Autorité de protection des données
Gegevensbeschermingsautoriteit

Litigation Chamber

Decision on the merits 11/2022 of 21 January 2022

Case File number: DOS -2018-05968

Subject: Cross border complaint relating to cookies

The Litigation Chamber of the Data Protection Authority, consisting of Mr Hielke Hijmans, Chairman, and Mr Yves Poullet and Mr Christophe Boeraeve, Members, ruling on the case in this composition;

Pursuant 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";

Pursuant to the Act of 3 December 2017 establishing the Data Protection Authority for Belgium, hereinafter the "LCA";

Pursuant to the Rules of Procedure as approved by the Belgian House of Representatives on 20 December 2018 and published in the Moniteur belge Official Journal of 15 January 2019;

Pursuant to the documents in the case file;

has taken the following decision concerning:

the complainant: Mr X

the defendant: Y , represented by its counsel, Maître Rue, Chaussée de La Hulpe, 177/12, 1170 Brussels.

I- Procedural antecedents

1. Pursuant to the complaint received via the IMI system by the Berlin Data Protection Authority (Commissioner for Data Protection and Freedom of Information) on 24 August 2018 to the Data Protection Authority (DPA);
2. Pursuant to the decision of 23 November 2018 of the Chairman of the Litigation Chamber to transfer the case file to the inspection service for investigation;
3. Pursuant to the Inspection Service's (hereafter, the IS) investigation report of 19 October 2019;
4. Pursuant to the exchanges between the Berlin Data Protection Authority (Berliner Beauftragte für Datenschutz und Informationsfreiheit) and the DPA, in the context of article 60 of the GDPR;
5. Pursuant the decision of 29 April 2020 of the Chairman of the Litigation Chamber that the case file was ready for investigation on the merits pursuant to Articles 95 § 1, 1° and 98 LCA, the Chairman invited the parties to submit by letter on the same date;
6. Pursuant to the submissions of the defendant, received on 9 June 2020;
7. Pursuant to the absence of submissions in response from the complainant;
8. Pursuant to the defendant's summary submissions, received on 21 July 2020;
9. Pursuant to the translation of exhibits of the procedure (inspection report and defendant's submissions) into the language of the plaintiff (German);
10. Pursuant to the hearing of 30 April 2021 in the presence of the defendant, represented by its legal counsel Maître Rue, in the absence of the plaintiff, although he was summoned;
11. Pursuant to the dispatch, to the parties, of the minutes of the hearing and the comments of the parties;

II- The facts of the complaint

12. The complainant raises in his complaint that the tool for selecting advertising preferences does not work, in that the cookie opt-out option for many third parties does not work (although he clicks on the opt-out option, the opt-in option is automatically reset). He thus argues that his consent to receiving these cookies is forced and therefore not free in the sense of article 4.11 and 7 of the GDPR.

13. He also claims that the website requires the user to accept cookies in order to be able to select their advertising preferences.

14. The cookie in question informs the defendant whether or not the user's browser accepts cookies from third parties. The Litigation Chamber therefore understands that the complainant objects to the placement of the cookie and the subsequent processing of his personal data by the defendant.

15. The Litigation Chamber will examine the facts reported by the complainant in the context of the task of monitoring compliance with the GDPR entrusted to the DPA (of which it is the administrative litigation body) by the European legislator (article 58 of the GDPR) and by the Belgian legislator (article 4 LCA), both in the light of the articles of the GDPR referred to in the complaint form that he introduced on 24 August 2018, and in the light of the articles of the GDPR as examined in the IS report.

16. The breaches identified in the IS report will be examined in the first instance. The grievances raised by the complainant in his complaint will then be examined.

III- Findings of the Inspection Service

17. As a result of its investigation the IS produced an investigation report in which it identified combined breaches of articles 5 and 6, 12 and 13, 24 and 30, 24 and 32, and 37 of the GDPR.

Report on the principles relating to the processing of personal data (article 5 of the GDPR) and on the lawfulness of processing (article 6 of the GDPR):

"*The technical analysis report of 03/07/2019 (exhibit no. 12), the relevant elements of which on pages 9/14 and 10/14 are quoted below, demonstrates the existence of the following practices which are incompatible with the principle of lawfulness, fairness, transparency of article 5 of the GDPR and with the obligation of lawfulness of processing of article 6 of the GDPR: "Upon connection to the site [...] on the home page (screenshot 8) a cookie is already loaded in the browser although no information has been delivered to the user. The cookie with the name "third_party_c_t" with the value "hey+there %21" from the domain Y is a cookie that informs Y whether or not your browser accepts third party cookies", and; "Selecting the country you are in brings up the screen in screenshot 9 which indicates that non-identifiable information is being collected. The fact that the information is non-identifiable does not make it any less personal. This box is not "transparent" and does not allow the user to have an idea of what is being collected and why*."

Report on the transparency of information and communications and arrangements for exercising the data subject's rights (article 12 of the GDPR) and the information to be provided when personal data are collected from the data subject (article 13 of the GDPR):

As for the transparency of information, the IS finds:

"The "Privacy Policy of [...]", *the text of which can be found on pages 19 to 24 and explanations on pages 9 and 10 of the document [...] which was communicated to the inspection service by Y via its email of 17/07/2019 (exhibit No. 14) does not comply with article 12(1) nor with article 13 of the GDPR, which are relevant here, for the following reasons:*

The information provided is not always transparent and comprehensible to data subjects as required by Article 12(1) of the GDPR. Firstly, the language used is not consistent and logical, as the notions "personal information" and "private data" are used, whereas the GDPR systematically refers to "personal data."

Furthermore, the fact that cookies are used is indicated, along with two warnings to the effect that "disabling cookies for this purpose will prevent the control tool from working effectively and may have undesirable consequences for your overall browsing experience" and also that "deleting or rejecting cookies may have undesirable consequences for your experience of our website." These warnings are not comprehensible to data subjects and prevent their free consent to the use of cookies as they do not explain what "undesirable consequences" actually means.

Finally, the reference to "additional information" on the Google, Firefox, Windows and Safari sites is not understandable for the data subjects as there is no explanation of this mentioned for the data subjects."

Concerning the fact that the information is allegedly incomplete, the IS finds:

"The information provided is incomplete because not all the information that must be provided according to Article 13 of the GDPR is actually provided to the data subjects. Firstly, the existence of the right to withdraw consent at any time, without affecting the lawfulness of the processing based on consent carried out prior to the withdrawal of consent, is not mentioned with regard to the processing of personal data by Y; this right is only mentioned with regard to the management of cookies on the website accompanied by the

aforementioned warning that "deleting or rejecting cookies may have undesirable consequences for your experience of our website."

Report on the log of processing activities (article 30 of the GDPR)

"The log of processing activities found in the document "[FR] Annex 1_(..) Register of GDPR controls" which was communicated to the inspection service by Y via its email of 17/7/2019 (exhibit no. 14) does not mention the identification of the third countries to which personal data are transferred for several processing activities. For these processing activities, the texts "Refer to (...)", *"Refer to* (...)", *"Refer to* (...)" *and "Refer to (...)" are mentioned in the column "Names of third countries or international organisations to which personal data are transferred (if possible)."*

Report on the responsibility of the Data Controller (article 24 of the GDPR) and on the security of processing (article 32 of the GDPR)

"The technical analysis report of 3/7/2019 (exhibit No. 12), the relevant elements of which on pages 8/14 and 9/14 are quoted below, demonstrates the existence of the following practices which are incompatible with the responsibility of the Data Controller in article 24 of the GDPR and with the obligation of security of processing in article 32(1) of the GDPR:

In screenshot 1 you can see that the link to the server is [...]. *This link is an http link and not an https link. This means that the communication protocol between the client station and the server in question is a protocol that conveys data in clear text, i.e. not encapsulated in a tunnel as the TLS protocol would for an https link. This means that the personal data provided by the user on this site does not have the guarantee stated in the information "Protection of your privacy" distributed at the following* link [...] of *which screenshot 7 shows the extract.*

In its guidelines on the protection of personal data through web services provided by the European institutions, the European Data Protection Supervisor (EDPS) recommends the use of secure protocols in the transmission of personal data through web services.

The use of an http link instead of an https link and the consequences for the security of the processing as mentioned above is also incompatible with the guarantee set out in the "Privacy Policy of [...]", *the text of which can be found on pages 19 to 24 and explanations on pages 9 and 10 of the document "[FR] Letter of response –* (...)" which *was communicated to the Inspection Service by Y via its email of 17/07/2019 (exhibit No 14). The Inspection Service*

refers in this respect to the following sentences mentioned in the above-mentioned text of the Y:

"We are committed to respecting and protecting the privacy of everyone we deal with, have dealt with or will deal with. As part of our commitment, we seek to give you clear information and control over the personal information we hold about you, as well as other non-personal data we may collect and use during your visit to this website." "No other personal information will be shared with any other third party."

Findings on the responsibility of the Data Controller (article 24 of the GDPR) and on the designation of the Data Protection Officer (article 37 of the GDPR)

"In the document "[FR] Letter of response – (...)" which was communicated to the inspection service by Y via its email of 17/7/2019 (exhibit No. 14) appears on pages 10-11 and pages 25-31 a motivation for the decision not to appoint a data protection officer within the organisation; according to "The summary of the submission is that the (...) is not obliged to appoint a dedicated Data Protection Officer."
The aforementioned "decision" and its motivation is not in line with article 24(1) GDPR, nor with article 37(1) GDPR for the following reasons: There is currently no official decision taken by SADC on whether or not to appoint a Data Protection Officer despite the obligation imposed by article 24(1) to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation." The document "Re DOS-2018 -05968 -0J0-VI M -questions in the framework of an inspection investigation_FR" which was communicated to the inspection service by the Y via its email of 9/9/2019 (exhibit no. 17) mentions on pages 10 to 11 that the above-mentioned decision "will be put on the agenda of our next Board of Directors meeting in November 2019 in order to make sure that the decision taken has been formally documented.

The elements of the technical analysis report of 03/ 07/ 2019 (exhibit no. 12) quoted above in the present report demonstrate that a cookie "informs Y as to whether or not your browser accepts cookies from third parties" which requires the designation of a Data Protection Officer on the basis of article 37, paragraph 1, b) of the GDPR. This cookie is clearly linked to the functioning of the website www.youronlinechocies.com given the explanations of Y regarding this website on pages 3 to 9 of the document "[FR] Letter of response – [...]" *which was communicated to the inspection service by Y via its email of 17/07/2019 (exhibit no. 14) and permits regular and systematic large-scale monitoring of data subjects."*

18. As a reminder, the IS is independent from the Litigation Chamber (henceforth the "LC"). The investigation report produced by the IS is only one of the elements on which the LC bases its decision.

IV- Motivation

IV.1- On the competence of the DPA

IV.1.1- On the competence of the DPA under the IMI system

19. Article 56 of the GDPR states that "*Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.*"

20. Article 4.23 of the GDPR explains the concept of cross-border processing in the following terms:

'*(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or*

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State."

21. The defendant has its sole place of business in Belgium, but its activities (more particularly, its website youronlinechoices, which can be visited from any EU Member State) substantially affect or are likely to substantially affect data subjects in several Member States, including the complainant in Germany. The Litigation Chamber bases its competence on a combined reading of Articles 56 and 4.23.b) of the GDPR. A case has been referred to the DPA by the Data Protection Authority in Berlin, following a complaint by the complainant to an authority in the Member State in which he is habitually resident, in accordance with Article 77.1 of the GDPR, and the DPA has declared itself to be the lead supervisory authority (Article 60 of the GDPR).

IV.1.2- On the competence of the DPA

22. In the section below, the Litigation Chamber recalls that the DPA's competence with respect to the ePrivacy Directive has been developed in previous decisions of the Chamber, including Decisions 12/2019 of 17 December 2019, 24/2021 of 19 February 2021, as well as 19/2021 of 12 February 2021. This section contains a summary of the Chamber's position.

23. Pursuant to Article 4 § 1 of the LCA [the Law of 3 December 2017 establishing the DPA, the DPA is responsible for monitoring the respect of the fundamental principles of data protection as affirmed by the GDPR and other laws containing provisions on the protection of personal data processing.

24. Pursuant to Article 33 § 1 of the LCA, the Litigation Chamber is the administrative litigation organ of the DPA. Among other things, it deals with complaints that are sent to it via the IMI system, on the basis of Article 56 of the GDPR.

25. Pursuant to Articles 51 et seq. of the GDPR and Article 4.1 of the LCA, it is the duty of the Litigation Chamber as the administrative litigation organ of the DPA to exercise effective control over the application of the GDPR, to protect the fundamental rights and freedoms of natural persons with regard to data processing, and to facilitate the free flow of personal data within the Union.

26. As the defendant acknowledges, the website collects personal data through three types of cookies (audience cookies, “chat box” cookies, and session cookies), and therefore processes this personal data.

27. The Litigation Chamber is competent to rule on cases concerning the processing of personal data, pursuant to Article 4, § 1 of the LCA and Article 55 of the GDPR, and in compliance with Article 8 of the Charter of Fundamental Rights of the European Union.

28. Furthermore, under Belgian law, the Belgian Institute for Postal Services and Telecommunications (BIPT) is the controller for the Electronic Communications Law (ECL hereinafter), including Article 129 of the ECL which implements Article 5.3 of Directive 2002/58[1] (hereinafter, the “ePrivacy Directive”), in accordance with Article 14, § 1 of the Law of 17/01/2003 on the status of the regulator of the Belgian postal and telecommunications sectors.

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, hereinafter the “ePrivacy Directive”).

29. In its Opinion 5/2019 on the interaction between the ePrivacy Directive[2] and the GDPR, the European Data Protection Board (hereinafter: "EDPB") confirmed that data protection authorities are competent to apply the GDPR to data processing operations, including in contexts where other authorities would be competent, pursuant to the national transposition of the ePrivacy Directive, to supervise certain aspects of personal data processing.

30. This Opinion also indicates that the ePrivacy Directive aims to "clarify and complement" the provisions of the GDPR with regard to the processing of personal data in the electronic communications sector, thereby ensuring compliance with Articles 7 and 8 of the EU's Charter of Fundamental Rights.

31. The Litigation Chamber notes in this respect that Article 8.3 of the Charter provides that the processing of personal data is subject to monitoring by an independent authority tasked with data protection.

32. In addition, the legal predecessor of the EDPB (the Article 29 Data Protection Working Party, hereinafter: Data Protection Working Party) also clarified that the requirements of the GDPR for obtaining valid consent apply to the situations that fall within the scope of the ePrivacy Directive[3].

33. In the Planet49 judgement, the Court of Justice of the European Union confirmed that the collection of data through cookies can be said to constitute personal data processing[4]. Therefore, the Court interpreted Article 5.3 of the ePrivacy Directive in the light of the GDPR[5], in particular on the basis of Article 4.11, Article 6.1.a of the GDPR (consent requirement), and Article 13 of the GDPR (information to be provided).

34. As mentioned above, the competence of the BIPT to monitor certain aspects of processing – such as the placement of cookies on the Internet user's terminal equipment – does not negatively impact the general competence of the DPA. As specified by the EDPB, data protection authorities remain competent for processing operations (or aspects of processing operations) for which the ePrivacy Directive does not lay down specific rules[6]. There is indeed a complementarity of competences between BIPT and the DPA in this case, insofar as on the basis of article 4 of the LCA, the DPA is responsible for

[2] EDPB, Opinion 5/2019 on the interactions between the "privacy and electronic communications" directive and the GDPR, in particular as regards the competence, tasks, and powers of data protection authorities, § 69

[3] Data Protection Working Party, Guidelines on consent under Regulation 2016/679, WP259, p. 4.

[4] Judgement of the Court of 1 October 2019, Planet49, C-673/17, ECLI:EU:C:2019:801, point 45.

[5] As well as in the light of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and the free circulation of such data.

[6] EDPB, Opinion 5/2019 on the interactions between the "privacy and electronic communications" directive and the GDPR, in particular as regards the competence, tasks, and powers of data protection authorities, § 69.

monitoring compliance with the fundamental principles of data protection (as affirmed by the GDPR and in the other laws containing provisions relating to the protection of personal data), and that consent is indeed a fundamental principle in this field.

35. Furthermore, the complaint also relates to the processing that takes place following the placement of the contentious cookie.

36. Furthermore, the aforementioned Opinion 5/2019 of the EDPB on the interaction between the ePrivacy Directive[7] and the GDPR also states that national procedural law determines what should happen when a data subject lodges a complaint with the Data Protection Authority regarding an instance of personal data processing (such as data collection by means of cookies), without also complaining about (potential) violations of the GDPR. This corresponds well to the present case.

37. In this respect, the Brussels Court of First Instance has clearly indicated that the legal predecessor of the DPA was competent to submit a request to a court "insofar as it concerned alleged violations of the Privacy Law of 8 December 1992, to which Article 129 of the ECL, which clarifies and complements it, expressly refers"[8]. As indicated below, Article 129 of the ECL is the implementation in Belgian law of Article 5.3 of the ePrivacy Directive.

38. The DPA is thus competent to verify whether or not the requirement of the fundamental principle of consent around the challenged cookie complies with the consent requirements of the GDPR.

39. The DPA is also competent to verify compliance with all other conditions made mandatory by the GDPR - such as transparency of processing (Article 12 of the GDPR) or information to be provided (Article 13 of the GDPR).

40. As confirmed by the Court of Justice in the Facebook et al. judgement, only the recording and reading of personal data by means of cookies falls within the scope of Directive 2002/58/EC, while "all prior operations and subsequent activities involving the processing of such personal data by means of other technologies fall within the scope of the [GDPR]".[9]

---

[7] EDPB, Opinion 5/2019 on the interactions between the "privacy and electronic communications" directive and the GDPR, in particular as regards the competence, tasks, and powers of data protection authorities, 12/03/2019, § 70.

[8] Brussels Court, 24th Chamber for Civil Cases, 16 February 2018, Docket No. 2016/153/A, point 26, p. 51, available at: https://www.autoriteprotectiondonnees.be/news/lautorite-de-protection-des-donnees-defend-son-argumentation-devant-lacour- dappel-de-bruxelles.

[9] Judgement of the Court of 15 June 2021, C-645/19, ECLI:EU:C:2021:483, point 74.

IV.2- As regards breaches of the principles of transparency (article 5.1.a and 12 and 13 of the GDPR) and lawfulness (article 6 of the GDPR)

IV.2.1.1-Reminder of the basic legal principles concerning the use of tracking tools and cookies

41. Before examining the corresponding breaches identified by the IS report, the Litigation Chamber considers it useful, for educational purposes, to provide a short introduction to the subject of cookies and to recall the basic legal principles concerning tools for tracking internet users, of which cookies are a part.

42. The term "trackers" includes cookies and HTTP variables, which may include web beacons, flash cookies, access to terminal information from APIs (LocalStorage, IndexedDB, advertising identifiers such as IDFA or Android ID, GPS access, etc.), or any other software or operating system generated identifier (serial number, MAC address, unique terminal identifier (UTI), or any data that is used to calculate a unique fingerprint of the terminal), or any other identifier generated by a software or an operating system (serial number, MAC address, unique terminal identifier (UTI), or any set of data that is used to calculate a unique fingerprint of the terminal (e.g. via fingerprinting).

43. These cookies and other trackers can be distinguished according to different criteria, such as the purpose they serve, the domain that sets them or their lifetime. Cookies can thus be used for many different purposes (among others, to support communication on the network - "connection cookie" -, to measure the audience of a website - "audience measurement, analytical or statistical cookies" -, for marketing and/or behavioural advertising purposes, for authentication purposes, etc.).

44. Cookies can also be distinguished according to the domain that sets them, so they are "first-party" or "third party." A first-party cookie is set directly by the owner of the website visited, whereas a third-party cookie is set by a domain other than the one visited (e.g. when the site incorporates elements from other sites such as images, social media plugins - the Facebook "Like" button for example - or advertisements). When these elements are retrieved by the browser or other software from other sites, these sites may also place cookies that can then be read by the sites that have placed them. These "third party cookies" allow these third parties to track the behaviour of internet users over time and across multiple sites and to create internet user profiles from this data.

45. Cookies can also be distinguished according to their validity period, between "session" and "persistent" cookies. "Session cookies" are automatically deleted when the browser is closed, whereas persistent cookies remain stored on the device used until their expiry date (which can be expressed in minutes, days or years).

46. From a legal point of view, a distinction should be made between trackers which require consent from the user and those that do not.

47. Trackers that do not require consent are those that are strictly necessary for the provision of an online communication service expressly requested by the user, or trackers that are intended to enable the transmission of the communication by electronic means. These trackers do not require the consent of users. The processing of personal data in the latter trackers is generally based on the legitimate interest of the data controller (article 6.1.f of the GDPR).

48. This does not prevent, however, in respect of the principle of transparency, informing Iinternet users of their use and reminding them that they can use their browser settings to block them and in this case mentioning the potentially negative effects, on the functioning of the site, on doing so. The associated processing of personal data obviously remains subject to the principles of the GDPR.

49. Cookies which do not require consent include those that retain the user's choice to store trackers, those that are used for authentication to a service, those that retain the contents of a shopping cart, or those that personalise the user interface (e.g. for language selection or service layout), where such personalisation is an intrinsic and expected feature of the service.

50. Prior consent must be obtained for other cookies and trackers. Moreover, processing on the basis of legitimate interest is also prohibited for these cookies. Thus, prior user consent is required for all cookies that do not have the exclusive purpose of enabling or facilitating communication by electronic means or that are not strictly necessary for the provision of an online communication service at the express request of the user. These may for example be related to the display of personalised or non-personalised advertising (since trackers are used to measure the audience of the advertising displayed in the latter case) or to sharing features on social networks. In the absence of consent (i.e. in the event of a refusal by the user), these cookies cannot be stored and/or read on the user's terminal.[10]

IV.2.1- As regards the breach concerning the use of a cookie without prior information of the user

51. In essence, the IS identifies two shortcomings in this regard:

[10] See the Knowledge Centre's Recommendation No. 01/2020 of 17 January 2020 on the processing of personal data for direct marketing purposes concerning many practical aspects and examples on the use of cookies in compliance with the GDPR, particularly concerning consent and transparency (p78 +s). See also the CNIL practical sheet "Cookies and trackers: how to make my website compliant", 01 October 2020, https://www.cnil.fr/fr/cookies-et-traceurs-comment-mettre-mon-site-web-en-conformite

- Article 12(1) of the GDPR provides that the controller must take appropriate measures to provide the data subject with any information referred to in particular in article 13 of the GDPR in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms. Article 12.2 of the GDPR provides that the data Controller must facilitate the rights of the data subject.

- Article 13(1) and (2) state, with regard to the information to be provided when personal data are collected from the data subject

'1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative; identity and contact details of the controller and, where appropriate, of the controller's representative

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) where the processing is based on point (f) of article 6(1), the legitimate interests pursued by the controller or by a third party;

e) the recipients or categories of recipients of personal data, if any; and

f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in article 46 or 47, or the second subparagraph of article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c) where the processing is based on point (a) of article 6(1) or point (a) of article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d) the right to lodge a complaint with a supervisory authority;

e) the existence of automated decision-making, including profiling, referred to in article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

52. The Litigation Chamber recalls that the purpose of the principle of transparency highlighted in articles 12, 13 and 14 of the GDPR is that the data subject should be able, in accordance with the principle of fairness in article 5.1. a), to determine in advance what the scope and consequences of the processing encompass so as not to be caught off guard at a later stage as to how his or her personal data have been used. The information should be concrete and reliable, not couched in abstract or ambiguous terms and not open to different interpretations. In particular, the purposes and legal basis for the processing of personal data should be clear.

53. In the Planet49 judgment[11], the Court of Justice of the European Union held that for the placement of cookies the data controller must provide information on the duration of the operation of the cookies as well as on whether or not third parties have access to these cookies, in order to ensure fair and transparent information (article 5.3 of the e-Privacy Directive regarding the placement of cookies is thus to be read in conjunction with the fairness principle (article 5.1. a) and the information obligations of article 13.2 (a) and (e) of the GDPR.

54. Pursuant to Articles 5.2 and 24 of the GDPR, the data controller must take appropriate technical and organisational measures to ensure and be able to prove that the processing of personal data using cookies is carried out in accordance with articles 12 and 13 of the GDPR.

55. In the case in point, the IS found, firstly, that when the user logged on to the defendant's website (homepage), a cookie was already loaded in the browser, although no information had been delivered to the user. Personal data were thus processed before the sharing of the information required by article 13 GDPR. The cookie was called "third_party_c_t", and informed the defendant whether or not the user's browser accepted third-party cookies (the preference cookies of the participating companies).

56. The defendant acknowledges in its submissions that the user was not informed in advance about the placement of the cookie, at least in the version of the website at the time of the investigation by the inspection service. The defendant points out that the cookie in question was deleted in April 2020 following a modification of the website, and then adds that it was a first-party cookie which could be described as essential (i.e. strictly necessary,

[11]Judgment of the Court of 1 October 2019, C-673/17, ECLI:EU:C:2019:801.

which the IS report does not dispute). Moreover, this cookie did not constitute a risk for the rights and freedoms of the data subjects because it was not similar to an identifier.

57. As regards the period between the entry into force of the GDPR on 25 May 2018 and the deletion of the cookie in April 2020, the defendant states that for technical reasons the cookie was deposited before the banner with information on the use of cookies by the site appeared. It also explains that it was impossible to display the information about the cookie in the user's language since it is on this page that the user had to select their language/country.

58. It also states that as this was an essential cookie, user consent was not required. This is not disputed in the IS report.

59. The Litigation Chamber takes note of the modification of the defendant's website, which, as the defendant states in its submissions, strengthens its compliance with the GDPR. It also notes the deletion in April 2020 of the cookie in question. The fact remains that between the entry into force of the GDPR (25 May 2018) and the deletion of the cookie in question in April 2020, the defendant collected and processed personal data without previously informing the user.

60. The arguments put forward by the defendant cannot be retained, the first according to which the cookie was loaded before the information banner appeared for "technical reasons", and the second according to which the information could not be communicated to the user before the cookie was loaded since it was precisely on the page visited that the user had to choose his language/country. As regards the argument that the user had not yet selected a language, it was therefore appropriate to display the warning of the use of the cookie in English, a widespread language commonly used by other websites, before the user's language was selected.[12]

61. The argument put forward by the applicant that the impact in terms of risks to users' rights and freedoms was low is likewise irrelevant: the obligation to provide prior information applies to all types of cookies, regardless of whether their impact on the data subject's right to data protection is low or not.

62. The Litigation Chamber finds a breach of articles 12 and 13 of the GDPR between the entry into force of the GDPR (i.e. 18 May 2028) and the removal of the "third_party_c_t" cookie in April 2020.

[12] The Litigation Chamber also refers to the extensive practical information on cookies available on the DPA website at https://www.autoriteprotectiondonnees.be/citoyen/themes/internet/cookies. See also Recommendation no. 01/2020 of 17 January 2020 on the processing of personal data for direct marketing purposes concerning many practical aspects and examples on the use of cookies in compliance with the GDPR, in particular concerning transparency (p78 +s)

IV.2.2- As regards the transparency of the box indicating that "non-identifiable information" is collected

63. The second breach identified by the IS report concerns the screen that appeared (at the time of the investigation, i.e. before the website was modified), when the user chooses their language and country. This screen stated: "*This website collects and uses non-identifiable information to analyse site activity to improve navigation. You can control how this information is collected and used*" and was accompanied by a hyperlink to the "*Privacy policy*" page.

64. The IS report points out that although this information is not identifiable, it is still personal data. According to the IS, this box is not "transparent" and does not allow the user to have an idea of what is being collected and for what purpose.

65. The defendant replies in this respect that a dialogue box has replaced the screen (or box) in question since the modification of the website. It also contests that for the period prior to the modification the box was not transparent, in that it was sufficient for the user to click on the hyperlink to obtain the information relating to the '*non-identifiable information*' collected. Moreover, this screen remained displayed throughout the user's visit, unless the user closed it. The defendant added that this information was available on other pages of the site and in the site's privacy policy document, and also pointed out that since these cookies were not subject to prior consent (since they were strictly necessary), the GDPR does not require the Data Controller to provide all relevant information in a single prior information box, which, the defendant argues, would not be feasible in practice.

66. The Litigation Chamber recalls the requirement of Recital 58 of the GDPR that "*The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.*

67. The Litigation Chamber also reminds the requirement of article 12.1 of the GDPR, which states that "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.*" (emphasis added)

68. In other words, this means that before the user's consent is requested, the principle of transparency requires that precise information be provided to the user on the data controller, the purposes of the cookies and other trackers that will be deposited and/or

read, the data they collect and their lifespan. The information must also cover the rights that the GDPR gives to the user (or data subject), including the right to withdraw consent.

69. As mentioned above, the information should be visible, complete and prominently displayed. It should be written in simple terms that are understandable to any user. This implies, in particular, that the information should be written in a language that is easily understood by the 'target audience' for which it is intended. For example, if the website is aimed at a French and/or Dutch-speaking audience, the information must be written in French and/or Dutch[13].

70. The Litigation Chamber considers that the defendant failed to comply with the transparency obligation before the modification of the website in that the box did not provide, at the very least, a direct link to the required information about the cookies used under Article 13 of the GDPR, instead of a general reference to the defendant's privacy policy.

71. In this respect, the Chamber agrees with the recent guidelines of the CNIL[14], which also emphasise that "Simply *inserting a link to the general conditions of use is not sufficient.*

At the very least, the following information must be given to users in advance to make sure that their consent is informed:
-the identity of the person(s) responsible for processing read or write operations;
-the purpose of the data reading or writing operations;
-how to accept or reject the trackers;
-the consequences of refusing or accepting the trackers;
-the existence of the right to withdraw consent."

72. The Litigation Chamber must here reiterate the key role of the principle of transparency in the respect of the data protection rights of the data subjects. This principle contributes to guaranteeing freedom of choice to users by giving them more control over their personal data, in particular in the context of the large-scale tracking practices of Internet users in our digital economy.

73. The Litigation Chamber notes from the outset and in the alternative that, in addition to the necessary respect for the principle of transparency, as developed below, the user's consent (for non-functional cookies) must also meet a number of requirements.

---

[13] As mentioned below, in the case in point, if the target language cannot be identified on the first page of the site, the Data Controller may use English to allow the user to choose his or her language.

[14] Deliberation No. 2020-091 of 17 September 2020 adopting guidelines on the application of Article 82 of the amended Act of 6 January 1978 to read and write operations on a user's terminal (in particular "cookies and other trackers") and repealing Deliberation No. 2019-093 of 4 July 2019, points 23-25

74. For information purposes, the Litigation Chamber refers to the DPA website[15], where there is a wide range of practical advice on how to use cookies in accordance with the GDPR.

75. In the present case, the Litigation Chamber notes that the defendant has rectified the above-mentioned breaches of the principle of transparency by modifying its website. The breach of the principle of transparency identified in the IS report is therefore no longer relevant.

IV.3- As regards the breaches of articles 12 and 13 of the GDPR

76. The IS report also states that the defendant's Privacy Policy document does not comply with articles 12 and 13 of the GDPR, firstly because the information contained therein is not always concise, transparent and understandable, and secondly because it is incomplete.

IV.3.1- As regards the fact that the information is not always transparent and understandable

77. The IS considers that the information in the defendant's Privacy Policy document is not always transparent and understandable for several reasons.

78. A- Firstly, the IS notes that the language used is not consistent and logical, since the terms "personal information" and "private data" are used, whereas the GDPR systematically refers to "personal data."

79. As mentioned above, article 12 of the GDPR requires that the information to be provided under articles 13 and 14 of the GDPR be communicated "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*." The Article 29 Working Party states in its Transparency Guidelines[16] that "*the requirement that such information be 'understandable' means that it should be comprehensible to the majority of the intended audience. Understandability is closely linked to the requirement to use clear and simple language*."

80. The Litigation Chamber considers that the defendant should be followed when it explains that the GDPR does not require the use of the term "personal data", and that the terms "personal information" and "private data" can be understood by the majority of the

[15] https://www.autoriteprotectiondonnees.be/citoyen/themes/internet/cookies. See also the CNIL website "Questions and Answers on the Amending Guidelines and Recommendation on Cookies and other Tracers" available at https://www.cnil.fr/fr/questions-reponses-lignes-directrices-modificatives-et-recommandation-cookies-traceurs.

[16] Article 29 Working Party, "Guidelines on transparency under Regulation (EU) 2016/679", Revised version adopted on 11 April 2018, WP260 rev.01, 17/EN, p.8.

intended audience (especially in the context of reading the paragraphs using them), and that they can be considered as synonyms.

81. The Chamber further notes that the defendant now only uses the term "personal data" in its updated Privacy Policy document.

82. This claim of breach made by the IS is therefore null and void.

83. B- Secondly, the IS argues that the warning of "undesirable consequences" in case of refusal of cookies is not comprehensible and therefore prevents free consent, since it does not explain what these undesirable consequences are.

84. The Article 29 Working Party put it in this way:

"A key aspect of the transparency principle highlighted in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing encompass so that he or she is not taken by surprise at a later stage as to how his or her personal data have been used. This is also an important aspect of the fairness principle under Article 5(1) of the GDPR, which is also linked to Recital 39, which states that 'Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data." More specifically, with regard to complex, technical or unscheduled data processing, the position of the G29 is that controllers should, in addition to providing the information set out in articles 13 and 14 (dealt with later in these Guidelines), separately and clearly define the main consequences of the processing: in other words, what the effect of the specific processing described in a privacy statement or notice will actually be for the data subject. In line with the principle of accountability and in accordance with Recital 39, controllers should assess whether there are specific risks for the natural person data subjects affected such processing that should be brought to the attention of the data subjects. Such an assessment could provide an overview of the types of processing that are likely to have the greatest impact on the fundamental rights and freedoms of data subjects with regard to the protection of their personal data."[17] *(our underlining)*

85. According to the defendant, it is clear that the words 'undesirable consequences', read in context, refer to the use of the site, which does not function optimally in the event of the rejection of an essential cookie. It points out that this warning is repeated in several different places on the site, and that in the new version of the site, a table explaining the effects of rejecting cookies has been added.

86. The Litigation Chamber is of the opinion that the use of these terms allows users to understand the practical consequence of rejecting the cookie. Nevertheless, beyond the

[17] Ibid

question of clearly informing the user of the "undesirable consequences" (namely, the impossibility to use the site or only in a limited way) resulting from the rejection of the cookie, the Litigation Chamber stresses that this practice of "cookie wall" cannot be considered as a violation of the law. In the alternative, the Litigation Chamber points out that this "cookie wall" practice can only be permitted d when the rejected cookie is a strictly necessary cookie (as opposed to a non-functional cookie) (see below, part IV.7.2 on this subject).

87. Therefore, it can be reasonably argued by the defendant that these terms refer sufficiently clearly to the use of the website.

88. C- Finally, the IS report argues that the reference to "additional information" about cookies on the Google, Firefox, Windows sites on the defendant's website is also not understandable without further explanation.

89. The defendant argues that this referral to "additional information" on cookies in the main browsers (Google, Firefox, Windows) is common practice. It states that most websites using cookies do the same, including the DPA website. The defendant argues that the site even has an additional information section called "Familiarise yourself with your computer's privacy settings", which provides concrete explanations with supporting images.

90. In this context, the Litigation Chamber is of the opinion that the reference to the "additional information" on cookies in the browsers (Google, Firefox, Windows) is sufficiently comprehensible for the user.

IV.3.2- As regards the fact that the information is not complete

91. The IS then argues that the information in the defendant's Privacy Policy document is not complete for two reasons.

92. A - Firstly, the IS points out that the existence of the right to withdraw consent at any time is not mentioned for the processing of personal data, but only for the management of cookies.

93. Article 7.3 of the GDPR sets strict conditions for the withdrawal of valid consent: (a) The data subject shall have the right to withdraw his or her consent at any time, (b) the data subject shall be informed thereof and (c) it shall be as easy to withdraw as to give consent. Pursuant to article 129, last paragraph of the ECL, the controller is obliged to give "free of charge" the possibility to the end-users of the terminal equipment concerned "to withdraw the consent in a simple way."

94. This right to withdraw consent must therefore be the subject of prior information (article 7(3)(b)) and must also be read in conjunction with the requirement of fair and transparent processing within the meaning of article 5 and article 13(2)(c) of the GDPR. No or incomplete information on the right to withdraw consent would imply that consent would de facto be given for an infinite period of time and that the data subject would be deprived of the right to withdraw consent. These rules apply to both "first party" cookies and "third party" cookies.

95. The defendant replies that, except for analytical cookies (and in the rare cases where personal data is contained in a contact form), the site does not process personal data for which consent is required. However, the privacy policy statement indicates that users of the site can delete cookies, which, according to the defendant, unequivocally amounts to withdrawing their consent. It submits that the additional mention of the existence of the right to withdraw consent was not necessary.

96. The defendant adds that the DPA does the same on its own website, i.e. also uses analytical cookies on the basis of consent (and contact forms), without explicitly mentioning the 'right to withdraw consent' in its 'Data Protection Statement.'

97. The Litigation Chamber notes that in the current version of the "Protection of your privacy" page, a specific reference to the existence of the right to withdraw consent for the processing of personal data has been inserted, and considers that the information is sufficiently complete.

IV. 4- As regards breaches of article 30 of the GDPR

98. The IS also points out that the processing register does not mention the third countries to which several categories of personal data are transmitted, but merely refers to documents of subcontractors with whom it has concluded agreements.

99. The defendant replies that the register is based on a European regulator's model, which includes cross-references. It explains that it works with various US subcontractors providing cloud computing services, and that the information on these third countries may vary depending on their servers and types of services. It adds that the purpose of cross-referencing these subcontractors' documents is to have complete and up-to-date information at all times. It also clarified that this concerns only a few boxes in the register, that the rest of the register is completed in accordance with the GDPR, and that the GDPR does not prohibit this.

100. The Litigation Chamber strongly recommends that the third countries be indicated and easily identifiable in the processing register, particularly in view of the recent case law of the CJUE in terms of transfers to third countries[18]. Thus, the Litigation Chamber, on the basis of article 100.9 of the LCA, orders the defendant to adapt its processing register by clearly indicating the third countries to which personal data are sent in order to better comply with the case law of the CJEU.

IV. 5- A regards breaches of articles 24 and 32 of the GDPR

101. The IS complains that the protocol (url link) used is http and not https, as this constitutes a breach of the security obligation.

102. The defendant replies that, since 15 January 2020, the site has switched to the https protocol. It also explains that this migration had been an ongoing project since 2014, but that its implementation had been long and difficult due to the fact that it had to collaborate with all its members (more than one hundred). The defendant adds that since its site handles little personal data, the risks to data subjects were low, and that given the risk-based approach of the GDPR, this migration to https was not strictly necessary.

103. Without ruling further on this matter, the Litigation Chamber notes the migration of the site to the https protocol, and notes that the claim of breach made in the IS report is therefore no longer relevant.

IV. 6- With regard to breaches of articles 24 and 37 of the GDPR

104. Furthermore, the IS complains that there is no official decision documenting the choice of whether or not to appoint a Data Protection Officer (DPO), and that the defendant should have appointed a DPO because it uses a cookie that allows for "regular and systematic large-scale tracking of data subjects."

105. The defendant points out that the GDPR does not require a formal procedure for the decision to appoint a DPO or not, and that documenting the reasons for the decision not to appoint one is a recommendation and not an obligation.

106. Secondly, concerning the cookie which, according to the IS, allows "regular and systematic large-scale tracking of data subjects", the defendant replies that the cookie has not been used since April 2020. It adds that even when it was used, this cookie did not justify the appointment of a DPO because this cookie was not an identifier since it was the

[18] Judgment of the Court of 16 July 2020, C-311/18, Facebook Ireland and Schrems, ECLI:EU:C:2020:559. ("Schrems II case")

same for everyone and therefore did not allow a user to be tracked. Nevertheless, insofar as this cookie contained personal data, it made it possible to identify data subjects.

107. The defendant argues that there was no "large-scale tracking", and that even if its cookies allowed for "systematic and large-scale tracking" -quod non-, this would still have to be a "core activity" of the defendant, which was not the case (the proof of which being that it continues its same activities today but without the cookie in question).

108. The Litigation Chamber is of the opinion that the defendant can reasonably argue that the GDPR does not require a formal procedure to be followed as to the decision to appoint a DPO or not, and that documenting the reasons for the decision not to appoint one is a recommendation and not an obligation.

109. As regards the obligation to appoint a DPO, the Litigation Chamber recalls the requirement of article 37(1)(b) of the GDPR, according to which the Data Controller must appoint a DPO if "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale." This article should be read in conjunction with the Guidelines on Data Protection Officers of the Article 29 Working Party[19]. In the absence of "systematic and large-scale monitoring", there can be no finding of a breach of article 37 of the GDPR.

IV.7- As to the content of the complaint

110. Having considered the breaches raised by the IS, the Litigation Chamber examines below the grievances as expressed by the complainant in his complaint.

111. As mentioned above in paragraphs 12-14, the complainant raises two claims in his complaint. Firstly, he states that the tool for selecting advertising preferences does not work, in that the cookie opt-out option for many third parties does not work (even if he clicks on the opt-out option, the opt-in option automatically resets). He thus argues that his consent to these cookies is forced and therefore not free in the sense of article 4.11 and 7 of the GDPR.

112. He also complains that the website forces the user to accept cookies in order to be able to select his advertising preferences. The cookie in question informs the defendant whether or not the user's browser accepts cookies from third parties. The Litigation

[19] WP243rev.

Chamber understands that the plaintiff objects to the placement of the cookie and the subsequent processing of his personal data by the defendant.

IV.7.1- Concerning the complainant's first grievance, relating to the malfunctioning of the tool for choosing advertising preferences

113. In response to the complainant's first complaint, the defendant asserts that it was clearly indicated on its site (in the preferences selection tool itself and in the General Terms of Use) that if ad blocking software was used, the selection tool might not work. It is also clear from the printscreen of the complainant's browser in the IS report that the complainant does use such software. The IS report (based in particular on the technical analysis report which includes a test of the proper functioning of the control tool) does not raise any malfunctioning of the control tool. Consequently, the Litigation Chamber cannot accede to the complainant's claim that his consent was forced, in violation of articles 4.11 and 7 of the GDPR.

IV.7.2- As regards the complainant's claim that the defendant's website requires the user to accept cookies in order to use the site, the so-called "cookie wall" practice

114. Before examining the specific issue of the cookie wall, the Litigation Chamber considers it useful to recall the rules on consent for educational purposes.

IV.7.2.1- Concerning the criteria for valid consent

115. Article 4.11 of the GDPR defines "consent" of the data subject as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action.*"

116. Article 7 of the GDPR also sets out the conditions for consent:

"1. *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data*.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. [4]*It shall be as easy to withdraw as to give consent.*

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia*, the performance of a contract, including the provision of a service, is*

conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

117. Therefore, according to recital 43 of the GDPR "Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case."

118. Furthermore, article 5.3 of the e-Privacy Directive, as transposed by Article 129 of the ECA, sets the condition that the user "has given their consent" for the placement and consultation of cookies on his terminal equipment, with the exception of the technical recording of information or the provision of a service expressly requested by the subscriber or end-user where the placement of a cookie is strictly necessary for this purpose.

119. As mentioned above, a cookie is considered to be "functional" if it is necessary to send a communication via an electronic communications network or to provide a specifically requested service.

120. Recital 17 of the e-Privacy Directive specifies that for its application, the notion of "consent" must have the same meaning as "consent of the data subject", as defined and specified in the Data Protection Directive 95/46[20], now replaced by the GDPR.

121. In the Planet49 judgment, the Court of Justice of the European Union clarified the consent requirement for the placement of cookies following the entry into force of the GDPR and explained that explicit active consent is now required:

"Active consent is now, therefore, expressly provided for by Regulation 2016/6. It is important to note in this respect that, according to recital 32 of this regulation, consent could be ticking a box when visiting an internet website. However, this recital specifically states…."Silence, pre-ticked boxes or inactivity should not therefore constitute consent." It follows that the consent referred to in articles 2(f) and 5(3) of Directive 2002/58, read in conjunction with articles 4(11) and 6(1)(a) of Regulation 2016/679, is not validly given where the storage of information or access to information already stored in the terminal equipment of the user of a website is authorised by a default tick box which the user must untick in order to refuse to give consent."[21]

[20] 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 the free flow of such data.

[21] Planet49 judgment, paragraphs 61 and 62

122. The consent must also be "specific." The Litigation Chamber refers to the Guidelines on consent under Regulation 2016/679[22] which have been ratified by the EDPB:

"Article 6(1)(a) confirms that the data subject's consent must be given in relation to "one or more specific purposes" and that the data subject has a choice "with regard to each of these purposes"[23]. This means "that a controller seeking consent for various specific purposes should provide separate consent for each purpose so that users can give consent specific to specific purposes." [24]

123. In particular, the user of the website should be provided with information on how to express his or her wishes regarding cookies, and how he or she can "accept all, some or none"[25].

124. For example, confirming a purchase or accepting general terms and conditions is therefore not sufficient to consider that consent has been validly given to the placement or reading of cookies. Nor can consent be given for the mere "use" of cookies, without any further specification as to the data collected via these cookies or as to the purposes for which these data are collected. The GDPR does indeed require a more detailed choice than a simple "all or nothing", but it does not require consent for each individual cookie. If the manager of a website or mobile application seeks consent for several types of cookies, the user must have the choice to give consent (or refuse) for each type of cookie, or even, in a second layer of information, for each cookie individually.

125. This position is also defended by the CNIL, which considers that the fact of "simultaneously collecting a single consent for several processing operations for distinct purposes (purpose matching), without the possibility of accepting or refusing purpose by purpose, is also likely to affect, in certain cases, the user's freedom of choice and therefore the validity of his or her consent."[26]

126. In this respect, the Litigation Chamber refers to the Data Protection Working Party's Guidelines on how to obtain consent. According to the Data Protection Working Party, consent must be obtained per cookie or per category of cookies[27].

---

[22] Data Protection Working Party, Guidelines on consent under Regulation 2016/679, WP259, p. 4

[23] *Ibid,* p. 14.

[24] *Ibid*, p. 14.

[25] Data Protection Working Party, Working Document 02/2013, setting out guidelines on the collection of consent for the deposit of cookies, p. 3, https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp208_fr.pdf

[26] Deliberation No. 2020-091 of 17 September 2020 adopting guidelines on the application of Article 82 of the amended Act of 6 January 1978 to read and write operations on a user's terminal (in particular "cookies and other trackers") and repealing Deliberation No. 2019-093 of 4 July 2019, points 17-19

[27] *Ibid.*

IV.7.2.2- Concerning the complainant's second grievance and the "cookie wall" practice

127. As regards the complainant's second complaint (i.e. that he is obliged to accept cookies in order to be able to select his advertising preferences and that he opposes the subsequent processing of his personal data), the Litigation Chamber recalls that consent must be free. Indeed, as mentioned above, the GDPR requires that " utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." According to recital 42 of the GDPR, which clarifies the requirement of freedom of consent laid down in article 4 of the GDPR, "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

128. In its recent guidelines[28], the EDPB condemns the practice of making the provision of a service or access to a website conditional on the acceptance of write or read operations on the user's terminal, or "cookie wall." It states that "*In order for consent to be freely given, access to services and functionalities should not be conditional on a user's consent to the storage of information, or access to information already stored, on a user's terminal equipment.*" The EDPB adds, regarding consent, that:

"The Data Controller must demonstrate that it is possible to refuse or withdraw consent without suffering any prejudice (recital 42). For example, the controller must prove that withdrawing consent does not incur costs for the data subject and that there is therefore no obvious disadvantage for those withdrawing consent.

47. Other examples of harm are deception, intimidation, coercion or any significant negative consequences if the data subject refuses to give consent. The Data Controller should be able to demonstrate that the data subject has a genuine choice as to whether or not to consent and that consent can be withdrawn without suffering harm.

48. If a controller can demonstrate that a service includes the possibility of withdrawing consent without suffering negative consequences, i.e. without the quality of the service being diminished to the detriment of the user, this may constitute evidence that consent has been freely given. The GDPR does not exclude all incentives, but it will be up to the Data Controller to demonstrate that consent was indeed freely given in all circumstances."

[28] EDPB, Guidelines 5/2020 on consent under Regulation (EU) 2016/679, 4 May 2020, point 39, p.13

129. The guidelines include concrete examples:

‘49. Example 8: When a user downloads a mobile application from the "lifestyle" category, the application asks for her consent to access the phone's accelerometer. This access is not necessary for the functioning of the application, but is useful for the controller to know more about the movements and activity levels of its users. When the user later withdraws her consent, she discovers that the application only works in a restricted way. This is an example of harm in the sense of Recital 42, which means that consent was never validly obtained (and the controller must therefore delete all personal data on the users' movements collected in this way).

Example 9: A data subject subscribes to a newsletter of a fashion retailer with general discounts. The retailer asks for the data subject's consent to collect more data about his or her shopping preferences in order to tailor offers to his or her preferences based on his or her purchase history or on a voluntary questionnaire. If the data subject later withdraws consent, he or she will again receive non-personalised discounts. This is not a loss, as only the permitted incentive will have been lost.

51. Example 10: A fashion magazine gives its readers the opportunity to buy new make-up products before their official launch.

52. The products will soon be available on the market, but readers of this magazine will benefit from an exclusive preview of these products. In order to take advantage of this benefit, readers must provide their postal address and consent to be put on the magazine's mailing list. The postal address is required for shipping and the mailing list is used to send out commercial offers for products such as cosmetics and t-shirts throughout the year.

53. The company explains that the data on the mailing list will only be used for sending products and advertising flyers by the magazine itself and will not be shared with other organisations under any circumstances.

54. If the reader does not wish to reveal his or her address for this purpose, he or she will not suffer any prejudice as long as the products are still accessible to him or her.”

130. The defendant responds to the complaint raised by the complainant in its submissions by asserting, that the service provided via the advertising preferences tool relies on the use of cookies sent by the participating companies in several places on the site in question,

and that if the user does not wish to receive cookies, then he or she should not use the service. More specifically, it states in its submissions (p19):

- *"The very first page of the YOC website (the one from which you can choose a country and language), contains a link entitled "How does this website work?", which leads to a page which states:*

  "When using the control tool function, small text files called "cookies" are used by many of the companies listed to check your current status and make the choice you wish to make. These files are essential to this feature and help identify errors in its functionality. If you wish to ensure that these cookies are not used, please see our top five tips for more details on how to manage cookies in your browser's privacy settings. However, if you do so, the monitoring tool will no longer work effectively" (exhibit 9 - pages 1 and 2).

- *The terms and conditions governing the use of the YOC Website and the YOC Tool state that:*

  "In order to use the YourOnlineChoices website, it is necessary for each of the participating companies to place a cookie on your web browser (the preference cookie) so that we can remember your selections. Information about cookies is available in our privacy policy: [...]. *If you use the YourOnlineChoices website with a different computer or browser, or if you delete/delete your cookies, we will not be able to remember your preferences. You will have to return to the YourOnlineChoices website to select your preferences again. In addition, the YourOnlineChoices website will not function properly if your browser is set to block cookies, as your preferences cannot be saved without the use of the preference cookie" (exhibit 9 - page 3).*

  - *The "Protecting your privacy" page states:*

  "This website covers the European Union/European Economic Area (EU/EEA), as well as Switzerland and Turkey and includes an easy-to-use feature (which any user can access from any of the listed countries) that will disable online behavioural advertising for users (of participating companies) who choose to do so [...] Please note that disabling cookies for this purpose will prevent the control tool from working."

131. The Litigation Chamber notes that the user is therefore well informed of the fact that the use of these preference cookies is necessary for the functioning of the site, and that the site imposes on him/her the choice between accepting this system or not using the website. The Chamber underlines that this reasoning can only be followed insofar as the cookies are strictly necessary, as they do not require the user's consent. In this case, the

processing is not based on consent, but on the legitimate interest of the data controller (article 6(1)(f) of the GDPR).

132. Conversely, this reasoning must be rejected in cases where the cookies are not strictly necessary. Indeed, the user must be able to accept or refuse, for each application and each website, the deposit of non-functional cookies without constraint, pressure or external influence. This requirement implies, in particular, that the user may not be denied certain services or benefits on the grounds that he or she has not consented to the use of non-functional cookies. A user who refuses a cookie requiring consent must be able to continue to benefit from the service, such as access to a site.

133. In this case, as the cookie in question is strictly necessary, the complainant's complaint cannot be upheld. There is therefore no breach of article 6(1)(a) of the GDPR in relation to the practice of "cookie walls."

134. In view of the importance of transparency regarding the decision-making process of the Litigation Chamber and in accordance with Article 100, §1, 16° of the DPA Act, this decision is published on the website of the Data Protection Authority. In view of the previous publicity surrounding this case, as well as the general interest to the public, the Litigation Chamber has decided not to delete the direct identification data of the parties and persons mentioned, whether natural or legal persons.

PAR CES MOTIFS,

ON THESE GROUNDS,

THE LITIGATION CHAMBER

Rules, after deliberation:

- On the basis of article 100, § 1, 9° of the LCA, an order for compliance of the defendant's processing register, as mentioned above
- On the basis of article 100, § 1, 5° of the LCA, a reprimand.

Pursuant to Article 108 (1) of the LCA, this decision may be appealed to the Contracts Court ("*Cour des marchés*") (Brussels Court of Appeal) within 30 days of its notification, with the Data Protection Authority as the defendant.

Hielke Hijmans

President of the Litigation Chamber