Judgment

AMSTERDAM DISTRICT COURT

Private law division

Case number / docket number: C/13/683377 / HA ZA 20-468

Judgment of 15 March 2023

in the matter of

DATA PRIVACY STICHTING,
a foundation having its registered office in Amsterdam,
claimant,
represented by J.H. Lemstra LLM of Amsterdam,

versus

1. **FACEBOOK NETHERLANDS B.V.**,
a private company with limited liability [*B.V.*]
having its registered office in Amsterdam,
2. **META PLATFORMS INC.**, formerly FACEBOOK INC.
a legal entity incorporated and existing under foreign law
having its registered office in Menlo Park (California, United States),
3. **META PLATFORMS IRELAND LTD.**, formerly FACEBOOK IRELAND LTD.,
a legal entity incorporated and existing under foreign law
having its registered office in Dublin (Ireland),
defendants,
represented by G.H. Potjewijd LLM of Amsterdam.

The claimant will hereinafter be referred to as Stichting, whereas the defendants will once again, in line with the judgment rendered earlier in the procedural issue, hereinafter be referred to as Facebook Netherlands, Facebook Inc. and Facebook Ireland (collectively: Facebook et al.).

1. The course of the proceedings

1.1. The course of the proceedings appears from:
- the judgment in the procedural issue of 30 June 2021[1] (hereinafter the judgment in the procedural issue) and the procedural documents referred to therein:
- the statement of defence, with exhibits,
- the reply statement, with exhibits,
- the rejoinder, with exhibits,

[1] ECLI:NLRBAMS:2021:3307

- the record of the oral hearing, held on 8 November 2022, and the documents referred to therein,
- the letter from the attorney representing Facebook et al. of 13 December 2022, containing comments about the record of the oral hearing.

1.2. In conclusion a date was set for judgment to be rendered.

1.3. To the extent relevant to the decisions to be made, this judgment is rendered with due observance of the comments made in respect of the record of the oral hearing.

2. Overview of this judgment

The subject matter of this case

2.1. This case concerns a collective action (under old law[2]) brought by Stichting against Facebook et al. Stichting represents the interests of Dutch users of the Facebook service. The main issue in these proceedings is whether Facebook et al. have acted unlawfully when processing personal data of Dutch Facebook users in the period 1 April 2010 - 1 January 2020 (hereinafter also: the relevant period). Important in this respect is the fact that Facebook et al. not only processed personal data of users of the Facebook service to provide the social network, but also for advertising purposes.

The district court's decision in broad outline

2.2. The district court's view is that Facebook Ireland has acted unlawfully in the way in which it has handled the personal data of Dutch Facebook users. The district court has limited its decision to the actions of Facebook Ireland, because only that party is responsible for the processing of personal data of Dutch Facebook users.

2.3. The unlawful conduct among other things consist in the processing of personal data for advertising purposes without a legally valid basis. Personal data may be processed only, if there is a basis for doing so specified by law, such as, for example, consent. Facebook Ireland did not have such a basis in the relevant period. A legally valid basis was also lacking when processing special personal data (such as sexual orientation or religion). Indeed, special personal data were processed for advertising purposes without the required explicit consent. This concerned both personal data that users themselves provided to Facebook Ireland and special personal data obtained by Facebook Ireland by tracking the surfing behaviour of Facebook users outside the Facebook service.
Furthermore, Facebook Ireland did not sufficiently inform the Facebook users about the sharing of their personal data with a number of third parties identified in greater detail in the judgment. In that context, not only personal data of the Facebook users themselves were shared, but also personal data of their Facebook friends.

[2] Old law here refers to the right of class action in effect before 1 January 2020.

2.4. The way in which Facebook Ireland processed the personal data of Dutch Facebook users for advertising purposes during the relevant period not only violated privacy laws, but also constituted an unfair commercial practice. Inadequately informing the Facebook user as a consumer about the use of personal data for commercial purposes was misleading, for the average consumer could not make an informed decision about joining the Facebook service.

2.5. Facebook Ireland did not act unlawfully by placing cookies on third-party websites, because Facebook Ireland transferred, and was allowed to transfer, the obligation to inform users about the placement of cookies and to ask for consent to the relevant website operator. It has also not been found in the proceedings that Facebook Ireland was unjustly enriched. This is because there was insufficient evidence that the unauthorized processing of personal data for advertising purposes by Facebook Ireland resulted in an actual impairment of the Facebook user's assets.

2.6. The declaratory decisions requested by Stichting will be granted in part. To what extent individual Dutch Facebook users are entitled to damages based on the established unlawful conduct by Facebook Ireland is a question that is not at issue in these proceedings.

The structure of this judgment

2.7. This judgment is structured as follows:

3. The facts

3.1. For reasons of clarity, any established facts that relate to specific issues have in this judgment been mentioned in the examination of the issues concerned.

3.2. Facebook Netherlands, Facebook Ireland and Facebook Inc. form part of the Facebook group. This group provides a social network service (hereinafter also: the Facebook service). The Facebook service operates as a social media platform, allowing users to, among other things, share experiences and come into contact with information and people. Over 2.7 billion people worldwide use the Facebook service.
The user does not pay for using the Facebook service. The Facebook group's business model is based on revenue from the sale of ads, or personalized ads.

3.3. Facebook Inc. was incorporated on 4 February 2004 and is headquartered in the United States. Facebook Ireland is a subsidiary of Facebook Inc. and was incorporated on 6 October 2008. Facebook Ireland operates as a contracting party to provide the Facebook service to users in the Netherlands (and Europe). In addition, Facebook Ireland sells ads through a self-service advertising platform. Facebook Netherlands was incorporated on 25 November 2010. The (ultimate) parent company of Facebook Netherlands is Facebook Inc. Facebook Netherlands provides marketing and sales support services, related to the sale of ads, to the Facebook group. In that context, Facebook Netherlands is among other things engaged in providing advice on, and promoting the sale of, advertising space on the Facebook service and other advertising products.

3.4. Stichting is a collective claims foundation that was set up on 25 February 2019. One of its objects is to represent the interests of aggrieved persons residing in the Netherlands, who at any moment have been the victims of a breach of their privacy.

3.5. The Facebook service is a personalized service. This personalization extends to the content of what a user is shown. Personal data is used to achieve a personalized user experience.

3.6. When registering for the Facebook service, a user must agree to the Terms of Use. The Terms of Use state that Facebook Ireland is the contracting party for Facebook users in Europe. Between 2010 and 2020, those conditions were known by various and various versions were in force.

3.7. In addition, Facebook Ireland uses a Data Policy for the use of the Facebook service, which may be viewed on the website and in the app. Again, several versions of this policy existed between 2010 and 2020.

3.8. Towards the end of 2014, the Dutch Data Protection Authority (Dutch DPA), or its legal predecessor, the data protection regulator in the Netherlands, started an inquiry into the processing of personal data of data subjects in the Netherlands by the Facebook group. In a report dated 21 February 2017, published on 16 May 2017, the Dutch DPA reported its findings. In it, it concluded that the Facebook group was on several points acting in breach of the Personal Data Protection Act (Wbp), when providing information about the processing of personal data for advertising purposes. This report did not lead to any enforcement decisions by the regulator.

4. Applicable law

4.1. In the judgment in the procedural it was ruled that Dutch law applies to this case.

5. The claims brought by Stichting

5.1. Stichting requests the district court to rule, by provisionally enforceable judgment to the extent possible:

a. that Facebook Netherlands, Facebook Ireland and Facebook Inc., jointly and/or each of them individually, as from 1 April 2010 until 1 January 2020, or at least during the period specified in paragraph 156 of the summons with respect to each individual breach, or at least for a period to be determined by the Court in the proper administration of justice, has and/or have acted unlawfully towards Stichting's Members, because they:

   i) have violated the rights, or the privacy rights, of the Members, by in violation of the duties, or duties of disclosure, of sections 33 and 34 Wbp and/or articles 12, 13 and 14 of the General Data Protection Regulation[3] (GDPR):

      1. allowing, or at least enabling and facilitating, external developers to dispose of and/or have access to personal data of the Members and to subsequently process those personal data, without having informed the Members of this sufficiently clearly and in a timely manner; and/or
      2. allowing, or at least enabling and facilitating, Aleksandr Kogan and/or Global Science Research Ltd., and/or Cambridge Analytica Ltd., Cambridge Analytica LLC and SCLE Elections Ltd. to dispose of and/or have access to personal data of the Members and to subsequently process those personal data, without having informed the Members of this sufficiently clearly and in a timely manner; and/or
      3. using telephone numbers of the Members, provided for the purpose of two-factor authentication, with a view to placing targeted advertisements, whether on the desktop version of its platform or otherwise, without having informed the Members of this sufficiently clearly and in a timely manner; and/or
      4. failing to inform the Members, or at least failing to inform them sufficiently clearly and/or in a timely manner, about the 'integration partnership' programme and the related processing of the personal data regarding the Members;

      and/or

   ii) have violated the rights, or the privacy rights, of the Members by:

      1. violating the legal basis requirement under sections 6 and 8 of the Wbp and/or breaching article 5 (1) (a) and article 6 (1) of the GDPR, in each case by processing personal data of the Members, despite the fact that such processing could not be based on an adequate and legally valid basis for processing;
      2. violating the prohibition on processing special data under section 16 of the Wbp and/or article 9 (1) of the GDPR, by using, in particular, (but not exclusively) personal

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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, OJ 2016, L 119.

data concerning sexual life, religious beliefs and ethnicity, and the content of messages from the Members revealing such information, for advertising purposes;

3. violating the duty of disclosure and the requirement of consent of section 11.7a (1) of the Telecommunications Act (Tw), or at least corresponding provisions in national privacy laws in other member states, by not, or not clearly or adequately and/or not in a timely manner, informing the Members about the tracking of surfing behaviour and app use outside the Facebook service with the help of cookies and/or similar technology and about the use of the data thus obtained for advertising purposes;

and/or

iii) towards Stichting's Members has/have engaged in commercial practices that are unfair within the meaning of article 193b (1) of Book 6 DCC and/or misleading within the meaning of articles 193c, 193d and 193g of Book 6 DCC, by:

1. failing to inform the Members sufficiently clearly and/or in a timely manner about the collection and further processing of their (confidential) personal data with a view to generating revenue with such data, by sharing such personal data with third parties, or at least using such data for the benefit of third parties;
2. failing to inform the Members sufficiently clearly and/or in a timely manner about the scale of the collection of this (confidential) personal data, and the sharing thereof with third parties, or at least the use thereof for the benefit of third parties;
3. until at least August 2019 making the misleading representations to the Members that the Facebook service would be free and would always remain so, while the Members de facto paid for the Facebook service by handing over the relevant (confidential) personal data to Facebook et al;

b. that Facebook Netherlands, Facebook Ireland and Facebook Inc., jointly and/or each of them individually, as from 1 April 2010 until 1 January 2020, or at least during the period specified in paragraph 156 of the summons with respect to each individual breach, or at least for a period to be determined by the Court in the proper administration of justice, has and/or have acted unlawfully towards Stichting's Members, by, by way of the Members, also having processed the data of friends of the Members in the unlawful manner referred to in a.i.1., a.i.2., a.i.3., a.ii.1. and a.ii.3. above;

c. that Facebook Netherlands, Facebook Ireland and Facebook Inc., jointly and/or each of them individually, was and/or were unjustly enriched at the expense of the Members in the period as from 1 April 2010 to 1 January 2020, or at least in a period to be determined by the district court in the proper administration of justice;

d. and to order Facebook Netherlands, Facebook Ireland and Facebook Inc. jointly and severally to pay the legal costs incurred by Stichting, to be increased by subsequent costs and statutory interest on the legal and subsequent costs.

5.2. The word "Achterban" (Members) used in the claim is defined by Stichting - briefly put - as the users, or former users, of the Facebook service at any moment in the period 1 April 2010 - 1 January 2020 (and/or their legal guardians), insofar as they were residing in the Netherlands at the time of that use, were not acting in the conduct of a profession or business, and whose interests Stichting represents according to its objects clause contained in the articles of association and in respect of whom a breach of their Privacy (as referred to in the articles of Association) at any moment has occurred.

5.3. Facebook et al. put forward a defence and move that the claims be ruled inadmissible or be dismissed, and that Stichting be ordered to pay the costs of the proceedings.

5.4. The parties' contentions will be addressed below in the assessment of the case, to the extent relevant.

The district court's assessment

6. Which parties are (still) conducting a defence in these proceedings?

6.1. During the oral hearing, Stichting has argued that Facebook et al. only presented arguments in the rejoinder on behalf of Facebook Ireland, and that Facebook Netherlands and Facebook Inc. have therefore forfeited their right to oppose Stichting's contentions.

6.2. The district court does not agree with Stichting in this respect. Facebook et al. have put forward a defence in these proceedings on behalf of the three Facebook entities and in that connection submitted, inter alia, various procedural documents, including a rejoinder. One of Facebook et al.'s arguments is that only Facebook Ireland is the responsible party for the conduct at issue in these proceedings. In that light, it is true that Facebook et al. frequently mention Facebook Ireland in the rejoinder, because in their view that is the only relevant party. From that (of course) it cannot be deduced that the defence conducted by Facebook et al. in these proceedings is limited to a defence of Facebook Ireland. During the oral hearing it was confirmed on behalf of Facebook et al. that the defence in these proceedings was conducted on behalf of the three Facebook entities.

7. Does Stichting have a sufficient interest?

7.1. In extremis, Facebook et al. have argued that Stichting has insufficient interest in the claims it has brought. To this end, Facebook et al., briefly put, have argued the following. The possibility of harm having been suffered by the Members has not been argued convincingly by Stichting with respect to any of its claims. Stichting merely relies on an alleged loss of control over personal data, without making clear why that might constitute damage in a legal sense. A mere breach of a privacy right does not in itself lead to damage, nor does a privacy infringement automatically give rise to a claim for compensation for non-material damage. The nature and seriousness of the alleged violation of standards does not mean that any adverse consequences for the Members are so obvious that an offence against the person as referred to in article 106 of Book 6 DCC opening words and in (b) may be assumed.

Facebook et al. furthermore refer to the Opinion of 6 October 2022 of the Advocate General (A-G) with the Court of Justice of the European Union (CJEU) in the case UI/Österreichische Post[4]. That case concerns the interpretation of the concept of damage in article 82 of the GDPR. Facebook et al. have requested the court to stay its decision, if necessary, until the CJEU has given its ruling in the UI/Österreichische Post case.

7.2. Stichting has argued that it has a sufficient interest in its claims. To that end, it has inter alia argued the following. Privacy breaches can cause both material and non-material damage, thus creating the possibility of damage. In the previous Privacy Directive[5] and in the currently applicable GDPR, a broad concept of damage was used, in which it is also explicitly provided that an aggrieved

[4] Case C-300/21, ECLI:EU:C:2022:756.

[5] 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, OJ EU 1995, L 281.

party can claim compensation for non-material damage. The damage suffered by the Members as a result of the violation of privacy regulations in any case consists in a loss of control over personal data and/or the inability to exercise control. The Members have experienced more than just annoyance as a result of the ongoing violations of their data protection rights. The violation of provisions under privacy law can be qualified as an offence against the person as referred to in article 106 of book 6 opening words and (b). Such an offence entitles to compensation for non-material damage. According to Stichting, the case at issue in the UI/Österreichische Post case is not comparable to its class action against Facebook et al.

7.3. The court holds as follows.

7.4. Article 303 of book 3 DCC provides that, without sufficient interest, no one has a right of action. By "sufficient interest" is meant enough interest to justify proceedings. In principle, it may be assumed that a sufficient interest in an action exists. The court should exercise restraint in ruling that insufficient interest exists in a legal action. If a declaratory judgment is sought that liability exists for damage or that wrongful acts have been committed, the court must assume that the plaintiff has an interest in its claim if the possibility of damage exists.[6] This also applies, if an order for payment of damages or for a case to be referred to follow-up proceedings for the determination of damages is not also sought.

7.5. In these proceedings, Stichting seeks declaratory judgments that Facebook et al. have acted unlawfully and have been unjustly enriched. In essence, Stichting bases this claim on the complaint that Facebook et al. unlawfully processed personal data of the Members in the period 2010-2020. By having the requested declaratory decisions awarded, Stichting aims to ultimately obtain compensation for the Members.

7.6. Within the context of the question regarding Stichting's interest in its claims, the court has to assess whether there is a possibility of damage if one or more of the complaints made by Stichting are justified. For the purpose of answering the question whether there is a possibility of damage, it is not necessary to follow the ruling of the CJEU on the interpretation of the concept of damage in article 82 of the GDPR. Even if the interpretation of the concept of non-material damage according to the current state of case law is assumed (and more specifically the requirements imposed on the concept of 'offence against the person in a different way', as referred to in article 106 of Book 6 DCC), in the District Court's opinion the possibility of damage as a result of the complaints made by Stichting is plausible in this case. To that end, the following reasons are relevant.

7.7. In a collective action such as the present one, inter alia with respect to the issue of interest, a certain abstract examination is appropriate. This means that the question of whether the possibility of damage is plausible must be answered in a general sense, that is, that the individual circumstances of Stichting's Members must be ignored. It is true that it cannot be said that the privacy violations and unfair commercial practices alleged by Stichting will automatically lead to damage, but on the other hand, the possibility of damage is not excluded either in advance and in a general sense. Indeed, it is quite conceivable that under certain circumstances the privacy violations alleged by Stichting (may) have resulted in material and/or non-material damage. That possibility is sufficient in the context of this class action to conclude that the possibility of damage is plausible. Whether and when such circumstances actually occur does not need to be answered in the context of these proceedings.

7.8. Since the possibility of harm is plausible, Stichting has a sufficient interest in the requested rulings.

---

[6] Supreme Court 27 March 2015. ECLI:NL:HR:2015:760

8. The reliance on the statute of limitations

8.1. Facebook et al. have argued that Stichting's claims, insofar as they relate to events prior to 30 December 2014, have become time-barred pursuant to article 310 of book 3 DCC. To that end, Facebook et al. have argued the following. Five years before 30 December 2019, the time of Stichting's filing of these proceedings, Stichting and the Members were already reasonably aware of, or at least should have been aware of, the breaches alleged by Stichting, the alleged damage and the person liable for them, for the Facebook users were already aware before 30 December 2014 of the data processing transactions relevant to Stichting's claims. Before that date, a widespread discussion had already been started in the media about the processing of personal data for the purpose of personalized advertising. Reference is made to a selection of news items that appeared in Dutch news media in the course of 2014, demonstrating that the public at large, including Dutch Facebook users, was aware that data processing for the provision of a personalized service (including personalized advertising) is at the heart of the Facebook service. Everyone also knew that advertisements are tailored to an individual's own online browsing and surfing behaviour. Facebook users were in any case informed enough to see that they had to perform further investigations into their possible damage or the person liable for that damage. The Members being able as far back as 2014 to bring claims is also evidenced by the fact that several hundred Dutch Facebook users in 2014 tried to join proceedings brought by Max Schrems in Austria.

8.2 Stichting disputes that Members were already aware of the damage and the person liable for it before 30 December 2014, and it argues the following to that effect. Without in-depth investigations, such as those conducted by the Dutch DPA, Facebook users could not have learned of what happened to their data and the incomplete and misleading way in which Facebook et al. informed users about it. The publications in the press referred to by Facebook et al. are not enough to be able to base any actual awareness of both the damage and the person liable for it on. Aggrieved persons should furthermore not be expected to rely on newspaper articles. There was no duty to investigate for users of the Facebook service. The Dutch DPA conducted an investigation into the operations of the Facebook service in the period November 2014 - 21 February 2017. Only after the publication of that investigation in 2017 could it be said that the Members could be familiar with the Dutch DPA's findings, according to Stichting.

8.3. The Court holds as follows. In view of Stichting's claims, the alleged harmful events must be considered to be the processing of personal data of the Members by Facebook et al. from 2010 to 2020 and the information provided by Facebook et al. in that period about it and about the Facebook service. Facebook et al.'s reliance on the statute of limitations is directed to the claims insofar as they relate to events prior to 30 December 2014.

8.4. Pursuant to article 310 (1) of book 3 DCC, the five-year limitation period mentioned therein takes effect on the day following that on which the aggrieved party became aware of both the damage and the person liable for it. According to established case law[7], the requirement that the aggrieved party has become familiar with both the damage and the person liable for it, must be interpreted in such a way that it concerns actual awareness, so that the mere presumption of the existence of damage or the mere presumption as to which person is liable for the damage does not suffice. The short limitation period of article 310 (1) of book 3 DCC does not begin to run until the day after that on which the aggrieved party is actually in a position to bring a legal action for compensation for the damage suffered by him. This will be the case if the aggrieved party has become sufficiently certain - which need not be absolute certainty - that the damage was caused by

[7] See, for example, Supreme Court April 22, 2022, ECLI:HR:2022:627

the negligent or incorrect conduct of the person involved. The answer to the question at what moment the limitation period started to run depends on the relevant circumstances of the case.

8.5. Since the reliance on the statute of limitations is an affirmative defence, it is up to Facebook et al. to allege, and if necessary prove, facts and circumstances that are required to justify the conclusion that in 2014 there was actual awareness among the Members of the damage and the person liable for it.

8.6. For the purpose of assessing the defence of the statute of limitations, the individual situation of those involved is in principle important in connection with the requirement of subjective awareness. However, an assessment of individual circumstances is not at issue in these collective proceedings, because individual cases must be ignored. For this reason, the question of whether the claims are partially time-barred lends itself less well to being dealt with in this class action. The reliance on the statute of limitations could be successful only in this case, if an individual approach could be dispensed with and if it could be established in a different manner that subjective awareness of both the damage and the person liable for it was present with respect to all the Members prior to 30 December 2014. Facebook et al. have not stated sufficient facts or circumstances on the basis of which that might be established. In a general sense, it is not possible to identify one specific moment at which the consequences of the allegedly unlawful events before 30 December 2014 manifested themselves. To that extent, therefore, it is not possible to point to one specific moment at which the (potential) damage and the subjective awareness with it occurred or may have occurred. The publications that appeared in the media in 2014 and the general knowledge about personalized advertisements alleged by Facebook et al. do not have the significance that Facebook et al. want to attribute to them. Based on that information, it might be assumed that the Members were aware that Facebook et al. were also processing personal data for advertising purposes and that a discussion was going on about the lawfulness thereof, but the relevant facts and circumstances in that respect were not yet known in 2014, or at least not to their full extent. For instance, it has not become apparent that, in those days, it was already generally known in what way and to what extent Facebook et al. exactly (allegedly) processed the personal data of Facebook users. As a result, there was not yet sufficient certainty among the Members in 2014 about any (alleged) inadequate or faulty conduct of Facebook et al. Moreover, it cannot be established either that the (possible) damage had already manifested itself at that time (in all cases).

8.7. This means that in 2014 there was not yet a question of any actual awareness among the Members of the damage resulting from the allegedly harmful events before 30 December 2014. Facebook et al.'s reliance on the statute of limitations must therefore be dismissed in these proceedings, whereby the court does not give an opinion on the question as to whether in an individual case the limitation period may have expired.

9. The request for a stay of the proceedings

9.1. Facebook et al. argue that several proceedings[8] are currently pending before the CJEU that concern the same issues as those in the present proceedings and that the present proceedings should be stayed, pending the outcome of those proceedings before the CJEU. Facebook et al. point out that those cases concern the bases of consent and contractual necessity and the qualification of special personal data.

9.2. The court has already held above that there is no reason to await the outcome in the UI/Österreichische Post case. In the other cases involving a reference for a preliminary ruling which

[8] Case No. C-252/21 (Facebook Inc., Facebook Ireland Ltd, Facebook Deutschland GmbH/Bundeskartellamt) and Case No. C-446/21 (Schrems)

are currently pending before the CJEU, the Court does not see sufficient reason either to stay this case, pending the outcome of those other proceedings. It is true that the proceedings cited by Facebook et al. also concern issues that are considered in this case, but that does not mean that the decisions of the CJEU will also answer the questions at issue in these proceedings on a one-to-one basis. Moreover, it is unclear when the CJEU will give its judgment in the aforementioned cases. Since the district court is obliged (pursuant to article 20 of the Dutch Code of Civil Procedure (DCCP)) to avoid any unreasonable delays, staying this case is also undesirable from a point of view of procedural economy. After all, this could potentially lead to a considerable delay in a case in the first instance that has already been pending before the court for a considerable period of time, while it is not at all certain whether staying the case will lead to further clarity.

10. Who is the controller?

10.1. The question is which part of Facebook et al. is to be regarded as the controller within the meaning of the Wbp and the GDPR respectively, regarding the processing of data at issue in this case.

10.2. Pursuant to section 1 (d) Wbp, which is the implementation of article 2 (d) of the Privacy Directive, a controller means, among other things, the legal person that, alone or jointly with others, determines the purpose of and the means for the processing of personal data. The explanatory memorandum to the Wbp among other things states the following in that respect:[9]

> When answering the question as to who is the controller, the starting point should be, on the one hand, the formal-legal power to determine the purpose and means of the data processing and, on the other hand - in addition to this – the functional content of the term. The latter criterion plays a role in particular, if several actors are involved in the processing of data and the legal powers have not been sufficiently clearly regulated so as to be able to determine which of the actors involved is to be regarded as the data controller within the meaning of the law. In such situations, it will have to be determined on the basis of generally accepted standards, to which natural person, legal entity or administrative body the processing in question should be attributed.
> (...)
> It is desirable to make it clear that the term "controller" refers to the one who, in formal-legal terms, controls the processing operations. (...)
> The starting point when defining the term "controller" is therefore the existing structure of the law of persons and the law of organisations under civil law and administrative law. For the private sector, this means that the formal-legal organization of the company is decisive. (. ..)
> The above also applies to group relationships. The controller is the legal entity under whose authority the operational data processing takes place. The actual power or influence of another legal entity within the group is irrelevant. The rationale behind it is that the data subject can know in social and economic life against whom he can exercise his rights if he so wishes. (...) The fact that those data processing operations carried out by the parent company or a subsidiary (also) benefit the group as such, is not in itself important for establishing responsibility. However, the bill does not preclude an arrangement whereby, in the articles of association of the legal entities concerned or by agreement, the power to determine the purpose and means of the data processing operations within the group is assigned to a particular legal entity within the group. The aforementioned legal entity - for example, the parent company - is in that case the responsible party within the meaning of the bill for all data processing operations that take place within the group, because legal control under the arrangement made rests with that legal entity. (...) It is in accordance with generally held views to attribute responsibility for the data processing operations to the legal entity that has been designated within the group as the legal entity authorized to carry out such operations.
> (...) Another important detail is that in certain situations there may also be joint or shared responsibility. With respect to a set of data processing operations, it is possible that several persons or bodies, i.e., a number of controllers, may be designated as such.(...)

[9] TK 1997/98, 25 8892 no.3, pp. 55-58

10.3. Pursuant to article 4 (7) of the GDPR, the term controller means, among other things, the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. In that context it must be assessed whether this legal person is capable to independently determine for which purpose and by which means the data are processed. It may be important that this legal person is legally authorized to do so, but that is not a requirement. It concerns a functional term, the aim of which is to assign the responsibility where the actual control or influence with respect to data processing lies.[10]

10.4. Under article 2 (c) of the Privacy Directive, "processing of personal data" means "any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Under article 4 (2) of the GDPR, "processing" means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data."

10.5. What matters, therefore, in the case of the controller, is that the person concerned exerts influence over the processing of personal data in question and thereby participates in the determination of the purposes and means of that processing.[11] The CJEU has held that the existence of joint responsibility does not necessarily imply equal responsibility. On the contrary, operators may be involved at different stages of that processing of personal data and to different degrees. This means, according to the CJEU, that the level of responsibility of each of them must be considered in light of all the relevant circumstances of the case.[12] A person may be jointly responsible with others for operations connected with the processing of personal data only, if he has jointly with those others determined the purposes and means of those operations. Without prejudice to any civil-law liability provided for under national law, that person cannot be held responsible for processing operations occurring earlier or later in the processing chain and of which and for which, respectively, he has not determined the purposes and the means.[13] All this means that it must be specified which Facebook entity determines the purposes and means for which processing operations.

10.6. In any case, Facebook Ireland can be considered a processor and a data controller, respectively, for Facebook Ireland must be regarded as the party that primarily determines the purposes of and the means for processing the personal data of Dutch Facebook users. This also follows from various (policy) documents and agreements. Facebook Ireland having this role is not in dispute between the parties.

10.7. Stichting argues that Facebook Inc. and Facebook Netherlands are also controller, or joint controllers. To that end, with reference to the Dutch DPA's report, it among other things argues as follows:

---

[10] Cf. Opinion 1/210, p. 12, of the Article 29 Data Protection Working Party, also known as Article 29 Working Party (hereinafter also WP29)

[11] CJEU 10 July 2018, C-25/17, ECLI:EU:C:20 18:551, Jehovan todisiajat, para. 68

[12] CJEU 5 June 2018, C-210/16, ECLI:EU:C:2018:388, Wirtschaftsakademie, para. 43, cf. also para. 3.2.2 of the European Data Protection Board's (hereinafter also: EDPB) Guidelines 07/2020 of July 7, 2021

[13] CJEU 29July 2019, C-40/17, ECLI:EU:C:2019:629, Fashion ID, para. 74

- Facebook Inc. itself speaks of a single financial operating unit in which the decision-making authority for all financial operations and results rests exclusively with Facebook Inc.'s chief operating decision maker, thus giving Facebook Inc. decisive control over the financial resources used to facilitate the processing of personal data.
- Facebook Inc. initiated the Facebook service in the Netherlands in 2006.
- Facebook Inc. had already determined the main purposes and means of processing personal data when Facebook Inc. and Facebook Ireland entered into the first processor agreements in 2013.
- Facebook Inc. performs the greater part of the processing operations essential to its business model.
- The 2015 processor agreement mentions that Facebook Inc. is responsible for assessing requests from U.S. intelligence and security agencies for access to personal data that Facebook Inc. processes.
- According to regulators, Facebook Inc. determines for which purposes, where and how data is processed.
- Facebook Netherlands exerts significant control over attracting, retaining and supporting advertisers, requiring it to use the processing of personal data by Facebook Ireland and Facebook Inc. in order to identify and reach the right target group.
- Facebook Netherlands generates reports on the effectiveness of advertisements using the Facebook service, which presumes that Facebook Netherlands processes personal data that are obtained.
- Facebook Netherlands may make selections at customer level and/or advertising campaign level from (aggregated) data it receives from Facebook Inc. and/or Facebook Ireland.

10.8. Facebook et al. dispute, with reasons, that Facebook Inc. and Facebook Nederland are controllers, or joint controllers and argue that these companies do not determine the purposes of processing as stipulated in the data policy. According to Facebook et al., Stichting has used incorrect circumstances as its basis and only Facebook Ireland is the data controller for users in Europe. Facebook et al. point out that Facebook Netherlands performs marketing and sales activities only, and, for example, does not personalize ads.

10.9. In the district court's view, it does not follow from the circumstances put forward by Stichting that Facebook Inc. and Facebook Nederland are controllers, or joint controllers, for the relevant period, for all these general contentions insufficiently disclose which specific processing operations Stichting has in mind and in which way Facebook Inc. and Facebook Netherlands respectively determine, or jointly determine, the means for and the purposes of the processing operations concerned. A sufficiently concrete statement by Stichting in this respect is lacking. The fact that Facebook Inc. initiated the Facebook service and, as parent company, has the (ultimate) financial control within the group is not decisive in this respect either. As explained in the parliamentary history, the actual power or influence of another legal entity within a group is not relevant. The internal rules within the group mean in this case that Facebook Ireland has been designated as the authorized legal person, so that the responsibility for the data processing at issue here is attributable to this legal person. A situation described in the explanatory memorandum to the Wbp[14] or the advice of the article 29 Data Protection Working Party[15], i.e. that of a number of actors where the legal powers have been regulated insufficiently, or where the obligations and responsibilities have not been clearly assigned, does not exist in this case.

10.10. The district court concludes that only Facebook Ireland qualifies as the controller for the relevant period.

[14] Cf. TK 1997/98, 25 8892 no.3, p. 55
[15] Cf. WP29 Opinion 1/2 10. p. 28

10.11. Since Facebook Ireland is the controller, the district court will focus its further assessment of the Wbp and the GDPR on Facebook Ireland. Although the parties' contentions also applied to Facebook Inc. and Facebook Netherlands, mentioning those two parties to that extent is no longer relevant for the remainder of the examination of the case.

11. Duty of disclosure for a number of specific processing operations

11.1. Firstly, Stichting accuses Facebook Ireland (see claim a.i.1 - a.i.4, as set forth in 5.1 above) of Facebook Ireland's failure to properly inform the Members about four specific processing operations of personal data of the Members. This claim focuses on, and is limited to, the alleged access of third-party developers, the company Cambridge Analytica and integrated partners of Facebook et al., to personal data of the Members, as well as the use of telephone numbers of the Members, provided in the context of two-factor authentication, for advertising purposes.

11.2. In addition, the parties have extensively debated the question whether Facebook Ireland has *in a general sense* adequately informed the Members within the meaning of sections 33 and 34 of the Wbp and articles 12, 13 and 14 of the GDPR about the processing of personal data (for advertising purposes). However, the district court need not answer that question in a general sense, because Stichting has not attached a (general) claim to it, but has limited its claim a.i. to the four specific processing operations mentioned there. The debate in a general sense between the parties about the duties of disclosure will therefore be discussed only, insofar as doing so will be relevant in the context of any specific claims.

Assessment framework

11.3. Stichting's allegations cover the period from 1 April 2010 - 1 January 2020. Between 1 April 2010 and 25 May 2018, the Wbp (being an implementation of the Privacy Directive, the predecessor of the GDPR) applied. On 25 May 2018, the GDPR entered into force. This distinction between the application of the Wbp and the GDPR is irrelevant in these proceedings in terms of the assessment of whether Facebook Ireland has fulfilled its duties of disclosure. Although the duties of disclosure have been tightened under the GDPR, the duty of disclosure is essentially the same under both legal regimes and Stichting's allegations relate to obligations that already existed under the Wbp as well.

11.4. Article 6 of the Privacy Directive reads as follows:

1. Member States shall provide that personal data must be:
a) processed fairly and lawfully;
b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2. It shall be for the controller to ensure that paragraph 1 is complied with.

11.5. Pursuant to section 6 of the Wbp, personal data shall be processed in accordance with the law and in a proper and careful manner.

11.6. Section 33 Wbp, which elaborates on section 6 Wbp and the principle of transparency, reads as follows:

> 1. If personal data are obtained from the data subject, the controller shall, before the moment of obtaining such data, disclose to the data subject the information referred to in the second and third paragraph, unless the data subject is already aware of this.
> 2. The controller shall inform the data subject of his/her identity and of the purposes of the processing for which the data are intended.
> 3.The controller shall provide further information insofar as this is necessary, having regard to the nature of the data, the circumstances under which they are obtained or the use to which they are to be put, so as to ensure proper and careful processing in respect of the data subject.

11.7. The GDPR has similar provisions. For example, article 5 (1) opening words and (a) of the GDPR stipulates that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Article 5 paragraph 2 GDPR reads: the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability").

11.8. Article 12 (1), first full sentence, of the GDPR provides, insofar as relevant for the purpose hereof, that the controller shall take appropriate measures to provide any information referred to in articles 13 and 14 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

11.9. Article 13 (1) opening words and (c) of the GDPR reads as follows:

> Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
> (...)
> c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

11.10. The idea behind informing the data subject is the transparency of data processing. The controller must actively and without being asked inform the data subject of the data processing, unless the data subject has already been informed. In this way, the data subject will be able to monitor the way in which data about him are processed and challenge certain forms of processing or unlawful behaviour of the controller in court. A processing of personal data about which the controller has not properly informed the data subject, is unlawful.[16]

11.11. In general, the controller cannot confine itself to communicating its identity and the purposes of the processing. In many cases, it will have to provide the data subject with further information insofar as this is necessary to enable proper and careful processing (see also section 33 (3) Wbp quoted above in para. 11.6). The nature of the data, the circumstances under which they are obtained or the use to which they are put determine whether this further information is required. The data controller will always have to ask itself whether these circumstances mean that the data subject can be expected to have a real interest in being provided with further information and, if so, what the extent of such information is.

[16] Cf. for the Wbp: Parliamentary Papers II l997/l998, 25 892, no. 3, pp. 149-150 and 155-156 (Explanatory Memorandum).

11.12. The extent of the duty of disclosure also depends on the way in which the contact is established. In principle, the controller will have an additional responsibility to inform, if it is the controller itself that takes the initiative to contact the data subject. The data subject who approaches the controller himself or herself will as a rule already be aware of that party's identity and intentions. In that case, however, the specific purpose of the data processing and any additional information must still be provided.

11.13. The Guidelines on transparency pursuant to Regulation (EU) 2016/679 of 11 April 2018 of the Article 29 Data Protection Working Party states, among other things, the following about the duty of disclosure in the digital context:

> 10. One of the key elements of the principle of transparency envisaged by these provisions is that data subjects should be able to determine in advance the scope and consequences of the processing and not be surprised later by other ways in which their personal data have been used. This is also an important aspect of the principle of fairness under article 5 (1) of the GDPR, and also relates to recital 39, which states that "natural persons should be made aware of the risks, rules, safeguards and rights in relation to the processing of personal data." With respect to complex, technical or unexpected data processing operations, the WP29's position is that, in addition to providing the information required by articles 13 and 14 (which will be addressed later in these guidelines), controllers should also explain separately, in unambiguous language, what the main effects of the processing will be. In other words, what effect will the specific processing described in the privacy notice/communication have on a data subject?
> (...)
> 35. In the digital context, and in light of the volume of information to be provided to the data subject, data controllers may take a layered approach when they choose to use a combination of methods to ensure transparency. In particular, to avoid information fatigue, the WP29 recommends using layered privacy statements/notices that include links to the different categories of information to be provided to the data subject, rather than displaying all the information in a single on-screen notice. (...) It should be noted that layered privacy statements/notices are not merely embedded pages that require users to click multiple times to get to the relevant information. The design and layout of the first layer of the privacy statement/notification should be such that the data subject has a clear overview of the information about the processing of his or her personal data that has been made available to him or her and where/how to find that detailed information within the layers of the privacy statement/notification. It is also important that the information in the different layers of a layered privacy notice/communication is consistent with each other and that no conflicting information is provided in the different layers.
> 36. With respect to (...) the content of the first layer of a layered privacy notice/notification, the WP29 recommends that details of the purpose of the processing, the identity of the controller and a description of the data subject's rights should be provided in the first layer/regulation. (Moreover, this information should be brought directly to the attention of the data subject when the personal data are collected, for example, by displaying the information when a data subject fills out an online form.) (...) The data subject should be able to understand from the information in the first layer/scheme what the consequences of the processing in question will be for him or her (...).

Obligation to state facts and burden of proof

11.14. Pursuant to article 150 DCCP, the party invoking the legal consequences of facts or rights asserted by it bears the burden of proving those facts or rights, unless a different allocation of the burden of proof arises from any special rule or from the requirements of reasonableness and fairness.

11.15. Application of the main rule of article 150 DCCP entails that - in the context of the special processing operations referred to in claims a.i.1-a.i.4 - the burden of proof that Facebook Ireland has not complied with the duties of disclosure of sections 33 and 34 Wbp and articles 12, 13 and 14 GDPR in principle is on Stichting.

11.16. The parties disagree as to whether a different burden of proof follows from the Wbp and the GDPR.

11.17. Article 6 (2) of the Privacy Directive provides that the data controller has the duty to ensure compliance with the provisions of paragraph 1 (in brief: lawful processing of personal data). This also follows from section 15 Wbp, read in conjunction with section 6 Wbp.

11.18. The explanatory memorandum to the Wbp among other things states as follows[17]:

> (...) In line with the directive, the present bill, in addition to the concept of "consent," also uses the terms "unambiguous consent" and "express consent." (...)
> There is a shift in the burden of proof towards the controller: if there is doubt as to whether the data subject has given his consent, he should verify whether he is justified in assuming that the data subject has consented. To a certain extent, this is a similar situation to the duties of disclosure of the controller under articles 33 and 34. Such verification does not necessarily have to lead to a request for explicit consent. The controller may also acquire information that removes his doubts in this regard in a different way. (...)
> The controller has to take into account a double burden of proof. ln the first place, in case of doubt, it must be possible to prove that a certain consent has been granted and for what purpose. If necessary, it should furthermore be possible to prove that the consent meets the relevant requirements. The controller should in that respect also be able to prove that he has done everything that could reasonably be expected of him, for example with respect to the provision of information to the data subject.

11.19. Pursuant to article 5 (1) and (2) GDPR, the controller must be able to demonstrate that the data processing is lawful, fair and transparent. Article 24 (1) GDPR states, briefly put, that the controller must take appropriate measures to ensure and be able to demonstrate that the processing is carried out in accordance with the GDPR.

11.20. In the district court's opinion, it follows from this that the Wbp and the GDPR contain a provision regarding the burden of proof that deviates from the main rule of article 150 DCCP, also with respect to whether or not the duties of disclosure of sections 33 and 34 of the Wbp and articles 12, 13 and 14 of the GDPR have been met. Although less explicitly worded in the Wbp than in the GDPR, this also follows from the transparency requirement. The data subject can only enforce his rights granted to him by the law, if he is aware of the processing. It is up to the controller to prove that the data processing is lawful.

This also includes adequately informing the data subject in advance about the data processing. The burden of proof that it has fulfilled its duties of disclosure is therefore on Facebook Ireland - in whose domain the factual data in question are also primarily located.

The duty of disclosure regarding the four specific data processing operations

11.21. Below, the four specific data processing operations of which Stichting alleges that Facebook Ireland has not informed the Members about, or not properly, will be discussed.

<u>1. External developers (claim a.i.1)</u>

11.22. As of April 2010, Facebook et al. have used an application programming interface (API) by the name of Graph API version 1. An API allows different types of systems, or software systems, to communicate and exchange information with each other. The Graph API allowed external developers, such as application builders or website administrators, to connect their application to

[17] Parliamentary Papers II l997/l998. 25892, no. 3, p. 66/67

the Facebook service. This included, for example, an application in the form of a game or quiz. The API technology also allowed a Facebook user to use the login function of the Facebook service to sign in to a third-party service.

11.23. Prior to the first use or installation of an application of an external developer, the Facebook user was asked to give his consent. Subsequently, the external developer obtained access via Graph API version 1 to data, or personal data, of the relevant Facebook user and, in addition, access to certain data, or personal data, of the Facebook friends of that Facebook user. This access also enabled the external developer to collect the aforementioned data.

11.24. In April 2014, the Graph API version 1 was (in part) replaced by Graph API version 2. With this second version, external developers were no longer granted access to the data, or personal data, of Facebook friends. For existing applications of external developers, i.e. applications that already had access to Graph API version 1 before 30 April 2014, a transition period applied. They retained access to the Graph API version 1 until 30 April 2015. After that date, a compulsory migration to version 2 applied, but it has been established - as insufficiently disputed it is established - that several so-called whitelisted developers could, with Facebook Ireland's permission, continue to use Graph API version 1 even after 30 April 2015. In June 2018, the use of Graph API version 1 was closed to the last external developers.

11.25. In essence, Stichting's complaint in this claim is that Facebook Ireland did not, or at least did not clearly, inform the Members throughout the relevant period about the access that Facebook Ireland had granted to external developers (via Graph API) to personal data of Dutch Facebook users and their Facebook friends.

11.26. Facebook Ireland takes the view that it did provide proper information about this. According to Facebook Ireland, the Terms of Use and the Data Policy mention how third-party developers were able to collect information from users, including information from secondary users (Facebook friends).

11.27. Furthermore, Facebook Ireland has put forward as its most far-reaching argument that, apart from Kogan's GSR application (which will be addressed separately below in the context of claim a.i.2.), Stichting has not identified any third-party developer's application that was used by the Members. Thus, according to Facebook Ireland, it has therefore not been established that data of Facebook users in the Netherlands was processed by third-party developers, let alone that such data was improperly processed.

11.28. The district court dismisses this argument. It is an established fact that many thousands of applications from third-party developers were connected to the Facebook service during the relevant period. These included applications of large and globally operating companies, such as Airbnb, Netflix and Spotify. Given this, it may be assumed that Dutch Facebook users, or a part of these, in the relevant period also used one or more applications from external developers. For that reason, the district court disregards Facebook Ireland's bare assertion that it has not been established that external developers also had access to personal data of Dutch Facebook users via the API technology, as not substantiated, or insufficiently substantiated.

11.29. As to the substantive question of whether the statutory duties of disclosure have been met, the court holds as follows.

11.30. It is not in dispute that, through API Graph versions 1 and 2, Facebook Ireland provided external developers with access to personal data of Facebook users and that in doing so, those external developers also had the ability to collect that data. Via API Graph version 1, external

developers were furthermore granted access to data, or personal data, of Facebook friends. The provision of access described above in this context is the relevant data processing for which Facebook Ireland is to be regarded as the controller.

11.31. Since Facebook Ireland is the controller vis-à-vis the Members as far as the aforementioned data processing is concerned, it is under the obligation to comply with the statutory duties of disclosure. It cannot therefore rely on the fact that the external developer has to provide information upon the first use or installation of an application. The circumstance that, during the relevant period, users could determine in their settings within their Facebook profile which data was shared with apps of external developers is not decisive in this regard either, for what matters is whether the user was informed in advance that personal data might be shared.

11.32. Below, the district court will address five separate complaints made by Stichting:
1. Facebook Ireland did not communicate that it shared personal data of Facebook users with third-party developers;
2. Facebook Ireland did not communicate the purposes of data processing;
3. Facebook Ireland did not, or not properly, communicate which types of personal data were shared with third-party developers;
4. Facebook Ireland did not, or not properly, communicate that Graph API version 1 also allowed the sharing of Facebook users' personal data with third-party developers via Facebook friends;
5. Facebook Ireland did not communicate that the whitelisted developers could continue to use Graph API version 1 and therefore retain access to Facebook friends' data even after the introduction of Graph API version 2.

11.33. The first issue to be assessed is whether Facebook Ireland informed the Members about the sharing of the Members' personal data with third-party developers. Facebook Ireland has argued that the Members were informed of this through the pop-up window that a Facebook user was shown prior to downloading and installing an external application.

11.34. The (sample) pop-up window to which Facebook Ireland refers looked as follows:

11.35. It is not in dispute that a Facebook user was shown a pop-up window prior to installing an application from a third-party developer. What the pop-up window looked like varied according to the application. Each pop-up window, as explained by Facebook Ireland without being contradicted, showed a list of types of data to which the application would gain access after the Facebook user had given his or her permission. Facebook Ireland illustrated this with the example of a pop-up window submitted by it.

11.36. The sample pop-up window submitted by Facebook Ireland is in English. The language of such an announcement plays a role in whether the text is sufficiently comprehensible for the average user. It has not become clear in the proceedings whether the example shown was also used for the Dutch Facebook user or whether a Dutch version was made for that purpose. Because the pop-up window shown in any case makes it sufficiently clear (also in English) that the external developer will gain access to the list of types of data shown in that window and it is therefore sufficiently clear to the average user that Facebook Ireland will share the data, or personal data, belonging to the information categories mentioned in the pop-up window with the external developer, the district court will not give its views on the question to what extent the use of the English language leads to less clarity in this case. All this means that the Members were informed about the data processing as such. This means that Stichting's first complaint accusation is not justified.

11.37. Secondly, it will be assessed whether Facebook Ireland informed the Members of the purposes for which it granted third-party developers access to Facebook users' personal data. According to Facebook Ireland, it provided information about this by way of the pop-up window that a Facebook user was shown prior to installing an external application and through Facebook Ireland's Data Policy.

11.38. Based on the (sample) pop-up window, the district court finds that the Facebook user was asked for permission to allow the third-party developer's application to access various categories of information about the Facebook user. However, as far as the court can ascertain[18], the pop-up window does not show that it mentions for what purpose the application will gain access those categories of information. This means that it must be assumed that the Facebook user was not informed in the pop-up window about the purposes of the data processing.

11.39. Facebook Ireland has furthermore referred to information in the Data Policy. It has explained what information had been included over time in the various versions of that Data Policy regarding access by external applications to personal data of Facebook users and their Facebook friends. The district court is of the opinion that it need not be discussed whether the Data Policy contained (sufficiently concrete) information about the purposes of this data processing, because in this case the Data Policy is not the appropriate place to provide the relevant information with respect to this specific form of data processing.
To this end, the following is important. The starting point is that the controller provides the relevant information about data processing to the data subject the moment that learning of that information is most relevant to the data subject, which in this case is the moment the Facebook user intends to install an external application. The information in question should therefore in principle be provided in the pop-up window, for at that moment such information is of interest and relevant to the Facebook user. As established above, the pop-up window did not mention anything about the processing purposes. To the extent that Facebook Ireland had wanted to inform the user with the help of the Data Policy, it should have included a reference to the Data Policy in the pop-up window, which it has not done either. It is true that a Facebook user's attention is drawn to the existence of the Data Policy at the time of his (first) registration with the Facebook service, but at that moment the data processing at issue here (the access of external developers to the Facebook user's personal data) is not yet occurring and is not yet of interest or relevant to the Facebook user. Therefore, a general reference to the Data Policy at the time of registration with the Facebook service cannot be regarded in this case as fulfilling the duty of disclosure for a specific, future form of data processing of which it is not yet certain at the time of registration whether it will take place.

11.40. It follows from the foregoing that Facebook Ireland has failed to inform the Members of the purposes for which Facebook Ireland is going to give third-party developers access to their personal data.

11.41. Incidentally, in these proceedings Facebook Ireland has not explained either in concrete terms for which exact purpose(s) it provides external developers access to personal data of Facebook users. From the explanation of the operation of API Graph, the court concludes that the purpose of said access was partly technical-functional, in the sense that with the help of API technology a Facebook user was enabled to use the login function of the Facebook service to log in to the service of a third party. However, it has neither been argued nor shown that the third-party developers' access to the Facebook users' personal data was limited only to such personal data as was necessary for the technical-functional operation of the API functionality. From the information contained in the

[18] The small text under the bold headings is illegible to the district court in the image submitted by Facebook Ireland.

pop-up window described in ground 11.34 above, it appears that a Facebook user grants permission to access a wide range of information and (personal) data. For a large part of that information and (personal) data it is difficult to see, without any further explanation, which is lacking, why access to it is necessary for the technical-functional operation of the API functionality.

11.42. Thirdly, it has to be assessed whether Facebook users were properly informed by Facebook Ireland about what types of personal data were shared with third-party developers.

11.43. According to Stichting, third-party developers had virtually unlimited access to the Members's personal data and Facebook did not inform Ireland about this in the first layer of information. According to Stichting, the Data Policy did not show either what types of personal data external developers had access to; that was hidden in the privacy settings.

11.44. In the district court's opinion, based on the list of types of data shown in the pop-up window, it was sufficiently clear to an average user which categories of information were given access to. Given the description of those categories (such as Access posts in my News Feed, Access my data any time, Access my profile information and Access my friends' information, see the sample pop-up window in ground 11.34), it was also sufficiently clear to the average user that the consent to be given had a (very) wide scope and thus included all (types of) personal data within the listed categories of information to which the requested consent applied.

11.45. Thus, the pop-up window adequately informed about the types of personal data to which an external developer's application was given access. With that, it no longer matters whether the Terms of Use or the Data Policy contained sufficient information on that point.

l 1.46. In the context of the question of compliance with the statutory duties of disclosure, Stichting's assertion that external developers had almost unlimited access to personal data of the Members does not have independent significance. To the extent that a different, independent complaint is contained in that assertion, it must be dismissed, because Stichting - in response to Facebook Ireland's position that the personal data to which an external application could gain access was limited to that information for which a Facebook user had given permission - has not argued, or not with reasons, that, in practice, external developers gained access to more categories of information than those listed in the pop-up window in question and for which Facebook users had given permission.

11.47. Fourth, it must be assessed whether Facebook Ireland informed the Members that Graph API version 1 allowed personal data of Facebook users to be shared with external developers through Facebook friends. According to Stichting, Facebook Ireland has failed to fulfil its duty of disclosure on this point as well.

11.48. Facebook Ireland argues that it informed users of the Facebook service in the Terms of Use and the Data Policy that and how users' personal data, depending on their individual privacy settings, could be shared by their Facebook friends with the applications those friends used on the Facebook service. To this end, Facebook Ireland refers in particular to the following passages:

- in the Terms of Use dated 8 June 2012, 11 December 2012 and 15 November 2013:

2. **Sharing content and information**
You own all content and Information you post on Facebook and In your privacy and app settings you can determine how this is shared. Furthermore, the following provisions apply:

(…)

3. When you use an application, it may happen that the application asks your permission to access your content and information, as well as the content and information that others have shared with you. We require applications to respect your privacy and your acceptance of that application determines the way in which the application can use, store and transfer your content and information. (For more information on the platform, see our Policy on the use of data and the Platform page).

- in the Data Policy of 15 November 2013:

Other websites and applications

About the Facebook platform

The Facebook platform (also simply called platform) refers to how we help you share your information with the games, applications and websites that you and your friends use. With the Facebook platform you can bring your friends with you, so that you can also connect with them outside of Facebook. In these two ways, the Facebook platform helps you make your experiences on the Internet more personal and more social.

However, remember that these games, applications and websites are created and maintained by other companies and developers that are not part of Facebook and are not controlled by Facebook. Therefore, make sure you always read their terms of service and privacy policies so that you know how they deal with your data.

Determine which data you share with applications

When you connect to a game, application or website, such as when you go to a game, sign in to a website with your Facebook account, or add an app to your timeline, we give that game, application or website (sometimes called "apps" for short) your general information (sometimes also called your 'public profile'), including your user ID and your public information. As part of this general data, we also give them the user IDs of your friends (sometimes called your 'friends list').

With your friends list, the application can make your experience more social, because you can find your friends In that application. Your user ID helps the application personalize your experience, by allowing your account in that application to be linked to your Facebook account and access your general data, including your public data and friends list. This also applies to data you make public and data that is always public. If the application wants more information, such as your reports, photos and Interests, you must give permission for this.

(…)

With the Apps setting you use, you can manage the applications you use. You can see the consent you have given these applications, the most recent moment the application used your data, and you can view the Facebook users for your timeline reports and activities that the application posts in your name. You can also delete applications you no longer want to use or disable all platform applications. If you disable all platform applications, your user ID will no longer be given to applications, even if your friends use those applications. But you will not be able either to use games, applications or websites through Facebook any longer.

(…)

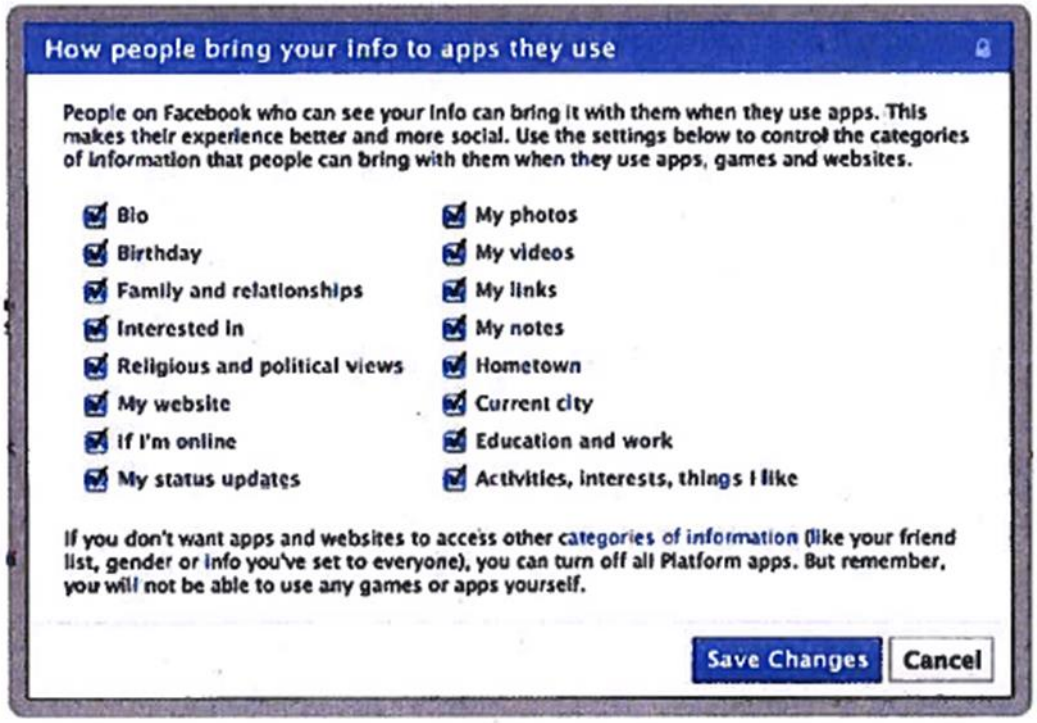
Determine what is shared when those with whom you share content use applications

The data that are shared on Facebook can be shared again, just like when you share data via email or elsewhere on the Internet. That means if you share something on Facebook, Everyone who can see it, can also share it with others, including the games, applications and websites they use.

Your friends and the other people you share things with often want to share your data with applications to make their experiences with those applications more personal and social. Example: one of your friends wants to use a music application with which she can see what her friends are listening to. To get the most out of this application, your friend needs to give the application her friends list (which contains your user ID) so that the application knows which of her friends are also using the application. Your friends might also want to share the music you 'like' on Facebook. If you have made that information public, the application will have access to it, as

do others. But if you have shared your interests with your friends only, the application may ask your friends for permission to share your interests.

You can manage most of the data others share with applications by using the Settings page Ads, apps and websites. However, with these Settings you cannot set restricted access to your public data and friends list.



If you want to block applications completely, so that they cannot get information about you when your friends and others use them, you need to disable all platform applications. This also means that you can no longer use Facebook-integrated games, applications or third-party websites.

If an application seeks permission from someone else to access your data, the application will only get permission to use that data in connection with the person who gave the permission and no one else.

- in the Data Policies dated 30 January 2015 and 29 September 2016:

Apps, websites and integration points of external parties using our services or are present on them. When you use external apps, websites or other services that make use of or are integrated in our services, these external services may receive information about what you post or share. For example, when you are playing a game with your Facebook friends, or use the Facebook button React or Share, the game developer or website may receive information about your activities in the game or the reactions or the link you share on Facebook from the website. If you download or use their services, external parties will furthermore gain access to your public profile, including your user name or user ID, your age group and country/language, your friends list and the data you share with these external services. Data collected by these apps, websites or integrated services are subject to the terms and conditions and policy rules of the external service concerned.

More information about how you can check the data that you and others share about you with these apps and websites

11.49. With Graph API version 1, an external developer not only obtained access to data, or personal data, of the Facebook user in question, but also to certain data, or personal data, of the Facebook friends of the Facebook user in question. In the opinion of the court, Facebook Ireland did not sufficiently inform its users about the latter. The reasons for this are as follows.

11.50. On the basis of the nature of the Facebook service, an average Facebook user did not have to be aware, when registering, that through a third-party application, which would be installed by a Facebook friend, an external developer would also gain access to the Facebook user's personal data. Such a specific and, to the average user, unforeseen form of data processing must therefore be clearly communicated. The passages in the Terms of Use cited by Facebook Ireland do not show that users' personal data could be shared with external applications by their Facebook friends. For the first time in the Data Policy of 15 November 2013, there is some information from which such data processing can be indirectly inferred. However, this was not done in sufficiently clear and understandable terms. Moreover, the Data Policy of 15 November 2013 is very extensive; it covers almost thirty pages of information. It must therefore be concluded that at this point there are communications in veiled language among a large amount of other detailed information in an underlying layer of information(the Data Policy). Such communications do not meet the requirements of providing transparent, understandable and easily accessible information about a relevant data processing operation. In the subsequently amended Data Policies of 30 January 2015 and 29 September 2016, the information provided is different in terms of scope and content. In those policies the relevant information is very concise. However, the passage cited by Facebook Ireland again does not show that users' personal data could be shared with external applications by their Facebook friends.

11.51. Facebook Ireland has furthermore argued that, in its Data Policy, it advised users to read the terms and policies of the third-party applications themselves, so as to understand how those applications would handle their data. This argument cannot benefit Facebook Ireland. As previously considered, Facebook Ireland is the controller when it comes to granting third-party developers access to Facebook users' personal data, so Facebook Ireland must comply with legal duties of disclosure in that regard.
The fact that Facebook users could additionally exercise control over the data shared with external applications cannot benefit Facebook Ireland either, because that does not detract from the fact that Facebook Ireland must provide proper information in advance about the data processing.

11.52. Lastly, it must be assessed if Facebook Ireland communicated that the whitelisted developers retained access to data of Facebook friends even after the introduction of Graph API version 2. The district court takes the view that Facebook Ireland has breached its duty of disclosure on this point as well. The court explains this as follows.

11.53. Facebook Ireland has not, or not sufficiently, refuted the course of events alleged by Stichting in this regard. This means that the following can be assumed. At the end of April 2014, at the launch of Graph API version 2, Facebook et al. publicly announced that, with this API, external developers would no longer have access to the data of Facebook friends. Facebook et al. did not add that existing applications retained access through Graph API version 1, including access to Facebook friends' data, at least through to 30 April 2015. Furthermore, Facebook users were never informed that so-called whitelisted developers could continue to use Graph API version 1 after 30 April 2015 and thus retain access to information and personal data of Facebook friends, even though Graph API version 1 allegedly had been shut down on 30 April 2015. The whitelisted developers were collectively responsible for 5,200 different Facebook applications. In June 2018, Facebook et al. shut down the use of Graph API version 1 for the last third-party developers.

11.54. The district court shares Stichting's view that Facebook Ireland should have communicated the fact that the whitelisted developers retained access to data of Facebook friends even after the introduction of Graph API version 2, because this is information that, given the circumstances under which the data of Facebook friends were obtained by the whitelisted developers, is required for the purpose of ensuring proper and careful processing. By failing to communicate this, Facebook Ireland acted in breach of the obligation in section 33 (3) of the Wbp.

11.55. It is concluded that throughout the relevant period, Facebook Ireland did not inform the Members about the purposes of the data processing (providing access to the external developers to personal data of Facebook users), that in the period 1 April 2010 - June 2018, Facebook Ireland did not properly inform the Members that Graph API version 1 also allowed the sharing of Facebook users' personal data with third-party developers via Facebook friends, and that in the period April 2014 - June 2018, Facebook Ireland did not inform the Members that the whitelisted developers could carry on using Graph API version 1 even after the introduction of Graph API version 2 and thereby retain access to Facebook friends' data. By doing so, Facebook Ireland acted in breach of the duties of disclosure of section 33 (2) and (3) and article 13 (1) GDPR, respectively. Since these processing operations were not properly communicated, they are unlawful. The declaratory judgment requested by Stichting can be granted as described above.

2. Cambridge Analytica (claim a.i.2)

11.56. Claim a.i.2 concerns Facebook Ireland allowing Alexandr Kogan and his company Global Science Research Ltd (hereinafter: GSR), among others, to have access to Personal Data of the Members. According to Stichting, Facebook Ireland did not (clearly) inform the Members about this. According to Stichting, the Members' personal data were subsequently transferred by Kogan and/or GSR to Cambridge Analytica. Facebook Ireland argues that there is no evidence that data of Dutch Facebook users were involved in the transfer by Kogan to Cambridge Analytica. According to it, no data of Facebook users located outside the United States was transferred by Kogan to Cambridge Analytica. Facebook Ireland furthermore refers to its defence against claim a.i.1.

11.57. Kogan and GSR provided an application (hereinafter "the GSR application[19]) that connected to the Facebook service via the Graph API version 1. Stichting has not disputed that the GSR application was subject to the same conditions and restrictions as the applications of other third-party developers. The GSR application was active from May 2014 to October 2015. Facebook Ireland has not disputed that data of Dutch Facebook users was also shared with Kogan/GSR.

11.58. It is not in dispute that the GSR application is an application of an external developer as referred to in claim a.i.1. What has been considered and ruled above about complaints 1 - 4 as mentioned in ground 11.32 (in the context of the question as to whether Facebook Ireland had informed the Members about the access to their personal data by external developers), therefore also applies to the GSR application. This means that claim a.i.2. in respect of Kogan and GSR is admissible the same way as claim a.i.1. is, with the understanding that, according to Stichting, the GSR application was only active from May 2014 to October 2015, so that the declaratory judgment is limited to that period. This therefore only constitutes a violation of the Wbp at this point.

11.59. With respect to Cambridge Analytica Ltd., Cambridge Analytica LLC and SCLE Elections Ltd (hereinafter collectively: Cambridge Analytica et al.) claim a.i.2. cannot be allowed. It is not relevant for the assessment in these proceedings whether personal data of Members also ended up with Cambridge Analytica et al. After all, even if the latter were the case, Facebook Ireland was not under an obligation to provide information in this respect as referred to in section 33 or 34 of the Wbp.

[19] This app used to be named 'CPWLab' and 'ihisisyourdigitallife'.

Facebook Ireland had no control over any access by Cambridge Analytica et al. to the personal data of the Members. At the time Facebook Ireland processed the personal data and granted Kogan/GSR access to it, it did not know that such data would in the future be (unlawfully) provided to a third party by Kogan/GSR. With respect to such further processing, Facebook Ireland did not determine the purpose and means, so it cannot be regarded as a controller for this, so that there was no duty of disclosure for Facebook Ireland in that respect as referred to in section 33 or 34 Wbp.

3. Telephone numbers for the purpose of two-factor authentication (claim a.i.3)

11.60. Claim a.i.3 relates to the use for advertising purposes of telephone numbers provided under the two-factor authentication.

11.61. Two-factor authentication (hereafter: 2FA) is a security measure to protect users from unauthorized access to their accounts. With 2FA, an (additional) verification of the identity of the user who wants to log into a website or application is performed.

11.62. Since May 2011, the Facebook service has allowed users to secure their account with 2FA. That functionality means that if Facebook users want to log into their account from a device that is not recognized, they must enter a separate login code (in addition to the username and password). Facebook users who have enabled 2FA will receive the separate login code by text message on their cell phone. When enabling the 2FA security feature, Facebook users must indicate which phone number they want to use for this purpose. In doing so, Facebook users have the choice between:
1) using the phone number already added to his account (to the extent that he had previously provided a phone number) (hereinafter also: choice 1) or
2) adding a new or using a different phone number (hereinafter also: choice 2).

11.63. Stichting argues that Facebook Ireland did not, or not properly, inform the Members that the phone numbers provided by the Members for the purposes of 2FA were also used for the placement of targeted ads. Facebook Ireland takes the position that it did always adequately inform Members that those phone numbers could also be processed for the purpose of providing personalized ads.

11.64. It is not disputed that Facebook Ireland has also processed telephone numbers provided to it for advertising purposes. In the district court's opinion, Stichting no longer has an independent interest in an opinion regarding the question as to whether Facebook Ireland properly informed the Members on this point. The reason for this is that in this judgment (see chapter 12) the court takes the view that Facebook Ireland had no legally valid basis for processing Personal Data of the Members for advertising purposes during the entire relevant period. Since a telephone number qualifies as personal data, that judgment given in Chapter 12 also applies to the telephone numbers provided in the context of 2FA, nor has Facebook Ireland alleged that it can rely on any other legally valid basis for processing those phone numbers for advertising purposes. In particular, Facebook Ireland has not alleged that it had obtained consent to use the phone numbers provided under 2FA for advertising purposes, nor does such consent appear from the module a Facebook user went through in the situation of either choice 1 or choice 2.

11.65. All this means that throughout the relevant period no basis existed for the processing by Facebook Ireland of those phone numbers for advertising purposes. The absence of a basis for processing is the most far-reaching opinion that can be given about a data processing operation and affects that processing in all its parts. The extent to which the controller complied with its duties of disclosure prior to processing without a valid basis is therefore no longer relevant to that extent. In view of this, it is hard to see what interest Stichting still has in an opinion about the declaratory judgment it has claimed in a.i.3. After all, that statement focuses on the failure to inform Stichting

about the use of the telephone numbers provided on behalf of 2FA for the placement of targeted advertisements. As far as the right to (possible) compensation or the extent thereof is concerned, a judgment in this respect has no added value either, given the more comprehensive judgment that no legally valid basis existed for the processing of personal data for advertising purposes.

11.66. Claim a.i.3 must therefore be dismissed for lack of interest.

4. 'Integration partnership' programme (claim a.i.4)

11.67. Claim a.i.4 relates to data transfers by Facebook Ireland to so-called integrated partners.

11.68. Integration partners are companies that Facebook Ireland has partnered with, including cell phone manufacturers, for the purpose of allowing Facebook users to access the Facebook service on a variety of devices, operating platforms and operating systems in the period when apps for cell phones were not yet available through app stores of, for example, Apple and Google. In the early days of the mobile phone era, there was a wide variety of cell phones. Facebook Ireland did not have the ability to build versions of the Facebook application that could be used on every type of phone and operating system. Therefore, it engaged device manufacturers such as Blackberry, Samsung, Microsoft and Sony to build device and platform integrations. Facebook Ireland granted the integration partners rights to use application programming interfaces (APIs) to build applications and functionalities for the Facebook service. Using those APIs, Facebook users could, for example, access the (main functionalities of the) Facebook service on their cell phones. Whenever a Facebook user used an application from an integration partner, the Facebook user's device necessarily interacted via an API. Through that API, the integration partners had access to the data, or personal data, of that Facebook user and their Facebook friends. As of 2015, integration partners no longer had access (with the exception of Blackberry) to the information of Facebook friends.

11.69. Stichting alleges that Facebook Ireland did not, or not clearly, inform the Members about the integration partnership program and the related processing of the Members's personal data. To this end, it argues the following. Research by The New York Times shows that integration partners had access to the personal data of Facebook users using the partnership in the same way as third-party developers, including access to the data of their Facebook friends. Moreover, for the purpose of making the Facebook service available on the devices of Facebook users, it was not necessary that integration partners gained access to then personal data of a user's Facebook friends. Given the extent of the sharing of personal data with integration partners, Facebook Ireland should have mentioned this in the first layer of information, but it did not do so. To the extent that the Data Policy should qualify as the first layer of information, that policy contains incomplete information. It did not inform about the purposes of the processing and what personal data are processed. Lastly, Stichting questions Facebook Ireland's view that Facebook Ireland had agreed with the integration partners that the personal data received by them were not to be used for their own purposes. No such agreement has been submitted, so it is uncertain whether Facebook Ireland's position is true. For this reason, Stichting disputes that position.

11.70. Facebook Ireland takes the view that it properly informed Facebook users about the integration partnership program and the circumstance that data could be shared with integration partners. To this end, it argues the following. Throughout the relevant period, Facebook Ireland clearly communicated about all aspects of this data processing. It has done so in the various versions of its Data Policy. Facebook users were made aware of their content before they registered with the Facebook service. Furthermore, Facebook Ireland stresses that integration partners were not allowed to use the data they received through the APIs for other purposes of their own without the Facebook user's consent. The integration partners had committed themselves by contract to Facebook Ireland that they would only use the data they accessed for the purpose of providing a Facebook experience.

11.71. The court first and foremost states that, as in the case of the external developers, a distinction must be made between the data processing by Facebook Ireland and the (further) data processing by the integration partners. As far as granting integration partners access to personal data of Facebook users is concerned, Facebook Ireland is the controller. After all, it (in part) determines the purpose and means for this. Granting this access is therefore to be regarded as relevant data processing in the context of claim a.i.4. It is to that data processing that the duties of disclosure relate. Any further data processing by the integration partners is beyond the responsibility, or processing responsibility, of Facebook Ireland. Indeed, Stichting has not stated any relevant facts or circumstances on the basis of which it may be established that Facebook Ireland determines, alone or with others, the purpose and means of any further (independent) data processing by the integration partners.

11.72. In line with the foregoing, it is also irrelevant in these proceedings whether Facebook Ireland, in its agreements with integration partners, has imposed restrictions on what the personal data obtained may be used for. It is true that Facebook Ireland has a general obligation to treat the personal data of its users with care, and under certain circumstances this entails an obligation to take measures to limit the (further) processing of personal data by those to whom that data are provided, but Stichting has not based its claims on any violation of such an obligation. The aforementioned obligation cannot be grouped either among the duties of disclosure of sections 33 and 34 of the Wbp or the articles 12, 13 and 14 of the GDPR, while the declaratory judgment requested by Stichting is based on the violation of those duties of disclosure.

11.73. This brings the court to the question of whether Facebook Ireland properly informed its users about the access that integration partners had to the data of Facebook users and their Facebook friends.

11.74. The starting point is that the controller provides the relevant information about data processing to the data subject the moment that being provided with that information is most relevant to the data subject. In this case, that is the moment when the Facebook user installs or activates the integration partner's software and then logs into the Facebook app on the integration in question. After all, that is when information about such data processing is of interest and relevant. Facebook Ireland has not stated whether, and if so how, at that time information was provided to the Facebook user about the integration partner's access to the personal data of the Facebook user and his Facebook friends. This means that the court cannot establish anything in this regard, so that it must be concluded that Facebook Ireland did not provide any information at all about this data processing at that time. There is no need to discuss whether the Data Policy about that data processing contained (sufficiently concrete) information, because it has neither been argued nor demonstrated that, when logging in for the first time using the integration partner's integration, reference was made to Facebook Ireland's Data Policy. The circumstance that the Facebook user was made aware of the existence of the Data Policy when he first registered and logged in to the Facebook service is not relevant, because at that point in time the data processing at issue in these proceedings was not necessarily at issue then, so that that was not the appropriate time to provide information. Therefore, a general reference to the Data Policy at the time of registration with the Facebook service cannot, under the circumstances, be regarded as fulfilling the legal duty of disclosure regarding this data processing.

11.75. The foregoing means that Stichting's argument succeeds. Facebook Ireland did not inform the Members about the access of integration partners to personal data of Facebook users and their Facebook friends. By doing so, Facebook Ireland violated the duties of disclosure of section 33 (2) and (3) of the Wbp and of article 13 (1) of the GDPR, respectively. Since the aforementioned data processing operations were not properly communicated, those processing operations are unlawful.

11.76. As to the period during which the breach of these duties of disclosure occurred, the following applies. Stichting has argued that throughout the relevant period, Facebook Ireland did not inform the Members about the provision of data to integration partners. It has not been disputed by Facebook Ireland that it had partnerships with integration partners throughout the relevant period and that, throughout that period, those partners had access to personal data of Facebook users using an API functionality of an integration partner. It is also established that until 2015, integration partners also had access to the personal data of those Facebook users' Facebook friends in that manner. As of 2015, Blackberry was the only integration partner that still had access to Facebook friends' data. It is thus established that the breach of the duty of disclosure occurred over the entire relevant period.

11.77. With due observance of the foregoing, the requested declaratory judgment can be allowed.

12. Basis for processing

12.1. Stichting argues that Facebook Ireland did not have a legally valid basis for processing personal data of the Members for advertising purposes. By nevertheless processing those personal data for advertising purposes, Facebook Ireland has violated the privacy rights of the Members, according to Stichting. It is to this allegation that claim a.ii.1 relates (see ground 5.1 above).

12.2. Both section 8 Wbp (which was the implementation of article 7 Privacy Directive) and article 6 GDPR contain an exhaustive list of grounds justifying data processing.

12.2.1. Section 8 Wbp read as follows, to the extent relevant:

Personal data may be processed only if:
a. the data subject has given his unambiguous consent to the processing;
b. the processing of data is necessary for the performance of a contract to which the data subject is a party, or for taking pre-contractual measures in response to a request from the data subject and which are necessary for the conclusion of a contract;
c. (. . .)
d. (. ..)
e (. . .)
f. the processing of data is necessary to safeguard the legitimate interest of the controller or of a third party to whom the data are disclosed, unless the interest or fundamental rights and freedoms of the data subject, in particular the right to privacy, prevail.

12.2.2. Article 6 (1) GDPR reads as follows, to the extent relevant.

Processing shall be lawful only 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;
b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(…)
f) 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.

12.3. Protection of personal data is a fundamental right protected by, inter alia, article 8 ECHR.[20] The principles of proportionality and subsidiarity must be met in any data processing, both under the Wbp and under the GDPR. This entails that the infringement on the interests of a data subject may not be disproportionate in relation to the purpose to be served by the processing, and that this purpose cannot reasonably be achieved in another way that is less prejudicial to the data subject.[21]

12.4. Under both the Wbp and the GDPR, it is up to the controller to prove that the data processing is lawful.[22] Thus, Facebook Ireland has to prove that it had a valid basis for processing personal data of Facebook users for advertising purposes.

12.5. For that part of the relevant period when the Wbp applied, Facebook Ireland relies on the following bases:
i) consent (article 8 opening words and (a) Wbp),
ii) necessary for the performance of a contract (article 8 opening words and (b) Wbp) and
iii) legitimate interest (article 8 opening words and (f) Wbp).

12.6. For that part of the relevant period when the GDPR applied, Facebook Ireland generally relies on, or only relies on, the basis of contractual necessity (article 6 (b) GDPR). For a number of specific situations, Facebook Ireland relies on consent under the GDPR (article 6 (a) GDPR). Whether in those specific situations the requirements for consent are met is not an issue to be assessed in these proceedings, with the exception of the processing of special personal data (see below chapter 13 of this judgment).

12.7. The court will first of all assess below the basis of contractual necessity (section 8 opening words and (a) Wbp; article 6 (1) (a) GDPR) put forward by Facebook Ireland, as this basis was invoked for the entire relevant period.

Contractual necessity as a basis for processing?

12.8. Facebook Ireland takes the view that the processing of personal data for advertising purposes was necessary to give effect to the agreement. To this end, it argues the following. The Facebook service in essence is a personalized service, which is reflected in the Terms of Use. The provision of personalized content included (targeted) advertisements. The Terms of Use, to which a user agrees upon registration, set forth the rights and obligations of the parties. Under those terms, Facebook Ireland undertook to provide the Facebook service. At the time of the Wbp, the Terms of Use always contained a section entitled "About ads and other commercial content provided or enhanced by Facebook." This described that the ads had to be valuable to users. At the time of the GDPR, it was also made clear to users in the terms and conditions that they would be shown advertising tailored to their interests. Thus, the processing of personal data for the purpose of being able to offer personalized content, including advertisements, was at the heart of the service Facebook Ireland offered and made available. Therefore, in its view, this processing was necessary for Facebook Ireland to fulfil its contractual obligations.

---

[20] In addition, Article 16 (1) of the Treaty on the Functioning of the European Union and Article 8 (1) of the Charter of Fundamental Rights of the European Union also provide that everyone has the right to the protection of their personal data.
[21] Supreme Court 9 September 2011, ECLI:NL:HR:2011:BQ8097, para. 3.3 and Supreme Court 3 December 2021, ECLI:NL:HR:2021:1814, ground 3.1.2.
[22] - See the Explanatory Memorandum to the Wbp (Parliamentary Papers 11 1997/1998, 25892, No. 3, p. 66/67) and the provisions of section 15 Wbp. See also the provisions of article 5 (2)(in conjunction with 5 (1) and 6), 7 (2) in conjunction with recital 42 of the preamble and 24 (1) GDPR.

12.9. Stichting disputes that the processing of personal data for advertising purposes was necessary for the purpose of performing the user agreement between Facebook Ireland and the Members. To this end, Stichting argues that for a user, the personalization of ads is not the reason for signing up to the Facebook service. The essence of the Facebook service is to provide a social network that allows users to interact with others. Users also did not have to expect to be offered targeted and personalized ads. Stichting refers to guidance from the EDPB from 2019 on the application of the GDPR. These state that the processing of personal data for 'behavioural advertising' is not necessary for the performance of a contract. Incidentally, according to Stichting, a social network, such as the Facebook service, can also be offered without processing personal data for commercial or advertising purposes.

12.10. The district court holds as follows.

12.11. The basis of contractual necessity relied on by Facebook Ireland requires that the processing of personal data for advertising purposes is necessary for the performance of the contract between Facebook Ireland and the user of the Facebook service. There is, also in view of what is considered below in ground 12.13, no reason to interpret this basis differently under the Wbp than under the GDPR. Moreover, in terms of wording, section 8 Wbp and article 6 GDPR correspond on this point.

12.12. It follows from CJEU case law that the concept 'necessary' in the various parts of article 7 of the Privacy Directive and article 6 GDPR is an autonomous concept of European Union law.[23] On the interpretation of the criterion 'necessary for the performance of the contract' the CJEU has not yet expressed an opinion.

12.13. For the interpretation of the 'contractual necessity' basis, the district court also attaches importance to the advice and guidelines of the Article 29 Data Protection Working Party (hereinafter also: WP29) and of the European Data Protection Board (hereinafter: EDPB). At the time of the Wbp, WP29 was the independent advisory and consultative body of European privacy supervisors and consisted of the national privacy supervisors of the EU Member States and the European Data Protection Supervisor (EDPS). The EDPS supervises the processing of personal data in EU institutions and bodies. WP29 had an independent and advisory status (article 29 (1) Privacy Directive) and its PRINCIPAL task was to contribute to a uniform application of the principles contained in the Privacy Directive (Article 30 (1) (a) Privacy Directive). EDPB has succeeded WP29 since the entry into force of the GDPR.

12.13.1. WP29's advice 06/2014 on Article 7 of the Privacy Directive (of which section 8 Wbp was the implementation) inter alia stated the following[24]:

> The provision [article 7 (b) of the Privacy Directive, [*addition district court*] should be interpreted strictly and does not cover situations where the processing is not actually necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Similarly, the fact that the processing of certain data is covered by a contract does not automatically imply that the processing is necessary for its performance. For example, Article 7 (b) is not an appropriate legal basis for profiling a user's tastes and lifestyle based on their click data on a website and the goods purchased. The reason for this is that the data controller is not appointed to compile a profile, but to provide, for example, certain goods and services. Even if these processing activities are specifically mentioned in the fine print of the contract, this fact alone is not sufficient to make the processing "necessary" for the performance of the contract.

[23] CJEU 16 December 2008, C-524/06, ECLI:EU:C:2008:724, Huber, para. 52.
[24] WP29 Opinion 06/2014 on the concept of "legitimate interest of the data controller" in article 7 of Directive 95/46/EC (WP217), adopted 9 April 2014, pp. 20-21.

There is a clear link here between the assessment of necessity and compliance with the purpose limitation principle. It is important to establish the exact underlying reason for the agreement, i.e., its content and basic purpose, as this will be used to assess whether the data processing is necessary for performance.

12.13.2. The EDPB's guidance 2/2019 regarding article 6 (b) of the GDPR in the context of the provision of online services states, among other things, the following[25]:

23.(...) it is important to note that the concept of what is "necessary for the performance of a contract" is not simply an assessment of what is permitted by or written into the terms of a contract. The concept of "necessity" has an independent meaning in European Union law, which must reflect the objectives of data protection law.
(…)

27. (. .) Where a controller seeks to establish that the processing is based on the performance of a contract with the data subject, it is important to assess what is objectively necessary to perform the contract. 'Necessary for performance' clearly requires something more than a contractual clause.

30. When assessing whether article 6 (1) (b) is an appropriate legal basis for processing in the context of an online contractual service, regard should be given to the particular aim, purpose, or objective of the service. For applicability of article 6 (1) (b), it is required that the processing is objectively necessary for a purpose that is integral to the delivery of that contractual service to the data subject. Not excluded is processing of payment details for the purpose of charging for the service. The controller should be able to demonstrate how the main subject-matter of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. The important issue here is the nexus between the personal data and processing operations concerned, and the performance or non-performance of the service provided under the contract.

(…)
32. The controller should be able to justify the necessity of its processing by reference to the fundamental and mutually understood contractual purpose. This depends not just on the controller's perspective, but also a reasonable data subject's perspective when entering into the contract, and whether the contract can still be considered to be "performed without the processing in question. "(…)

33. In order to carry out the assessment of whether article 6 (1) (b) is applicable, the following questions can be of guidance:
- What is the nature of the service being provided to the data subject? What are its distinguishing characteristics?
- What is the exact rationale of the contract (i.e. its substance and fundamental object)?
- What are the essential elements of the contract?
- What are the mutual perspectives and expectations of the parties to the contract? How is the service promoted or advertised to the data subject? Would an ordinary user of the service reasonably expect that, considering the nature of the service, the envisaged processing will take place in order to perform the contract to which they are a party?

(…)
51. Online behavioural advertising, and associated tracking and profiling of data subjects, is often used to finance online services. (...)

52. As a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services. Normally, it would be hard to argue that the contract had not been performed because there were no behavioural ads. (...)

[25] Guidelines 2/2019 on the processing of personal data under Article 6.1.(b) of the GDPR in the context of the provision of online services to data subjects, October 8, 2019, pages 9-1 l and 16-17.

> 53. Further to this, article 6 (1) (b) cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service. Although such processing may support the delivery of a service, this in itself is not sufficient to establish that it is necessary for the performance of the contract at issue. The controller would need to consider the factors outlined in paragraph 33.

12.14. It follows from the above that the processing basis of contractual necessity must be interpreted strictly, whereby it is important to determine whether the processing is actually and objectively necessary for the performance of the contract. This includes what the user could reasonably expect.

12.15. The most essential feature of the agreement that a user of the Facebook service enters into with Facebook Ireland is, in the court's opinion, the provision of (a profile on) a social network. This is also what an average user was entitled to understand as the main objective of the user agreement. After all, the Facebook service presents itself as a social media platform and a social network. For example, prior to registration or login, the home screen of the Facebook service's website states in large letters, "With Facebook, you are connected and share everything with everyone in your life." The emphasis on the nature of social networking and keeping in touch with others is also evident in the way (a profile on) the Facebook platform is set up, with prominent attention to (finding) friends and sharing information. The fact that Facebook Ireland additionally shows its users personalized ads and has committed itself to this in the user agreement, is to that extent of minor importance and thus not decisive.

12.16. Since the main and mutually understood objective of the user agreement is to provide a profile on a social network, the question of necessity must be assessed in light of that objective. It has neither been stated nor shown that the provision of a profile on the social network cannot actually be carried out if the processing of personal data for advertising purposes does not take place. Such being impossible has not been established. Therefore, in order to provide a profile on the social network of the Facebook platform, it is not objectively and actually necessary for Facebook Ireland to process personal data of a user for advertising purposes.

12.17. The conclusion is therefore that the processing of personal data for advertising purposes is not necessary for the performance of the contract between Facebook Ireland and a user of the Facebook service. Thus, Facebook Ireland cannot successfully rely on contractual necessity (as referred to in section 8 opening words and (b) of the Wbp and article 6 (1) (b) of the GDPR, respectively) as a basis for processing, either under the Wbp or the GDPR.

12.18. This means that during the part of the relevant period when the GDPR was in force, there was no legally valid basis for Facebook Ireland's processing of (general) users' personal data for advertising purposes.

12.19. For the period when the Wbp applied, the two other bases (consent and legitimate interest) relied on by Facebook Ireland will be further assessed below.

Consent as a basis for processing?

12.20. Facebook Ireland adopts the position that it obtained consent from users to process their personal data for advertising purposes and it argues the following in this regard. Under the Wbp, consent could be obtained by providing data subjects with terms and policies informing them about data processing and ensuring that data subjects confirmed having read the terms and policies. In its Data Policy, Facebook Ireland informed users about the processing of personal data for advertising purposes. Until 2015, Facebook Ireland ensured that users confirmed that they had read (and in the

period 2015-2018 agreed to) the Data Policy before registering with the Facebook service. Facebook users thus expressly consented to the processing of their personal data in accordance with the Data Policy when they registered. In all versions of the Data Policy in effect over time, it was always made clear that Facebook Ireland used the personal data collected to personalize ads. There is no obligation to provide all information about data processing in the first information layer to be provided. According to WP29's recommendations, a layered information structure is permissible and even preferred, in part to prevent information fatigue. Facebook Ireland's Data Policy was designed to be as easy as possible for users to read and navigate. In that Data Policy, links were provided to other pages where further information could be found. Incidentally, users were also subject to a certain duty to investigate. Existing users were informed of changes to the Data Policy by means of, among other things, notifications and e-mails.

12.21. Stichting takes the view that Facebook Ireland did not obtain legally valid consent. To this end, it argues, in brief, the following. At no time during the relevant period did Facebook Ireland properly inform the Members about the processing of personal data for advertising purposes. Information about the purposes of data processing was fragmented and did not appear in the first layer of information. Facebook Ireland's layered privacy policy was laid out in such an unclear and cluttered manner that it was difficult for users to understand what was happening with their personal data. Instead of providing all relevant information about data processing succinctly and clearly in the first layer of information, it was offered in a fragmented and cluttered manner. Even if the Data Policy in its entirety were to be considered the first layer of information, the relevant information was not there in a concise, transparent and clearly worded manner. The requested consent for data processing was hidden in the Terms of Use. The Members could not know what they would consent to. Thus, the requested consent did not meet the requirements of free, specific, informed and unambiguous.

Assessment framework

12.22. With respect to the meaning and interpretation of the term consent, the court holds as follows.

12.23. Consent must be obtained prior to data processing.

12.24. In Article 1 opening words and (i) Wbp (implementing article 2 (h) of the Privacy Directive), the concept of consent is defined as follows: any freely-given, specific and informed expression of will by which the data subject accepts that personal data concerning him or her may be processed. Section 8 opening words and (a) Wbp stipulates that consent must have been given unambiguously.

12.25. This means that an expression of will must meet the following requirements before it constitutes consent as referred to in section 8 Wbp. The expression of will must be 1) free, 2) specific, 3) informed and 4) unambiguous. In addition, the expression of will must be aimed at acceptance of the processing of personal data concerning the data subject.

12.25.1. That the expression of will must be free means that the choice is made freely, i.e. without, for example, deception, intimidation or coercion. Nor should it be the case that the individual runs the risk of significant negative consequences if he does not consent.

12.25.2. That the expression of will must be specific means that it must relate to a particular data processing operation. It must be clear which processing, of which data, for which purpose will take place, and whether this involves disclosure to third parties, and which third parties.[26]

[26] See Parliamentary Papers II 1997/1998, 25 892, no. 3, p. 65.

12.25.3. That the expression of will must be based on information (informed consent) implies that the person concerned must have been provided with sufficient information to enable him to make a well-informed decision. The data subject must be informed in a clear and comprehensible manner about all relevant aspects. In this context, the duties of disclosure of sections 33 and 34 of the Wbp are also important. The Explanatory Memorandum to the Wbp states, among other things, the following about the requirement of informed consent[27]:

> (...) the data subject can only give his consent responsibly if he is informed in the best possible manner.(...) Seeking the data subject's consent implies that he must be informed of the course of events regarding the data processing. In principle, this duty, or duty of disclosure, rests with the responsible party and/or the data processor. The data subject must be adequately and comprehensibly informed by the controller about the various aspects of data processing that are of interest to him. The duty of disclosure of the controller is limited by the facts that the data subject already knows or should know. The duty of disclosure of the responsible party does not imply that the individual bears no responsibility. The data subject has a certain duty to investigate before forming his opinion. What is decisive for the extent to which the person responsible must inform the data subject or the data subject himself must has to perform an investigation is what may reasonably be expected in society. This will have to be determined by weighing all the circumstances of the specific case. Factors that may play a role in such weighing are the type of data in question, the processing operations that the controller intends to carry out as well as the context in which these operations will take place, any third parties to whom the data may be provided, etc., but also the social position and mutual relationship between the controller and the data subject as well as the manner in which they have come into contact with each other.

12.25.4. The requirement that consent be unambiguous means that there is no reasonable doubt as to the individual's intent in giving consent. The data subject must express his consent by affirmative action. The Explanatory Memorandum to the Wbp inter alia states the following about this requirement[28]:

> Tacit or implied consent is insufficient: the data subject must have expressed his or her will to consent to the data processing in question by word, writing or conduct. This explicit expression of will can come about in different ways. The most obvious is, of course, the data subject's explicit verbal or written consent to the processing. But under circumstances, the data subject's explicit consent may also be inferred from his or her behaviour. For example, filling out a form for the purpose of requesting a certain service may, under certain circumstances, be regarded as the granting of explicit consent by the data subject, namely if it is clear to the data subject from the context in which he or she fills out the form that his or her personal data are being processed and for what purpose.

12.26. For the interpretation of the concept of consent in the Privacy Directive, the district court also considers the opinions of WP29 important. In addition, since these proceedings concern services that take place online, the court also considers the EDPB guidelines in this regard, insofar as those guidelines deal with duties of disclosure in the digital context.

12.27. In 2011, WP29 issued a comprehensive opinion on the definition of consent in the Privacy Directive. Among other things, that opinion stated the following[29]:

> For a consent to be specific, it must first of all be comprehensible: it must be clear from the wording of the consent that the data subject is precisely aware of the scope and consequences of the data processing for which he is giving his consent. The consent cannot cover an open-ended set of processing activities.(...) The various elements of processing must be clearly defined and consent is required for each element. In particular, consent relates to the data being processed and the purposes for which it is being processed.

---

[27] Parliamentary Papers I 1997/l998, 25 892, no. 3, pp. 65-66.
[28] Parliamentary Papers II 1997/1998, 25 892, no. 3, p. 67.
[29] Opinion 15/2011 on the definition of "consent" (WP 187), adopted 13 July 2011, pp. 20, 23, 40 and 41.

Its understanding must be based on the reasonable expectations of the parties. It is therefore inherent in a "specific consent" that it is based on information (informed consent). For consent given in relation to the various elements of a processing operation, there is the requirement of differentiation: consent cannot be deemed to relate to "all legitimate purposes" of the controller. Furthermore, it (...) can only concern processing operations that are reasonable and necessary in view of their purpose.

(…)

- Quality of the information - The way the information is given (in plain text, without use of jargon, understandable, conspicuous) is crucial in assessing whether the consent is “informed”. The way in which this information should be given depends on the context: a regular/average user should be able to understand it.

- Accessibility and visibility of information - information must be given directly to individuals. It is not enough for information to be “available” somewhere. (…) The information must be clearly visible (type and size of fonts), prominent and comprehensive. Dialogue boxes can be used to give specific information at the time when consent is requested. As mentioned above in relation to “specific consent”, on-line information tools are especially useful in relation to social network services, in order to provide sufficient granularity and clarity to privacy settings. Layered notices can also be a useful tool here, as they contribute to giving the right information in an easily accessible way.

  (…)

- Consent must be specific. Blanket consent without determination of the exact purposes does not meet the threshold. Rather than inserting the information in the general conditions, this calls for the use of specific consent clauses, separated from the general terms and conditions.

- Consent must be informed. (...) The need for consent to be "informed" translates into two additional requirements. First, the way in which the information is given must ensure the use of appropriate language so that data subjects understand what they are consenting to and for what purposes. This is contextual. The use of overly complicated legal or technical jargon would not meet the requirements of the law. Second, the information provided to users should be clear and sufficiently conspicuous so that users cannot overlook it. The information must be provided directly to individuals. It is not enough for it to be merely available somewhere.

  (…)

- For data other than sensitive data, article 7 (a) requires consent to be *unambiguous*. "Unambiguous" calls for the use of mechanisms to obtain consent that leave no doubt as to the individual's intention to provide consent. In practical terms, this requirement enables data controllers to use different types of mechanisms to seek consent, ranging from statements to indicate agreement (express consent), to mechanisms that rely on actions that aim at indicating agreement.

- “Consent” based on an individual's inaction or silence would normally not constitute valid consent, especially in an on-line context. This is an issue that arises in particular with regard to the use of default settings which the data subject is required to modify in order to reject the processing. For example, this is the case with the use of pre-ticked boxes or Internet browser settings that are set by default to collect data.

  (…)

12.28. Also relevant in this context are the Guidelines on Transparency under Regulation (EU)2016/679 of 1 April 2018 of the Article 29 Data Protection Working Party on layered privacy statements in the digital context mentioned above in 11.13.

Assessment of individual periods

12.29. During the time that the Wbp was applicable, the provision of information by Facebook Ireland and the manner in which it sought consent for the processing of personal data differed. For example, over time the registration process differed and Facebook Ireland successively applied different Terms of Use and Data Policies. Like the parties, the district court will therefore distinguish between three periods of time (periods A, B and C) in its assessment.

- PERIOD A (1 April 2010 - 8 June 2012)

12.30. Facebook Ireland has explained (which has not been contradicted) that the account registration of a new user during this period consisted of two steps and went as follows. After the new user had entered his initial information, such as name, email address and password, he was directed to a second page. On that second page, he could click on a "Register" button. This stated, that by clicking the 'Register' button the user confirmed that he agreed to the terms and conditions and that he had read the Data Policy. This text contained a hyperlink to the Terms of Use and the Data Policy.

12.31. The versions (in English) of the Data Policy applicable in those days (called: Privacy Policy) were always four or five pages in a relatively small font. In the version of the Data Policy of 22 December 2010, the following was among other things mentioned:

> **5. How We Use Your Information**
>
> We use the information we collect to try to provide a safe, efficient, and customized experience. Here are some of the details how we do that:
>
> **To manage the service**. We use the information we collect to provide our services and features to you, to measure and improve those services and features, and to provide you with customer support. We use the information to prevent potentially illegal activities, and to enforce our Statement of Rights and Responsibilities. We also use a variety of technological systems to detect an address anomalous activity and screen content to prevent abuse such as spam. These efforts may on occasion result in a temporary or permanent suspension or termination of some functions for some users.
>
> **To contact you.** We may contact you from time to time. You may opt out of all communications except essential updates on your account notifications page. We may include content you see on Facebook in the emails we send to you.
>
> **To serve personalized advertising to you.** We don't share your information with advertisers without your consent. (...) We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are. You can see the criteria advertisers may select by visiting our advertising page. Even though we do not share your information with advertisers without your consent, when you click on or otherwise interact with an advertisement there is a possibility that the advertiser may place a cookie in your browser and note that it meets the criteria they selected.

To serve social ads. We occasionally pair advertisements we serve with relevant information we have about you and your friends to make advertisements more interesting and more tailored to you and your friends. For example, if you connect with your favourite band's page, we may display your name and profile photo next to an advertisement for that page that is displayed to your friends. We only share the personally identifiable information visible in the social ad with the friend who can see the ad. You can opt out of having your information used in social ads on this help page.

To supplement your profile. (...)

To make suggestions. (...)

To help your friends find you. (. ..)

(…)

12.32. The other versions of the Data Policy in effect during this period contained information in the same or similar terms about how Facebook Ireland uses its users' information.

12.33. The question to be answered is whether the reading confirmation obtained by Facebook Ireland in period A when registering its users can be considered a legally valid consent to the processing of personal data for advertising purposes. The district court answers that question in the negative.

12.34. It is not in dispute that information about data processing was in the Data Policy. However, users did not give their consent with respect to the content of the Data Policy upon registration. As the course of events outlined by Facebook Ireland shows, upon registration, a user merely stated their agreement with the Terms of Use. With respect to the Data Policy, upon registration, a user confirmed having read only that policy. The confirmation of having read something does not, at least not automatically, qualify as a statement of agreement to its contents. From the way Facebook Ireland had structured the registration process, it could not, or not sufficiently, be clear to the average user in this case that they were being asked for consent to processing purposes included in the Data Policy. After all, unlike in the case of the Terms of Use, the user was not expressly asked for consent with regard to the Data Policy. Thus, there was no unambiguous and acceptance-oriented expression of will. Moreover, the registration process did not make it clear that the Data Policy contained information about the processing of personal data. As a result, the reading confirmation in the registration process also cannot be an expression of will aimed at acceptance of the processing of personal data concerning the user.
In view of the foregoing alone, the reading confirmation does not constitute consent.

12.35. To the extent that Facebook Ireland has intended to argue that the reading confirmation upon registration combined with the use of the Facebook service qualifies as such as a valid consent because of the expectations that the user was entitled to have, the court rejects that position. A user who signs up for the Facebook service may expect his personal data to be processed by Facebook Ireland for the purpose of Facebook Ireland facilitating the user's participation in the social network provided by the Facebook platform. In the opinion of the court, on the other hand, an average user - contrary to what Facebook Ireland has argued - does not have to be aware that his personal data are also processed for other purposes, such as the advertising purposes used by Facebook Ireland. For this reason, it also cannot be said that the user was under a duty to investigate in this regard. In this case, therefore, the use of the Facebook service does not imply (unambiguous) consent to the processing of personal data for advertising purposes.

12.36. The circumstance that users (on other pages that may be reached through the Data Policy) within the Facebook platform could themselves set up how Facebook Ireland was allowed to process their personal data for advertising purposes is not important. Indeed, what matters is that the user must be informed in advance of such data processing and that prior consent must be obtained.

12.37. The foregoing means that Facebook Ireland cannot rely on the reading confirmation of the Data Policy upon registration for the required consent to process personal data for advertising purposes.

12.38. Facebook Ireland has furthermore referred to subsequent statements of agreement that existing users gave, according to Facebook Ireland, when changes were made to the Data Policy. Again, this cannot benefit Facebook Ireland. In those cases, a user received a message or notification stating that, by continuing to use Facebook Ireland's services, the user agreed to updated Terms of Use, Data Policy and Cookie Policy. The continued use after having read such a notice cannot be regarded as a specific, informed and unambiguous expression of will for the processing of personal data for advertising purposes. Indeed, the information relevant to such processing was not provided in the message or notice, and the mere reference therein to amended Terms of Use and/or Data Policy does not meet the relevant requirements.

12.39. It has neither been alleged nor demonstrated that, in addition to what has been discussed above, Facebook Ireland sought and obtained consent to the processing of personal data for advertising purposes in any other way.

12.40. It is therefore concluded that in period A, Facebook Ireland did not obtain legally valid consent from the Members for data processing operations for advertising purposes.

- PERIOD B (8 June 2012 - 30 January 2015)

12.41. Facebook Ireland has explained (which has not been contradicted) that that a new user seeking to register with the Facebook service during this period was shown the following:

If you click Register, you confirm that you agree not to our Terms and Conditions and that you have read our Privacy Policy, including our use of cookies

Image 43 (2012 - 2014)

By clicking Register, you agree to our terms and conditions and confirm that you have read our data policy, including our policy on the use of cookies

Image 44 (2014 - 2018)

ln the text above the ‘Register' button were hyperlinks to the Terms of Use, Data Policy and the cookie policy.

12.42. The versions of the Data Policy (in Dutch) applicable during this period covered about seven pages in a relatively small font. The version of the Data Policy of 8 June 2012 among other things stated the following:

How do we use the information we receive

We use the data we receive about you for the services and functions we provide to you and other users, such as your friends, our partners, the advertisers who buy ads on the site and the developers who create the games, applications and websites you use. For example, we may use the information we receive about you:
- to keep Facebook products, services and integrations secure;
- to protect the rights or the property of Facebook and others;
- to provide you with location features and services, such as notifying you and your friends that an event is taking place nearby;
- to measure or better understand the effectiveness of the ads you and others see, such as displaying ads that are relevant to you;
- to make suggestions to you and other users on Facebook, such as: that your friends can use the contact import function because you also found friends this way, or that another user adds you as a friend because the user imported the same email address as you, or that your friend tags you in a photo with you in it that he or she uploaded, and;
- for internal operations, such as troubleshooting, data analysis, testing, research and service improvement.

By giving us this permission, you not only enable us to offer Facebook as it is today, but you also let us develop innovative features and services that use the information we receive about you in new ways.

You remain the owner of all your data, even if you give us permission to use the data we hold about you. Your trust is important to us and therefore we will not share data about you with others unless we:
- have your permission to do so;
- have notified you of this by, for example, informing you through this policy; or
- have removed your name or other information that could identify you personally from it.

Of course, for information about you that others share, they determine how it is shared.

12.43. The other versions of the Data Policy in effect during this period contained information in the same or similar terms about how Facebook Ireland uses its users' information.

12.44. In the district court's opinion, in period B the method of registration, the reading confirmation by the user and the content and method of providing information by Facebook Ireland were not substantially different from period A. Therefore, what the District Court considered above in grounds 12.33-12.39 regarding period A also applies to period B. This means that the required consent for period B too cannot be based on the reading confirmation upon registration or on subsequent statements of agreement to changes to the Data Policy.

12.45. The above means that, also in period B, Facebook did not obtain legally valid consent from the Members for data processing for advertising purposes.

- PERIOD C (30 January 2015 – 19 April 2018)

12.46. Facebook Ireland has explained (which has not been contradicted) that a new user seeking to register with the Facebook service during this period was shown the following:

By clicking Register, you agree to our terms and conditions and confirm that you have read our data policy, including our policy on the use of cookies

Image 44 (2014 - 2018)

In the text above the 'Register' button were hyperlinks to the Terms of Use, Data Policy and the cookie policy.

12.47. The version of the Terms of Use (in Dutch) applicable during this period (with effect from 30 January 2015) (entitled *Statement of Rights and responsibilities*) covered four pages in a relatively small font and contained 18 different provisions. At the end of the Terms of Use it stated (in bold):

> **By using or accessing Facebook services, you agree that we may use and collect this content and information in accordance with the Data policy that may be amended from time to time.**

12.48. The versions of the Data Policy (in Dutch) applicable during this period covered approximately two pages in a relatively small font. In the version of 30 January 2015 of the Data Policy, the following is among other things stated:

I. What types of data are collected?

We collect different types of information from and about you, depending on the services you use.

- **Things you do and data you provide.** We collect the content and other data you provide when you use our services, including when you sign up for an account, create or share items, and when you send messages and communicate with others. This may relate to data in and about the content you provide, such as the location of a picture or the date a file was created. We also collect data about how you use our services, such as the types of content you view and respond to, or the regularity and duration of your activities.
- **Things others do and data they provide.** We also collect content and information that other people provide when they use our services, including data about you, when, for example, they share a picture of you, send you a message, or upload, synchronise or import your contact data.
- **Your networks and connections**. We collect data about the people and groups you are connected to and how you treat these people and groups, such as the people you communicate with the most or the groups you share a lot with. We also collect contact information you provide when you upload, synchronise or import this data (such as an address book) from a device.
- **Payment Data**. When you use our services for purchases or financial transactions (such as when you buy something on Facebook, make a purchase in a game, or make a donation), we collect information about the purchase or transaction. Among other things, we collect your payment information, such as your credit or debit card number and other card information, other account and authentication information, and details related to billing, shipping, and contact information.
- **Device Data.** We collect data from and about the computers, phones and other devices on which you install or access our services, depending on what you have consented to. We may link the data collected to your different devices. This helps us offer consistent services across all your devices. Here are some examples of the data we collect:
    - Features such as operating system, hardware version, device settings, file and software names and file and software types, battery and signal strength, and device IDs.
    - Device locations, including certain geographical locations determined via GPS, Bluetooth or Wi-Fi signals.
    - Connection information such as the name of your mobile carrier or Internet service provider, browser type, language and time zone, cell phone number and IP address.
- **Information from websites or apps that use our services.** We collect information when you visit third-party websites and apps that use our services (for example, when they offer the Like button, Facebook sign-in feature, or use our measurement and advertising services). Among other things, we collect information about the websites and apps you visit, your use of our services on those websites and apps. and the information the developer or publisher of the app or website gives you or us.

- **Data from external partners.** We receive data about you and your activities from external partners, such as when a partner and Facebook offer services together, or data from an advertiser about your experiences and your interactions.
- **Facebook companies.** We receive data about you from companies owned or controlled by Facebook in accordance with the terms and policies of those companies. Learn more about these companies and their privacy policies.

II. How do we use this data?

We are enthusiastic about creating interesting and customized experiences for people. We use the data in our possession to deliver and support our services. Here's how this works:

- **Deliver, improve and develop services**. We can provide our Services, personalized content and suggestions by using data to understand how you use our Services and interact with the people or things you are connected to and interested in on and off our services.

We also use this data to offer you shortcuts and suggestions. For example, we may suggest your friend to put you in a photo by comparing your friend's photos with the data we've collected from your profile photos and the other photos you've been tagged in. If this feature is enabled for you, you determine whether we suggest other users to layer you in a photo. You do this using the options in the Timeline and tagging settings.
When we have location data, we use it to customize our services for you and others, such as helping you check in and find local events, displaying deals in your area or letting your friends know you're nearby.

We conduct surveys and research, test features under development, and analyse our data to evaluate and improve our products and services, develop new products and features. We also conduct audits and troubleshoot problems.

- **Communicating with you.** We use your information to send you marketing messages, communicate with you about our services, and notify you about our policies and terms. We also use your information to respond when you contact us

- **Measure and display ads and services.** We use the data we hold to improve our advertising and measurement systems so that we can show you relevant ads on and off our services and measure the effectiveness and reach of ads and services. More information about advertising through our services and how you can check the manner in which personal data is used to personalize the ads you see.
- **Promoting Safety and Security**. We use the information in our possession to help verify accounts and activities, and to promote safety and security on and off our services, such as by investigating suspicious activity or violations of our terms and policies. We work hard to protect your account with a team of technicians, automated systems and advanced technology such as encryption and machine language. We also offer easy-to-use security tools as an additional layer of protection for your account. To learn more about promoting security on Facebook, visit Facebook's Security Help centre.
(…)

III. How will this data be shared?

(…)
<u>Sharing with external partners and customers</u>

We partner with outside companies that help us offer and improve our services, or use advertising or related products. These partnerships allow us to run our businesses and offer free services to people around the world.

The following are the types of outside parties with whom we may share your data:

- **Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only).** We want our ads to be as relevant and interesting as the other information on our services. With this in mind, we use all of our information about you to show you relevant ads. We do not share information that makes you personally identifiable (personally identifiable information is information such as a name or an e-mail address that can be used to contact you or identify you) with partners for advertising, measurement, or analytics purposes unless you consent. We can provide these partners with information about the reach and effectiveness of their ads without disclosing information that personally identifies you, or we may aggregate multiple people's information to the same effect. For example, we may tell an advertiser how its ads are performing, how often the ads have been shown or how often an app has been installed after displaying an ad, or provide non-personally identifiable demographic data (e.g., a 25-year-old woman in Madrid who is interested in software development) to these partners to give them insight into their target audience or customers, but we only do this after the advertiser has agreed to abide by our advertising guidelines. View your advertising preferences for an explanation of why you see a particular ad on Facebook. You can customize your ad preferences if you want to control and manage your experience of ads on Facebook.

12.49. The other version of the Data Policy in effect during this period contained, in the same or similar terms, information about how Facebook Ireland uses and shares its users' information.

12.50. It must be assessed whether Facebook Ireland validly obtained consent to the processing of personal data for advertising purposes in period C during the registration process of a new user.

12.51. It is well established that the information at the "Register" button in period C was the same as in periods A and B. The user was also informed at the "Register" button in period C that he agreed to the Terms of Use. When it came to the Data Policy, the user only confirmed that he had read that policy. Facebook Ireland has argued that the user nevertheless agreed to the Data Policy because that agreement was in the Terms of Use in Period C. The court considers that this graduated form of obtaining consent in this case does not meet the requirements for consent under article 7 Privacy Directive. The reasons for this are the following.

12.52. Although the user was asked to agree to the Terms of Use in the registration screen, in order to see what he agreed to, he had to click through and consult the Terms of Use. That in itself is not an impermissible method of obtaining consent, but in that case that document must contain the most important information about data processing. That was not the case here. It was neither stated nor shown that the Terms of Use contained (adequate) information about data processing for advertising purposes. At the end of the Terms of Use it was stated that, by using or accessing Facebook services, the user agrees that Facebook Ireland may use and collect such content and information in accordance with the Data Policy. Such ‘consent’, hidden in Terms of Use, which moreover in turn refers to another layer of information, is too indirect to qualify as an unambiguous expression of will. An average user, when clicking the "Register" button, even after consulting the Terms of Use, will not reasonably be aware of which data processing operations he is deemed to have given his consent to.

12.53. This indirect and veiled way of attempting to obtain consent also fails to meet the requirements that the requested consent must be sufficiently specific and information-based. The generally worded 'consent' at the end of the Terms of Use is simply not specific enough. Also, the information about data processing was not provided directly where consent was requested (in the screen to register or in the Terms of Use), but in another place, namely in the Data Policy. In this way, Facebook Ireland has made it too difficult for the average user to be adequately informed of the relevant information about data processing. The above means that an average user was not able to understand the full extent of the consequences of the data processing.

12.54. Thus, when registering a new user, Facebook Ireland did not obtain consent for data processing for advertising purposes, nor was consent otherwise obtained. In this regard, the same applies as what has been held above in grounds 12.36, 12.38 and 12.39.

12.55. Even in period C, therefore, Facebook did not obtain legally valid consent from the Members to process their data for advertising purposes.

Legitimate interest as a processing basis?

12.56. Facebook Ireland takes the position that under the Data Protection Act it had a legitimate interest in processing personal data for advertising purposes. To this end, it argues the following. Facebook Ireland has always been able to offer users a free service thanks to advertisements. Facebook Ireland's business model is based on the sale of personalized advertising space on the Facebook platform. Such an "ad-driven" business model has become commonplace among online service providers, and there is also a legitimate economic interest in that model. Without revenue from personalized ads, Facebook Ireland would not be able to offer its users a free service. Facebook Ireland's legitimate interest in providing a personalized experience did not interfere with the interests or fundamental rights and freedoms of users. On the contrary, both Facebook Ireland and users benefit from personalization providing users with a better experience on the Facebook platform. If any rights or interests of data subjects were at stake, it is hard to see why they prevailed over Facebook Ireland's legitimate interest. Indeed, users could reasonably expect that the Facebook service would be provided free of charge and that their personal data would be processed for advertising purposes and personalized ads. Moreover, users had several opportunities to exercise control over their data processing and advertising preferences through privacy settings.

12.57. Stichting disputes that Facebook Ireland can use the "legitimate interest" basis to process personal data for advertising purposes. To this end, it argues the following. The commercialization of a service supposedly offered for free is not a legitimate interest. In addition, the processing is not necessary to pursue that interest. Indeed, offering personalized ads is not necessary to offer the Facebook service; the Facebook service works even without personalized ads. Also relevant with respect to the requirement of necessity is the fact that Facebook Ireland has not transparently informed its users. This means that the same purpose could have been achieved by less infringing means. Finally, the requirement that the interests or fundamental rights of users are not disproportionately affected has not been met, because Facebook Ireland has not performed any actual balancing of interests. The abstract balancing of interests made by Facebook Ireland is not sufficient.

12.58. In assessing whether data processing for advertising purposes is necessary to pursue the legitimate interest of the data controller, the district court will not only consider the case law of the CJEU, but also the opinions of WP29.

12.59. According to established case law[30] of the CJEU, three cumulative conditions must be met in order for personal data to be processed on the basis of legitimate interest:

1. processing is necessary for the purposes of the legitimate interests pursued by the controller (or by the third party or parties to whom the data are disclosed);
2. there must be a need to process personal data for the purposes of the legitimate interests pursued, and
3. the fundamental rights and freedoms of the person whose personal data are processed do not take precedence.

12.60. CJEU case law shows that a legitimate interest (the first condition) must be present and effective as at the date of the data processing and must not be hypothetical at that date.[31]

12.61. WP29 issued an opinion on the concept of legitimate interest in article 7 of the Privacy Directive (whose implementation was section 8 Wbp). Among other things, that opinion stated the following[32]:

> The concept of "interest" is closely related to, but different from, the concept of "purpose" mentioned in article 6 of the Directive. In the data protection context, the "purpose" is the specific reason why the data are processed: the objective or purpose of the data processing. However, interest is a broader concept and refers to the value to the controller of the processing or the benefit that the controller, or society, may derive from the processing.
>
> An interest must be articulated with sufficient clarity to perform the balancing with the interests and fundamental rights of the data subject. Moreover, the processing must also be necessary for "the protection of the relevant interest of the controller." This requires a real and present interest, something corresponding to current activities or benefits expected in the very near future. In other words, interests that are too vague or speculative are insufficient. The nature of the interest may vary. Some interests are weighty and benefit society as a whole, such as the press's interest in publishing information about corruption in government or the interest in conducting scientific research (subject to appropriate safeguards). Alternatively, interests may be less pressing for society as a whole or at least the consequences of pursuing them for society may be more mixed or controversial. This may be the case, for example, with a company's economic interest in knowing as much as possible about potential customers so that advertisements about its products or services can be better targeted.
>
> (...) The Working Party considers that the concept of "legitimate interest" can encompass a wide range of interests, to a greater or lesser extent weighty, obvious or controversial. At the second step, when these interests must be balanced against the interests and fundamental rights of the data subject, a more limited approach and more substantial analysis must then be followed.
>
> An interest may therefore be considered legitimate as long as the data controller can pursue it in a manner consistent with data protection laws and other laws. In other words, a legitimate interest must be "acceptable under the law."
>
> Therefore, to be relevant under article 7 (f), a "legitimate interest" must:
> - be lawful (i.e. in accordance with applicable EU and national law);
> - be articulated with sufficient clarity to allow for a balancing with the interests and fundamental rights of the data subject (i.e., sufficiently specific);
> - represent a real and present interest (i.e. must not be speculative).

---

[30] See, for example, CJEU 29 July 2019, C-40/17, ECLI:EU:C:2019:629 (Fashion ID), para. 95.
[31] CJEU 11 December 2019, C-708/18, ECL[:EU:C:2019:1064(TK /M5A-Scara), para. 44.
[32] WP29 Opinion 06/2014 on the notion of “the legitimate interest of the data processor” in article 7 of Directive 95/46/EC (WP217), adopted 9 April 2014, pages 29-31.

12.62. With regard to the second condition - that the data processing is necessary to pursue the legitimate interest of the controller - according to established case law of the CJEU, the exceptions to the protection of personal data and their limitations must remain within the limits of what is strictly necessary.[33]

12.63. WP29's 2014 opinion[34] includes the following on the second condition:

> This condition complements the necessity requirement under article 6 [of the Privacy Directive, addition district court] and requires a link between the processing and the interests served. This "necessity requirement" is applicable in all the processing operations listed in article 7 (b) - (f) [of the Privacy Directive, addition district court], but is particularly important in the case under (f) to ensure that data processing on the basis of legitimate interest does not lead to an overly broad interpretation of the criterion on the necessity to process data. As in other cases, this involves considering whether less intrusive means are available to achieve the same purpose.

12.64. In determining whether the necessity requirement is met, the requirements of proportionality and subsidiarity must be assessed in particular. The principle of proportionality means that the interference with the interests of the data subject should not be disproportionate in relation to the purposes to be served by the processing. Under the principle of subsidiarity, it should not be reasonably possible to achieve the purposes for which the personal data are processed in another way, which is less prejudicial to the data subject.

12.65. As regards the third condition – the (further) balancing of the relevant rights and interests - established case law of the CJEU has ruled that such balancing and the outcome thereof depends in principle on the specific circumstances of a particular case.[35]

12.66. WP29's 2014 opinion[36] among other things states the following about the third condition:

> It is useful to present both the legitimate interest of the data controller and the interest and rights of data subjects on a spectrum. Justified interest can range from insignificant to somewhat important to weighty. Similarly, the impact on the interest and rights of the data subject may be more or less significant and range from insignificant to very serious.
>
> (…)
>
> *Key factors to be taken into account in the balancing of interests*
>
> Based on the foregoing, the useful factors to be considered in the balancing of interests include:
>
> • <u>the nature and source of the legitimate interest</u>, including:
> - the circumstance whether or not the data processing is necessary for the exercise of a fundamental right, or
> - is otherwise in the public interest or recognized in the relevant community socially, culturally or by law or regulation;
>
> • <u>the impact on those affected</u>, including:

[33] See, for example, CJEU May 4, 2017, C-13/16, ECLI:EU:C:2017:336(Rigas), para. 30.
[34] WP29 Opinion 06/2014 on the concept of legitimate interest of the data controller" in Article 7 of Directive 95/46/EC(WP217), adopted April 9, 2014, page 35.
[35] See, for example, CJEU 4 May 2017. C-13/16, ECLI:EU:C:2017:336 (Rigas), para. 31.
[36] WP29 Opinion 06/2014 on the concept of "the legitimate interest of the data controller" in article 7 of Directive 95/46/EC (WP217), adopted 9 April 2014, pages 36 and 60- 62.

- the nature of the data, such as whether or not the processing involves data that may be considered sensitive or obtained from publicly available sources,
- the manner in which the data are processed, including whether or not the data are made public or otherwise accessible to a large number of individuals or whether large amounts of personal data are processed in combination with other data (e.g., in the case of profiling, for commercial, law enforcement or other purposes),
- the reasonable expectations of the data subject, particularly with regard to the use and disclosure of the data in the relevant context,
- the status of the data controller and the data subject, including the balance of power between the data subject and the data controller and the factor of whether the data subject is a child or otherwise belongs to a more vulnerable segment of the population;

• additional safeguards to prevent undue impact on data subjects, including:
- data minimization (e.g. strict limitation of data collection, or the immediate deletion of data after use),
- technical and organizational measures to ensure that data cannot be used to make decisions or take other actions regarding individuals ("functional separation"),
- extensive use of anonymization techniques, data aggregation, privacy enhancing technologies, "Privacy by Design," privacy and data protection impact assessments,
- improved transparency, a general and unconditional right to opt-out, data portability and related measures to provide greater control to data subjects.

Accountability, transparency, the right to object and more

In connection with these safeguards and the overall balancing of interests, three issues often play a crucial role in the context of article 7 (f), and therefore require special attention:

- the existence of some, and possible need for, additional measures to improve transparency and accountability;
- the data subject's right to object to the processing, and beyond that objection, the availability of an opt-out option without the need for further justification;
- giving data subjects more control: data portability and the availability of useful mechanisms for data subjects to access their own data and modify, delete, transfer or otherwise further process it (or have third parties further process it).

12.67. In the context of the first condition, it must be assessed whether Facebook Ireland has a legitimate interest in processing personal data for advertising purposes. The interest that Facebook Ireland claims to pursue with such processing is related to the business model it uses, which is based on the sale of personalized advertising space, and includes being able to offer users a personalized experience. Without the revenue from personalized advertising, Facebook Ireland argues, it would not be able to offer its users a free service. This shows that commercial interests play an important role for Facebook Ireland when processing personal data for advertising purposes.

12.68. The CJEU has not yet ruled on the question of whether commercial interests can constitute a legitimate interest. On that question, the administrative judge of this court recently submitted preliminary questions to the CJEU.[37] For the assessment of the dispute between Stichting and Facebook Ireland, however, it is not necessary to await the answer to those questions by the CJEU. Reference is made to the opinion to be given below in rulings 12.69-12.71.
Contrary to what has been argued by Stichting, the district court for the present moment sees no reason to assume that commercial interests could not be regarded as a legitimate interest within the meaning of article 7 (f) of the Privacy Directive and section 8 opening words and (f) of the Wbp. The case law of the CJEU does not show this and neither does the WP29 opinion. On the contrary, the WP29 opinion also cites economic interests of companies as examples. The requirements mentioned

[37] Amsterdam District Court Sept. 22, 2022, ECLI:NL:RBAMS:2022:5565.

by the CJEU and in the WP29 opinion, namely that the alleged legitimate interest must be existing, actual (present), not of hypothetical nature (effective) and legitimate, are in any case satisfied by the legitimate interest alleged by Facebook Ireland. The court therefore presumes that Facebook Ireland had a legitimate interest when processing personal data for advertising purposes and that the first condition has therefore been met.

12.69. As a second condition, the necessity requirement must be met. This requires an assessment in the light of the requirements of proportionality and subsidiarity. To make that assessment possible, Facebook Ireland - on whom the burden of proof of lawful data processing rests - must provide insight into the considerations it has made and provide sufficient relevant factual information. It has not done so sufficiently. Facebook Ireland has not clearly addressed the requirements of proportionality and subsidiarity in its arguments. It has merely stated that its interests and those of its users run parallel because users also benefit from personalization. By doing so, Facebook Ireland fails to recognize that users have a right to, and an interest in, the protection of their privacy and their personal data, and that the processing of personal data for advertising purposes may prejudice this. Furthermore, the controller must take into account the reasonable expectations of data subjects. It has not been shown that Facebook Ireland has actually done so. It has merely argued that users of the Facebook service reasonably expected that their personal data would be processed, because they had been clearly informed about this. The court does not follow Facebook Ireland in this. For the question of whether sufficient clear information was provided in this regard, it must be taken into account that users of a service presented as free often are not fully aware of the extent to which their personal data are processed and their activities are tracked. The controller should therefore be transparent about those processing operations and about its business model. This means that it must also be made clear to users that in return for offering the service for free, users' personal data will be processed for advertising purposes. Facebook Ireland has not been sufficiently transparent about this in its terms and conditions and its data policy. Moreover, when it comes to the possibilities that Facebook Ireland claims to have offered users to exercise control over the processing of their personal data and advertising preferences through the various privacy settings, it is noted that these settings were scattered over many different sections and web pages of the Facebook platform and were therefore not very clear. In addition, asking for consent to data processing should be less infringing. The consent requested by Facebook Ireland did not meet the necessary requirements. By not validly requesting consent where it could have been requested, the requirements of proportionality and subsidiarity were not met either.

12.70. Finally, it can be added to the above that Facebook Ireland has not refuted Stichting's position that Facebook Ireland can also limit itself to the sale of advertisements that are not personalized, or less personalized. This can also generate advertising revenue. It has neither been argued nor shown that in such a case offering the Facebook service for free would not be possible. This means that it must be assumed that the purpose for which the personal data were processed could also be achieved in this respect in another manner, which would be less detrimental to the data subject.

12.71. What has been held above means that Facebook Ireland has not demonstrated that its data processing for advertising purposes meets the requirements of proportionality and subsidiarity. Since the second condition of section 8 opening words and (f) of the Wbp has not been met, the third condition no longer requires discussion.

12.72. The conclusion is that it has not been established that the processing of personal data for advertising purposes was necessary for a legitimate interest of Facebook Ireland. Therefore, for such processing during the Wbp period, the provisions of section 8 opening words and (f) Wbp cannot serve as a basis for processing either.

Conclusion processing bases

12.73. In conclusion, Facebook Ireland cannot rely on any of the processing bases it has relied on with regard to the processing of personal data for advertising purposes. It has neither been argued nor shown that any other processing basis qualifies for such processing. This means that the processing of Personal Data of Members for advertising purposes throughout the period 1 April 2010 - 1 January 2020 was not permissible. By processing those personal data for advertising purposes, without having a legal basis for doing so, Facebook Ireland infringed the Members' fundamental right to data protection as protected by, inter alia, article 8 ECHR. By so acting, Facebook Ireland has acted unlawfully towards the Members. The declaratory judgment as requested by Stichting in a.ii.1 may therefore be granted for the entire period 1 April 2010 - 1 January 2020.

13. Special personal data

13.1. Under section 16 Wbp and article 9 GDPR, the processing of special personal data is prohibited, subject to exceptions specified in the law. Special personal data include data relating to a person's religion, belief, race, political affiliation, health, sexual life and trade union membership. Since the entry into force of the GDPR, genetic and biometric data are also covered by the prohibition.

13.2. One of the most important grounds for exception under which it is permitted to process special personal data is obtaining explicit consent. Under both the Wbp, and the GDPR, the burden of proof that explicit consent has been given is on the party processing the special personal data.

13.3. Stichting claims that Facebook Ireland violated the ban on processing special personal data by using such Members data for advertising purposes without their consent during the relevant period.

13.4. Facebook Ireland disputes the alleged violation. Facebook Ireland argues that it does not use special personal data for advertising purposes. Facebook Ireland only looks at likes and which ads a user clicks on. Facebook Ireland's ad interest categories compiled from that information do not represent special personal data, nor did Facebook Ireland intend to infer these from those categories. These interest categories merely reflect interests, they do not concern personal qualifications and do not reveal these either. Furthermore, Facebook Ireland uses an unambiguous "user consent module" that requires the users' explicit consent before Facebook Ireland starts to process any special personal data of those users. The documents referred to by Stichting in support of its contentions refer to the period before the introduction of the GDPR and do not suffice as substantiation.

Does Facebook process special personal data?

13.5. Facebook Ireland's most far-reaching position is that it does not process any special personal data at all for advertising purposes. In the debate in this regard, the parties make a distinction between (i) data that Facebook Ireland obtains by allowing users to fill in special data in the profile fields when signing up for the Facebook service (voluntarily) and (ii) data that Facebook Ireland obtains by monitoring users' surfing behaviour and deriving certain interests from it.

(i) profile fields

13.6. Stichting argues that Facebook Ireland uses the special data obtained from the profile fields for advertising purposes, basing its argument in particular on the Dutch DPA report. Facebook Ireland

disputes Stichting's allegations and argues that it does not process data entered in a user's profile fields for the purpose of offering personalized ads.

13.7. The court does not agree with Facebook Ireland's view. The Dutch DPA report shows that it conducted its own investigation, using a fictitious user of the Facebook service and a fictitious website. Based on that investigation, the Dutch DPA concludes that the Facebook group (to which Facebook Ireland belongs) processes special data of sexual orientation for advertising purposes. According to the Dutch DPA, the Facebook group enables advertisers to show targeted ads to people in the Netherlands based on their sexual orientation as they have indicated these themselves in their profiles. The Dutch DPA conducted a further investigation, further to the argument that Facebook Ireland does not use data from the content of profiles. Using ten accounts that had been created (with which no activities were subsequently performed), the Dutch DPA found that information from the profile fields was in fact used, as some of these accounts received ads related to their profile. Facebook Ireland has insufficiently specifically challenged the findings and outcomes of the Dutch DPA's investigation. It has not come up with a logical explanation for these findings, limiting itself to the argument that the court is not bound by the content of the report and that, since no sanctions were imposed as a result of the report, Facebook Ireland did not have the opportunity to challenge the content of the report. However, given the results of the investigation in the Dutch DPA report, Facebook Ireland cannot confine itself to a mere challenge. Apart from the fact that the report shows that Facebook et al. were given the opportunity to respond and that this did not lead to a different conclusion, in the present proceedings Facebook Ireland has failed to dispute the results of the Dutch DPA report in concrete terms and with reasons.

13.8. The court therefore finds that Facebook Ireland processed special personal data for advertising purposes that users entered in the profile fields. Regarding the period after the date of the Dutch DPA Report (21 February 2017), Stichting has not provided any reasoned substantiation for its claim, so that, in view of Facebook Ireland's challenge, the district court is unable to establish whether it also processed special personal data from profile fields in that period for advertising purposes.

(ii) online behavioural advertising

13.9. Stichting argues that the interests that Facebook Ireland derives from the personal data it obtains by tracking the surfing behaviour of members of the Members also fall under special data within the meaning of section 16 of the Wbp and article 9 of the GDPR. Stichting points out that, according to the Dutch DPA's investigation, at least in the period 8 June 2012 - 30 January 2015 and in the period 30 January 2015 - 19 April 2018, Facebook Ireland offered advertisers the option to choose from interests that were divided into main categories and subcategories. It follows from the Dutch DPA's report that advertisers could select on the basis of, for example, "health," "Islam" or "pregnancy" or by sexual orientation.

13.10. Facebook Ireland disputes this, arguing that the data obtained only show possible interest by a user in a particular theme. The interests are at most indirectly related to special personal data and are not to be regarded as a processing thereof within the meaning of the law. By way of illustration; if a Facebook user likes a page about "pregnancy" (clicks the like button), this of course does not mean that he or she is pregnant, it could also be, for example, a midwife. There is no direct connection between interest in pregnancy and special personal data relating to a person's health.

13.11. The court does not agree with Facebook Ireland in this. Contrary to what Facebook Ireland argues, when special personal data are processed, such a high level of protection applies, that a direct connection between the interest and the user's special personal data is not required. This applies under both the Wbp and the GDPR. What matters is whether the processing of data may

reveal special personal data. That not all processing resulting from the tracking of the surfing behaviour of users reveals special personal data - as in the example cited above by Facebook Ireland - is correct, but it may be assumed that the tracking of surfing behaviour and the grouping of users into interest categories such as "interested in men" or "interested in women" may lead to the processing of special personal data. If this processing takes place for advertising purposes without the user's consent, there is no legal basis, thus causing it to be unlawful. Unlike Facebook Ireland argues, the processing of special personal data is moreover subject to such a high level of protection, that the accuracy of the data collected or the purpose of the collection is irrelevant. The court sees support for this opinion in the CJEU judgment of 1 August 2022 (OT/Vtec)[38] which states as follows in 127:

> Consequently, those provisions cannot be interpreted as meaning that the processing of personal data that are liable indirectly to reveal sensitive information concerning a natural person is excluded from the strengthened protection regime prescribed by those provisions, if the effectiveness of that regime and the protection of the fundamental rights and freedoms of natural persons that it is intended to ensure are not to be compromised.

13.12. The above also follows from EDPB Guidelines 8/2020 on the targeting of social media users dated 13 April 2021, which concludes that if a social media provider uses data from users and classifies them into categories of personal data such as religion, philosophical belief or political opinion, this classification is "obviously" considered special data processing, even if that classification is incorrect. It is true that the EDPB does not set binding rules, but that does not mean that the opinions of this independent European body are meaningless.

13.13. Given the high level of protection of special personal data that the Privacy Directive was intended to provide, there is no reason to think that this was substantially different under the Wbp.

13.14. Facebook Ireland has not (sufficiently) disputed that, as established in the Dutch DPA Report, it offered main categories and subcategories of areas of interest in the field of, for example, health, religion and political or sexual orientation to advertisers throughout the relevant period, from which it follows that Facebook Ireland in any event used personal data from these categories for advertising purposes. Consequently, it is sufficiently established that, also by tracking users' surfing behaviour and classifying the information thus obtained into interest categories, Facebook Ireland processed special personal data of the Members for advertising purposes during the relevant period.

Did Facebook Ireland obtain permission for the processing of special personal data?

13.15. The next question to be answered is whether Facebook Ireland obtained express consent to process special personal data for advertising purposes and thus is covered by the exception provided by the law.

13.16. Over the period up to the introduction of the GDPR, it has not been stated or shown that explicit consent was requested or obtained for the processing of special personal data for advertising purposes. This applies to both information derived from profile fields, as well as information derived from users' browsing behaviour and the use of it for determining interest categories.

13.17. As for the period after the implementation of the GDPR, Facebook Ireland has not alleged that it sought consent to infer categories of interest from users' surfing behaviour for advertising

[38] CJEU 1 August 2022, C- 184/20, ECLI:EU:C:2022:60l

purposes, so that the district court concludes that no express consent within the meaning of article 9 (2) (a) of the GDPR was obtained.
In the alternative (so the district court understands), Facebook Ireland, when using personal data from profile fields, regarding the period after the introduction of the GDPR, relies on the "user consent module" or "the GDPR module" it uses, which the user must go through before accessing the Facebook service. The answer to the question as to whether that module explicitly requests consent for the processing of special personal data, can be left unanswered, as the court cannot determine, with respect to the period after 21 February 2017, whether Facebook Ireland in that period too continued to process special data from profile fields for advertising purposes (see 13.8 above).

13.18. Consequently, a violation of section 16 of the Wbp and article 9 of the GDPR has been established.

Declaratory judgment

13.19. Facebook Ireland argues that the declaratory judgment sought by Stichting is not admissible, because the infringement alleged by Stichting did not occur to everyone. Facebook Ireland in that respect also points to the judgment in the interim proceedings.

13.20. This argument fails. In ground 7.13 of the judgment in the interim proceedings, the following is stated:

> "7.14 To the extent that Stichting seeks an opinion on one or more specific events, it is noted that the related claims may likewise be grouped together. In this case too, the first question is whether the event in question occurred and whether the conduct of Facebook et al. is lawful or unlawful. In these collective proceedings it is not yet necessary to be able to determine which individual interested parties may have been affected. It is sufficient that, based on the court's judgment, a Member can determine whether he or she has been affected by a possible privacy breach. On the basis of the claims formulated by Stichting, it should be possible to determine this, since the court's assessment may, if necessary, distinguish according to, for example, statutory provisions, time period and/or event."

13.21. In the judgment in the procedural issue, the court ruled that the similarity requirement of the old article 305a of Book 3 of the Dutch Civil Code has been met. In the court's opinion, the circumstance that not every Facebook user belongs to the Members because he or she did not fill in any profile fields, does not prevent the granting of the declaratory judgment (see also below under 19.6). The argument is rejected.

14. Cookie-tracking-, information and permission to use cookies?

What are cookies?

14.1.
The use of cookies is a technology in which a party places a piece of software on devices of users of apps or websites, such as a laptop or phone. Through cookies, information is stored on, and obtained from, those devices. Cookies can be used for a variety of purposes, such as storing a password that makes it easier for a visitor to access a particular website or remembering default settings. These types of cookies are also called functional cookies.

14.2. There are also cookies that track the user's browsing behaviour. These are called tracking cookies. A website operator that places tracking cookies on the user's device can track the user when the user visits the operator's website. There are also tracking cookies that allow the website operator

to also track the user on third-party websites, also called "third-party" cookies. Such tracking cookies make it possible, based on the user's browsing behaviour, to create a profile that can be used to offer ads specifically targeting that user.

Assessment framework

14.3. Parties using third-party cookies must thereby comply with section 11.7a (1) of the Telecommunications Act (Tw). This provision is the implementation of article 5 (3) of the E-Privacy Directive (2002/58/EC). The E-Privacy Directive intends to protect users against interference in their private lives, regardless of whether such interference relates to personal data. This means that the protection provided by the directive applies to any information stored in terminal equipment, regardless of whether or not it is personal data. In particular, the directive intends to protect the user from the risk that hidden identifiers and other similar devices, also called 'peripherals', enter his or her equipment without their knowledge.[39]

14.4. Section 11.7a (1) Tw provides that storing or gaining access to information in a user's peripheral equipment is only permitted if 1) a user has been clearly and fully informed (in any case about the purposes for which the information obtained by cookies will be used) and 2) the user has given consent. Information and consent must take place in accordance with the Wbp, and (after its implementation) the GDPR.

14.5. Section 11.7a Tw has been in force since 5 June 2012 (and amended in 2013, 2015 and 2018). Before that, article 4.1 of the Universal Service and End Users Interests Decree (Bude) (which was repealed as of 5 June 2012) applied. This stipulated that the user should be informed in advance about the purposes of cookies and that an opportunity should be given to refuse the placing of cookies.

Stichting's claim

14.6. In summary, Stichting seeks a declaratory judgment that Facebook Ireland has not, or at least insufficiently, complied with the duty of disclosure and the requirement of consent, by not informing, or not clearly, or to a sufficient extent, and/or not in a timely manner, the Members about the tracking of surfing behaviour and app use outside the Facebook service by means of cookies and/or similar technology and the use of the data thus obtained for advertising purposes.

Challenge Facebook

14.7. Facebook Ireland argues that Stichting's claim relates to tracking cookies that Facebook Ireland uses to obtain information from third-party websites. It is not Facebook Ireland, but the operator/manager of the website in question who installs the software provided by Facebook Ireland. This means that the obligations as referred to in section 1.7a (1) Tw rest on that operator and not on Facebook Ireland, so that, for that reason alone, the claim fails. Facebook Ireland relies in this respect on the judgment of the CJEU of 29 July 2019 (Fashion ID[40], mentioned earlier in this judgment. Facebook Ireland not being obliged to comply with section 11.7a (l) Tw if it receives personal data through cookies on third-party websites also follows - as far as the period before the implementation of the GDPR is concerned - from the explanatory memorandum to the Tw[41] and communications from the Netherlands Authority for Consumers and Markets (ACM). In addition, Facebook Ireland requires the website operator to agree to the terms of the Facebook Business Tools

[39] CJEU 1 October 2019, C-673/17, ECLI:EU:C:20 19:801, Planet49, para.70
[40] CJEU 29 July 2019, C-40/17, ECLI: EU::C:2019:629, Fashion ID
[41] Parliamentary Papers Il 2010/11. 32 549, no. 3 and Parliamentary Papers 1 2011/12, 32 549, E

(hereinafter: BTT) and its Platform Policy, which requires the website operator to provide the necessary information and obtain consent from the user.

14.8. Facebook Ireland has further provided clear and appropriate information to users at all times regarding the use of cookies and the data obtained from them.

14.9. Furthermore, the Tw was revised four times in the relevant period, and section 11.7a (1) Tw did not enter into force until 5 June 2012. No breach can have occurred before that period in any case. The non-binding reports by the Dutch DPA and the Catholic University of Leuven cited by Stichting, cannot serve as evidence. Moreover, the Dutch DPA report was finalized on 21 February 2017. For the period after that date, the report is irrelevant. Moreover, Stichting's claim is unsubstantiated, as it does not mention anything about the period after the entry into force of the GDPR.

The district court's assessment

14.10. In its assessment, the court takes as its starting point that Stichting's claim relates to cookies insofar as they are placed via third-party websites, the "third-party cookies." During the oral hearing, Stichting alleged that the claim also relates to cookies that are placed on Facebook Ireland's website that track the Members outside the Facebook service. To the extent that the district court should understand this as meaning that these would concern third-party cookies other than those referred to above, the court will ignore this, since the actual course of events for this type of cookies has not been sufficiently explained. On this point, therefore, Stichting has not fulfilled its obligation to state facts.

<u>Applicable law/relevant period</u>

14.11. As explained in 14.5 above, the use of cookies before the entry into force of section 11.7a (1) Tw meant that article 4.1 of the Universal Service and End Users Interests Decree (Bude) had to be complied with. Since Stichting's claim concerns a violation of section 11.7a subsection 1 Tw, or at least corresponding provisions, the court will disregard Facebook et al. Ireland's argument that, before section 11.7a (1) entered into force, there could be no violation, for prior to the implementation of the Tw, article 4.1 Bude applied, which contains a similar obligation.

14.12. Furthermore, it has not been shown that a revision of the Tw leads to a different assessment of the relevant obligations mentioned therein, so that the court also ignores this argument. Insofar as Facebook Ireland argues that Stichting's claims do not relate to the period after the implementation of the GDPR, that argument is incorrect. In addition, the court is of the opinion that Facebook Ireland has not sufficiently specifically disputed that it used third-party cookies after the introduction of the GDPR. To this end it is relevant its own policy in that period also refers to the use of third-party cookies.

<u>Does section 11.7a (1) Tw apply to information obtained through cookies via third-party websites?</u>

14.13. Facebook Ireland's most far-reaching argument is that it is not bound by the obligations in section 11.7a (1) Tw when it receives information about the Members through cookies placed on third-party websites.

14.14. It is not in dispute that, by placing cookies on third-party websites, information is exchanged between the user's browser and Facebook's server. According to the Dutch DPA’s report, in 2016 more than half of the 500 most visited websites in the Netherlands contained advertising cookies from Facebook. The question is who in those cases is responsible for the duty of disclosure

and the obligation to request consent under the Tw: the operator of the website the user visits and/or the advertiser (in this case Facebook Ireland) of which party a cookie is placed on the user's device.

14.15. The obligations under section 11.7a Tw rest with the party responsible for placing data in the peripherals and accessing the data stored in the peripherals. Facebook Ireland is also responsible in the case of third-party cookies, for the cookies are placed on the third-party website at its request. However, the advertiser can agree with the relevant website operator that the obligations under section 11.7a Tw will be exercised by the website operator[42]. Facebook Ireland's contention that it enters into such agreements with website operators and that website operators must agree to Facebook Ireland's BTT and Platform Policy, which requires the website operator to provide the necessary information and obtain consent, has not been sufficiently contested by Stichting. This means that, if the website operator provides information about and obtains consent to the placement of cookies, Facebook Ireland does not have to do so as well. In view of Facebook Ireland's challenge, it should have been up to Stichting to argue convincingly that Facebook Ireland does not enter into agreements with website operators, or does not monitor compliance with them, for instance by means of examples of websites of third parties on which third-party cookies of Facebook Ireland are placed and in which the website operator has not complied with the obligations in section 11.7a Tw. Since Stichting has failed to do so, it cannot be established that Facebook Ireland has violated section 11.7a Tw (or article 4.1 Bude), so that claim a.ii.3 will be dismissed.

14.16. The foregoing does not alter the fact that Facebook Ireland must comply with the requirements of the GDPR and the Wbp when processing personal data obtained through the use of cookies. This means that a legally valid processing basis must exist for those personal data obtained through cookies. As held above in chapters 12 and 13, Facebook Ireland did not have a valid processing basis for processing (ordinary and special) personal data for advertising purposes. That opinion also applies insofar as those personal data were obtained and/or processed through cookies.

15. Friends of the Members

15.1. Claim b relates to friends of the Members. Stichting argues that the conduct alleged against Facebook et al. with respect to data processing also extended to the Facebook friends of Facebook users. Because these friends are also Facebook users, to the extent that they lived in the Netherlands during the relevant period, they belong to the Members. If a Facebook friend lived abroad and does not himself belong to the Members, then the processing of personal data of friends without a processing basis is not only unlawful towards those friends, but also towards the Facebook user whose friends they are, for Facebook et al. unlawfully appropriated the data that a Facebook user kept on his account about his friends, according to Stichting.

15.2. 'Facebook et al. have argued against this that the basis for this claim is unclear and lacking. The Wbp and GDPR do not entitle to the bringing of claims that concern the processing of personal data of others. Stichting’s object under the articles of association is limited to Facebook users and the claims revolve around alleged actions against the Members. As far as Facebook users are concerned, such claims are already covered by claim a.i.1.

15.3. The district court is of the opinion that claim b cannot be allowed. Insofar as the allegation relates to a Facebook friend who belongs to the Members, this conduct is covered by claim a. Stichting has not sufficiently explained that there is a separate, distinct unlawful action against the Members. Insofar as the allegation concerns a Facebook friend who does not belong to the Members, contrary to Stichting's contention, unlawful processing of a friend's personal data cannot

[42] Parliamentary Papers II 2010/11, 32549, 3, p. 80-81

be regarded as unlawful conduct towards the Members. After all, the processing concerns that friend's personal data. To the extent that Stichting means to argue that the unlawful conduct also concerns friends of the Members who do not belong to the Members, it has no right of action in view of the group of persons whose interests Stichting represents in this collective action according to its object under the articles of association.

16. Location details

16.1. In its pleadings, Stichting has argued that Facebook Ireland failed to provide information, or at least clear information, to the Members about the use and processing of location data of the Members that were retrieved through the Members's friends. According to Stichting, Facebook Ireland determined the location of the Members in part on the basis of location data it retrieved through Members' friends on the Facebook service and used that location data for advertising purposes.

16.2. The district court notes that Stichting has not put brough a separate claim specifically addressing the processing of location data. Apparently, Stichting's argument should be read in light of its claim a.i. and/or its claim a.ii.1.

16.3.
To the extent that the location data may be grouped as data about whose processing Facebook Ireland did not adequately inform the Members (see the decision regarding claim a.i.) and/or as data that Facebook Ireland processed without a valid processing basis (see the decision regarding claim a.ii.1), those decisions also apply to the location data. To that extent, therefore, the processing of location data does not require a separate discussion. In all other respects, Stichting has not made it clear in light of which other claim(s) a (separate) decision on the location data is relevant.

17. Unfair commercial practice?

17.1. Stichting argues that Facebook et al. are also guilty of unfair and/or misleading commercial practices. To that end, it argues as follows, briefly put.

- Facebook Inc., Facebook Ireland and Facebook Netherlands are traders within the meaning of the Unfair Commercial Practices Directive (hereinafter also referred to as the UCPD)[43].
- Facebook et al. has acted unlawfully as a trader for the following reasons:
    1. Facebook et al. processed (confidential) personal data for the purpose of generating turnover and did not inform Facebook users sufficiently clearly and/or in a timely manner timely about that purpose (article 193b (1) and/or article 193d (2) and (3) of Book 6 DCC)
    2. Facebook et al. did not inform Facebook users sufficiently clearly and/or in a timely manner about the scale of the collection of (confidential) personal data and making them available to third parties, or at least the use thereof for the benefit of third parties (article 193b (1) and/or article 193d (2) and (3) of Book 6 DCC). The data policy and cookie policy used by Facebook et al. do not demonstrate the unprecedented scale of the data processing and merely discuss the revenue model in veiled terms.
    3. Facebook et al. pretended that the Facebook service was free while Facebook users paid with their personal data (article 193b (1) and/or article 193c (1) (a) and (d) of Book 6 DCC in conjunction with article 193g (t) of Book 6 DCC). The Facebook service is not free. Personal data may qualify as a prize within the meaning of the UCPD. Until August 2019,

[43] Directive 2005/29/EC of the European Parliament and of the Council of l May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council

Facebook's home page stated under "Register": "It is free (and it will stay free)". Since August 2019, this text has no longer been used. The Terms of Use then stated, "We do not charge for using Facebook (...)."

17.2. Facebook et al. disagree with Stichting's contentions. Thery point out that claims a.iii.1 and a.iii.2(as also explained above in grounds 17.1 (1) and (2)) are entirely identical to claim a.i. They also argue in that respect that the unfair commercial practices claims are based entirely on a violation of the right to data protection, whereas the right to data protection is a *lex specialis*, leaving no room for claims under the UCPD with respect to the necessary provision of information to users. Facebook et al. additionally dispute that Facebook Inc. and Facebook Netherlands are traders. They have made no disclosures to the Members that are relevant to the claims on this basis. Finally, Facebook et al. dispute the existence of an unfair commercial practice on the three alleged grounds. Facebook et al. in that respect among other things point out that Facebook Ireland does not sell its users' data to generate revenue, but that it generates revenue by allowing advertisers to show their ads to a specific audience (without sharing information that identifies users personally). It has always been transparent about its business model and the fact that personalized ads are part of it. Facebook et al. argue that they have provided sufficient (and not misleading) information and that the no-charge statement is not misleading and unfair either. There is no evidence that any of the Members was influenced in his or her transaction decision.

Assessment Framework

17.3.
When assessing whether there an unfair commercial practice has occurred, the following context is important. The UCPD has been implemented in articles 193a et seq. of Book 6 DCC.

17.4. A trader acts unlawfully towards a consumer under article 193b (1) of Book 6 DCC, if it engages in a commercial practice that is unfair. A commercial practice is unfair, according to article 193b (2) of Book 6 DCC, if the trader acts (a) contrary to the requirements of professional diligence, and (b) the average consumer's ability to make an informed decision is or may be noticeably limited, as a result of which this consumer makes or may make a decision about a contract which he or she would not otherwise have made. The consumer must therefore be given the opportunity to reach an informed decision, in any case when deciding whether or not to enter into the agreement. In order for article 193b (2) to be successfully relied upon, it is required that the average consumer's ability to make an informed decision is limited to such an extent that it causes him or may cause him to make a transactional decision he or she would not otherwise have made. Under the third paragraph of this provision, a commercial practice is particularly unfair if a trader engages in a misleading commercial practice as referred to in articles 193c - 193g of Book 6 DCC.

17.5. A commercial practice is to be regarded as misleading within the meaning of article 193c of Book 6 DCC, if information is provided that is factually incorrect or that misleads or is likely to mislead the average consumer, whether or not due to the general presentation of the information, such as with respect to:

(a) the existence or nature of the product, or
(…)
(d) the price or the manner in which the price is calculated, or the existence of a specific price advantage

Pursuant to article 193g (t) of Book 6 DCC, it is misleading under all circumstances to describe a product as free, free of charge or at no cost, if the consumer has to pay something other than the inevitable costs of accepting the offer and collecting the product or having it delivered. For the situation of article 193g (t) of Book 6 DCC, no requirement of causality exists.

17.6. A commercial practice is also misleading pursuant to article 6:193d of the Dutch Civil Code if there is a misleading omission. According to the second paragraph, this is the case when essential information that the average consumer needs so as to make an informed decision about a transaction is omitted, as a result of which the average consumer makes or may make a transactional decision that he or she would not otherwise have made. According to the third paragraph, a misleading omission also occurs if essential information as referred to in the second paragraph is concealed or provided in an unclear, incomprehensible, ambiguous manner or in an untimely manner, or fails to reveal the commercial intent, if not already clear from the context.

17.7. Pursuant to article 193a of Book 6 DCC, the term "trader" shall, insofar as relevant, mean the legal person acting in the exercise of a profession or business or the person acting on his behalf. The term "commercial practice" means any act, omission, conduct, representation or commercial communication, including advertising and marketing, of a trader, which is directly related to the promotion, sale or delivery of a product to consumers.

17.8. In principle, the burden of proof regarding the unfairness of a commercial practice rests on the consumer. Only insofar as it concerns the material accuracy and completeness of the information provided, does a reversed burden of proof arise (article 193j of Book 6 DCC).

17.9. The European Commission's Guidelines for the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices of 25 May 2016 - which are intended only as guidance - explain the prohibition on wrongly representing something as free as follows:

> This prohibition is based on the idea that in claiming that something is "free," consumers expect exactly that, i.e. that they get something without having to give money in return.

17.10. In these 2016 Guidelines, the European Commission further explained the following about the interaction with data protection law:

> A trader's violation of the Data Protection Directive or of the ePrivacy Directive will not, in itself, always mean that the practice is also in breach of the UCPD.
> However, such data protection violations should be considered when assessing the overall unfairness of commercial practices under the UCPD, particularly in the situation where the trader processes consumer data in violation of data protection requirements, i.e. for direct marketing purposes or any other commercial purposes like profiling, personal pricing or big data applications.
> From a UCPD perspective, the first issue to be considered concerns the transparency of the commercial practice.
> Under Articles 6 and 7 of the UCPD, traders should not mislead consumers on aspects that are likely to have an impact on their transactional decisions. More specifically, Article 7(2) and No 22 of Annex I prevent traders from hiding the commercial intent behind the commercial practice.
> The data protection information requirement of consumers about the processing of personal data, not limited only in relation to commercial communication, may be considered as material (Article 7(5)).
> Personal data, consumer preferences and other user generated content, have a "de facto" economic value and are being sold to third parties.
> Consequently, under Article 7(2) and No 22 of Annex I UCPD if the trader does not inform a consumer that the data he is required to provide to the trader in order to access the service will be used for commercial purposes, this could be considered a misleading omission of material information.
> Depending on the circumstances, this could also be considered a violation of the EU data protection requirements to provide the required information to the individual concerned as to the purposes of the processing of the personal data.

17.11. On 29 December 2021, the European Commission issued new guidance[44] in connection with the Modernization Directive[45]. The Modernization Directive amended the UCPD and some other directives in 2022 and thus does not cover the period to be assessed by the court in this case. This Guidance among other things states as follows:

> This ban is based on the idea that consumers expect a 'free' claim to be exactly that, meaning they receive something without giving money in exchange.
> (…)
>
> Products presented as 'free' are especially common in the online sector. However, many such services collect personal data of users such as their identity and email address. Importantly, the UCPD covers all commercial practices concerning 'free' products and does not require payment with money as a condition for its application. Data-driven practices involve an interplay between EU data protection legislation and the UCPD. There is an increasing awareness of the economic value of information related to consumers' preferences, personal data and other user-generated content. The marketing of such products as 'free' without adequately explaining to consumers how their preferences, personal data and user-generated content are going to be used could be considered a misleading practice in addition to possible breaches of data protection legislation

17.12. The Modernization Directive, by the way, did not explicitly include the situation of providing a digital service in exchange for providing personal data in the UCPD.

Concurrence

17.13. Articles 193a et seq. of Book 6 DCC are the implementation of the UCPD. This directive aims at maximum harmonization. This means that member states may offer consumers neither less nor more protection than provided in the directive. Article 3 (2) of the UCPD states that this directive is without prejudice to contract law and, in particular, to the rules on the validity, formation or effect of a contract. From this it can be deduced that the consumer is in principle entitled to a freedom of choice, if a situation falls both within the scope of the unfair trade practice and within the scope of another regime, all this with the exception of the situation of specific community law provisions referred to in article 3 (4), which are not at issue in the present case. In the event of concurrence, the basic principle is that both sets of rules may apply side by side, except for a rule to the contrary in the regime in question. There is no evidence to suggest that the Union legislator intended for the Privacy Directive and the GDPR, respectively, to apply exclusively on this point, quite the contrary. The CJEU confirmed in 2022 that the violation of a rule on the protection of personal data can simultaneously lead to the violation of rules on consumer protection or unfair commercial practices.[46] Facebook's position to the contrary therefore, finds no support in law and for that reason is not followed. This means that the court will assess Stichting's unfair trade practice claims.

Who is a trader?

17.14. As to the question of who can be regarded as a trader, the Court is of the opinion that, in light of Facebook et al.'s substantiated challenge, it has not become evident that Facebook Inc. and

---

[44] Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market of the European Commission of 29 December 202 l, 2021/C 526/01

[45] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011l /83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of consumer protection rules in the Union (OJ 2019, L 328)

[46] CJEU 28 April 2022, C-319/20, ECU:EU:C:2022:322,paragraphs 78 and 66 Meta Plat-forms Ireland Limited v. Bundesverband der Verbraucherzentralen und Verbraucherver-bände - Verbraucherzenirale Bundesverband e.V.

Facebook Nederland have provided information to the Members that is relevant in the context of unfair commercial practices. That the conduct of Facebook Ireland should be attributed to Facebook Inc. and/or Facebook Nederland has not been established. In any event, the assertion disputed by Facebook et al. that Facebook Inc. and Facebook Netherlands created certain pieces of information that Facebook Ireland subsequently showed to Facebook users is not sufficient for that purpose. Also the circumstance put forward by Stichting that the management of Facebook Nederland had an overlap with the management of Facebook Ireland does not give decisive weight to this. The Court therefore does not follow Stichting in its (insufficiently substantiated) position that Facebook Inc. and Facebook Nederland can also be regarded as traders with respect to the Members.

Did an unfair commercial practice occur?

17.15. The district court then turns to the essential question: has Facebook Ireland been guilty of an unfair commercial practice?

17.16. The district court will first of all address Stichting's third, independently presented, complaint: the free of charge statement. The court will have to assess this matter in the light of the applicable regulations in the relevant period.
It was (and still is) not permitted to describe a product as free if the consumer does not have to pay to accept the offer and to collect the product, or have the product delivered, but has to do something else in exchange. The issue at the relevant time, as explained in the 2016 guidance (and, for that matter, also in the 2021 guidance), was that when a consumer is told that something is "free," he or she expects exactly that, i.e. that he or she will get something without having to pay money in exchange. The statement that the Facebook service is free can therefore be understood as indicating that the use of the service does not require a monetary consideration.
Since it has been established that no money has to be paid for the Facebook service, the free-of-charge statement in the relevant period as such is therefore not misleading to that extent. To the extent that a different approach could possibly also be inferred from the 2021 Guidance, the district court does not attach decisive weight to it in these proceedings. In the district court's opinion, the free-of-charge statement in itself in the relevant period did not constitute an unfair trade practice within the meaning of article 193g (t) DCC and the claim directed to it must therefore be dismissed. However, all this does not alter the fact that this free-of-charge statement may well play a role in assessing the first allegation below.

17.17. In view of the assessment framework outlined above, it is not permissible to mislead consumers about aspects that may affect their decision on a transaction. From what has been considered above in the context of privacy law, it follows that, when Members entered into the agreement to use the Facebook service, Facebook Ireland did not sufficiently inform them about the purpose for which and the way in which personal data was processed. Facebook Ireland was insufficiently transparent about exactly how preferences, personal data and user-generated content were used. In doing so, Facebook Ireland has not been sufficiently clear about its business model. The prominent statement that the Facebook service is free does not contribute to that clarity. Insofar as Facebook Ireland has referred to the content of (the different versions of) its Data Policy, that is not proper information within the meaning of the regulations on unfair commercial practices, because the information relevant for the average consumer is concealed in veiled language in an underlying layer of information. Failing to inform Members, or to inform them sufficiently clearly, at the time they entered into the agreement, of the circumstance that the data, or personal data, provided by the consumer to Facebook Ireland in order to access the Facebook service would also be used for advertising purposes in the way they are used, must be considered a misleading omission of essential information that the average consumer - i.e. the reasonably informed, circumspect and observant consumer – needs in order to make an informed decision about participating in the Facebook service as meant in article 193d of Book 6 DCC. This is essential information in this case,

also because the processing of data, or personal data, of an individual user by Facebook Ireland for advertising purposes was comprehensive and in principle extended to all data, or personal data, of that user, including special personal data. This omission is sufficiently material to be capable of misleading the average consumer. A further decision on any causal link need not be made in these proceedings - a class action. Only in the context of determining liability towards an individual consumer does the issue arise as to whether and, if so, to what extent, he or she was actually influenced in his decision by the misleading communication and harmed as a result.

17.18. Stichting also accuses Facebook Ireland of failing to provide information about the size and scale of the data processing. However, it has remained unclear what independent meaning this accusation has in relation to what has already been ruled above, nor has it become sufficiently clear what Stichting specifically means by "the size and scale" and "the unprecedented scale" in relation to the question of whether an unfair commercial practice occurred. All this means that Stichting has failed to meet its burden of proof on this point as well.

17.19. The conclusion is that in the relevant period Facebook Ireland has been guilty of an unfair commercial practice (and thus has acted unlawfully) as described above in ground 17.17.

18. Unjust enrichment?

18.1. Stichting argues that Facebook et al. have unjustly enriched themselves, by processing the personal data at the expense of the Members. The processing (and further) use of personal data of Facebook users was not permitted, due to the absence of a basis. The personal data represent an economic value. With the personal data of the Members, the assets of Facebook et al. increased, thus causing the enrichment. The earnings model of Facebook et al. is almost entirely based on collecting personal data and making it available to third parties in return for payment, so that it actually sells access to, or the use of, personal data that are capable of being expressed in monetary terms. The counterpart of the enrichment of Facebook et al. is the impoverishment of the Members, because they have has lost assets that include the loss of control over personal data and the fact that personal data have turned from inaccessible to accessible.

18.2. Facebook et al. dispute any impoverishment of the Members and any enrichment of Facebook et al., as well as the causal link between the two and the unlawfulness of the enrichment. They inter alia argue that the loss of control over personal data alleged by Stichting did not result in material damage and that this was not explained by Stichting either. According to Facebook et al. during the relevant period, there was no market for individual users to sell their personal data and, if it were otherwise, such data is not competitive in nature. Thus, Facebook et al.'s processing of such data would not change the value of an individual's data.

18.3. Under article 212 (1) of Book 6 DCC, he who has been unjustly enriched at the expense of another is obliged, in so far as this is reasonable, to compensate the loss up to the amount of the enrichment. For a claim based on unjust enrichment to be allowed, four requirements must be met: (1) impoverishment (damage), (2) enrichment (increase in assets), (3)a connection between the enrichment and the impoverishment, and (4) the enrichment must be unjustified in the sense that there is no reasonable cause or justification for it. Stichting is under the burden of establishing, and if necessary proving, the facts and circumstances necessary to conclude that unjust enrichment has occurred, it has to prove the four aspects mentioned above. In ground 7.16 of the judgment in the interim proceedings it was ruled that the extent of any enrichment does not yet need to be answered in this class action, but that all that should be decided on is unjust enrichment has at all occurred.

18.4. The question of whether unjust enrichment has occurred must be answered pursuant to article 212 of Book 6 DCC. One of the requirements is that there is impoverishment/damage. This means, contrary to what Stichting appears to argue, that the possibility of damage is not sufficient for granting the requested declaratory judgment that Facebook et al. have been unjustly enriched. To that extent, therefore, a different standard applies than with respect to requests for declaratory judgments on the basis of an unlawful act.

18.5. The parties have discussed at length the question of whether personal data represents value. That this personal data has value for Facebook et al. may be clear; its service is based on it. Indeed, it uses such data by collecting it in a certain way and using the information obtained from it to achieve personalization. However, in light of Facebook et al.'s reasoned challenge, Stichting has not sufficiently explained that Facebook et al.'s use of the personal data actually impairs and thus impoverishes the Facebook user's assets. How the loss of control results in a decrease of the Facebook user's assets, Stichting has not made sufficiently clear.
18.6. The conclusion is that the claim based on unjust enrichment cannot be allowed. Whatever further submissions the parties have made on this issue therefore need no further discussion.

19. Final observations and conclusion

19.1. It follows from the court's assessment in this judgment that Facebook Ireland has acted unlawfully towards Dutch Facebook users in the period 1 April 2010 - 1 January 2020.

19.2. Briefly put, Facebook Ireland Hs violated the privacy rights of Dutch Facebook users and engaged in an unfair commercial practice.

19.3. With respect to privacy rights, Facebook Ireland in particular:

a) has violated the requirement of a basis of sections 6 and 8 Wbp and articles 5 (1) (a) and 6 (1) GDPR, respectively, by processing personal data of Dutch Facebook users for advertising purposes without such processing being capable of being based on a legally valid ground for processing;
b) has violated the ban on processing special data of section 16 of the Wbp and article 9.1 of the GDPR, respectively, by processing special personal data (e.g. on religion, ethnicity, sexual preference and political affiliation) for advertising purposes;
c) has breached the duties of disclosure of section 33 Wbp and article 13 GDPR respectively, by:
    - allowing external developers to access personal data of Dutch Facebook users, without Facebook Ireland having (properly) informed those users about a) the purposes of such data processing, b) the circumstance that Graph API version 1 also allowed personal data of Facebook users to be shared with external developers via Facebook friends, and c) that whitelisted developers could continue to use Graph API version 1 even after the introduction of Graph API version 2 and therefore retained access to personal data of Facebook friends;
    - allowing Kogan and GSR to access personal data of Dutch Facebook users, without Facebook Irelan having provided information about the purposes of that data processing and the circumstance that Graph API version l also allowed personal data of Facebook users to be shared with Kogan/GSR through Facebook friends;

- not providing information about the 'integration partnership program' and the related processing of Dutch Facebook users' personal data, consisting of integration partners' access to their personal data and that of their Facebook friends.

19.4. For the specific periods during which the individual breaches occurred, please refer to the related chapters and grounds.

19.5. Facebook Ireland has furthermore argued that the requested declaratory judgments are not admissible, because Stichting has not made clear which of its allegations relate to which group of users. According to Facebook Ireland, therefore, no declaratory judgments can be granted that relate to all of Stichting's Members.

19.6. The district court does not follow Facebook Ireland in this. The term Members refers to the description given to it by Stichting according to its articles of associations (see ground 5.2). A person belongs to the Members if he or she can be regarded as a victim in the sense of the articles of association, which means, among other things, that a breach of privacy (also defined in the articles of association) has taken place. In this judgment it has been ruled that Facebook Ireland has acted unlawfully. That unlawful act may be broken down into various data processing operations and acts. Partly on the basis of this judgment, it may be determined who belongs to the Members of Stichting. This means that it can be ruled that unlawful conduct towards the Members has occurred. There is no further need to differentiate. The exact size of the Members need not be established in these proceedings. That can be addressed in any follow-up proceedings. However, from the nature of the unfounded processing of personal data for advertising purposes, it seems to follow that in any event, with regard to this privacy breach, (virtually) all Dutch Facebook users (who were not acting in the course of a profession or business) who used the Facebook service at any time between 1 April 2010 and 1 January 2020, were affected.

19.7. The claims against Facebook Ireland can be allowed in the manner to be set forth In the decision below.

19.8. Insofar as Stichting intended to argue that Facebook Inc. and Facebook Netherlands, even though they do not qualify as controllers or traders (within the meaning of article 193a of Book 6 DCC), are nevertheless liable, or jointly liable, for the alleged unlawful acts, the district court rejects that view. Stichting has not substantiated on which basis entities other than the controller and the trader, respectively, would in this case be liable, or jointly liable, for the alleged non-compliance with the obligations resting on Facebook Ireland as the processor and trader.

19.9. The claims against Facebook Netherlands and Facebook Inc. will therefore be dismissed.

20. Costs of the proceedings

20.1. Facebook Ireland as the more unsuccessful party will be ordered to pay Stichting's legal costs. The district court assigns 4 points to Stichting's procedural acts (with 2 points for the oral hearing in connection with the extensive time of dealing with the case). Due to the complexity and size of the case, as well as the interests involved, the court considers the maximum flat rate of EUR 4,247 per point appropriate. The costs on the part of Stichting, taking into account the foregoing, are assessed at:

- summons	EUR	99.01
- court fees	EUR	656.00
- attorney's fees	EUR	16,988.00 (4 points x rate EUR 4,247.00)
Total	EUR	17,743.01

20.2. In the dispute between Stichting on the one hand and Facebook Netherland and Facebook Inc. on the other hand, Stichting is to be regarded as the more unsuccessful party. Since Facebook et al. put up a joint defence, while that defence was the same for all three defendants with regard to the vast majority of the points of dispute, and to that extent it has not been shown that Facebook Netherlands and Facebook Inc. have incurred costs separately, there is no reason to give an order for costs at the expense of Stichting in favour of Facebook Netherlands and Facebook Inc.
20.3. The statutory interest claimed on the legal costs to be paid by Facebook Ireland will be allowed in the manner stated below under the decision. The same applies to the claimed subsequent costs and statutory interest on the subsequent costs.

21. The decision

The district court

21.1 rules that Facebook Ireland has acted unlawfully toward Stichting's Members because Facebook Ireland has violated the privacy rights of the Members in the manner held in chapter 11, chapter 12 and chapter 13 of this judgment,

21.2. rules that Facebook Ireland has acted unlawfully towards Stichting's Members because Facebook Ireland has engaged in a commercial practice towards Stichting's Members which is unfair within the meaning of article 193b (3) (a) in conjunction with article 193d of Book 6 DCC, as referred to in ground 17.17 of this judgment,

21.3. orders Facebook Ireland to pay the costs of the proceedings, assessed on the part of Stichting to date at EUR 17,743.01, to be increased by the statutory interest as referred to in article 119 of Book 6 DCC on this amount with effect from the fourteenth day after the date of this judgment until the day full payment is made,

21.4. orders Facebook Ireland to pay the costs incurred by Stichting after this judgment, assessed at EUR 173 in attorney's fees, to be increased, if Facebook Ireland has not complied with the judgment within fourteen days after notice has been given and service of the judgment has subsequently been effected, by an amount of EUR 90 in attorneys' fees and the costs of serving the judgment, to be increased with the statutory interest as referred to in article 119 of Book 6 DCC with effect from the fourteenth day after service until the day full payment is made,

21.5. declares this judgment to be provisionally enforceable with respect to the order for costs,

21.6. Dismisses all other applications.

This judgment was rendered by C. Bakker, L. Voetelink and J.T. Kruis, Judges, and pronounced in open court on 15 March 2023.