?
>
> It is not possible to establish with certainty the type of role in public life an individual must have to justify public access to information about them via a search result.

[52] See below, points 123 et seq.

[53] See below, points 99-107.

[54] See below, points no. 109 et seq.

[55] See above, point 93.

[56] Point 48 of the EDPB Guidelines.

> However, by way of illustration, politicians, senior public officials, business-people and members of the (regulated) professions can usually be considered to fulfil a role in public life. There is an argument in favour of the public being able to search for information relevant to their public roles and activities.
>
> A good rule of thumb is to try to decide where the public having access to the particular information – made available through a search on the data subject's name – would protect them against improper public or professional conduct.
>
> It is equally difficult to define the subgroup of "public figures". In general, it can be said that public figures are individuals who, due to their functions/commitments, have a degree of media exposure.
>
> The Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy provides a possible definition of "public figures". It states that "Public figures are persons holding public office and/or using public resources and, more broadly speaking, all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain."
>
> There may be information about public figures that is genuinely private and that should not normally appear in search results, for example information about their health or family members. But as a rule of thumb, if applicants are public figures, and the information in question does not constitute genuinely private information, there will be a stronger argument against de-listing search results relating to them. In determining the balance, the case-law of the European Court on Human Rights (hereinafter: ECtHR) is especially relevant.'

101. In light of this, both plaintiff and Google raise points that might be used to show that plaintiff has played and continues to play a role in Belgian public life.

102. It should first be noted that neither the Article 29 Working Party Guidelines nor the EDPB Guidelines require the data subject to be a *political* figure to play a role in *public* life.

103. In his complaint, plaintiff states that he is a senior executive at the Z company and that 'as a [senior executive] of [the Z company], [he] unquestionably has a significant degree of media exposure'. However, plaintiff does state immediately afterwards that the facts in question are not likely to contribute to debate in a democratic society and that the public does not have (or no longer has) a

legitimate interest in accessing this information. He also notes that he is not a political figure, although, as noted above, this is not central to the evaluation of his role in public life.

104. The Z company operates in Belgium, and plaintiff has for years been a senior executive at the W company, which has close ties to the Z company.

105. In its written submissions, Google also lists a series of positions that plaintiff has held in the past, showing, in its opinion and in the opinion of the Litigation Chamber as well, that plaintiff has also played a role in public life in the past.

106. For instance, in addition to plaintiff's current responsibilities as described above, over a period of some twenty years, his various positions have included: a role on the staff of a minister from the Y party; Government Commissioner at Entity A; member of Entity B; a manager in a government department; Government Commissioner in Entity D; a high-level role at Organisation E; and a high-level role at Public Entity F.

107. In other words, plaintiff has occupied and continues to occupy public positions and/or positions in which he has used and continues to use public resources; is and has been subject to media exposure; and acts and has acted in a public context as a public figure and, more specifically, as a senior civil servant or manager in government roles.

108. In conclusion, on the basis of the foregoing information,[57] the Litigation Chamber has determined that plaintiff has played and continues to play a role in public life.

6.2. Regarding plaintiff's affiliation with 'the Y party'

109. In his complaint and his submissions, plaintiff claims that Google lists sensitive data regarding plaintiff. In his words:

> 'In this case, Google's search index shows [plaintiff] as a person affiliated with [the Y party]. [Plaintiff's] political opinions are sensitive data within the meaning of article 9 of the GDPR. This data is subject to additional legal protection. Consequently, Google's processing of this data is prohibited, as it is not subject to any of the applicable exceptions (article 9.2 of the GDPR and article 8 §1 of the Personal Data Processing Protection Act of 30 July 2018).'

[57] See above, points 99-106.

110. Plaintiff further insists that content depicting him as 'affiliated with the Y party' is inaccurate and therefore that its delisting is justified, and that Google's assumptions as to the association between plaintiff and the Y party are overly hasty and based on faulty data (this point is covered below[58]).

111. In its final written submissions, Google states that in light of plaintiff's circumstances and his role in Belgian public life, it 'is clear to the public that his party affiliation in no way dictates his real or presumed political opinions, but only the political party with which he has professional ties and which supported his campaign for public office.'[59] In its written submissions, Google attempts to prove the professional ties between plaintiff and the Y party. In particular, Google cites Professor David Renders' arguments that the recruitment of senior civil servants is political in nature to justify its view that information on political affiliations plays an important role in promoting relevant public debate in the general interest, due to the way (senior) civil servants and public officials are chosen in Belgium. In the same vein, the second paragraph of the newspaper article published less than ten years ago on www.lecho.be described plaintiff and recounted his appointment to a senior position at Public Entity F (Google Exhibit B.14).

112. **The 'political affiliation' of a government manager/senior civil servant and article 9 of the GDPR**. In the specific context of the instant case, the Litigation Chamber has determined that the reference to the political affiliation of a government manager or senior civil servant does not in itself automatically reveal an underlying political 'opinion'. In principle, it merely shows that the data subject receives professional support[60] in his or her public life[61] – and, more specifically, in the context of his or her career as a government manager and senior civil servant. Nothing bars a political party from providing professional support to a person in obtaining a senior government position due to his or her personal profile and achievements, without regard for his or her political views. Incidentally, plaintiff underscores the fact that he is not a *member* of the Y party.

113. In other words, this must be determined on a case-by-case basis for each search listing at issue, and each listing must be evaluated to determine whether it points to not just the data subject's political affiliations, but also to his or her political opinions.

114. It is in this spirit, incidentally, that Article 9.1 of the GDPR is drafted, providing that '*Processing* of personal data *revealing* […] political opinions […] shall be prohibited.' [Emphasis added by the Litigation Chamber] Thus, even supposing that the initial processing of the sources listed by the search

[58] See below, points 116-122.

[59] Final written submissions, p. 22, point 29.

[60] See above, point 106.

[61] See above, points 101-108.

engine (the newspapers mentioned being covered by the freedom of the press[62]) reveals a political opinion – which is not the case – it is difficult to convincingly argue that the processing carried out by Google reveals a political opinion: the referencing does not pursue such a purpose, and in this case points to names of individuals.

115. In the same spirit, but more explicitly, article 6 of Modernised Convention 108 of the Council of Europe for the Protection of Individuals with Regard to the Processing of Personal Data[63] provides that:

> 'Article 6: Special categories of data
> 1. The processing of:
> […]
> - personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life;
> shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.
> 2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.'[64]

116. **On the inaccuracy of plaintiff's 'affiliation with the Y party'**. Determining whether a public official receives support from one or more political parties in a context in which nominations to these posts are political in nature[65] is a complex question requiring investigative work (whether journalistic or otherwise) and involving some judgment, as it is ultimately also the expression of an opinion regarding the data subject. It is not irrelevant to the instant case that search listings 2, 3, 4, and 5 lead to articles from the Belgian press, that search listing 6 leads to an article from a public news website (msn.com) and that search listing 1 leads to a Belgian website in website specialised on the issue of transparency and politicians who simultaneously hold multiple offices in Belgium (www.cumuleo.be).

117. It is not within the Litigation Chamber's purview to exhaust the debate on the accuracy of such information that has led to a dispute between a search engine provider and a data subject – and not, it bears mentioning, a dispute with the authors of this information – within the context of an issue

[62] See below, points 123 et seq.

[63] Protocol (CETS no. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS no. 108) adopted on 18 May 2018 by the Committee of Ministers of the Council of Europe at its 128th ministerial session.

[64] Emphasis added by the Litigation Chamber.

[65] See above, point 111.

that is clearly related to the general interest and results in public debate. In essence, with regard to public debate, it is a question of transparency in the appointment to and exercise of public office in Belgium, a subject that is at the heart of democracy and must be examined from time to time. Additionally, article 17(3)(a) of the GDPR does not require that such a debate be exhausted.

118. In this case, to justify the existence of political affiliations, Google cites the following five elements. First, plaintiff had a position on the staff of a minister from the Y party some twenty years ago. Second, one article that plaintiff asked to have delisted alleges that he violated the Y party's official rules for holding multiple offices, citing an extract from a letter from Politician P sent a letter to plaintiff approximately fifteen years ago to explain the rules on holding multiple offices within the party. Third, plaintiff was a speaker at a Y party convention less than 5 years ago. Fourth, he gave yet another speech to the Y party, according to a tweet posted by a Y party MEP several years ago. Fifth, he appears to have worked at the Y party's think tank, according to a high-level public official (in office at the time) quoted by a journalist in an article[66] in which plaintiff was described. This article incidentally described plaintiff as 'affiliated with the Y party'.

119. Plaintiff counters Google's position by arguing that depicting him as being affiliated with the Y party is inaccurate, thereby justifying the request for delisting. He argues that he has never been a member of the Y party; that concluding that close ties between the applicant and party Y are shown to exist in search listing 3 (the reference to the letter from Politician P) is a hasty assumption based on erroneous information; that plaintiff has not held multiple offices in a way infringing the rules that apply to him; and that the letter from Politician P (which, incidentally, constitutes private correspondence revealed in violation of Article 22 of the Constitution, Article 8(2) of the ECHR and Article 314 of the Criminal Code) does not demonstrate that plaintiff is a member of the Y party (which he is not – the letter, addressed to plaintiff, stated simply that '[…] if you are a member of the Y party, […]').

120. At the hearing, plaintiff noted, among other things, that much time has passed since he worked on the staff of a minister from the Y party nearly twenty years ago, and that relationships can also change over time. He contends that regardless of whether he is regularly in contact with members of the party (and other parties), that does not make him a member of the Y party, and that this is a dangerous shortcut that undermines the way he is perceived by the public and his company.

121. That being said, Google does not rely on those aspects alone, as shown by the search listings at issue and the Google's arguments described above.[67] In addition – and more importantly – plaintiff does not

[66] Article on www.lecho.be.

[67] See points 123 et seq. above and points 105 and 118 below.

deny having received professional support from the Y party in his public life, and, more specifically, in his career as a government manager and senior civil servant.[68]

122. In light of the foregoing,[69] the Litigation Chamber has determined that plaintiff's arguments as to the accuracy of his being depicted as affiliated with the Y party in the search listings at issue do not preclude the application of article 17(3)(a) of the GDPR.

6.3 The search listings at issue

123. Unless otherwise noted, the factual information set out below regarding the search listings at issue is cited from exhibit 1 of plaintiff's written submissions. The search listings at issue are also described in further detail in Google's final written submissions and the related exhibits.

124. **Search listing 1**. This listing leads to the website cumuleo.be, and is on the topic of the offices, positions, and professions of plaintiff, who is described as 'affiliated with the Y party'.

125. In light of the role played by plaintiff in public life;[70] in light of the fact that political affiliations constitute information related to transparency in the appointment to and exercise of public office (a subject at the heart of the democratic debate and one that must be examined from time to time); having regard to the Mandatory Declaration of Offices, Professions, and Assets Act of 2 May 1995 (particularly article 2, paragraph 2 thereof); in light of the fact that in the instant case, the mention of plaintiff's affiliation with the Y party does not reveal any of his political opinions;[71] and given the fact that the accuracy of the content is not disputed (apart from plaintiff's criticism of being depicted as affiliated with the Y party[72]), the Litigation Chamber has determined that search listing 1 is necessary for the exercise of the right to freedom of expression and information, and that, consequently, pursuant to article 17(3)(a) of the GDPR, Google did not err in maintaining it.

126. **Search listing 2**. This search listing leads to an article from the newspaper *Le Soir* (www.lesoir.be).

---

[68] See above, point 106.

[69] Points 116-122.

[70] See above, points 99-108.

[71] See above, points 112-115.

[72] See above, points 116-122.

127. This is a result for an article from a Belgian news outlet, the accuracy of which regarding plaintiff's work life is not contested (apart from plaintiff's criticism of being depicted as affiliated with the Y party[73]); in light of the role played by plaintiff in public life;[74] in light of the fact that political affiliations constitute information related to transparency in the appointment and exercise of public office (a subject at the heart of the democratic debate and one that must be examined from time to time); and in light of the fact that in the instant case, the mention of plaintiff's affiliation with the Y party does not reveal any of his political opinions,[75] the Litigation Chamber has determined that search listing 2 is necessary for the exercise of the right to freedom of expression and information, and that, consequently, pursuant to article 17(3)(a) of the GDPR, Google did not err in maintaining it.

128. **Search listing 3**. This search listing leads to an article from the online news outlet *RTL Info* (www.rtl.be).

129. This is a result for an article from a Belgian news outlet, the accuracy of which regarding plaintiff's work life is not contested (apart from plaintiff's criticism of being depicted as affiliated with the Y party[76]); in light of the role played by plaintiff in public life;[77] in light of the fact that political affiliations constitute information related to transparency in the appointment and exercise of public office (a subject at the heart of the democratic debate and one that must be examined from time to time); and in light of the fact that in the instant case, the mention of plaintiff's affiliation with the Y party does not reveal any of his political opinions,[78] the Litigation Chamber has determined that search listing 3 is necessary for the exercise of the right to freedom of expression and information, and that, consequently, pursuant to article 17(3)(a) of the GDPR, Google did not err in maintaining it.

130. While it is true that search listing 3 refers to information that is more than 10 years old that is therefore relatively dated, this information still remains relevant because at the time, plaintiff played a professional role in public life – as he still does today.

131. **Search listing 4**. This search listing leads to an article from the newspaper *La Libre Belgique* (www.lalibre.be).

132. This is a result for an article from a Belgian news outlet, the accuracy of which regarding plaintiff's work life is not contested (apart from plaintiff's criticism of being depicted as affiliated with the Y

[73] See above, points 116-122.
[74] See above, points 99-108.
[75] See above, points 109-115.
[76] See above, points 116-122.
[77] See above, points 99-108.
[78] See above, points 109-115.

party[79]); in light of the role played by plaintiff in public life;[80] in light of the fact that political affiliations constitute information related to transparency in the appointment and exercise of public office (a subject at the heart of the democratic debate and one that must be examined from time to time); and in light of the fact that in the instant case, the mention of plaintiff's affiliation with the Y party does not reveal any of his political opinions,[81] the Litigation Chamber has determined that search listing 4 is necessary for the exercise of the right to freedom of expression and information, and that, consequently, pursuant to article 17(3)(a) of the GDPR, Google did not err in maintaining it.

133. **Search listing 5**. This search listing leads to an article from the newspaper *La Libre Belgique* (www.lalibre.be).

134. This is a result for an article from a Belgian news outlet, the accuracy of which regarding plaintiff's work life is not contested (apart from plaintiff's criticism of being depicted as affiliated with the Y party[82]); in light of the role played by plaintiff in public life;[83] in light of the fact that political affiliations constitute information related to transparency in the appointment and exercise of public office (a subject at the heart of the democratic debate and one that must be examined from time to time); and in light of the fact that in the instant case, the mention of plaintiff's affiliation with the Y party does not reveal any of his political opinions,[84] the Litigation Chamber has determined that search listing 5 is necessary for the exercise of the right to freedom of expression and information, and that, consequently, pursuant to article 17(3)(a) of the GDPR, Google did not err in maintaining it.

135. As with search listing 3, while it is true that search listing 5 refers to information that is over 10 years old and is therefore also relatively dated, this information still remains relevant because at the time, plaintiff played a professional role in public life – as he still does today.

136. **Search listing 6**. This search listing leads to an article from the online news outlet www.msn.com.

137. Google contends that the URL of search listing 6 leads to a page that no longer exists. However, plaintiff does not err in his claim that it is Google's search listing itself that is at issue.

138. Google responded in its final written submissions that not only is URL 6 not listed in the first ten pages of search engine results – it is no longer listed at all. At the hearing, Google confirmed that URL 6 is

[79] See above, points 116-122.
[80] See above, points 99-108.
[81] See above, points 109-115.
[82] See above, points 116-122.
[83] See above, points 99-108.
[84] See above, points 109-115.

no longer listed, and plaintiff did not contest this fact. Accordingly, plaintiff's delisting request with regard to search listing 6 is moot.

139. **Search listing 7**. This search listing leads to a press release from the GERFA on www.gerfa.be. The GERFA (*Groupe d'étude et de réforme de la fonction administrative*) is a Belgian think tank. Google explains in its final written submissions that GERFA is a group founded in response to the massive politicisation of the public service sector in Belgium in order to raise awareness and spark reflection about how to improve the way they are managed. Google also explains that it became an authorised labour union in 1990 that now has approximately 1,500 members.

140. Google contends here as well that the URL of search listing 7 leads to a page that no longer exists. However, plaintiff does not err in his claim that it is Google's search listing itself that is at issue.

141. Google responded in its final written submissions that not only is URL 7 not listed in the first ten pages of search engine results – it is no longer listed at all. At the hearing, Google confirmed that URL 7 is no longer listed, and plaintiff did not contest this fact. Accordingly, plaintiff's delisting request with regard to search listing 7 is moot.

142. **Search listing 8**. This search listing leads to an article from the online news outlet www.7sur7.be.

143. This is a result for an article from a Belgian news outlet, the accuracy of which regarding plaintiff's work life is not contested (apart from plaintiff's criticism of being depicted as affiliated with the Y party which is discussed above in further detail[85]); in light of the role played by plaintiff in public life;[86] in light of the fact that political affiliations constitute information related to transparency in the appointment and exercise of public office (a subject at the heart of the democratic debate and one that must be examined from time to time); and in light of the fact that in the instant case, the mention of plaintiff's affiliation with the Y party does not reveal any of his political opinions,[87] the Litigation Chamber has determined that search listing 8 is necessary for the exercise of the right to freedom of expression and information, and that, consequently, pursuant to article 17(3)(a) of the GDPR, Google did not err in maintaining it.

144. As with search listings 3 and 5, while it is true that search listing 8 refers to information that is over 10 years old and is therefore also relatively dated, this information still remains relevant because at the time, plaintiff played a professional role in public life – as he still does today.

---

[85] See above, points 116-122.

[86] See above, points 99-108.

[87] See above, points 109-115.

145. In light of the foregoing considerations, the Litigation Chamber concludes that Google did not err in refusing plaintiff's delisting requests for the delisting of information related to his alleged political affiliations. The Litigation Chamber therefore denies the complaint regarding the request to delist search results 1 to 8.

6.4. Regarding allegations of harassment

146. **Search listings 9 to 12** all lead to online articles from Belgian news outlets (respectively www.lalibre.be, www.dhnet.be, www.7sur7.be, www.sudinfo.be), all dating back approximately a decade in the past, regarding a complaint for harassment against plaintiff within the civil service administration.

147. The existence of this complaint is not contested.

148. However, in the delisting request submitted to google via its form on 31 May 2019, plaintiff wrote the following, in relevant part: 'These listings refer to news stories claiming that [plaintiff] was the target of a harassment complaint. This complaint was dismissed for lack of merit in 2010. The fact that this information has not been brought up to date justifies the request for delisting pursuant to article 17 of the GDPR.'

149. In exhibit 7 of its submissions, plaintiff included what appears to be the first page (of 22) of a 'Decision following a detailed complaint, Law of 11 June 2002 as amended by the Law of 10 January 2007, Confidential' issued by 'ARISTA, External workplace protection and prevention service', in addition to a partially redacted 20th page on which the following text remains:

> '[…] On the basis of this definition, the information in our possession, and the points discussed above, ***we cannot deem this situation to constitute a case of workplace harassment***. 9. CONCLUSIONS […] We do not have information allowing us to conclude that abusive conduct or harassment were committed by the accused.'

150. In light of this, plaintiff first notes that the document (the authenticity or integrity of which Google has not contested) is dated 2 December 2010, and that the complaint against plaintiff was dismissed for lack of merit. The remaining exhibits presented here fail to show that the complaint in question was ever subject to other proceedings, or even that other similar complaints were ever filed against plaintiff at a later time. In other words, the information listed on the search engine is no longer current or relevant.

151. Second, it must be noted that the articles referred to date back approximately ten years prior and refer to alleged events from nearly a decade ago. As such, not only was the alleged conduct never proven, but the alleged events are also not recent.

152. Third, in light of this context, search listings pertaining to a complaint for harassment against plaintiff might potentially have harmful repercussions for plaintiff, both personally and professionally.

153. Even if the search listings at issue might have, at one point, contributed to the public debate on a matter of general interest, the Litigation Chamber has determined that, today, for the reasons set out above, they are no longer current and have become obsolete. Accordingly, they cannot be deemed necessary for the exercise of the right to freedom of information under article 17(3)(a) of the GDPR.

154. In this case, Google cannot maintain these search listings on the basis of article 6(1)(f) of the GDPR, as the rights and interests of plaintiff prevail for the reasons set out above. Consequently, Google must delist them.

155. In light of these considerations, the Litigation Chamber declares that there has been a breach of articles 17(1)(a) and 6(1)(f) of the GDPR and orders Google Belgium SA to render its processing compliant and, to this end, implement any effective technical solutions needed to remove search listings 9 to 12.

156. Consequently, it is not necessary to assess plaintiff's remaining arguments regarding the other content at issue in search listing 10, in relation to an annual budget allocated by a government agency.

7. Violations of the GDPR

157. Upon submitting the delisting request form to Google on 31 May 2019, under the heading 'Reason for deletion', plaintiff, through his counsel, informed Google that the harassment complaint had been dismissed for lack of merit in 2010, and that the information listed was therefore no longer current.[88] Regardless of the proof furnished in plaintiff's exhibits (mentioned earlier in this decision[89]), the fact remains that at this early stage of the process, this fact had already been brought to Google's attention when the delisting form was submitted – by a lawyer, no less.

[88] See above, point 148.

[89] See above, point 149.

158. Also at the same time, Google had to have been aware of the fact that this listed content was approximately a decade old and dealt with incidents from over ten years prior.

159. The Litigation Chamber is therefore of the opinion that upon receipt of the delisting request form submitted by plaintiff, Google was effectively aware of the age of the harassment complaint, of the fact that the information had not been updated, and, lastly, because the complaint in question was for alleged harassment, of the fact that it might reasonably result in harm to plaintiff. Stated another way, Google was already, at that time, effectively aware of sufficiently serious reasons to require the content to be delisted on the basis of article 17(1)(a) of the GDPR, reasons that later led the Litigation Chamber to hold that search listings 9 to 12 must be delisted.[90]

160. Yet on 18 June 2019, 'The Google Team' only answered plaintiff as follows:

> *'After weighing the interests and rights associated content in question, including factors such as your role in public life, Google has decided not to block it.'*
>
> *For the moment, we have decided to not take action regarding these URLs.*
>
> *We encourage you to send your request for deletion directly to the webmaster in charge of the website in question. This individual has the power to delete the content in question from the web or to prevent it from appearing in search engines. To learn how to contact the webmaster […].*
>
> *If the obsolete content of the website continues to appear in Google's search results, you can ask us to update or delete the page in question. To do so, use this tool […].*
>
> *'If you do not agree with our decision, you have the right to take the issue up with the data protection authority in your country.*

161. **Violations of articles 17(1)(a) and 6(1)(f) of the GDPR.** By refusing to delist search listings 9 to 12 on 19 June 2019, even though Google LLC should have promptly delisted them because it had actual knowledge of sufficiently serious reasons to require the content to be delisted on the basis of article 17(3)(a) of the GDPR[91] – with it being understood that Google LLC could also have temporarily delisted them in order to verify the facts pertaining to the allegedly serious reasons in greater detail with plaintiff and his counsel – Google LLC failed to comply with its obligations under Article 17(1)(a) of the GDPR.

---

[90] See above, point -153.

[91] See above, points 157-159.

162. This conduct also constitutes a violation of article 6(1)(f) of the GDPR, as in the instant case and for the aforementioned reasons,[92] the interests of plaintiff, who required his personal data to be protected, prevail over the legitimate interests of Google to list web content.

163. The Litigation Chamber holds these violations committed by Google to be serious in nature. Although the provisions that Google violated contain rules that are subject to interpretation and data protection is not an absolute right, delisting is a clear obligation for search engines under the *Google Spain* ruling. As the Court of Justice noted, the potential seriousness of the infringement is high, and the rights of data subjects prevail, in principle, over the interest of the public to find this information by searching for the data subject's name.[93]

164. In the instant case, Google was perfectly aware of all of the facts of the case, and, following plaintiff's request, failed to act diligently by refusing to delist the content in question, despite the fact that plaintiff had furnished proof of the fact that it was no longer current. The Litigation Chamber therefore holds, in light of this context, that these elements are similar to those observed in the *Google Spain* ruling, including, in particular, those relating to the content's inadequacy and age. Consequently, upholding plaintiff's claim does not require a nuanced legal analysis. The Litigation Chamber adds that, in these circumstances, there is not, as Google Belgium SA contends, any disproportionate infringement of the freedom of expression and information.

165. **Violation of articles 12.1 and 12.4 of the GDPR.** Lastly, with regard to the analysis of the balance between the rights and interests of the parties to be determined in accordance with article 17(3)(a) of the GDPR and related Court of Justice of the European Union case law,[94] by only responding to plaintiff that '[a]fter weighing the interests and rights associated content in question, including factors such as your role in public life, Google has decided not to block it,' Google violated its obligations under article 12.1 and 12.4 of the GDPR. Indeed, the reason given to plaintiff for refusing his application was far from exhaustive, and did not allow him to fully understand and be aware of Google's reasoning. Google also closed the door to all discussions with plaintiff by informing him that, if he did not agree with Google's decision, he could simply file a complaint with the data protection authority in his country. In conclusion, Google's response as the reason for its refusal to delist the content is opaque and insufficiently understandable, and therefore violates articles 12.1 and 12.4 of the GDPR.

---

[92] See above, points 150-153.

[93] CJEU, 13 May 2014, C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, points 81 and 97.

[94] See above, points 92-96.

8. **Corrective and dissuasive measures**.

166. First, the Litigation Chamber orders Google Belgium SA, pursuant to article 100, paragraph 1, points 8 and 9 of the DPAA, to render its processing compliant, and, accordingly, to implement any effective technical solutions required to **remove search listings** numbers 9 to 12, for all the search engine's websites in every language, but only for users visiting them from the European Economic Area, no later than seven days after receiving notice of this decision, and to inform the Litigation Chamber by email within the same time frame that it has complied with this order at litigationchamber@apd-gba.be.

167. In addition to the obligation to delist search listings numbers 9 to 12, the Litigation Chamber has also determined that the two violations referred to above require additional dissuasive administrative fines.

168. We note that the purpose of imposing an administrative fine is not simply to put a halt to a violation, but rather – more importantly – to ensure that the rules of the GDPR are complied with. As stated in recital 148 of the GDPR, sanctions – including administrative fines – are appropriate in the event of serious infringement, in addition to or instead of any appropriate action ordered to be taken. As such, the Litigation Chamber is acting pursuant to article 58(2)(i) of the GDPR. The primary aim of the administrative fine is therefore not to put a halt to the infringement. The aim can be achieved via a variety of corrective measures, including orders from the data protection authority, which are cited in article 100, §1, points 8 and 9 of the DPAA and provided for in the GDPR. When determining the amount of the administrative fine to be imposed, the Litigation Chamber takes into account the nature and seriousness of the violation.

169. It should be noted that this decision is not the first time Google has been sanctioned with an administrative fine for data protection violations in the area of delisting. Sweden's supervisory authority, for instance, imposed a SEK 75 million fine (approximately €7 million) on Google on 11 March 2020 for multiple violations of its obligation to delist results.[95]

170. On 4 June 2020, Google Belgium SA was sent a form to allow it to make its arguments regarding the imposition of an administrative fine in this case.[96]

171. In response to this form, Google Belgium SA proffered several arguments. First, Google Belgium SA contends that no sanctions should be imposed, as this would be 'totally inappropriate, dangerously

[95] EDPB, 'The Swedish Data Protection Authority imposes administrative fine on Google', 11 March 2020, available on www.edpb.europa.eu.

[96] See above, point 10.

counterproductive, and even illegal'.[97] In addition, Google Belgium SA argues that 'the proposed sanctions violate the principle of the proportionality of sanctions. Furthermore, a public sanction against Google Belgium SA would be counterproductive.'[98] Even more incidentally, Google Belgium SA believes that the way in which amount of the sanction was determined was not properly justified, as 'the Litigation Chamber has used certain faulty criteria […] and has also failed to take into account certain mitigating circumstances.'[99] Google Belgium SA also believes the amount of the fine to be an issue, as it has no way of controlling the scale, formula, and manner of calculation used to determine it.

172. In response to these arguments, the Litigation Chamber notes that it has relied on article 83 of the GDPR in reaching the conclusion that an administrative fine is justified and calculating its amount. The Litigation Chamber justifies its decision on the basis of the observations set out below.

173. As indicated in the form regarding the imposition of a fine, in determining Google Belgium SA's revenues – a criterion that is used to calculate the fine – the Litigation Chamber relies on the opinion of the European Data Protection Committee, which is as follows:

> 'In order to impose fines that are effective, proportionate and dissuasive, the supervisory authority shall use for the definition of the notion of an undertaking as provided for by the CJEU for the purposes of the application of Article 101 and 102 TFEU, namely that the concept of an undertaking **is understood** to mean an economic unit, which may be formed by the parent company and all involved subsidiaries. In accordance with EU law and case-law, an undertaking must be understood to be the economic unit, which engages in commercial/economic activities, regardless of the legal person involved (Recital 150).'[100]

174. Consequently, the Litigation Chamber takes into consideration the revenue of the presumed parent company of Google Belgium SA, the Alphabet group, whose revenues for the last three years are as follows:

.

- Alphabet revenues – 2019: $161,857 bn.
- Alphabet revenues – 2018 $136,819 bn.
- Alphabet revenues – 2017 $110,855 bn.[101]

---

[97] Google Belgium SA's response to the form regarding the imposition of a fine, 24 June 2020, p. 2.

[98] *Ibid.*

[99] *Ibid.*

[100] 'Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679', WP 253, adopted on 3 October 2017, p. 6, available on www.edpb.europa.eu.

[101] Available at: https://www.macrotrends.net/stocks/charts/GOOG/alphabet/revenue.

175. With regard to the violation of articles 17(1)(a) and 6(1)(f) of the GDPR, the Litigation Chamber, in accordance with article 83(2) of the GDPR, has decided to impose an administrative fine of EUR 500,000, taking into account the following elements:

(i) from at least 19 June 2019 to the date of the hearing in this case, 6 May 2020, a period of 10 months, and despite plaintiff having provided Google with the notice of dismissal of the harassment issued by ARISTA in his written submissions,[102] Google maintained search listings 9 to 12, even though it had been presented with sufficiently serious reasons to require content to be delisted since 19 June 2019. The fact that search listings 9 to 12 were kept in place caused (and might continue to cause) significant harm to plaintiff's reputation, because plaintiff saw a particularly negative news article on him remain listed by the search engine for over ten months, despite having asked for it to be removed and having proven the inaccuracy of the information. The Litigation Chamber has determined that this decision directly affects plaintiff and indirectly affects every internet user that might have searched for information on him using the search engine. During this period, the search listings at issue were kept in place by Google without any legal basis under article 6.1 of the GDPR, which constitutes a serious violation of the GDPR. The violation of article 17(1)(a) also constitutes a violation of an essential principle of the GDPR, and at the very least is a sign of serious negligence;

(ii) The foregoing constitutes a serious violation of the GDPR and negligent infringement on the part of Google Belgium SA (article 83(2)(b) of the GDPR). Consequently, Google Belgium SA cannot avail itself of the fact that it made a dedicated online form available to data subjects, that it trained teams and set up a legislative committee, or that it accepts a large number of delisting requests. This is part of Google's responsibilities under the GDPR, which must be proportionate to the risks created by the processing (article 24.1 of the GDPR). Neither can Google Belgium SA lessen its responsibility for the violations by citing the DPA's front office's failure to hold mediation. This is because, pursuant to article 62 §2 of the DPAA, only a request for mediation (as opposed to a complaint) can result in mediation with the DPA's front office. Complaints that are admissible must be directly passed on to the Litigation Chamber (article 62 §1 of the DPAA). In this case, plaintiff had submitted a complaint, not a request for mediation.[103] In addition, the Litigation Chamber notes that administrative fines are not corrective measures but are in fact dissuasive measures[104] to which mediation cannot be a response;

---

[102] See above, point 149.

[103] Passage from complaint's original complaint: [Plaintiff] has instructed me to submit a complaint with your Authority following GOOGLE's refusal of his requests to delist content, sent using the personal data deletion request forms.'

[104] See above, point 168.

(iii) To date, Google has taken no steps – even temporary – to limit the harm suffered by plaintiff, despite it being made aware of the fact that the Litigation Chamber had concluded that there was a violation of the GDPR and was considering imposing sanctions (article 83(2)(c)), when respondent was sent the form regarding the imposition of a fine on 4 June 2020. On this point, the Litigation Chamber notes that it has no obligation to suggest or require respondent to take measures to reduce the amount of the fine in question or to pay no fine at all;

(iv) As has been repeatedly noted,[105] Google LLC has been involved in extensive litigation regarding its implementation of the right to be forgotten and the associated legal provisions – for instance, in France, in Spain, and in Sweden. It cannot be denied that in spite of this legal precedent, the group's *modus operandi* does not always allow it to fully and sufficiently meet its obligations concerning the right to be forgotten. While it does require a case-by-case approach, the right to be forgotten remains a clear obligation.[106] The Litigation Chamber does note, however, that it is technically not possible to speak of a 'repeat offence' when the legal entities in question are not the same (article 83(2)(e);

(v) The data in question is sensitive personal data, as it concerns criminal accusations – even if, in the instant case, no criminal charges were filed for the harassment complaint against plaintiff referred to in the search listings at issue (article 83(2)(g);

(vi) Regarding article 83(2)(i), the Chamber refers the reader to point (iv) above;

(vii) Lastly, the fact that Google's search engine is widely used by internet users and that the group possesses vast resources (its annual worldwide revenues totalled $161,857 bn in 2019), constitutes an aggravating factor. Google's obligations to delist content are proportionate to its importance and to the amount of the group's revenues. In light of the significant litigation that Google has faced in the Court of Justice of the European Union,[107] the Litigation Chamber is of the opinion that Google should since have improved its expertise in this area in order to avoid violations such as those observed by the Chamber in the instant case. This also justifies the fact that greater diligence is expected from Google (article 83(2)(k) of the GDPR).

176. The Litigation Chamber further notes that, under article 83(5)(b) of the GDPR, it has the authority to impose fines up to EUR 20,000,000 or up to 4% of the company's revenues. The amount of the fines imposed under this decision is significantly below these limits, and represents a reasonable amount compared to the Google group's overall revenues ($161,857 bn in 2019). Therefore, it cannot be deemed disproportionate.

[105] See above, notes 6-9.

[106] See above, point 163.

[107] See, in particular, notes 6, 7, and 8 above.

177. With regard to the violation of articles 12.1 and 12.4 of the GDPR, the Litigation Chamber, in accordance with article 83(2) of the GDPR, has decided to impose an administrative fine of EUR 100,000, taking into account the following elements:

(i) in light of the key role played by Google's search engine in the dissemination of information on the internet and its broad use by internet users, the absence of a transparent and understandable justification for its refusal to delist content that might harm a data subject constitutes a serious violation of the GDPR – a violation that might also be seen as mistreating the data subject who, upset at receiving an ostensibly thoughtless standard response, at feeling the injustice of not being listened to as he should by an entity such as Google (regarding this, see the next point), and at being given no other choice, if he is unsatisfied with the response, but to bring his grievance to another entity (the publisher of the listed content or his country's data protection authority) (article 83(2)(a) and (b) of the GDPR);

(ii) Points 177, (iv), (vi), (vii), and 178 above.

Regarding the delisting request and response forms

178. Previously, in points 71 to 79 of this decision, the Litigation Chamber noted that the process of handling requests to delist content used by Google LLC maintains a certain level of ambiguity as to the identity of the data controller, who is not clearly and unequivocally identified. The facts set out in that part of this decision constitute a violation of articles 12.1, 12.2, and 14(1)(a) of the GDPR. Google does not clearly identify which specific legal identity is the data controller responsible for the processing of the search listing (and delisting) activities of Google's search engine, which renders it more difficult for data subjects to exercise their rights, as they cannot know who, ultimately, they are corresponding with.

179. The Litigation Chamber has decided to order Google Belgium SA to modify the online delisting forms it makes available and provides to users of its online search engine services in Belgium, in order to clearly and precisely identify the legal entity/entities acting as the data controller(s) and state which legal entity/entities is/are the data controller(s) for each separate processing activity.

9. <u>Administrative transparency</u>

180. In light of the importance of transparency in decision-making process and the decisions of the Litigation Chamber, and in light of the scope of this decision, which concerns a very large number of data subjects – i.e. all Belgian residents, and by extension all residents of the EEA – who might be listed by Google's search engine in search queries using their first and last names as keywords, this decision will be published on the website of the Data Protection Authority.

181. In the instant case, the Litigation Chamber has decided not to redact Google's identifying information. It has, however, decided to redact the personal information of plaintiff and the other individuals cited. The Chamber is of the opinion that these redactions are necessary to the pursuit of plaintiff's objective, which is to be delisted by Google.

182. In its reaction to the form regarding the imposition of a fine, Google Belgium SA contended, among other points, that publication of the decision would be counterproductive and would stigmatise Google. This argument is unconvincing. First, Google Belgium SA argues that publishing the decision would be counterproductive because it would pointlessly incite data subjects to contact Google Belgium SA rather than Google LLC. This argument is faulty: requests to delist content sent not by mail, but by an online form made available by Google LLC. It is impossible to contact the wrong entity when requesting that content be delisted, because it is Google LLC that makes the web page available and processes the complaint. Except in extremely marginal cases, the Litigation Chamber fails to see how anyone could send their request to delist content to Google Belgium SA.

183. Next, regarding the argument that Google would be stigmatised, the Litigation Chamber feels it necessary to note that publishing decisions with the identity of the respondent fulfils two aims. It first fulfils an objective in the general interest, as it explains the responsibilities of Google and its EU subsidiaries under the GDPR. In light of the importance of Google's search engine for a vast number of internet users and the fact that a significant share of individuals living in Belgium are listed by Google's search engine in one way or another, the Litigation Chamber feels it relevant to give this decision sufficient publicity to raise awareness among internet users of their rights under the GDPR. In this respect, even if the only person directly concerned by the decision is plaintiff, the decision is of general interest for a large segment of the general public. It is therefore entirely appropriate to publish the decision.

Publishing the decision also serves the aim of discouraging future violations. The Litigation Chamber does not agree, as respondent contends, that the decision is discriminatory. Article 100, §1, point 16 of the Data Protection Authority Act of 3 December 2017 grants the Litigation Chamber authority to decide whether to publish its decisions 'on a case-by-case basis'. In the past, the Chamber has decided to publish decisions bearing the identity of the respondent whenever it has deemed such publication

to be of value in ensuring rapid compliance in correcting the situation at issue and in reducing the risk of repeated offences,[108] and also whenever pseudonymisation would only be illusory in nature.

10. Operative part of the decision

ON THESE GROUNDS,

the Litigation Chamber of the Data Protection Authority hereby decides, after deliberation:

(1) in accordance with article 100, paragraph 1, point 2 of the DPAA, rejects the complaint's requests to delist search listings 1 to 8;

(2) in accordance with article 100, paragraph 1, points 8 and 9 of the DPAA, orders Google Belgium SA to render its processing compliant, and, accordingly, to implement any effective technical solutions required to **remove search listings** numbers 9 to 12, for all the search engine's websites in every language, but only for users visiting them from the European Economic Area, no later than seven days after receiving notice of this decision, and to inform the Data Protection Authority (Litigation Chamber) that it has complied with this order within the same time frame (at the email address litigationchamber@apd-gba.be);

(3) in accordance with articles 100, point 13 and 101 of the DPAA and article 83 of the GDPR, orders Google Belgium SA to pay a **fine** of EUR 500,000 for its violation of articles 17(1)(a) and 6(1)(f) of the GDPR;

(4) in accordance with articles 100, point 13 and 101 of the DPAA and article 83 of the GDPR, orders Google Belgium SA to pay a **fine** of EUR 100,000 for its violation of articles 12(1) and 12(4) of the GDPR;

(5) in accordance with article 100, paragraph 1, point 9 of the DPAA, orders Google Belgium SA to **adapt the electronic forms** it makes available and provides to users of its online search engine services in Belgium, in order to clearly and precisely identify the legal entity/entities acting as the data controller(s) and state which legal entity/entities is/are the data controller(s) for each separate processing activity, no later than two months after

[108] See, for instance, Litigation Chamber, 9 July 2019, Decision on the merits 05/2019; Litigation Chamber, 23 June 2020, Decision on the merits 34/2020.

receiving notice of this decision, and to inform the Data Protection Authority (Litigation Chamber) that it has complied with this order within the same time frame (at the email address litigationchamber@apd-gba.be).

In accordance with article 108, §1 of the DPAA, the losing party may appeal this decision to the Market Court within thirty days of receiving notice of it, with the Data Protection Authority listed as respondent.

Hielke Hijmans
Chairman of the Litigation Chamber