



Litigation Chamber (Geschillenkamer)

Decision on the merits 25/2020 of May 14th 2020

File number : DOS-2019-01156

Subject: Legal basis for the processing of personal data by a social media platform

The Litigation Chamber of the Data Protection Authority, composed of Mr. Hielke Hijmans, president, Mr. Dirk Van Der Kelen and Mr. Jelle Stassijns, members;

Having regard to Council Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on *the protection of individuals 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 GDPR;

In view of the Act of 3 December 2017 *establishing the Data Protection Authority*, hereinafter DPA Act;

Having regard to the internal rules, as approved by the House of Representatives on December 20, 2018 and published in the Belgian Official Gazette (Belgisch Staatsblad) on 15 January 2019;

Having regard to the documents in the file;

has taken the following decision on:

- processing of personal data by the controller: Y ("defendant");

1. **Facts and procedure**

1. On November 28, 2018 the Executive Committee of the Belgian Data Protection Authority (DPA) decided to initiate a case by its Inspection Service on the basis of Article 63, 1 ° of the DPA Act. The reason for the aforementioned referral was the practice of the social network website "W" of inviting "*friends/contacts*" of those members.
2. The Inspection Service informed the defendant about the decision of the Executive Committee in a letter dated 12 March 2019.
3. The Inspection Service sent the defendant two letters dated March 12, 2019 and May 16, 2019, with questions concerning alleged infringements of Articles 5, 6, 7, 30, 37 and 38 of the GDPR. More specifically, the Inspection Service asked questions regarding the categories of personal data of non-users which have been gathered and the retention of such data; an extract from the record of processing activities of the defendant and questions concerning the Data Protection Officer (place in the organization, activities, professional qualities, commitment to responding to the questions of the Inspection Service).
4. The defendant replied to the questions of the Inspection Service by letters dated 12 March 2019, 3 April 2019 and 14 June 2019. The defendant explained as follows the processing of personal data of the invitation functionality "W" website: "*Any personal information that we collect will depend on the platform used, if a user chooses to upload contacts from the phone book of his or her cell phone, we will collect telephone numbers and names that the user attaches to the phone. If a user chooses to upload contacts from their e-mail account, the basic contact information uploaded will be determined by the own e-mail provider of the user, as clearly set out in the upload permission screen from this provider*".¹ If a user chooses to upload his or her contacts from his/her phone these contacts are synchronized correctly, so that the user can invite the new people who are not members of "W" to register.
5. The defendant explained that in addition to the consent button, this paragraph with information is displayed: "*On a regular basis we will import contacts and save them, so we can notify you when registering acquaintances in "W" and can invite them to register you when your contacts are not yet members of "W". You decide who you add. You can stop the import at any time and delete all contacts. More Information*".

¹ Letter from the defendant dated 14 June 2019.

6. When the user clicks on "more information", he or she will see the following additional information:
*"When you import your address book we will periodically import information on your contacts, such as names, phone numbers and other information as illustrated on the consent screen of the provider to our servers. We use this information to inform you about who you already know on W and then you can invite your contacts who are not yet members. The aforementioned suggestions are made directly to the service and through e-mail. We cannot store your password or e-mail anyone without your consent. You can stop synchronising your address book at any time via your settings. When you do this, it will delete all previously imported contacts. For more information on how we handle your personal information we refer to our Privacy Policy."*².
7. The defendant further explains that the contacts of the user in the database of the defendant are kept until the user decides to stop synchronizing his contacts, or if a user deletes specific contacts. When an account is closed, the contacts (either consciously or after two years of inactivity) are removed within three months, the defendant explains³.
8. In his letter of 9 March 2020, the defendant explains that the user can choose to withdraw his consent and no longer have his contacts synchronized, with the result that existing contacts will be deleted from the "W" database. In case the user does not choose this option, the contact details (including those of non-users of the website) will be retained for a minimum of three months⁴.
9. The defendant remitted an extract from the record of processing activities to the Inspection Service showing the categories of personal data about customers (users of the website) that are processed *"profile information, personal identification, analytical data, user generated content, user account information, contact information and third party information (for users who register via Facebook)."* According to the record, the invoked legal basis for processing is *"the execution of a contract" and "consent of the data subject"*⁵.
10. Regarding the legal basis for the collection of non-users' personal data, the defendant explained as follows that the legal basis of *"consent"* - in his opinion - should not have been used: *"We believe that we are not obliged to collect the contact person's consent. Indeed, we do not send promotional messages because it is the user who sends personal communication to his or her contact through our platform. This interpretation is in line with the vision set put in Opinion 5/2009"*

² Ibid.

³ Ibid.

⁴ See also Art. 11 of the defendant's Privacy policy, exhibit 5 of the Inspection report.

⁵ Ibid.

of the Working Party 29 Working Party on online social networking⁶ and we have ensured that our process is fully in line with the four criteria set forth in [the] opinion "⁷⁸

11. In his letter dated 14 June 2019, the defendant replied in detail to the questions of the Inspection Service regarding the activities and competence of its data protection officer⁹. The defendant referred inter alia to the professional experience of the person, in particular his experience as EMEA Senior Privacy Counsel at a company engaged in online payments and as lawyer at the IT department of a law firm. This person also holds an IAPP CIPP/E and CIPM¹⁰ certification.
12. On 18 June 2019, the Inspection Service remitted its report to the Litigation Chamber, under Article 92, 3° of the DPA Act.
13. The inspection report identifies potential infringements of art. 5, paragraph. 2 of the GDPR, of Article 6 of the GDPR, items 4, 11), and 7 of the GDPR, as well as of articles 37 and 38 of the GDPR.
14. Concerning the alleged breaches of accountability (art. 5, paragraph. 2 of the GDPR), the lawfulness of processing (Article 6 of the GDPR), and the definition of and conditions for authorization (Articles 4, 11) and 7 of the GDPR), the inspection report makes a distinction between, on the one hand, the consent of the personal data of the user of the website and, on the other hand, the consent relating to the personal data of the contacts of the user.
15. Regarding the argument of the defendant that he is not required to collect *consent of the contacts (non-members of "W")*, since it would involve "*personal communication*" by the user, the Inspection Service notes that the exception for personal or household activities can indeed be invoked by social media users, but not by the social network "W" itself, in accordance with paragraph 18 of the GDPR which reads as follows: "*personal or household activities [outside the scope of GDPR] may include [...] social networks and online activities in the context of such activities. This Regulation does apply to controllers or processors who provide the means for processing personal data for such personal or household activity*" (Inspection Report, p. 4).

⁶ Opinion 5/2009 of Group 29 on social networks, 12 June 2009 (WP 163). All Group 29 and EDPB quoted in this decision are available via www.edpb.europa.eu.

⁷ Letter to the Inspection Service dated April 3, 2019.

⁸ Letter from the defendant dd. 14 June 2019.

⁹ Letter from the defendant dd. 14 June 2019.

¹⁰IAPP is a globally recognized private organization that offers certifications on European data protection law (CIPP/E) and data protection management (CIPP/M), see the following web page: <https://iapp.org/certify/cippe/>

16. The reference by the defendant to Opinion 5/2009 on online social networking of the Working Party 29 of 6/12/2009 is not considered relevant by the Inspection Service, since that opinion relates to the former Data Protection Directive¹¹ and "*because the GDPR imposes more extensive obligations on controllers, including the accountability of Article 5, paragraph 2 of the GDPR and the requirements of an unambiguous indication in Article 4, 11) and Article 7 of the GDPR*" (Inspection Report, p. 5).
17. Regarding the *consent by the social media users (members of "W")*, the Inspection Service notes that there are options previously ticked in the procedure of adding contacts. Therefore, the consent of the user whether or not to use the personal contacts is not considered valid in a context where Recital 32 of the GDPR explicitly clarified that "*pre-ticked boxes*" do not constitute consent. The Inspection Service notes that the defendant is willing to "*cease his practice on the basis of which he contacts pre-selected persons*", which has now happened (two working days after the receipt of the inspection report)¹².
18. The defendant has meanwhile removed previously ticked options from the platform "*voluntarily and without any disadvantageous acknowledgment*" from the platform, upon receipt of the second letter of the Inspection Service dated May 16, 2019. The defendant, however, alleges in his conclusion that the pre-ticked options are not related to obtaining the consent of the user to import contacts, and, moreover, this does not require consent, taking into account the principles of the Opinion 5/2009 of Working Party 29 on online social networking (see the conclusion of the defendant, p. 13).
19. The Inspection Service also noted that it is not indicated in relevant privacy information that consent may be withdrawn, as required by Article 7 GDPR. In his conclusion (p. 19 and 20) and in his letter of 14 June, the defendant replied that the possibility to withdraw the consent is indeed available on the website. Users are informed that they can stop the import at any time and delete all contacts.
20. Before starting this procedure, the defendant had been in contact with the GDPA after a previous complaint received concerning the method used on the "*W*" platform. The complaint was on the fact that the information relating to privacy could only be read only after creation of an account and after accepting the terms of use and privacy policy. The DPA had informed "*W*" that this was

¹¹ 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, Pb L 281/31 ("Data Protection Directive").

¹² Conclusion of the defendant, p. 13 and 42.

not a valid way to obtain consent for the "invite a friend" e-mail; consent was the legal basis used by "W" for the processing of user data.¹³

21. During the hearing on 9 July 2019, the Litigation Chamber decided under Article 98 of the DPA Act that the file was ready for handling on the merits.
22. On 10 July 2019 the defendant was informed of this decision by registered letter, and was also given the inspection report, and the inventory of the documents on the file which had been transferred to the Litigation Chamber by the Inspection Service. In addition, the defendant was informed of the provisions mentioned in Article 98 of the DPA Act and the defendant was, based on Article 99 of the DPA Act, informed of the deadlines to submit his defence. The deadline for receipt of the briefs ("conclusion") of the defendant was established on 4 September 2019.
23. By letter and e-mail on 15 July 2019 the defendant asked to be heard. The Litigation Chamber informed the defendant of the date of the hearing by letter dated 30 August 2019.
24. On 4 September 2019, the Litigation Chamber received the defence conclusion of the defendant.
25. On 1 October 2019, the hearing took place. The file was retaken with other members of the Litigation Chamber. The controller was heard and was given the opportunity to put forward his arguments in response to the questions put to him by members of the Litigation Chamber, regarding the foreign reach of the "W" website, the legal basis for the processing of personal data of users and non-users of the "W" website and the role and working methods of the data protection officer.
26. During the hearing, the defendant made the following statements that confirm and/or complement its conclusion:
 - The defendant provides a platform so new people meet in private without limitation (friend or relation); there are 4.5 million active users per month across the world, with 1.5 million users in the EU. It employs 33 people at "W" and 100 people in various places in the world for the helpdesk (no employees of Y, but only contractual services).
 - The defendant complains that the constitutive components of the alleged "offense" are not disclosed to "W" in the inspection report (see also conclusion of the defendant, p. 6); the defendant finds that the indictment was issued in this case without a prior detailed account

¹³ Letter from the DPA to the defendant dated 7/03/2018

of the alleged infringement. The defendant believes that the allegations regarding the "accountability" is particularly unclear.

27. The defendant also explained how the invitation process takes place on the "W" site:¹⁴

- The website users are informed about the processing taking place in the context of the "invite a friend" feature.
- Under the message "*W is better with friends*", the Internet user has the possibility to import an address book from various service providers (Outlook, Google Mail, Yahoo, Facebook, Telenet, Skynet). The user is not required to select a service provider and can skip the "invite a friend" feature completely. If the user wants to make use of this feature he must select one of the service providers. Then a screen is shown from this service provider, by which the Internet user can allow his contact addresses to be read. This is, as explained by the defendant, "*the permission screen is of the service provider.*" If the internet user agrees, all addresses stored in the address book then are stored by "W". The feature offered by such service consists in allowing users to give limited contact information to share with the "W" platform for limited purposes.
- In a next step, the internet user gets the possibility to select the recipients of the invitations e-mails.
- A first version of the website had all addresses ticked, with the possibility to deselect all the recipients with one click. Addresses are no longer pre-ticked since 12 July 2019¹⁵, and the user has the choice between two options: designate the recipients one by one, or select all prior contacts with one click. In the previous version of the website, the user also had the opportunity to deselect pre-selected recipients one by one.
- In a letter dated 4 November 2019, the defendant insists that the users have the possibility to withdraw their consent for the use of the "*invite-a-friend feature*" at any time. The website announced that all previously imported contacts are then removed.

28. The defendant furthermore states that the details of the contacts can only be used for the invite feature. No profiles are prepared on the basis of this contact according to the defendant.

¹⁴ See also conclusion of defendant, p. 7-20.

¹⁵ Conclusion defendant, p. 13, nb. 28.

29. With regard to the alleged legal basis, the defendant alleges the following: when a user sends an invitation to his friends, it is a personal communication, not a marketing message which is subject to the anti-spam rules in the e-Privacy Directive; the defendant used only one legal basis, i.e. the consent of the users; *the "GDPR does not say that you do not need consent from contacts. We have the consent of the user, to import data,"* the defendant argued at the hearing. When asked by the Litigation Chamber whether the consent of the user according to the defendant is valid also for non-users of the "W" website, the defendant replied positively, *"since it regards one and the same purpose"* of processing. The defendant thus confirmed the positions taken in its conclusion, and which was summarized as follows by the defendant:

"With regard to the alleged legal basis, the defendant states the following: Y processes the contact details of the user for a single purpose: providing the "invite a friend" feature. To fulfil this sole purpose, the contacts of the user are uploaded and then invitation e-mails are sent on behalf of the user to the contacts that the user has selected. The legal basis on which Y relies for the processing of personal data under the "invite a friend" feature, is the consent of the user. Y is of the opinion that it is not required to distinguish the consent of the contacts from the user's request, since the processing of personal data is already justified by the consent of the user under Article 6 of the GDPR and as the invitation message sent on the other hand is not a direct marketing message subject to the ePrivacy Directive. This was explicitly confirmed by the Article 29 Working Party. When asked by the Litigation Chamber whether the consent of the user is valid for non-users of the "W" website, the defendant provides a positive answer: in the context of the 'invite a friend' feature and, more generally, of all services and functions that enable the users to process personal information of the contacts and other information from people they know (eg. e-mail services, messaging systems, operating systems, cloud services where people upload photos to show to their friends and family, ...), the data are in the first place of the user himself." (Letter of the defendant to the Litigation chamber of 4 November 2019, in response to the draft minutes of the hearing, p. 3).

30. The defendant then shows by using printed screens of the website that the user can see and edit the template before it is sent as part of the invitation e-mail (p. 12 of the hearing briefs). The defendant reiterates he feels he has taken all measures to ensure that this processing would meet the requirements of *"personal communication"* as set out in Opinion 5/2009 of the Article 29 Working Party on online social networking. According to the defendant, the Inspection Service falsely alleges that the opinion is no longer valid because it dates from before the entry into force of the GDPR and the consent requirements are since strengthened (see also conclusion, p. 23). The defendant also discusses the question whether or not there is a marketing message within

the meaning of Article 13 of the ePrivacy Directive. By letter dated 4 November 2019 the defendant gave further clarification: *"Y has never claimed that the GDPR would not apply to the processing operations carried out in the context of the W platform. Y is of the opinion that the invitation message transferred to the selected contacts of the user contains personal communication for which it is not required to obtain consent from such contacts according to the ePrivacy Directive."*¹⁶

31. The Litigation Chamber then asks whether users in the invitation e-mail that the "W" platform gives are informed or not that their data may be corrected or deleted. The defendant refers to his hearing briefs that include a printed version of the screen to show what the recipient of such invitation sees: Under the message "X. sent you a message", two blue buttons offer the following option: " Register and reply " or " Read-only message. " Under these buttons the following explanation appears: *"When you click on " Register and Sign", you agree to create an account for you on W and agree with our [hyperlink] Terms and Conditions. Please read our [hyperlink] Privacy Policy and our [hyperlink] Cookie Policy. "* The defendant explains that the recipient of the invitation e-mail obtains information on his rights through the Privacy and Cookie Policy of "W" and that the recipient also in the e-mail itself will get the following information: *"Click here if you do not want to receive commercial e-mails about our products or services "* (p. 17 of the hearing briefs).
32. With regard to the data protection officer, the defendant refers to documents showing that this person has been clearly involved in the definition of the invitation feature, including an e-mail of 13 August 2018 that has already been communicated to the Inspection Service (p. 15 of the hearing bundle). The defendant states that his data protection officer can report to the highest management, and that he actually does so according to the defendant (letter of the defendant to the Litigation Chamber dated 4 November 2019, p. 4). The defendant also argues that there is no evidence in the Inspection report that this person would not be independent (that he would receive instructions from the management, for example).
33. The defendant refers to a positive and recent assessment report demonstrating that the person does not have to fear for his job. According to the defendant, this positive assessment proves that the data protection officer is able to carry out his duties independently, and that V was the natural choice for a data protection officer. The data protection officer is based in Dublin but can communicate in English and French with the staff of the defendant, and there is also a local "privacy lead" in U. The defendant argues that the data protection officer meets the employees of Y regularly in person and that most meetings are via "video conferencing" software. The professional qualifications of the person emerge from his CV. The data protection officer states

¹⁶ Letter of the defendant to the Litigation Chamber dd. 4 November 2019, p. 4.

that he also works for another social media platform ("Z") and that there is no predetermined distribution with respect to its activities between the two platforms, and that he can rely on a team of four full-time employees in addition to the local privacy lead in U.

34. In view of the cross-border nature of the processing carried out by the defendant, the Litigation Chamber decided to launch the procedure of Art 56 GDPR, in order to identify the lead supervisory authority and the concerned supervisory authorities. The DPA claimed that it was the potential lead supervisory authority. The authorities from the following countries declared to be concerned authorities: The Netherlands, Germany (Lower Saxony, Baden-Württemberg, Brandenburg, Rhineland-Palatinate Mecklenburg-Western Pomerania, Bavaria, North Rhine Westphalia, Berlin), Portugal, Sweden, Ireland, Latvia, Italy, Norway, Hungary, Austria, Spain, France, Cyprus, Slovak Republic, Denmark, Slovenia.
35. On 3 October 2019, the Litigation Chamber sent a registered letter to the defendant with the financial statements of the defendant as attachment for the fiscal years 2018, 2017 and 2016, with the question whether the defendant could confirm the therein contained figures including turnover. The turnover figures are as follows:
- year 2016: XXX EUR;
 - year 2017: XXX EUR;
 - year 2018: XXX EUR.
36. On 17 October 2019, the counsel for the defendant confirmed on behalf of the latter that the statements listed above are correct. Through this letter, the defendant wanted to draw the attention of the Litigation Chamber to an attached forecast for fiscal year 2019 (see below).
37. Minutes of the hearing were sent by e-mail for information purposes dated 30 October 2019 to the defendant, asking him to respond within 2 working days if he has any comments. The defendant was informed that this would not reopen the debates and that the comments should only relate to the display of the oral debates.
38. The defendant submitted his comments to the Litigation Chamber and urged, among other things, to take into account *"the fact that Y was always willing to cooperate since long before the official start of the investigation and that the DPA was repeatedly asked for feedback which was never given."*¹⁷

¹⁷ Letter from the defendant to the Litigation Chamber dated 4 November 2019, p. 1.

39. On 5 November 5 2019 the matter was discussed again at a meeting of the Litigation Chamber. The Litigation Chamber concluded to initiate the cooperation procedure provided for in Article 60.3 GDPR.
40. An English translation of the draft decision was handed over to the concerned DPA on 8 January 2020, in line with Article 60.3 GDPR. The defended was informed of this by letter dated 15 January 2020.
41. The Netherlands filed a relevant and reasoned objection on 4 February 2020. The Netherlands asked amongst other things to include more references to ECJ case law as regards the analysis of the defendant's legitimate interest to send invitation e-mails to third parties not using the social media platform. The Netherlands also challenged the relevance of a reference to an investigation report dated 2013 and which relates to the legitimate interest of social media platforms to send invitation e-mails.
42. The Litigation Chamber decided on 14 February 2020 to uphold the filed objection, in particular as regards the assertion that the application of the legal basis of legitimate interest *in the present case* requires an assessment in *concrete* terms of all relevant factual elements, taking into account the case law of the Court of Justice. The Litigation Chamber decided to reopen the debates as regards the analysis of the legitimate interest of the defendant.
43. The Litigation Chamber informed the defendant by registered letter of 18 February 2020 of this relevant and reasoned objection, as well as of its content, and invited the defendant to respond by 09 March 2020 at the latest regarding the possible invocation of legitimate interest as a legal basis for the disputed data processing operations. The defendant submitted its reply by letter of 09 March 2020.
44. The Litigation Chamber then took note of the defendant's arguments regarding their legitimate interest and, following the Inspection Report and taking into account the defendant's argumentation, ruled that it would impose a fine of €50,000 on the basis of the violations of the GDPR which it had established.
45. In order to give the defendant the opportunity to defend themselves on the amount of the fine proposed by the Litigation Chamber, the latter decided to list the relevant infringements in its standard "*form for reaction against the proposed fine*", which was sent by e-mail of 7 April 2020, stating that the defendant was free to further complete this document with its reaction on the particular circumstances of the case, the proposed amount of the fine and the annual figures

submitted¹⁸ The defendant replied by e-mail of 28 April 2020¹⁹ with its arguments concerning the amount of the fine as well as new information concerning the turnover for the fiscal year 2019, which exceeds €10,000,000 EUR according to the latest forecast of the defendant.

46. In the meantime, the Litigation Chamber decided to submit a revised draft decision to the relevant authorities on 23 April 2020 in accordance with Article 60.5 of the GDPR. This international procedure ended on 08 May 2020, without any reasoned objection.

47. The Litigation Chamber then adjusted its decision to take into account the defendant's arguments regarding the fine²⁰.

2. Decision

2.1 Qualification of the controller and of the processing

48. The defendant is the controller for the processing of the data of the users of the social media platform "W" and for the processing of the non-users' contact details (names, phone numbers or e-mail addresses) and other information of the contacts²¹ that are stored on the servers of "W" *in response to the synchronization of the address book (phone or e-mail) of the users of the website.*

49. Under Article 4.7 GDPR the controller is indeed "*a natural or legal person, public authority, agency or any other body, whether a third party or not, to whom/which the personal data are disclosed. [...]*"

50. The Court of Justice has at various occasions explained that the concept of 'controller' should be defined broadly as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data, with the aim of ensuring the effective and complete protection of the persons concerned. In addition, the "concept does not necessarily refer to a single entity and may concern several actors

¹⁸ This invitation to submit limited submissions was sent by e-mail in the context where the Litigation Chamber was unable to accept this invitation to submit limited submissions by registered letter in accordance with Art. 95 LCA, and with the notification that if necessary the Litigation Chamber was prepared to grant longer periods to the defendant to lodge submissions (in the context of the Coronavirus outbreak). The defendant did indeed receive this e-mail and was able to respond within 3 weeks.

¹⁹ The defendant's arguments in this respect are discussed under the heading 'Decision regarding the penalty'.

²⁰ See the title "Decision concerning the penalty".

²¹ See the conclusion of the defendant, p. 11: "*This app wants consent to: See your Google contacts; Edit your Google contacts; Delete your Google Contacts; your contacts may include the names, phone numbers, addresses and other information about the people you know.*"

taking part in that processing, with each of them then being subject to the applicable data protection provisions.”²²

51. In accordance with the Opinion 1/2010 of the Group of 29 on the concepts of "controller" and "processor", the Litigation Chamber assesses the role and status of controller *in practice*.²³
52. In this case, the defendant is responsible for storing the contact details of the website users, as the defendant has determined the means and purposes of the processing (sending invitation e-mails).²⁴ As for the means and conditions for the processing, for example, the retention period of contact details is decided by the defendant under Article 11 of its privacy policy. This period is 3 months after the account closure of the user, or immediate erasure when the website user deselects "*Contact Sync*".²⁵
53. The defendant is also in this case the controller of personal data consisting of sending invitation e-mails in the name and on behalf of "W" to contacts of current users.
54. However, the transfer to the recipients of the invitation e-mails and the processing of personal data in the message itself is not covered by the GDPR to the extent that the exception "household exemption" applies, i.e. in the case of a purely personal or household activity within the meaning of article 2.2 of the GDPR.
55. The defendant himself cannot invoke this exceptional "household exemption", as clarified in recital 18 of the GDPR: "This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities." The defendant is responsible for sending invitation e-mails even though the user of the website can invoke the household exemption regarding the processing of personal data related to him.

²² See e.g. CJEU, C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388, paras 27-29.

²³ See Working Party 29, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169), as illustrated by the Belgian DPA in a note " Overview of the concepts of controller/processor in the light of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data (GDPR) and some specific applications for professions such as lawyers; see also CPVP, Decision of 9 November 2008 regarding the control and recommendation procedure regarding SWIFT, p. 5.

²⁴ See Opinion 5/2009 of Working Party 29 on online social networking, June 12, 2009 (WP163), p. 5: "*Providers of social network services are data controllers within the meaning of the Data Protection Directive. They provide the means for the processing of user data and provide all the basic services related to user management (eg, opening and deleting accounts)*".

²⁵ Privacy policy dated 02-15-2019 –annex 5 to the inspection report.

56. The defendant does not contest that the GDPR applies to the processing operations at stake and does not invoke the household exception.²⁶

2.2 Clarification with regard to the household exemption and the concept of "personal communication".

57. The defendant states that he considers the invitation e-mails as a "*personal communication*". In his conclusion and during the hearing, the defendant explained that this defense has nothing to do with the exception "*household exemption*" and that he never claimed that the GDPR would not apply. According to the defendant, the concept of "*personal communication*" merely refers to the fact that it is not a marketing message within the meaning of Article 13.2 of the ePrivacy Directive according to the criteria defined by Working Party 29 in the Opinion 5/2009 on online social networking.

58. The defendant therefore does not contest the application of the GDPR and that he is the controller, as regards sending out invitation e-mails.²⁷

59. In addition, the Litigation Chamber finds that if the recipients of the invitation e-mail from the online social platform are predetermined (e.g. pre-ticked), the user of the website in question has no control over an important aspect (indicating the recipients) of the purposes of the processing. The pre-ticking of recipients by the defendant is thus an additional element for the defendant to be regarded as a controller.

60. Finally, it is therefore established that the defendant is responsible for the processing of personal information of the users of the website "*W*", both in terms of storage of this data and as regards sending an invitation e-mail.

²⁶ Conclusion defendant, p. 22.

²⁷See on this also Art 29 Working Party 29 29 , Opinion 5/2009 on online social networking (p.11) stating that if the recipients of an invitation e-mail are pre-determined (e.g., ticked in advance) through the online social platform, the message cannot be considered a "personal communication". It is then a commercial message for the benefit of the social media network in accordance with Article 13.2 of the ePrivacy Directive (Groep 29, Opinion 05/2009 on social networks, 12 June 2009 (WP 163), p. 11.).

2.3 The legal basis for processing the contact details of users and non-users of the website "W"

61. As data controller in the context of the "Invite a friend" feature, the defendant must ensure that this processing complies with the principles of data processing and is legitimate in the sense that the process rests on a proper legal basis (art. 5 and 6 GDPR).
62. The processing concerns personal data of users and non-users of the website "W", and is twofold: storing the contact details on the defendant's servers and sending invitation e-mails.
63. The defendant invokes that the procedure elaborated on the website "W" ensures that he obtains free, specific, informed and unambiguous consent from the user of the website, in accordance with the requirements of articles 4.11, 6.1 and 7 of the GDPR with regard to the "Invite a friend" feature (conclusion defendant, p. 19).
64. In particular, the defendant raises that the consent of the recipient of the message is not required, neither to store their contact details on the servers of the website, or to send an invitation e-mail, and this because the user of the website has given consent to import his address book:

"First and foremost it should be noted that the import of contact details of the contacts is a processing of personal data that is part of the purpose of the "invite a friend" feature. As explained above, Y has processed for this purpose personal data contained in the address book of a user who has given his consent. Y can therefore invoke a valid legal basis for the import of the personal data of these contacts." (conclusion defendant, p. 21)

65. The defendant reiterated this argument during the hearing and has also made clear that he has no other legal basis he wishes to invoke.
66. The defendant also refers to other online services where users can "upload" their address book (Gmail, Hotmail, Whatsapp and Messenger) and to operating systems (such as iOS, Android and Windows) where users upload their address book and photos:

"If the Inspection Service seeks show that whenever a service user uploads personal data relating to people he knows, the company proposing this service, must obtain the consent of these people, this would undermine the operation of online communication in general. Such a position would not only apply to "invite a friend" features such as Y and other online social networking sites, but also (i) messaging services such as Gmail, Hotmail, Whatsapp and Messenger, where users upload their address book, on (ii) operating systems such as iOS,

*Android and Windows, where users upload their address book and photos, and on (iii) other services such as booking services and aircraft check-in services, where users can upload personal data of people they know, etc. "*²⁸

3. Motivation and decision regarding the merits of the case

3.1 The processing of personal data of non-users

3.1.1 No valid consent

67. The Litigation Chamber does not follow the defendant in his statement that the user of the social media website may give his own consent to import third party personal data from third parties into his address book, with a view to sending an invitation e-mail.

68. Under the GDPR, only the data subject whose personal data are being processed can give valid consent to the processing of this data, except for cases of parental consent (Art. 8.1 GDPR) or any legal mandate.²⁹ In the hypothesis that data from a third party are used, this third party must give consent in accordance with the requirements laid down in Article 7 and Article 4.11 of the GDPR, as interpreted by the Group of 29.³⁰ No such consent is given here. In addition, this consent can *de facto* solely be given by existing members of "W", if and to the extent - at the time they join the platform - they would have consented to the use of their personal data in accordance with the terms of the GDPR.

69. In this context, the Litigation Chamber also points to a study by the Dutch Data Protection Authority on Whatsapp, dating from before the entry into force of the GDPR. In the context of the mobile application Whatsapp, this authority ruled that the user of social media cannot give valid consent in the name and on behalf of a non-user of the social media platform: *"Whatsapp users cannot give (unambiguous) consent on behalf of the non-users in their address book for a processing by WhatsApp of their contact details, without being authorized by the non-users involved. Only the non-users involved (or their legal representatives) can give such consent. Since WhatsApp does not obtain unambiguous consent from non-users in the address book of Whatsapp*

²⁸ Conclusion defendant, p. 22, see also letter defendant 9 March 2020.

²⁹For an application of these principles, see for example the letter from the Working Party 29 dated October 20, 2017 to "Sinc.ME", footnote 2, available via the following webpage : https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwim5d6nlr_IAhUQyKQKHVW1BCAQFjAAegQIARAC&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fjust%2Fdocument.cfm%3Fdoc_id%3D47966&usq=AOvVaw2bxnDXC8XXENQ-UdNiNDLs.

³⁰Working Party 29 Guidelines for consent under Regulation 2016/679 (WP 259 rev01), April 10, 2019.

users for the processing of their personal data but still carries out this processing, and WhatsApp also has no basis for this data processing, WhatsApp acts in breach of Article 8 of the (Dutch) Data Protection Act ^{31, 32}.

3.1.2 Possibility to invoke a legitimate interest

70. In this case, no other legal basis than the "*consent*" is invoked by the defendant. The defendant invokes a "*legitimate*" interest by way of subordinate claim in its answer to the questions raised by the Litigation Chamber after the reasoned and relevant objection raised by the Netherlands. The Litigation Chamber therefore examines whether the contested processing of personal data of non-users has a legal basis under Article 6 GDPR, and whether the processing is therefore "*lawful*" or not within the meaning of Article 5.1 GDPR.
71. In the absence of any possibility to request consent regarding the processing of personal data of non-users, the Litigation Chamber examined to what extent the social media platform "*W*" could process the data of third party non-users based on its legitimate interest (art. 6.1.f) of the GDPR, with a view to precisely defined purposes, as explained below.
72. The Litigation Chamber understands that the website "*W*" has an interest to process third party non-users' personal data in order to encourage an increase in the number of members of the platform.
73. In this case, the data of third party non-users are not only processed for the purpose of identifying members of the website "*W*". The contact details (including third party non-users) are potentially kept three months by the website after the user has closed a "*W account*".³³
74. The website "*W*" also processes potentially more data than necessary to send an invitation e-mail as the concerned types of data are not defined by the website itself in a limitative way (ex. names, phone numbers and e-mail addresses): on the contrary, the processed data include potentially other types of data determined by third party providers of information society services, i.e. "*other*

³¹Article 8 of the former Data Protection Act implemented article 7 of the Data Protection Directive and equals article 6 GDPR.

³²Executive Protection of personal data, Investigation of the processing of personal data within the mobile WhatsApp application by WhatsApp Inc. dated January 15, 2013, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2013-whatsapp-cbp-definitieve-bevindingen-nl.pdf, p. 32. Decision of the CBP, the legal predecessor of the Dutch Autoriteit Persoonsgegevens.

³³ Letter from the defendant to the Inspection Service dated 14 June 2019.

information as illustrated on the permission screen of the provider, about importing your contacts on our servers".³⁴

75. Article 6.1.f of the GDPR states that the legal ground can be used in so far " *the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"

76. The case law of the Court of Justice of the European Union requires that in order to invoke Article 6.1.f) AVG a controller must fulfil "*three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence*".³⁵

77. In other words, the controller must demonstrate that:

- 1) The interests pursued by the processing, can be recognized as *legitimate* ("purpose test");
- 2) The intended processing is *necessary* for the purposes of the intended processing ("necessity test"), and
- 3) The *balancing* of these interests against the fundamental rights and freedoms of the persons concerned by the data protection weighs to the favour of the controller or of a third party ("balancing test").

➤ **Purpose test**

78. The Court of Justice clarifies that the legitimate interests "*must be present and effective as at the date of the data processing and must not be hypothetical at that date.*"³⁶

79. The Litigation Chamber also refers to the recent Guidelines 3/2019 on processing of personal data through video devices³⁷. In these guidelines the EDPB repeats that the controllers or third parties could pursue legitimate interests of a varied nature, such as legal, economic and immaterial

³⁴ Conclusion of the defendant, p 11, and a letter of the defendant to the Inspection Service dated 14 June 2019.

³⁵ CJEU, 4 May 2017, C-13/16, Rīgas, ECLI:EU:C:2017:336, para 28, ECLI:EU:C:2019:1064, and 11 December 2019, C-708/18, Asociația de Proprietari bloc M5A-ScaraA "M5A-ScaraA", para 40.

³⁶ CJEU, 11 December 2019, C-708/18, TK t/ Asociația de Proprietari bloc M5A-ScaraA, para 44.

³⁷ EDPB, "Guidelines 3/2019 on processing of personal data through video devices", 29 January 2020, nr. 18.

interests.³⁸ In this context, the EDPB also refers to the ruling of the Court of Justice that “*there is no doubt that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest*”.³⁹

80. Based on the Court’s case law and the guidance of the EDPB, the Litigation Chamber takes the view that the legal ground of legitimate interest potentially includes a wide range of interests, provided that these interests are sufficiently specific. In the context of the present case, the Litigation Chamber does not need take a position on the question whether, as such, an economic interest could qualify as a legitimate interest under Article 6.1.f, GDPR.

81. *In the present case* the defendant states that “*The objective of the W platform exists in essence in allowing users to connect which each other and to have interesting conversations and exchanges with other users*”, and that

- *Y, as controller has an interest to offer the users a possibility to find contacts that are already user and/or contacts that are not yet users and invite them to become members;*
- *The user of W, as a third party or as a controller using the platform under the household exception (recital 18 GDPR) has an interest in finding and inviting persons he or she knows in order to easier extend his network.”⁴⁰*

82. The defendant also claims that the development of the “*invite a friend*” feature was driven by the fact that certain users asked to have an easy way to find or invite persons they know and that the experience on the social platform “*W*” becomes more pleasant by this “*invite a friend*” feature. The defendant underlines that this interest is a real and present interest that is neither vague nor speculative.

83. The Litigation Chamber rules that the defendant – on the basis of these facts and arguments – sufficiently shows the existence of a legitimate interest, that this interest is sufficiently specific, as follows from the detailed submissions of the controller.

³⁸ The guidelines refer to Opinion 06/2014 of the Working Party 29 on notion of “legitimate interest of the data controller” (WP217).

³⁹ Arrest Rigas, C-13/16, para 29.

⁴⁰ Letter defendant, 9 March 2020, p. 4.

➤ **The necessity test**

84. The Court of Justice clarifies that the test of necessity requires to ascertain *"that the legitimate data processing interests pursued [...] cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter."*⁴¹
85. The Court of Justice also ruled that the condition of necessity should be assessed in connection with the principle of data minimisation as laid down in article 5.1.c), GDPR.⁴²
86. The defendant claims that the "W" platform only processes elementary contact details of the contacts of its users.⁴³ It appears from the facts of the case that the defendant retains the personal data in principle for a period of three months, unless the user of the platform decides to end the synchronization of his contacts.
87. The Litigation Chamber rules that the collection of these contact details – by users and by non-users of the website – would only comply with the criterion of necessity, in so far as these details are deleted immediately after their initial use.
88. The Litigation Chamber decides in connection to non-users that it would be possible for the social media platform "W" to base itself on legitimate interest, however solely to identify existing members of the "W" platform, in order to help the users to identify their contacts that are already member of "W" and, hence, consented to use the messaging feature of the de website "W" as communication tool.
89. It is in this context relevant that these members have given their unambiguous consent to "W" in order to collect their mobile phone number or their email and to use for this purpose. In addition, "W" should implement the appropriate technical and organisational measures in order to comply with the requirements of data protection by design and by default under article 25 GDPR.
90. The Litigation Chamber refers in this context also to the Opinion 5/2009 of Working Party 29 on online social networking which states that social media networks have no other basis for processing data of non-users than the legitimate interest, and that it is not possible to invoke this basis to retrieve contact details of non-members from uploaded address books and to use them

⁴¹ TK t/ Asociația de Proprietari bloc M5A-ScaraA Rigas, para 47.

⁴² Ibid., para 48.

⁴³ Letter defendant to Litigation Chamber, 9 March 2020, p. 6.

for the creation of new social media profiles: *"Many social network services allow their members to give information about others, such as adding a name to a picture, assigning ratings to people, drawing up lists of people who want to meet or have met members. Through these tags non-members can also be identified. However, the processing of such data about non-members by a social networking service is only allowed if one of the criteria in Article 7 of the Data Protection Directive [now Article 6.1.f GDPR "legitimate interest"] is met. There is no legal basis for creating ready-made profiles of non-members by collecting data provided independently by members, including relationship data derived from uploaded address books."*⁴⁴

91. This opinion is still relevant in principle, since the legal basis of legitimate interest has not been substantially modified since the entry into force of the GDPR. The defendant claims that he does not create profiles, but only sends invitation emails to non-members on the basis of contact details. However, this does not make the sending of those emails necessary for the purpose pursued.

92. The Working Party 29 has refined this opinion and the general interest of social media networks defined in the context of invitation e-mails, given the fundamental rights and freedoms of third party non-users. The Working Party 29 explained in its opinion regarding the notion of *"legitimate interest"*, the limitations of the legitimate interest regarding third party contact details by way of example:⁴⁵

"Example 25: Access to mobile phone numbers of users and non-users of an app: 'compare and forget'

"Personal data of individuals are processed to check whether they had already granted unambiguous consent in the past (i.e., 'compare and forget' as a safeguard).

An application developer is required to have the data subjects' unambiguous consent for processing their personal data: for example, the app developer wishes to access and collect the entire electronic address book of users of the app, including the mobile phone numbers of contacts that are not using the app. To be able to do this, it may first have to assess whether the holders of the mobile phone numbers in the address books of users of the app have granted their unambiguous consent (under Article 7(a)) for their data to be processed. For this limited initial processing (i.e., short-term read access to the full address book of a user of the app), the app developer may rely on Article 7(f) as a legal ground, subject to safeguards. These safeguards should include technical and organisational measures to ensure that the company only uses this access to help the user identify which of his contact persons are already users, and which therefore

⁴⁴Opinion 5/2009 of the Working Party 29 on online social networking (WP163), p. 9.

⁴⁵Opinion 6/2014 of the Working Party 29 on the notion of "legitimate interest of the data controller" (WP217).

had already granted unambiguous consent in the past to the company to collect and process phone numbers for this purpose. The mobile phone numbers of non-users may only be collected and used for the strictly limited objective of verifying whether they have granted their unambiguous consent for their data to be processed, and they should be immediately deleted thereafter".⁴⁶

93. In summary, the Working Party 29 is of the opinion that, in the circumstances described in the example above, third party contact details of non-users should only be used to check whether or not they already a member of the website, and therefore already have given their consent to use their contact details in order to communicate through the relevant website. As said, the Litigation Chamber bases its decision also on this consideration of the Working Party 29 and finds that the storage of contact details of non-users of the social media Y is only strictly necessary in the context of a "*compare and forget*" action under certain restrictive and protective safeguards.
94. The Litigation Chamber observes, however, that the retention period for these contact detail is not limited to what is strictly necessary to identify existing contacts. Moreover, the website "*W*" also processes potentially more data than necessary to send an invitation e-mail as the concerned types of data are not defined by the website itself in a limitative way (ex. names, phone numbers and e-mail addresses): on the contrary, the processed data include potentially other types of data determined by third party information society service providers, i.e. "*other information as illustrated on the permission screen of the provider, about importing your contacts on our servers*".⁴⁷
95. For the above mentioned reasons and circumstances, the Litigation Chamber finds that the storage of contact details of non-users of the social media Y is only strictly necessary in the context of a "*compare and forget*" action under certain restrictive and protective safeguards. These safeguards are not met.

➤ **The balancing test**

96. The Court of Justice clarifies that "*the assessment of that condition necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the*

⁴⁶ Zie in dezelfde zin, College bescherming persoonsgegevens, Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie WhatsApp door WhatsApp Inc. dd. 15 januari 2013, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2013-whatsapp-cbp-definitieve-bevindingen-nl.pdf, p. 32.

⁴⁷ Conclusion of the defendant, p 11, and a letter of the defendant to the Inspection Service dated 14 June 2019 - document 12 of the defendant.

particular case in question, and in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter."⁴⁸

97. The criterion relating to the seriousness of the infringement of the data subject's rights and freedoms is an essential component of the weighing or balancing exercise under article 7.1.f GDPR on a case-by-case basis.⁴⁹ In this context, the Court of Justice requires taking "*into account, inter alia, of the nature of the personal data at issue, in particular of the potentially sensitive nature of those data, and of the nature and specific methods of processing the data at issue, in particular of the number of persons having access to those data and the methods of accessing them.*"⁵⁰
98. The Court underlines that "*the data subject's reasonable expectations that his or her personal data will not be processed when, in the circumstance of the case, that person cannot reasonably expect further processing of those data, are also relevant for the purposes of the balancing exercise.*"⁵¹. The Litigation Chamber refers in this context also to Recital 47 of the GDPR which states the importance whether "*a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.*"
99. The defendant refers in connection with the seriousness of the breach to the following specific circumstances: "*The nature of the personal data processed by Y in the context of its 'invite a friend' feature was not excessive. Y has never processed sensitive data, only the absolute minimum of personal data (i.e. elementary contact details) with one goal, namely sending of invitation emails on request and in name of the user of the W platform*".⁵² The Litigation Chamber observes, again, that the retention period for these contact detail is not limited to what is strictly necessary to identify existing contacts. Moreover, the defendant does not define the processed contact data in a restrictive manner and also refers to any "*other information as clarified on the permission screen of the e-mail provider about importing your contacts on our servers*".⁵³.
100. The defendant refers, as concerns the reasonable expectations of the data subject, to services of online email providers such as Google, or services of providers of operating systems such as Android, iOS and Windows, or providers of social networks such as LinkedIn⁵⁴. The Litigation Chamber discusses the relevance of practices of these other providers in Section 3.1.3 below and

⁴⁸ Asociația de Proprietari bloc M5A-ScaraA "M5A-ScaraA, para 52.

⁴⁹ Ibid, para 56.

⁵⁰ Ibid, para 57.

⁵¹ Ibid., para 58.

⁵² Letter to the Litigation Chamber, 9 March 2020, p. 6.

⁵³ Conclusion of the defendant, p 11, and a letter of the defendant to the Inspection Service dated 14 June 2019.

⁵⁴ Letter to the Litigation Chamber, 9 March 2020, p. 5.

takes the view that the arguments relating to these practices fall outside the scope of the present procedure.

101. The Litigation Chamber decides in view of the above that in the present case the third condition of article 6.1, f) AVG and the case law of the Court of Justice is not fulfilled.

➤ **Conclusion**

102. The defendant could not in a legally valid manner base itself on "*legitimate interest*" as ground for the (further) processing of the personal data for direct marketing. In conclusion, the defendant infringes Article 6.1, f) GDPR.

103. Moreover, in this case, the Litigation Chamber decides that legitimate interest can only be used as legal ground for the processing of personal data of non-users with the aim of a "*compare & forget*" action, in order to select existing users amongst the contact details and to send possible invitation emails only to existing customers.

104. The Litigation Chamber decides more specifically in this case that the processing should be limited to the personal data which are strictly necessary for the purposes of "*invitation to the website*" and to the extent it is technically impossible to distinguish in the address book between members and non-members, without a minimal data processing. In addition, the defendant should in accordance with article 32 GDPR implement the appropriate technical and organizational measures to protect the processing of these data in a proper manner. Only under these conditions, the processing could be based on the legitimate interest of the defendant.

105. The Litigation Chamber takes into account that the user of the website "*W*" is free to send invitations through other channels (such as social media websites or e-mail providers) which are already used by the third party.

3.1.3 Defence regarding the processing of data of third persons by other information society service providers

106. The defendant compares its practices with the processing of third parties data by services such as "Whatsapp" and "Gmail", "Windows", "Linkedin".⁵⁵ The defendant states for instance that data subjects may reasonably expect that their contact details will be used by several on line service providers, because – according to the defendant it is "common practice" that "an individual stores contacts details in its contact list, in order to simplify communications"⁵⁶.
107. The Litigation Chamber finds that the defence regarding the processing of personal data of third persons does not hold relevance for the reasons stated below.
108. Firstly, practices of other service providers are outside of the scope of this case.
109. Secondly, the requirement of a proper legal basis for the processing of data of non-users applies to all service providers, including those referred to by the defendant in its submissions.
110. Thirdly, these service providers may not process personal data of third parties in a manner that would affect their rights and freedoms, whatever the legal basis for the processing might be. As the Working Party 29 clearly explained in the context of the right of portability, information society service providers or telecommunications service providers should not prejudice the rights and freedoms of non-users of their services, if a user gives his consent to the storing of personal data of non-users on their servers.⁵⁷ In the context of the transfer of personal data, the Working Party 29 reiterated the inadequacy of the user consent to process data of non-users: there must be a different legal basis, and the legitimate interest of the service provider appears to be the most appropriate basis⁵⁸.
111. The Litigation Chamber considers that these views of the Working Party 29 support the earlier regarding the infringement - in this case - of the GDPR. In summary, the unlawfulness of the data

⁵⁵ Letter of the defendant to the Litigation Chamber, 9 March 2020, p. 5.

⁵⁶ Ibid., p. 5.

⁵⁷ Working Party 29, "Guidelines on the Right to data portability", April 5, 2017, p. 5-6: " *'A person who takes the initiative to send his/her data to another controller, authorizes the new controller to process the operating data or concludes a contract with that data controller. When the data set also includes personal data of a third party, another legal basis has to be found for processing. [...] For example, at a webmail a service can be created with list of contacts, friends, acquaintances, relatives and the wider environment of the individual. [...] Therefore, to avoid any breaches of third parties, the processing of such personal data by another controller is permitted only when the data remain under the exclusive control of the requesting user and managed only for purely personal or household activities. A receiving "new" data controller (to whom the data can be transmitted at the request of the user) may use the transmitted data to third parties not use for their own purposes, such as to offer those other third parties involved marketing products and services to imagine [...] Otherwise such processing in all probability is illegal and unfair, especially if the third parties were not informed of their rights as stakeholders cannot exercise their rights "*

⁵⁸ Ibid.

processing of the website "W" is due to the fact that this website processed data of non-members without a proper legal basis, to the extent that this processing was not limited to a "*compare and forget*" action as set out above.

3.1.4 Personal data of non-users used to send invitation e-mails

112. The Litigation Chamber considers that storing contact details of non-users of a website in order to send an invitation e-mail is only allowed in the context of a "*compare and forget*" action, as set out above. Therefore it is only possible to send invitation e-mails to existing members via the website "W". The Litigation Chamber will therefore only discuss the existence of a legal basis with regard to sending invitation e-mails to non-users in the remainder of this decision.
113. As previously mentioned, the defendant stated that the invitation e-mails are a "*personal communication*" in respect of the user of the website "W" so that it does not require a separate legal basis for sending this message. However, the defendant, stated in his conclusion and confirmed at the hearing that he does not intend to invoke the exception "*processing in the course of a household activity*" from Recital 18 of the GDPR.⁵⁹
114. By "*personal communication*", the defendant means that these invitation e-mails do not constitute a marketing message, except that advertising messages by e-mail - without exception - can only be sent after prior permission (see Article 13.2 of the ePrivacy Directive⁶⁰ and its implementation in Article VI.110 § 2 of the Code of Economic law).⁶¹
115. In its Opinion 5/2009 on online social networking⁶², the Working Party 29 outlines under which conditions invitation messages sent via a social media platform do not constitute an online advertising message for the platform:

⁵⁹See above under heading 2.1 Qualification of the data controller and of the litigious processing.

⁶⁰ "*Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.*"

⁶¹Article VI.110 § 2 of the Code of Economic Law provides: "*Subject to Article XII.13 the use of other techniques for transmitting unsolicited communications for purposes of direct marketing referred to in paragraph 1 is permitted if the addressee, natural or legal person, here evidently not objected or, in respect of direct marketing to subscribers, provided it is in compliance with the provisions in articles VI.111 to VI.115.*"

⁶²Opinion 5/2009 on online social networking (WP163).

"Some social networking services allow their users to send invitations to third parties. The ban on the use of e-mail for direct marketing does not apply to personal communications. The exemption for personal communication only applies if the social networking service meets the following conditions:

- *there is no pressure exerted on the transmitter or receiver;*
- *the provider should not choose the recipient of the message (i.e. the practice by some SNS to send invitations indiscriminately to the entire address book of a user is not allowed);*
- *the identity of the user sending the message should be clearly indicated;*
- *the user sending the message must be aware of the full content of the message to be sent on his behalf.* ⁶³

116. The defendant refers to implementing these four conditions⁶⁴, and therefore believes he can send these messages without prior consent.

117. The fact that sending marketing e-mails is partly regulated by the ePrivacy Directive does not affect the competence of the Litigation Chamber to supervise the application of the GDPR with regard to the consent requirement or conditions for invoking the legitimate interest.⁶⁵

118. In this context, the Litigation Chamber decided that the social media network "*W*" should not, basically, request consent to send e-mail messages that users send to other users if the four conditions set out in the Opinion social media are met, subject to compliance with all other GDPR principles such as Article 25 (data protection by design and by default).

119. In that case, "*W*" can invoke its legitimate interest, including for storing the data on its servers, provided that the data of non-members are immediately deleted as soon as it appears that the user has not selected the recipient for the purpose of sending an invitation e-mail.⁶⁶

120. However, the Litigation Chamber considers that in respect of the strict GDPR rules with regard to the consent, also applicable in the context of the ePrivacy Directive, leave no room for such tolerance, and that the legal basis "*legitimate interest*" should be interpreted restrictively to the extent that data of third parties are involved.⁶⁷

⁶³Ibid., P. 11.

⁶⁴ Conclusion of the defendant, p. 23.

⁶⁵As explained by the EDPB in its advice on the Interplay between ePrivacy and GDPR: "Data Protection Authorities are competent to enforce the GDPR. The mere fact that a subset of the processing falls within the scope of the ePrivacy directive, does not limit the competence of data protection authorities under the GDPR."

⁶⁶See explanation on the limits of the legitimate interest under Title 3.1.2.a of this decision.

⁶⁷Working Party 29 Guidelines on consent under Regulation 2016/679 (WP 259 rev01), April 10, 2019, p. 9: "*With regard to the existing e-Privacy Directive, WP29 notes that references to the repealed Directive 95/46/EC should be read as references to the GDPR. This includes references to approval in the current Directive 2002/58/EC [...]. Article 95 GDPR has not imposed additional obligations regarding processing associated with the provision of publicly available electronic communications services in public communications networks in the Union, provided they are subject under the e-Privacy Directive to specific obligations with the*

121. Regarding the consent, Article 4, paragraph 11 with Article 7 of the GDPR defines states that the consent of the data subject means the following:

- free;
- specific;
- informed and;
- unambiguous indication of the data subject's wishes by which he or she, accepts through a statement or a clear affirmative action, the processing of personal data.

122. In addition, this consent must be obtained prior to the processing, as is apparent from the preamble of Article 6.1 of the GDPR: *the processing is only lawful if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes, [...]*"⁶⁸

123. Therefore, the Litigation Chamber believes that the GDPR does not allow sending e-mails to third parties with a view to obtaining their consent. This reasoning applies to the requirement of consent under the GDPR (requirement of a legal basis) and under the ePrivacy rules (requirement of "opt-in" for sending marketing messages)⁶⁹.

124. Furthermore, the Working Party 29 clearly states in its Opinion 5/2009 on online social networking regarding online social media that sending non-members of a social media website an invitation by e-mail to get access to their data is contrary to the prohibition in Article 13, paragraph 4 of the ePrivacy Directive:

*"To create ready-made profiles of non-members by collecting data which are provided independently by members, including relationship data inferred from uploaded address books, has no legal basis. Even though the social networking service would enable the non-user to inform about the existence of personal data relating to him, then a possible invitation by e-mail to join in order to gain access to the personal data is contrary to the prohibition in Article 13, paragraph 4 of the ePrivacy Directive on the sending of unsolicited electronic mail for direct marketing purposes."*⁷⁰

same objective. WP29 notes that the requirements for approval are not considered under the GDPR as an "additional duty", but as a precondition for lawful processing. Therefore, the requirements of the GDPR for obtaining valid consent apply in situations falling within the scope of the e-Privacy Directive."

⁶⁸ The Working Party 29 confirms that consent prior to the start of the processing must be achieved, Guidelines for consent under Regulation 2016/679, April 10, 2019, p. 20.

⁶⁹ Article 1(2) of the ePrivacy Directive reads as follows: "The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons." References to the repealed Directive 95/46/EC shall be construed as references to Regulation 2016/679 (GDPR).

⁷⁰Opinion 5/2009 on online social networking (WP 163), p. 9.

125. With regard to the legitimate interest, the Litigation Chamber rules that this legal basis does not allow sending such e-mails, given the impossibility for the third party to exercise control over its data in the context where those data were first uploaded to the website servers then used in the context of an invitation e-mail.

3.2 Storing personal data of existing users under the contacts of the person and sending invitation e-mails to existing users (contacts)

126. The defendant invokes the consent of the users for storing contact details of other users on its servers and for processing that data in the context of invitation e-mails.

127. However, the Litigation Chamber finds that the users' consent was not free to the extent that the first version of the website pre-selected the recipients of the invitation e-mails. This is the direct consequence of Recital 32 of the GDPR. The Court of Justice confirmed in *Planet49* that consent is not validly obtained if pre-ticked boxes are used:

"51. Article 2(h) of Directive 95/46 defines 'the data subject's consent' as being 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

52 Thus, as the Advocate General stated in point 60 of his Opinion, the requirement of an 'indication' of the data subject's wishes clearly points to active, rather than passive, behaviour. However, consent given in the form of a preselected tick in a checkbox does not imply active behaviour on the part of a website user.⁷¹

128. As long as the recipients of the e-mails were ticked in advance, the defendant could therefore not invoke the legal basis of "*consent*" with regard to the storing of the contact details of existing users, and sending invitation e-mails to existing users.

129. The Litigation Chamber considers that the processing in question is not necessarily unlawful within the meaning of Article 5.1 of the GDPR, and that the social media network "*W*" basically should not request an GDPR consent for sending e-mail messages from users to other users, to the extent such reports would fall under the legal basis "*necessary for the performance of a contract*" or "*legitimate interest*" (Article. 6.1.b or Article 6.1.f of the GDPR).

⁷¹CJEU, 1 October 2019, C-673/17, *Planet49*, paras 51-52.

130. In particular, the website may invoke its legitimate interest if the e-mails do not constitute a marketing message within the meaning of Article 13.2 of the ePrivacy Directive, provided that the defendant complies with the conditions set out by the Working Party 29 (such as for example not letting the website itself determine the recipients).
131. In this case, the Litigation Chamber notes that the recipients of the invitation e-mails were originally ticked beforehand.
132. Even if the defendant does not invoke these legal bases, the Litigation Chamber observes that ticking the recipients beforehand would be problematic in the context of the legal basis of "*legitimate interest*" or "*performance of a contract*": sending e-mails in bulk does not correspond to the principle of data minimisation (Article 5.1.c GDPR) and the principles of Article 25 GDPR (data protection by design and by default). It does not matter whether the website user had the option to deselect the pre-ticket recipients one by one in the previous version of the website.
133. Finally, since the defendant voluntarily removed the pre-ticked options - in response to the grievances of the Inspection Service in this respect -, the controller "*W*" is eligible to send such e-mails based on its legitimate interest in the name and on behalf of its users to other users.
134. As an alternative to the legitimate interest, the Litigation Chamber believes that the social media network "*W*" basically had not to ask GDPR consent to send e-mail messages from users to other users, as far as such messages by "*W*" could fall under the legal basis of "*necessary for the performance of a contract*" (art. 6.1.b of the GDPR). The possibility of invoking such a basis obviously depends on the definition of the service provided and the extent to which the persons concerned have been informed about it⁷². The Litigation Chamber does not have sufficient facts to judge the lawfulness of the processing under the legal basis of "*performance of a contract*", but decides that the processing could at least be carried out under the legal basis of "*legitimate interest*", and therefore was not unlawful after removal of the pre-selection of recipients of the invitation e-mails. Finally, the Litigation Chamber observes that the defendant should be transparent about the legal bases used for processing.

⁷² Zie EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.

3.3 The grievances of the Inspection Service with respect to the data protection officer

135. Furthermore the Litigation Chamber decides not to follow the grievances of the Inspection Service regarding the data protection officer, given the *prima facie* expertise of this person shown by the submitted resume, and the documents and the hearings show that this person duly has been involved in developing the "*invite a friend*" feature. In addition, at the hearing the defendant has sufficiently explained the role and position of the data protection officer.

3.4. The defence regarding the lack of concrete recommendations from the DPA

136. The defendant complains that the DPA did not propose concrete recommendations or comments regarding the "*invite*" feature in response to the letter of 12 October 2018⁷³ in which the DPA pointed out to the defendant the requirement to obtain a valid consent under the GDPR for the "*Invite a friend*" feature (p. 3 of the conclusion). The defendant gives the same accusation against the Inspection Service (conclusion, p. 5). As the defendant rightly points out (conclusion, p. 4), the Inspection Service did not propose a recommendation regarding the invitation functionality, and she chose to ask for information.

137. The task of the Inspection Service is to gather evidence regarding indications of practices that may give rise to an infringement of the fundamental principles of data protection (Article 63 and following of the DPA ACT). The Inspection Service is not responsible for providing customized advice regarding the investigated infringements. More generally: Under Articles 5.2 and 24 of the GDPR, the controller is subject to the principle of accountability. Accountability is a core feature of the GDPR. A controller cannot denounce his accountability by a claim that he did not receive sufficient guidance from a supervisory authority. Pursuant to Article 57.1.d) of the GDPR, any supervisory authority must promote the awareness of controllers and processors as regards their obligations under the GDPR. However, the GDPR and the DPA ACT let the DPA – including its Inspection Service - a large discretion as to whether or not ask the attention of a controller for a possible infringement.

⁷³ Answer to a letter of 3 July 2018.

3.5 Decision regarding the sanction

138. Following the inspection report and taking into account the arguments of the defendant, the Litigation Chamber has identified the following infringements of the GDPR:

1. The defendant has no legal basis for storing the personal data of non-users of the website "W" in its files and for further processing them with a view to sending an invitation e-mail: This constitutes an infringement of Articles 5 and 6 of the GDPR;
2. The defendant has no legal basis for sending invitation e-mails to existing users of the website during the period in which the recipients of the invitation e-mails were ticked beforehand: infringement of Article 5.1 in conjunction with 6.1.a), 7 and 4.11 of the GDPR.

3.5.1. Jurisdiction of the Litigation Chamber with regard to sanctions

139. Pursuant to Article 100 of the DPA ACT, the Litigation Chamber has jurisdiction to order that the processing is brought into line (Art. 100.9 DPA ACT) and to impose penalties (art. 100.2° DPA ACT). The Litigation Chamber is also empowered to impose administrative fines (Art. 100.13°, 101 and 102 DPA ACT) and to publish the decision on the website of the Data Protection Authority (Art. 100.16° DPA ACT). In determining the level of the fines, the Litigation Chamber must take into account the criteria outlined in Article 83 of the GDPR depending on the circumstances. In the present case, the Litigation Chamber considers the following circumstances which it considers sufficient to sustain the decision relating to the sanction:

- the nature, severity and duration of the infringement: this is a lack of legal basis, which is a serious infringement according to the Litigation Chamber, in particular as regards the right of non-members of the website "W" to keep control over their data and not to run the risks of data processing (Recital 75 GDPR);
- the intentional nature of the infringement: the defendant was aware of a problem with regard to the processing of personal data on the website since the first letter from the DPA of 12 October 2018.

3.5.2. The mitigating circumstances invoked

140. The defendant is in subordinate order of the opinion that the sanctions pronounced should take into account the following mitigating circumstances (conclusion, p. 42):

- The defendant has not been "*negligent*" and would have acted in good faith taking into account the Opinion 5/2009 of the Working Party 29 on online social networking. The Litigation Chamber states that the defendant cannot simply rely on an opinion from 2009, long before the establishment of the GDPR, which moreover - as described above - is not sufficiently clear. In addition, the controller could have kept abreast of the discussions on the use of social media sites of data from non-members, as shown in Opinion 06/2014 of the Working Party 29 on the notion "*legitimate interest*";
- Any possible infringements would not have caused any material damage: Here, the Litigation Chamber notes that the right to data protection is a fundamental right and that the subsistence of any material damage is not relevant in order for such a right to be infringed⁷⁴. The infringements in this particular cause a loss of control over the personal data of many individuals which is explicitly referred to in paragraph 75 of the GDPR as potential non-material damage;
- The defendant stopped using pre-ticked options. The defendant was aware of the infringement since 3 April 2019 (conclusion, p. 42) and has awaited receiving a second letter from the Inspection Service (May 2019) to stop this practice (conclusion of the defendant, p. 13). The Litigation Chamber believes that this infringement was intentional or at least caused by grave negligence, since it is clearly established in Recital 32 of the GDPR that a consent is not valid if the offered options are ticked in advance.⁷⁵ The defendant therefore had to know that the consent of the users of the website to process their data in order to send invitation e-mails was not valid as regards the selection of the recipients. In addition, a controller is supposed to know that a website user is not in a position to provide consent for the use of personal data of third persons.

141. In their reaction of 28 April 2020 entered on the form, the defendant developed additional arguments with regard to the penalty proposed by the Litigation Chamber.

142. The defendant argues that they were not negligent and that the alleged infringements did not constitute a clear breach of the GDPR, but rather "*a problem of interpretation in which regard even the supervisory authorities adopt different standpoints.*" The defendant wrongly deduced this from the fact that the Dutch authority had adopted⁷⁶ a relevant and reasoned objection. The

⁷⁴ Cour of Appeal, Brussels, 9 October 2019, "DPA v. Installé Marc" 2019/AR/1006.

⁷⁵ As clarified later in CJEU, 1 October 2019, C-673/17, Planet49, paras 51-52 (see above).

⁷⁶ As explained to the defendant in the context of the reopening of the debates on legitimate interest, the Netherlands in this case asked for more references to the case law of the Court of Justice as regards the analysis of the defendant's legitimate interest to send invitations to third parties who are not members of its social media platform, on the one hand, and disputed the relevance of references to a research report from 2013 concerning the legitimate interest of a social medium to send invitation emails, on the other hand.

Dutch authority did not object to this final decision, and all the authorities concerned have validated the reasoning set out above regarding the amount of the fine.

143. The Litigation Chamber agrees with the defendant that a discussion was possible on the extent to which the defendant could or could not invoke a legitimate interest to address third party non-users by means of an invitation e-mail.
144. However, the Litigation Chamber found that no discussion was possible and ruled that the legal basis invoked by the defendant was invalid: the existing users of a website cannot give permission on behalf of third party non-users⁷⁷. The defendant thus misapplied the legal basis "*consent*" (or exemption from consent), and it is in any case not permissible to invoke the legal basis "*legitimate interest*" a posteriori in order to justify⁷⁸ processing which has already started.
145. For the sake of clarity, the Litigation Chamber reminds the defendant that it did not invoke the "*legitimate interest*" basis (and did not examine its conditions of application) in its original privacy policy, nor later in the context of its arguments before the Litigation Chamber, despite a clear question from the Litigation Chamber in that respect at the hearing, and up to and including the reopening of the debates by the Litigation Chamber on that point. This constitutes a clear breach of their information obligations set out in Article 12-13 GDPR and the requirement under Article 5-6 GDPR to have an appropriate legal basis before data processing begins.
146. It is also beyond dispute that with regard to invitations sent to existing members of the social media platform "*W*", the defendant could not invoke the legal basis of "*consent*" whereby the addressees of the invitation e-mails were originally ticked in advance⁷⁹.
147. For this reason, the Litigation Chamber decides that the defendant has been negligent and deserves a fine as regards the sending of invitation emails both to members and to third party non-members of the social media platform "*W*", and that a fine is justified, even if there was a possible debate regarding the limits and conditions of the defendant's justified interest as regards the sending of invitation emails by social media to third party non-members. In view of the circumstances presented to it, the Litigation Chamber decides upon this question in this case.

⁷⁷ See reasoning under heading 3.3.1.

⁷⁸ See Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017, last revised and adopted on 10 April 2018, p. 27: "*It is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals. In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. **Because of the requirement to disclose the lawful basis which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.***" [bolding of the Litigation Chamber]

⁷⁹ See reasoning under heading 3.2.

148. In determining the amount of the fine, the Litigation Chamber shall take into account the circumstances invoked under 3.5.1 and 3.5.2 of this decision.
149. The Litigation Chamber also takes note of the fact that the defendant, according to the information provided in their response of 28 April 2020, stopped the sending of invitation emails as of 07 February 2020.
150. However, the Litigation Chamber did not require such a far-reaching measure and reopened the debates on legitimate interest in order to allow the defendant to properly carry out their assessment of the latter.
151. In the original draft decision, as submitted to the data protection authorities concerned in the context of the cooperation procedure provided for in Article 60.5 of the GDPR, the Litigation Chamber had ordered that the processing be brought into compliance with Articles 5 and 6 of the GDPR within 3 months of the date of this decision, by ensuring that the storage and processing of personal data for the purpose of sending invitation e-mails to third party non-members of the website be either discontinued or be founded on a legal basis (e.g. consent, legitimate interest). However, this intended order no longer has any *raison d'être* in view of the fact that the defendant - according to the statements made by their counsel in their response of 28 April 2020 - spontaneously stopped the sending of invitation emails as of 07 February 2020.
152. The fact that the defendant stopped sending invitation e-mails is a sign of goodwill, but does not alter the fact that the defendant was negligent in determining a legal basis, not only for the beginning of the data processing in question but also in the context of their reasoning submitted to the Litigation Chamber, despite the reopening of the debates by the latter. The fact that the defendant has stopped using pre-ticked options only has a positive impact on the legal basis of "*consent*" for the invitation e-mails sent to existing users, but not with regard to the third-party non-users of the website.
153. Nevertheless, it appears from the above there is a willingness by the defendant to devote attention to the GDPR in the development of the processing. This is important for determining the level of the sanction.
154. The Data Protection Authority considers that the annual turnover of the defendant from 2017 onwards (including for the financial year 2019, for which closure is still ongoing) will still exceed €10,000,000. The Litigation Chamber decided that when determining the amount of the fine that an amount of 0.5% of the annual turnover would be appropriate, and therefore set the amount of the fine at €50,000.

155. Given the importance of transparency in relation to the decision of the Litigation Chamber, this decision will be published on the website of the Data Protection Authority. Publication of the present decision is also in the interests of the development of the law and the consistent application of the GDPR in the European Union. However, it is not necessary for the defendant's identification data to be disclosed directly for that purpose.

FOR THESE REASONS,

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

to impose a fine of 50,000 Euro for processing personal data of non-members of the website "W" without an appropriate legal basis, as well as personal data of members, the latter during the period in which the recipients to such e-mails were ticked in advance.

Against this decision and based on art. 108, §1 of the Act of 3 December 2017, an appeal can be lodged within thirty days after service of the notice at the Marktenhof (Court of Appeal in Brussels) with the DPA as a defendant.

Hielke Hijmans,
President of the Litigation Chamber

Publication of May 28th 2020