"*? "JHRIF "*

YOUI11S

AMSTERDAM COURT

Private Law Department

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

Judgment of March 15, 2023

in the case of

the foundation
DATA PRIVACY **FOUNDATION,**
based in Amsterdam, plaintiff,
Advocate J.H. Lemstra of Amsterdam,

against

1. the private company with limited liability FACEBOOK NETHERLANDS B.V.,
based in Amsterdam,
2. the legal person under foreign law
META PLATFORMS, INC., formerly FACEBOOK lNC,
based in Menlo Park(California, United States),
3. the legal person under foreign law
META PLATFORMS IRELAND LTD., formerly FACEBOOK IRELAND LTD,
domiciled in Dublin, Ireland,
defendants,
attorney at law Mr. G.H. Potjewijd in Amsterdam.

Plaintiff will hereinafter be referred to as the Foundation and defendants will hereinafter again, following the earlier judgment in incident, be referred to as Facebook Netherlands, Facebook Inc. and Facebook Ireland (collectively: Facebook et al.).

1. The procedure

1.1. The course of the proceedings appears mit:
- the judgment in incident dated June 30, 202-1''(hereinafter, the judgment in incident) and the pleadings referred to therein,
- the statement of reply, with exhibits,
- the statement of reply, with exhibits,
- the rejoinder, with exhibits,
- the minutes of oral proceedings held on November 8, 2022, and the documents referred to in the minutes,

' ECLl:NL:RBAï'vlS:2021:3307

- Facebook et al.'s attorney's letter dated Dec. 13, 2022, with comments on the record.

1.2. Finally, judgment was rendered.

1.3. To the extent relevant to the decisions to be made, this judgment is rendered with due regard to the comments on the record.

2. Overview of this judgment

What this case is about

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

The court's decision in outline

2.2. The court's verdict is that Facebook Ireland acted unlawfully in the way it handled the personal data of Dutch Facebook users. The court limited the conviction to the actions of Facebook Ireland because it alone is responsible for the processing of personal data of Dutch Facebook users.

2.3. Unlawful conduct includes processing personal data for advertising purposes without a legally valid basis. Processing of personal data is only allowed if there is a basis for doing so specified by law, such as 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 behavior of Facebook users outside the Facebook service. Furthermore, Facebook Ireland did not sufficiently inform Facebook users about the sharing of their personal data with a number of third parties specified in the judgment. In doing so, not only personal data of the Facebook users themselves were shared, but also personal data of their Facebook friends.

2.4. The way 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.

[2] Old law here refers to collective action law in effect before Jan. 1, 2020.

Inadequately informing the Facebook user as a consumer about the use of personal data for commercial purposes was misleading. Indeed, the average consumer could not make an informed decision about participating in 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 to the relevant website operator the obligation to inform users about the placement of cookies and to seek consent. It was also not established 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 actual impairment of the Facebook user's assets.

2.6. The declarations requested by the Foundation 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 before us in these proceedings.

Structure of this judgment

2.7. This judgment is structured from here on as follows:

3. The facts

3.1. For the readability of the judgment, established facts pertaining to specific issues have been included in the assessment of the relevant issues.

3.2. Facebook Netherlands, Facebook Ireland and Facebook Inc. belong to the Facebook group. The Facebook service serves as a *social* media platform that allows users to share experiences and connect with information and people. Over 2.7 billion people worldwide use the Facebook service.
The user does not pay a financial fee for using the Facebook service. The Facebook group's business model is based on revenue from the sale of (personalized) ads.

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

3.4. The Foundation is a collective claims foundation established on February 25, 2019. Among its objectives is to represent the interests of aggrieved persons residing in the Netherlands against whom a privacy violation has occurred at any time.

3.5. The Facebook service is a personalized service. This personalization works its way into the content of what a user sees. 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 terms have had different names and different versions in force.

3.7. In addition, Facebook Ireland applies Data Policies for the use of the Facebook service that can be accessed on the website and in the app. Several versions of these also existed between 2010 and 2020.

3.8. At the end of 2014,(the legal predecessor of) the Personal Data Authority(AP), the data protection supervisor in the Netherlands, initiated an investigation into the processing of personal data of data subjects in the Netherlands by the Facebook group.In a report dated February 21, 2017, published on May 16, 2017, the AP reported its findings. In it, it concluded that the Facebook group violates the Personal Data Protection Act (Wbp) in several respects 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. The judgment in incident decided that Dutch law applies to this case.

5. The Foundation's claims

5.1. The Foundation claims that the court by judgment, so far as possible enforceable:

a. rule that Facebook Netherlands, Facebook Ireland and Facebook Inc., jointly and/or each in their own right, from April 1, 2010 to January 1, 2020, or at least during the period specified in marginal 156 of the summons for each separate violation, or at least for a period to be determined by the Court in good faith, acted and/or have acted imputably unlawfully toward the Foundation's constituency because they:

i) violated the (privacy) rights of the Supporters by violating the (information) duties of Articles 33 and 34 Wbp and/or Articles 12, 13 and 14 General Data Protection Regulation[3] (AVG):

1. Allowing, or at least enabling and facilitating, external developers to dispose of and/or have access to Personal Data of Supporters and subsequently process such Personal Data, without having informed Supporters sufficiently clearly and timely; and/or
2. allow, or at least enable and facilitate, 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 Backbenchers and to have these could subsequently process personal data without having informed the constituency in a sufficiently clear and timely manner; and/or
3. use telephone numbers of Supporters provided for the purpose of two-factor authentication to place targeted advertisements, whether on the desktop version of its platform or otherwise, without having informed the Supporters in a sufficiently clear and timely manner; and/or
4. failing to inform, or at least failing to inform sufficiently clearly and/or timely, the constituency about the integration partnership program and related processing of personal data concerning the constituency;

and/or

ii) violated the (privacy) rights of the constituency by:

[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.

1. violation of the basis requirement under Articles 6 and 8 of the PDPA and/or violation of Article 5(1)(a) and Article 6(1) of the AVG,in each case by processing constituency data without such processing being able to be based on an adequate and legally valid processing basis;
2. violation of the processing prohibition for special data under Article 16 of the PDPA and/or Article 9, first paragraph, of the AVG,by using in particular(but not exclusively) personal data concerning sexual life, religious beliefs and ethnicity, and the content of messages from the Supporters revealing such information, for advertising purposes;
3. violation of the duty to inform and the consent requirement of article 11.7a, paragraph 1, Telecommunications Act (Tw), or at least corresponding provisions in national privacy legislation in other member states, by not, or not clearly or sufficiently and/or not timely informing the Supporters about the tracking of surfing behavior and app use outside the Facebook service with the help of cookies and/or similar technology and the use of the data thus obtained for advertising purposes;

and/or

iii) towards the Foundation's constituency has/have engaged in commercial practices that are unfair within the meaning of Article 6:193b(1) of the Civil Code(BW)and/or misleading within the meaning of Article 6:193c, 193d and 1939 BW, by:

1. failing to inform the Supporters sufficiently clearly and/or timely about the collection and further processing of their (confidential) personal data in order to generate revenue, by sharing that personal data with third parties, or at least using that data for the benefit of third parties;
2. failing to inform its constituency sufficiently clearly and/or timely 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 to make the misleading announcement to the constituency that the Facebook service would be free and would always remain so, while the constituency *de facto* paid for the Facebook service with the handing over of the relevant (confidential) personal data to Facebook et al;

b. rule that Facebook Nederland, Facebook Ireland and Facebook Inc., jointly and/or individually, from 1 April 2010 until 1 January 2020, at least during the period mentioned per separate violation in margin 156 of the summons, or at least during a period to be determined by the Court in good judicial discretion, have acted towards the Supporters in a culpably unlawful manner by also processing, via the Supporters, the data of friends of the Supporters in the manner referred to above under a.i.1 .., a.i.2., a.i.3., a.ii.1. and a.ii.3. above;

c. rule that Facebook Netherlands, Facebook Ireland and Facebook Inc., jointly and/or each of them, unjustly enriched and/or have been unjustly enriched at the expense of the Backers in the period from April 1, 2010 to January 1, 2020, or at least a period to be determined by the court in good court;

d. Ordered Facebook Nederland, Facebook Ireland and Facebook Inc. jointly and severally to pay the legal costs incurred by the Foundation, to be increased by subsequent costs and statutory interest on the legal and subsequent costs.

5.2. The word "constituency" used in the claim defines the Foundation, in short, as (former) users of the Facebook service at any time in the period from April 1, 2010 to January 1, 2020(and/or their legal guardians) insofar as they were residing in the Netherlands at the time of that use, not acting in the exercise of a profession or business, and for whom the Foundation stands up by virtue of its purpose statement, and against whom a Privacy Violation(as referred to in the Articles of Association) has occurred at any time.

5.3. Facebook et al. put forward a defense and moved that the claims be declared inadmissible or dismissed, and that the Foundation be ordered to pay the costs of the proceedings.

5.4. The parties' contentions are addressed below under the assessment, insofar as relevant.

The court's assessment

6. Who is (still) defending in these proceedings?

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

6.2. In this the Foundation is not followed. Facebook et al. put forward a defense in these proceedings on behalf of the three Facebook entities and in that connection submitted, inter alia, various procedural documents including a statement of rejoinder. One of Facebook et al.'s arguments is that only Facebook Ireland is the responsible party for the acts at issue in these proceedings. In that light, Facebook c.s. indeed frequently mentions Facebook Ireland in the rejoinder, because in its view that is the only relevant party. From that (of course) it cannot be deduced that the defense of Facebook c.s. in these proceedings is limited to a defense of Facebook Ireland. During the oral hearing it was confirmed on behalf of Facebook et al. that the defense in these proceedings was conducted on behalf of the three Facebook entities.

7. Does the Foundation have a sufficient interest?

7.1. Most far-reachingly, Facebook et al. argued that the Foundation has insufficient interest in the claims it has brought. To this end, Facebook et al. submitted, in summary, the following. For none of its claims has the Foundation made plausible the possibility of harm to the Backers. The Foundation merely relies on an alleged loss of control over personal data without making clear why that could constitute damage in a legal sense. A mere breach of a privacy right does not in itself result in harm. Nor does a privacy violation automatically give rise to a claim for compensation for immaterial damages. The nature and seriousness of the alleged violation of standards does not mean that adverse consequences for the Achterban are so obvious that an interference with the person as referred to in Section 6:106 opening words and under b of the Dutch Civil Code can be assumed.

Furthermore, Facebook et al. refer to the Opinion of October 6, 2022 of the Advocate General(A-G)at the Court of Justice of the European Union(CJEU)in the case UI v. Österreichische Post'. That case concerns the interpretation of the concept of damages in Article 82 AVG. Facebook c.s. asks the court to stay its decision, if necessary, until the ECJ EU has ruled on the UI/Österreichisch Post case.

7.2. The Foundation has argued that it has a sufficient interest in its claims. To this end, it has argued, inter alia, the following. Breaches of privacy can cause both material and immaterial damage. Thus, the possibility of harm is plausible. In the previously applicable Privacy Directive' and in the currently applicable AVG, a broad concept of damage was used. These also explicitly provide that an injured party can claim compensation for immaterial damage. In any event, the damage suffered by the Subordinates as a result of the violation of privacy regulations consists of loss of control over personal data and/or the prevention of being able to exercise control. The Supporters have suffered more than mere annoyance from the ongoing violations of their data protection rights. The violation of privacy rights can be qualified as an impairment in the person as referred to in Article 6:106 opening words and under b of the Dutch Civil Code. Such an impairment entitles to compensation for immaterial damages. The case at issue in the UI v. Österreichische Post case is not comparable to its class action against Facebook et al, according to the Foundation.

7.3. The court considered the following.

7.4. Article 3:303 BW provides that without a sufficient interest no one is entitled to a legal claim. By "sufficient interest" is meant enough interest to justify proceedings. In principle, it may be assumed that a sufficient interest in a claim exists. The court should be reluctant to rule that insufficient interest exists in a legal claim. If a declaratory judgment is sought that liability exists for damages or that wrongful acts have been committed, the court must assume that the plaintiff has an interest if the possibility of damages is plausible.' This applies even if an order for damages or referral to the damages state procedure is not also sought.

7.5. In these proceedings, the Foundation seeks declaratory judgments that Facebook et al. acted unlawfully and was unjustly enriched. In essence, the Foundation bases this claim on the allegation that Facebook et al. unlawfully processed the personal data of its supporters during the period from 2010 to 2020. By granting the claimed declarations, the Foundation aims to ultimately obtain compensation for the Backers.

7.6. On the question of the Foundation's interest in its claims, the court must assess whether the possibility of harm is plausible if one or more of the allegations made by the Foundation are justified. In answering the question of whether the possibility of harm is plausible, it is not necessary to follow the ruling of

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

'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.

°High Council March 27, 2015. ECLI:NL:HR:2015:760

waiting for the ECJ EU on the interpretation of the concept of damage in Article 82 of the AVG. Even if the interpretation of the concept of immaterial damage according to the current state of jurisprudence is assumed (and more specifically the requirements imposed on the concept of "impairment in the person in another way" as referred to in Section 6:106 of the Dutch Civil Code), in the District Court's opinion the possibility of damage as a result of the reproaches made by the Foundation is plausible in this case. To this end, the following reasons are relevant.

7.7. In a collective action such as the present one, with respect to the interest question, among other things, a certain abstract test is appropriate. This means that the question of whether the possibility of damage is plausible must be answered in a general sense, that is, abstracted from individual circumstances of members of the Supporters. It is true that it cannot be said that the privacy violations and unfair trade practices alleged by the Foundation will automatically lead to damages, but on the other hand, the possibility of damages is also not excluded in advance and in a general sense. Indeed, it is quite conceivable that under certain circumstances the privacy violations alleged by the Foundation (may) have resulted in material and/or immaterial damages. That possibility is sufficient in the context of this class action to establish that the possibility of damage is plausible. Whether and when such circumstances actually occur does not need answering in the context of these proceedings.

7.8. Since the possibility of harm is plausible, the Foundation has a sufficient interest in the declarations it seeks.

8. The appeal of prescription

8.1. Facebook et al. have argued that the Foundation's claims, insofar as they relate to events prior to December 30, 2014, are vejaard pursuant to Section 3:310 of the Dutch Civil Code.To this end, Facebook et al. have argued the following. Five years before December 30, 2019, the time of the Foundation's filing of these proceedings, the Foundation and the Supporters were reasonably a1 aware, or at least should have been aware, of the violations alleged by the Foundation, the alleged damages and the person liable for them. Indeed, the Facebook users were already aware before
December 30, 2014 on data processing relevant to the Foundation's claims. Before that date, there was already widespread discussion in the media about the processing of personal data for the purpose of personalized advertising. Reference is made to a selection of news articles that appeared in Dutch news media during 2014. This demonstrates that the general public, including Dutch Facebook users,was aware that data processing for the provision of a personalized service(including personalized advertising) is at the core of the Facebook service. Everyone also knew that advertisements are tailored to one's own search and surfing behavior on the Internet. In any case, Facebook users were sufficiently informed to have to investigate further about their possible damages or the liable person. That the Achterban aì in 2014 was able 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. The Foundation disputes that Backers were already aware of the damage and the person liable for it before December 30, 2014, and it argues the following to that effect. Without in-depth investigations, such as those conducted by the AP, Facebook users could not have been aware of what happened to their data and the incomplete and misleading way in which Facebook et al. informed users about it. The **press publications referred to by Facebook** et al. **are insufficient to** base actual awareness of both the damage and the liable person on them. Victims should also not be expected to rely on newspaper articles. There was no duty of inquiry for users of the Facebook service.The AP conducted an investigation into the operation of the Facebook service in the period November 2014 through February 21, 2017.Only after the publication of that investigation in 2017 could it be said that the Backers could be familiar with the AP's findings,according to the Foundation.

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

8.4. Pursuant to article 3:310 paragraph 1 BW, the five-year limitation period mentioned therein begins to run on the day following that on which the injured party became aware of both the damage and the person liable for it. According to established case law', the requirement that the injured party has become aware of 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
ve aring period of Article 3:310 paragraph 1 BW does not begin to run until the day after that on which the injured 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 injured party has sufficient security
- which need not be an absolute certainty - has obtained that damages were caused by the negligent offensive conduct of the person concerned. The answer to the question of when the statute of limitations began to run depends on the relevant circumstances of the case.

8.5. Since prescription is a liberating defense, it is up to Facebook et al. to establish, and if necessary prove, facts and circumstances necessary to conclude that in 2014 there was actual awareness on the part of the Backers of the damage and the liable person.

8.6. For the evaluation of the ve aring defense, in connection with the requirement of subjective familiarity, the individual situation of those involved is in principle important. However, an assessment of individual circumstances is not at issue in these collective proceedings, because individual cases must be abstracted from. For this reason, the question of whether the claims are partially time-barred lends itself less well to consideration in this class action. The reliance on prescription could only succeed in this case if an individual approach could be dispensed with and otherwise

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

established that subjective awareness of both the injury and the liable person was present with respect to all members of the constituency prior to Dec. 30, 2014. Facebook et al. has not alleged sufficient facts or circumstances on the basis of which that can 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 December 30, 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 familiarity with it occurred or could have occurred.
The publications that appeared in the media in 2014 and the general knowledge about personalized advertisements claimed by Facebook et al. do not have the significance that Facebook et al. want to assign to them. Based on that information, it could possibly be assumed that the supporters were aware that Facebook c.s. was also processing personal data for advertising purposes and that there was a discussion about the lawfulness thereof, but the relevant facts and circumstances in that respect were not yet known in 2014, at least not to their full extent. For instance, it did not appear that at that time it was already generally known in what way and to what extent Facebook c.s. processed the personal data of Facebook users exactly (allegedly). As a result, in 2014 there was not yet sufficient certainty among the Supporters about(alleged) faulty offensive actions of Facebook c.s. Moreover, it cannot be established either that the(possible) damage had occurred at that time a1(in all cases).

8.7. This means that in 2014 of actual awareness by the constituency of the damage resulting from the allegedly damaging events before December 30, 2014 was not yet an issue. Facebook et al.'s reliance on prescription must therefore be rejected in these proceedings. In doing so, the court does not give an opinion on the question whether in an individual case there may be prescription.

9. The request for arrest

9.1. Facebook et al. argue that several proceedings' are currently pending before the CJEU that concern the same questions as 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 previously held that there is no reason to await the outcome in UI v. Österreichische Post. The Court also sees insufficient reason to stay the case pending the outcome of the other pending preliminary ruling proceedings. It is true that the proceedings cited by Facebook et al. also relate to topics that are at issue in this case, but this 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 ECJ will rule in the aforementioned cases. Because the court is obliged (pursuant to Article 20 of the Dutch Code of Civil Procedure) to avoid unreasonable delay, it is undesirable to stay proceedings in this case, also from the point of view of procedural economy. After all, this could potentially lead to a considerable delay in a

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

now already long-running case in the first instance, while there is no certainty whether that detention will lead to further clarity.

10. Who is (processing) controller?

10.1. The question is which of Facebook et al. qualifies as a data controller within the meaning of the Wbp and processing controller within the meaning of the AVG, respectively, for the data processing at issue in this case.

10.2. Pursuant to Article 1 under d Wbp,which is the implementation of Article 2 under d of the Privacy Directive, responsible person means, among other things, the legal person who, alone or together with others, determines the purpose of and the means for processing personal data. The explanatory memorandum to the Wbp states, among other things, the following:'

> In answering the question of who is the data controller, the starting point should be, on the one hand, the formal-legal authority to determine the purpose and means of data processing and, on the other hand - in addition to this - a functional content of the concept. The latter criterion plays a role in particular if several actors are involved in the data processing and the legal competence is not sufficiently clearly regulated to be able to determine which of the actors involved is to be regarded as a data controller within the meaning of the law. In such situations, the natural person, legal entity or administrative body to which the processing in question should be attributed must be determined on the basis of generally accepted standards.
>
> It is desirable to make it clear that the term "controller" refers to the person who formally-legally controls the processing. (...)
> The starting point in the interpretation of the term "responsible person" is therefore the existing structure of civil and administrative law of persons and organization. For the private sector, this means that 4th formal-legal organization of the company is decisive. (. ..)
> The above also applies to corporate relationships. Controller is the legal person 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 is that the data subject can know in society against whom he can exercise his rights if he so wishes. (...) The fact that those data processing operations carried out by the parent or a subsidiary are (also) for the benefit of the group as such is not in itself important for establishing responsibility. However, the bill does not preclude an arrangement whereby the articles of association of the legal entities concerned or by agreement grant a particular legal entity within the group the authority to determine the purpose and means of data processing within the group. The said legal entity - for example, the parent company - is then the controller within the meaning of the bill for all data processing operations that take place within the group, because the legal control under the arrangement made rests with that legal entity. (...) It is in accordance with social discourse to attribute responsibility for data processing to the legal entity designated as the authorized legal entity pursuant to **an** internal arrangement within the **group**.

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

(...) Another important nuance 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 plurality of controllers, may be designated as such.(...)

10.3. Pursuant to Article 4 under 7 of the AVG, a data controller means, among other things, the legal person which, alone or jointly with others, determines the purposes and means of processing personal data. It must be assessed whether this legal person is capable of independently determining the purpose and means for which data are processed. It may be important that this legal entity is legally authorized to do so but that is not a requirement. This is a functional concept that aims to place responsibility where the actual control or influence with respect to data processing lies."

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, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

Under Article 4(2) of the AVG, "processing" means "any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automatic 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, blocking, erasure or destruction of data."

10.5. Thus, what matters to the (processing) controller is that the person concerned exercises an influence over the processing of personal data in question and thereby participates in determining the purposes and means of such processing. [1] The CJEU has held that the existence of joint responsibility does not necessarily result in equal responsibility. On the contrary, individuals may be involved in the processing at different stages and to different degrees. This means, according to the CJEU, that the level of responsibility of each must be considered in light of all the relevant circumstances of the case.' A person may be jointly responsible with others for operations connected with the processing of personal data only if he has jointly determined with those others the purposes and means of those operations. Such person cannot, without prejudice to any civil liability provided for under national law, be held responsible for processing operations occurring earlier or later in the processing chain and for which respectively he has not determined the purpose

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

' ECJ EU 10July **2018**, C-25/17, ECLI:EU:C:20 **18:551**, Jehovan todisiajat, para. 68

" ECJ EU 5June 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**

and determines the means.[3] This means that it must be made concrete which Facebook entity determines the purposes and means for which processing.

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

10.7. The Foundation argues that Facebook Inc. and Facebook Netherlands are also co (processing) controllers. To this end, referring to the AP's report,it puts forward, among other things, the following:

- Facebook Inc. itself speaks of a single financial operating unit in which decision-making authority for all financial operations and results rests exclusively with Facebook Inc.'s *chief operating decision ntaker*, 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 most of the processing essential to its business model. The 2015 processor agreement states 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 what data is processed for, where and how it is processed.
- Facebook Netherlands exercises significant control over attracting, retaining and supporting advertisers, requiring it to use the processing of personal data by Facebook Ireland and Facebook Inc. to identify and reach appropriate target audiences.
  Facebook Netherlands generates reports on the effectiveness of advertisements using the Facebook service, which assumes that Facebook Netherlands processes personal data obtained.
- Facebook Netherlands may make selections at the customer and/or ad campaign level from (aggregated) data it receives from Facebook Inc. and/or Facebook Ireland.

10.8. Facebook c.s. disputes, with reasons, that Facebook Inc. and Facebook Nederland are co (processing) controllers and argues that these companies do not decide on the purposes of processing as stipulated in the data policy. According to Facebook et al. the Foundation assumes incorrect circumstances and only Facebook Ireland is the data controller for users in Europe. Facebook c.s. points out that Facebook Netherlands only conducts marketing and sales activities and does not personalize ads, for example.

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

10.9. In the opinion of the Court it does not follow from the circumstances put forward by the Foundation that Facebook Inc. and Facebook Nederland are co(processing) responsible for the period at issue. This is because from all these general statements it is insufficiently clear which concrete processing operations the Foundation has in mind and in which way Facebook Inc. respectively Facebook Nederland then (co-)determines the means and purpose of the processing operations concerned. A sufficiently concrete statement by the Foundation 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 arrangement within the group means in this case that Facebook Ireland has been designated as the competent legal person, so that responsibility for the data processing at issue here is attributable to this legal person. A situation described in the explanatory memorandum to the Wbp" or the opinion of the Article 29 Data Protection Working Party" of different actors in which the legal competence is insufficiently clearly regulated or in which the obligations and responsibilities are not clearly assigned does not exist in this case.

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

10.11. Since Facebook Ireland is the (processing) responsible party, the Court will focus its further assessment on the Wbp and the AVG on Facebook Ireland. Although the parties' contentions also applied to Facebook Inc. and Facebook Netherlands, mentioning those two parties is no longer relevant for the remainder of the assessment to that extent.

11. **Disclosure requirements for** some **specific processing operations**

11.1. Firstly, the Foundation accuses Facebook Ireland (see claim a.i.1 to a.i.4, as reproduced above under 5.1) of Facebook Ireland's failure to properly inform the Supporters about four specific processing of Personal Data of the Supporters. 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 Supporters, as well as the use of telephone numbers of the Supporters, 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*** properly informed the Supporters within the meaning of Sections 33 and 34 of the Wbp and Sections 12, 13 and 14 of the AVG about the processing of personal data (for advertising purposes). However, the Court need not answer that question in a general sense, because the Foundation did not attach a(general) claim to it, but limited its claim a.i. to the four specific processing operations mentioned there. The debate in a general sense between the parties about the information obligations will therefore

" Cf. **TK 1997/98, 25** 8892 no.3, p. 55
' Cf. WP29 Opinion 1/2 10. p. 28

be discussed only insofar as relevant in the context of concrete claims.

Review framework

11.3. The Foundation's allegations cover the period from April 1, 2010 to 1 January 2020. From April 1, 2010 to May 25, 2018, the Wbp (as implementation of the Privacy Directive, the predecessor of the AVG) was applicable. As of May 25, 2018, the AVG is applicable. This distinction between the application of the Wbp and the AVG is irrelevant in these proceedings for the assessment of whether Facebook Ireland has fulfilled its information obligations. Although the information obligations have been tightened under the AVG, the information obligation is essentially the same under both legal regimes and the Foundation'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 provide that personal data:
a) must be processed fairly and lawfully;
b) must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of the data for historical, statistical or scientific purposes shall not be considered incompatible provided that the Member States provide appropriate safeguards;
c) adequate, relevant and not excessive in relation to the purposes for which they are collected or for which they are subsequently processed;
d) should be accurate and, if necessary, updated; all reasonable steps should be taken to erase or correct data that are inaccurate or incomplete based on the purposes for which they are collected or for which they are subsequently processed;
e) in a form which permits identification of data subjects must be kept 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 provide appropriate safeguards for personal data stored for longer than specified above for historical, statistical or scientific purposes.
2. The controller has the duty to ensure compliance with the provisions of paragraph 1.

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

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

1. If personal data are obtained from the data subject, the responsible party shall, prior to the time of obtaining them, communicate to the data subject the ínformation referred to in the ti second and third 1id, unless the data subject is already aware of it.
2. The controller shall inform the data subject of his/her identity and 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, to ensure proper and careful processing in respect of the data subject.

11.7. The AVG has similar provisions. For example, Article 5 paragraph 1 opening words and under a of the AVG prescribes that personal data must be processed in a way that is lawful, proper and transparent with respect to the data subject. Article 5 paragraph 2 AVG states: the controller is responsible for compliance with paragraph 1 and can demonstrate it ("accountability").

11.8. Article 12(1), first sentence, of the AVG provides, insofar as relevant here, that the controller shall take appropriate measures to ensure that the data subject receives the information referred to in Articles 13 and 14 in connection with the processing in a concise, transparent, intelligible and easily accessible form and in clear and plain language.

11.9. Article 13 paragraph 1 opening words and c of the AVG reads as follows:

> When personal data relating to a data subject are collected from that person, the controller shall already provide the data subject with the following information when the personal data are obtained:(...)
> c)the processing purposes 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 (processing) controller must actively and unsolicited inform the data subject of the data processing, unless the data subject is already informed. In this way, the data subject is able to follow how data about him are processed and challenge certain forms of processing or unlawful behavior of the processing controller in court. A processing of personal data about which the (processing) controller has not properly informed the data subject is unlawful.'[6]

11.11. In general, the (processing) controller cannot suffice with communicating his identity and the purposes of the processing. In many cases, he will have to provide the data subject with further information insofar as this is necessary to enable proper and careful processing (see also Article 33(3) Wbp quoted above at 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 necessary. 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 further information and, if so, what the scope of this information is.

11.12. The extent of the information obligation also depends on how the contact is established. In principle, the controller or data controller will have an additional responsibility to inform if he or she takes the initiative to contact the data subject. The data subject who approaches the controller himself or herself will usually already

'[6] Cf. for the Wbp: Parliamentary Papers II 1997/1998, 25 892, no. 3, pp. 149- 150 and **155-156**(MoT).

be aware of its identity and purposes. In this 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 1April 2018 of the Article 29 Data Protection Working Party stated, among other things, the following about the information obligation in the digital context:

> 10. One of the kem 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 AVG, and also relates to Recital 39, which states that "[n]atural **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 (...).

Duty and burden of proof

11.14. Pursuant to Article 150 of the Code of Civil Procedure(Rv)the party invoking the legal consequences of facts or rights asserted by it bears the

burden of proving those facts or rights, unless from any special rule or from the requirements of reasonableness and fairness results in a different allocation of the burden of proof.

11.15. Application of the main rule of Article 150 Rv entails that - in the context of the special processing operations referred to in claims a.i.1 to a.i.4 - in principle, the Foundation bears the burden of proof that Facebook Ireland has not complied with the information obligations of Articles 33 and 34 Wbp and Articles 12, 13 and 14 AVG.

11.16. The parties differ on whether a different burden of proof follows from the PDPA and the AVG.

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 Article 15 Wbp read in conjunction with Article 6 Wbp.

11.18. The explanatory memorandum to the Wbp states, among other things,'[7] :

> (...) In line with the directive, the present bill, in addition to the concept of "consent," also used the terms "unambiguous consent" and "express consent." (...)
> There is a shift in the burden of proof in the direction of the data 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 some extent, this is a similar situation to the information obligations of the data controller under Articles 33 and 34. This verification does not necessarily have to lead to the request for explicit consent. Opk may otherwise acquire information that dispels his doubts in this regard. (...)
> The responsible party has to take into account a double burden of proof. In the first place In case of doubt, it must be possible to prove that a certain permission has been granted and for what purpose. If necessary, it must also be possible to prove that the consent meets the requirements set. The data controller will also have to be able to prove that he or she has done everything that could reasonably be expected of him or her, for example with respect to the provision of information to the data subject.

11.19. Under Article 5(1) and (2) AYG, the controller must be able to demonstrate that the data processing is lawful, proper and transparent. Article 24(1) AYG states, in brief, that the controller must take appropriate measures to ensure and be able to demonstrate that the processing is carried out in accordance with the AVG.

11.20. In the Court's opinion, it follows from this that the Wbp and the AVG contain a rule of burden of proof that deviates from the main rule of Section 150 Rv, also with respect to whether or not the information duties of Sections 33 and 34 of the Wbp and Sections 12, 13 and 14 of the AVG have been met. Although less explicitly worded in the Wbp than in the AVG,this also follows from the transparency requirement. The data subject can only realize his rights under the law if he is aware of the processing. It is up to the controller to prove that the data processing is lawful.

'[7] Parliamentary Papers II 1997/1998. **25892**, no. 3, p. 66/67

This also includes informing the data subject sufficiently in advance about the data processing. On Facebook lerland - in whose domain the factual data in question are also primarily located - therefore rests the burden of proof that it has fulfilled its information obligations.

The inforniation requirement for Your four specific data process'ngs

11.21. The following will1 address the four specific data processing operations that the Foundation alleges Facebook lreland has not (properly) informed its constituents about.

1. External developers(requisition a.i.l)

11.22. As of April 2010, Facebook et al. used an ***application programming fnterface*** (API) called Graph API version 1. An API allows different types of(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 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 by an external developer, the Facebook user was asked for permission. Thereafter, the external developer obtained access via Graph API version 1 to (personal) data of the relevant Facebook user and, in addition, access to certain (personal) data of the Facebook friends of that Facebook user. This access also allowed the external developer to collect the aforementioned data.

11.24. In April 2014, Graph API version 1 was (partially) replaced by Graph API version 2. With this second version, external developers were no longer granted access to Facebook friends' (personal) data. For existing applications of external developers, that is, applications that had access to Graph API version 1 before April 30, 2014 a1, there was a transition period. They retained access to Graph API version 1 until April 30, 2015. After the latter date, a forced migration to version 2 applied, but - as insufficiently disputed it is established - several so-called ***whitelisted developers*** with Facebook lerland's permission could continue to use Graph API version 1 after April 30, 2015. In June 2018, the use of Graph API version 1 was closed to the last whitelisted developers.

11.25. At its core, the Foundation's allegation in this claim is that Facebook lerland did not, or at least did not clearly, inform the Achterban throughout the relevant period about the access that Facebook lerland granted (via Graph API)to external developers to personal data of Dutch Facebook users and their Facebook friends.

11.26. Facebook lerland takes the position that it did provide proper information about this. According to Facebook lerland, the Terms of Use and the

Data policy how third-party developers were able to collect information from users, including information from secondary users(Facebook friends).

11.27. Furthermore, Facebook Ireland 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.), the Foundation has not identified any third-party developer's application that was used by the constituency. Thus, according to Facebook Ireland, it is not 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 court rejected that argument. What is certain is 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 can be assumed that (part of the) Dutch Facebook users in the relevant period also used one or more applications from external developers. 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 is therefore not (sufficiently) substantiated by the Court.

l 1.29. On the substantive question of whether the statutory information duties have been met, the court considers the following.

11.30. It is not in dispute that through API Graph versions 1 and 2, Facebook lerland 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 l, external developers were additionally granted access to (personal) data of Facebook friends. The provision of access described above is in this context the relevant data processing for which Facebook Ireland is to be regarded as the (processing) responsible party.

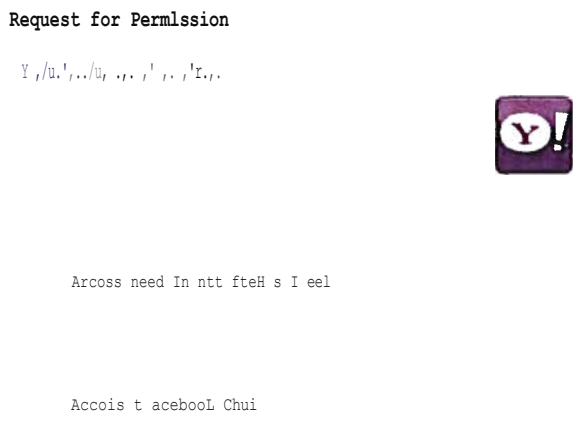
11.31. Since Facebook Ireland is the (processing) controller vis-à-vis the Achterban as far as the aforementioned data processing is concerned,it is under the obligation to comply with the statutory information obligations.It cannot therefore rely on the fact that the external developer has to provide 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 also not decisive in this regard. After all, what matters is whether the user was informed in advance that personal data could be shared.

11.32. The court addresses five separate allegations made by the Foundation below:
1. Facebook lerland did not inform THAT it shared personal data of Facebook users with third-party developers;
2. Facebook lerland has not informed about the purposes of data processing;
3. Facebook lerland did not (properly) inform what types of personal data were shared with third-party developers;

4. Facebook lerland failed to inform (properly) that Graph API version 1 also allowed the sharing of Facebook users' personal data with third-party developers via Facebook friends;
5. Facebook Ireland failed to inform *whitelisted developers* that they 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 lerland informed the constituency about the sharing of the constituency's personal data with third-party developers. Facebook Ireland brought forward that the constituency was 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 referenced by Facebook Ireland looked like this:



11'.35. '''Not at issue is 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 from application to application. Each pop-up window,Facebook Ireland undisputedly explained, showed a list of types of data the application would access after the Facebook user gave permission. Facebook
Ireland illustrated this with the example of a pop-up window she submitted.

11.36. The sample pop-up window submitted by Facebook Ireland is in the English language. The language of such an announcement plays a role in whether the text is sufficiently understandable 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 variant was made for that purpose. Because the pop-up window shown in any case (also in English) makes it sufficiently clear that the external developer will have access to the list of types of data shown in that window and is therefore sufficiently clear to the average user that Facebook Ireland will share the (personal) data belonging to the information categories mentioned in the pop-up window with the external developer, the Court will leave unanswered the question to what extent the use of the English language leads to less clarity in this case. Thus, about the data processing as such, the Achterban has been informed. This means that the Foundation's first accusation is not justified.

11.37. The second will assess whether Facebook Ireland informed the Achterban of the purposes for which it gave third-party developers access to Facebook users' personal data. According to Facebook Ireland, it informed about this through 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 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", the pop-up window does not show that it states for what purpose the application will access those categories of information. That means it must be assumed that the Facebook user was not informed in the pop-up window about the purposes of that data processing.

11.39. Facebook lerland further referred to information in the Data Policy.It explained what information had been included over time in the various versions of that Data Policy about access by external applications to personal data of Facebook users and their Facebook friends. The Court is of the opinion that it can be left open 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 (processing) controller provides the relevant information about data processing to the data subject at the moment when taking note of that information is most relevant to the data subject. In this case, that means the moment at which the Facebook user intends to install an external application. Thus, the information in question should in principle be provided in the pop-up window, because that is when that information is current 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 using the Data Policy, it should have included in the pop-up window a reference to the

'" What is written in the smaller letters under the bold headings. in the image submitted by Facebook Ireland is illegible to the court.

Data Policy should have included. Nor has it done so. Although 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, at that time the data processing at issue here (the access of external developers to the Facebook user's personal data) is not yet underway and is not yet current or relevant for the Facebook user. Therefore, a general reference to Data Policy at the time of registration with the Facebook service cannot be regarded in this case as fulfilling the information obligation 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 Achterban of the purposes for which Facebook Ireland is going to give third-party developers access to their personal data.

11.41. Moreover, in these proceedings Facebook Ireland has also not explained in concrete terms for which exact purpose(s) it gives 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 not been stated or shown that the third-party developers' access to Facebook users' personal data was limited to only those personal data necessary for the technically-functional operation of the API functionality. From the information contained in the aforementioned in
r.o. 11.34 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, without further explanation, which is lacking, it is impossible to see why access to it is necessary for the technical-functional operation of the API functionality.

11.42. The third is to assess whether Facebook users were properly informed by Facebook Ireland what types of personal data were shared with third-party developers.

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

11.44. In the 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 being accessed. Given the description of those categories (such as ***Access posts in my News Feed, Access my data any time, Access my profile inforntation* and *Access my friends information,*** see the example pop-up window in r.o. 11.34), it was also sufficiently clear to the average user that the consent to be given had a(very) broad scope and thus included all(types of) personal data within the enumerated 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 granted access. With that, it no longer matters whether the Terms of Use or the Data Policy contained sufficient information about that.

I 1.46. In the context of the question of compliance with the statutory information obligations, the Foundation's assertion that external developers had almost unrestricted access to personal data of the Achterban does not have independent significance. To the extent that a different, independent accusation is contained in that assertion, it must be rejected, because the Foundation - in the face of 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 (substantiated) argued 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 that Graph API version 1 allowed personal data of Facebook users to be shared with external developers through Facebook friends. According to the Foundation, Facebook Ireland also failed to fulfill its information obligation on this point.1.

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 June 8, 2012, December 11, 2012 and November 15, 2013:

2. Inhoud en informatie delen

3rd you own all Content and Infomation **you post on Facebook and In your jxwacy and** app settings **you can determine foe this wom galedd. Furthermore, the following provisions apply:**

3. When}e tapped an appliclng,len it djn that the appliclng asks your permission to access your Infoud Cn Information aIs'xtk the Infoud and Information that others have' i **shared with you. We require applicdngeri to respect your p+¥acy and your acceptance of that appliclng Is determines how the toq'asstng** lon **gebvlken, store and transfer your** Content and Information. **{For rre¢r Informade**

- in the November 15, 2013 Data Policy:

Other **websites and** applications

About the Facebook platform

The Facebook platfom (also called simply platfom) refers to how we help you share)e Information with the games, applications and websites that jl) and your friends use. Pete the Facebook platfom you can bring your wlenden with you so you can connect with them outside of Facebook. In these Mee ways, the Facebook platform helps you make your experiences on the Internet more personal and soclaler.

However, remember that these games, applications and websites are created and maintained by other companies and onMikkers that are not part of Facebook and are not controlled by Facebook. Therefore, make sure you always read their terms of service and prlvacy policies so that)e know how they handle)e data.

Determine what 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 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)e 'friends list').

With your friends list, the application can make your experience more soclaler by allowing you to find your friends In dle application. Your user ID helps the applicIng personalize your experience by allowing)e account in that application to be linked to your Facebook account and access your general data, including your public data and wiener list. Dlt also applies to data you make public and data that is always public. If the application wants more Infomation, such as your reports, photos and Interests, you must give permission for it.

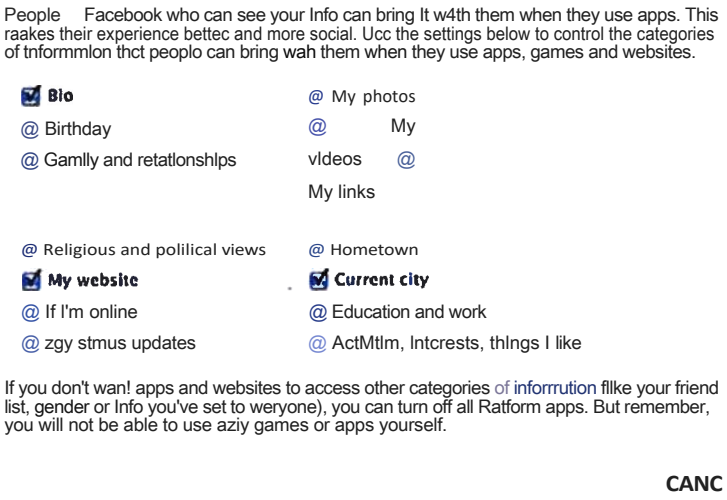
The Apps you use setting allows you to manage the applications you use. You can see the permissions you have given these applications, the last time the application used)e data, and you can view the Facebook audience for your timeline reports and activities that the application posts on your behalf. You can also delete applications you no longer want to use or disable all platform applications. If you disable all pladorm applications, your user ID will no longer be given to applications, even if your friends use those applications. But you also can no longer use games, applications or websites through Facebook.

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

The data that)e 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 dle can see it dlt also share it with others, Incluslef the games, applications and websites they use.

Your friends and the other people you share dlngen 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 muslektoepasslng 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 (and that includes your user ID) so that the applicIng knows which of her friends are also using the application. the wieners might also want to share the music dle JiJ "leike" on Facebook. If you have made that information public, the application has access to it, as do others. To if you have only shared your interests with your friends, the applicIng may ask your friends for permission to share your interests.

You can manage most of the data others share with applications using the Settings paglna Ads, apps and websites. To 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 can't get information about you when your friends and others use them, you need to disable all pbbom 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 Policy dated January 30, 2015 and September 29, 2016:

- **Apps, websites en integratiepunten van externe partijen die onze services gebruiken of erop aanwezig zijn.** Als je externe apps, websites of andere services gebruikt die gebruikmaken van of geïntegreerd zijn met onze services, kunnen deze externe services gegevens ontvangen over wat je plaatst of deelt. Wanneer je bijvoorbeeld een game speelt met je F[illegible]-vrienden of de Facebook-knop Reageren of Delen gebruikt op een website, ontvangt de gameontwikkelaar of website mogelijk informatie over je activiteiten in de game of de reactie of link die je vanaf de website deelt op Facebook. Daarnaast krijgen externe partijen als je hun services downloadt of gebruikt, toegang tot je openbare profiel, waaronder je gebruikersnaam of gebruikers-ID, je leeftijdsgroep en landstaal, je vriendenlijst en de gegevens die je met deze externe services deelt.Gegevens die worden verzameld door deze apps, websites of geïntegreerde services zijn onderhevig aan de voorwaarden en beleidsregels van de betreffende externe services.

  Meer informatie over hoe je de gegevens kunt controleren die ill en anderen over jou met deze apps en websites delen.

11.49. With Graph API version 1, an external developer not only obtained access to (personal) data of the Facebook user in question, but also access to certain (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. Due to 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 for the average user unforeseen form of data processing must therefore be clearly informed. 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 November 15, 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 November 15, 2013 Data Policy is very voluminous; 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 Policy of January 30, 2015 and September 29, 2016, the disclosure is different in scope and content. There, the relevant information is very concise. However, the passage cited by Facebook lerland again does not show that users' personal data could be shared with external applications by their Facebook friends.

1 1.5 1. Facebook Ireland still argued that in its Data Policy, it advised users to read the terms and policies of the third-party applications themselves to understand how those applications would handle their data. This argument cannot help Facebook Ireland. As previously considered, Facebook Ireland is the (processing) responsible1y when it comes to granting third-party developers access to Facebook users' personal data, so Facebook Ireland must comply with legal information obligations 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 must properly inform Ireland in advance about the data processing.

11.52. ln the last place, it must be assessed whether Facebook informed lreland that the ***whitelisted developers*** retained access to Facebook friends' data even after the introduction of Graph API version 2.The court held that

Facebook Ireland also breached its information obligation on this point. The court explains this as follows.

11.53. Facebook Ireland has not (sufficiently) refuted the course of events alleged by the Foundation 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 April 30, 2015. Furthermore, Facebook users were never informed that so-called ***whitelisted developers*** could continue to use Graph API version 1 after April 30, 2015 and thus retain access to Facebook friends' information and personal data, even though Graph API version 1 was purportedly formally closed on April 30, 2015. The ***whitelfsted 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. With the Foundation, the Court finds that Facebook Ireland should have informed about 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***, it is necessary to ensure proper and careful processing. By failing to inform about this, Facebook Ireland violated 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 constituency about the purposes of the data processing(providing access to the external developers to personal data of Facebook users),that in the period from April 1, 2010 to June 2018, Facebook Ireland did not properly inform the Supporters 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 from April 2014 to June 2018, Facebook lerland did not inform the Supporters that the ***whitelisted developers*** could continue to use 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 violated the information obligations of Article 33 paragraphs 2 and 3 Wbp and Article 13 paragraph 1 AVG, respectively. Since these processing operations were not properly informed, they are unlawful. The declaratory judgment claimed by the Foundation is allowable as described above.

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

11.56. Claim a.i.2 relates to Facebook lerland's allowing Alexandr Kogan and his company Global Science Research Ltd(hereinafter: GSR), among others, to have access to Personal Data of the constituency. According to the Foundation, Facebook Ireland did not (clearly) inform the constituency about that access. According to the Foundation, the Subordinates' 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. Further, Facebook Ireland refers to its defense to claim a.i.1.

11.57. Kogan and GSR offered an application(hereinafter "the GSR application")that connected to the Facebook service via the Graph API version 1. The Foundation did not dispute 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 did not dispute 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 allegations 1 to 4 as mentioned in r.o. 11.32(in the context of the question whether Facebook Ireland informed the Backers 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 similarly admissible as claim a.i.1., with the understanding that, according to the Foundation, 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.

l 1.59. With respect to Cambridge Analytica Ltd., Cambridge Analytica LLC and SCLE Elections Ltd (hereinafter together: Cambridge Analytica et al.) claim a.i.2. is not assignable. It is not relevant for the assessment in these proceedings whether personal data of members of the Achterban 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 or34 of the Wbp. Facebook Ireland had no control over any access by Cambridge Analytica et al. to the personal data of the Achterban. At the time Facebook Ireland processed the personal data and granted Kogan/GSR access to it, it did not know that such data would be provided (unauthorized) by Kogan/GSR to a third party in the future. Thus, for such further processing, Facebook Ireland did not determine the purpose and means. For that reason it cannot be regarded as a (processing) controller for that purpose, so there was no information obligation for Facebook lreland for that as referred to in article 33 or34 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 two-factor authentication.

11.61. Two-factor authentication(hereafter: 2FA)is a security method 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 takes place.

" This app previously heene "CPWLab" and "ihisisyourdigitallife.

11.62. As of May 2011, the Facebook service allows 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 of:
1) use 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) add a new or use a different phone number (hereinafter also: choice 2).

11.63. The Foundation argues that Facebook Ireland did not (properly) inform the Supporters that the phone numbers provided by the Supporters 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 Supporters that those phone numbers could also be processed for the purpose of serving personalized ads.

11.64. It is not disputed that Facebook Ireland also **processed** telephone numbers provided to it for advertising purposes.In the District Court's opinion, the Foundation no longer has an independent interest in a judgment on the question of whether Facebook Ireland properly informed the Backers on this point. The reason for this is that in this judgment (see chapter 12) the court comes to the opinion that Facebook Ireland had no legally valid basis for processing Personal Data of the Supporters 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 claimed that it can rely on any other legally valid basis for **processing** those phone numbers for advertising purposes. In particular, Facebook Ireland has not claimed that it obtained consent to use the phone numbers provided under 2FA for advertising purposes. Nor is such consent evident from the module a Facebook user went through in either the Choice 1 or Choice 2 situation.

11.65. Thus, there was no basis for Facebook Ireland's processing of those phone numbers for advertising purposes throughout the relevant period. The absence of a processing basis is the most far-reaching judgment that can be given about a data processing operation and affects that processing in all its parts. The extent to which the (data controller) complied with its information obligations 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 the Foundation still has in a judgment on the declaratory judgment it has claimed as a.i.3. After all, that statement focuses on the failure to inform the Foundation 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 also has no added value in view of the more comprehensive judgment that there was no legally valid basis 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' program(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* from the likes of 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 prograniniing 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 (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 Facebook friends' information.

11.69. The Foundation claims that Facebook Ireland did not (clearly) inform the constituency about the *integration* partnership program and the related processing of the constituency's personal data. To this end, it argues the following. Research by *The New York Tfmes* 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, making the Facebook service available on Facebook users' devices did not require integration partners to access a user's Facebook friends' personal data. Given the extent of sharing personal data with integration partners, Facebook should have informed lerland about 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. Finally, the Foundation questions Facebook Ireland's position that Facebook Ireland agreed with the integration partners that the personal data received by them may not be used for their own purposes. That agreement has not been submitted, so it is uncertain whether Facebook Ireland's position is true. For this reason, the Foundation disputes that position.

11.70. Facebook Ireland argues 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 clearly informed Ireland 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 stressed that integration partners were not allowed to use the data they received through the APIs for other proprietary purposes without the Facebook user's consent. The integration partners also contractually committed to Facebook lreland that they would only use the data they accessed for the purpose of providing a Facebook experience.

11.71. The court first states that, as with 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 (processing) responsible1. After all, it (also) determines the purpose and means for this. Granting this access is therefore to be considered relevant data processing in the context of claim a.i.4. It is to that data processing that the information duties relate. Any further data processing by the integration partners is beyond the (processing) responsibility of Facebook Ireland. Indeed, the Foundation has not stated any relevant facts or circumstances on the basis of which it can be established that Facebook Ireland (co)determines 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 lreland, 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 circumstances this entails an obligation to take measures to limit the (further) processing of personal data to whom those data are provided, but the Foundation has not based its claims on any violation of such an obligation. The aforementioned obligation also cannot be subsumed under the information obligations of Articles 33 and 34 of the PDPA or Articles 12, 13 and 14 of the AVG,while the declaratory judgment claimed by the Foundation is based on the violation of those information obligations.

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 (processing) controller provides the relevant information about data processing to the data subject at the moment when taking note of that information is most relevant for 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 that data processing is current and relevant. Facebook lerland 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. The question can be left open as to whether the

Data Policy about that data processing contained (sufficiently concrete) information. because it has neither been stated nor shown 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 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 here was not necessarily at issue, so that is not the appropriate time to inform. Therefore, a general reference to Data Policy at the time of registration with the Facebook service cannot, under the circumstances, be regarded as fulfilling the legal obligation to inform regarding this data processing.

11.75. The foregoing means that the Foundation's argument succeeds. Facebook Ireland did not inform Achterban about the access of integration partners to personal data of Facebook users and their Facebook friends. By doing so, Facebook Ireland violated the information obligations of Article 33 paragraphs 2 and 3 of the PDPA and Article 13 paragraph 1 of the AVG, respectively. violated. Since the aforementioned data processing operations were not properly informed, those processing operations are unlawful.

11.76. As to the period during which the violation of these information obligations occurred, the following applies. The Foundation has argued that throughout the relevant period, Facebook Ireland did not inform the Achterban about the provision of data to integration partners. It has not been disputed by Facebook Ireland that it had collaborations 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 violation of the information obligation occurred over the entire relevant period.

11.77. In consideration of the foregoing, the claimed declaratory judgment is allowable.

12. Basis for processing

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

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

12.2.1. Article 8 Wbp, as far as relevant, read as follows:

> Personal data may be processed only if:
> a. the data subject has given his unambiguous consent to the processing;

b. data processing 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 necessary for the conclusion of a contract;
c. (. . .)
d. (. ..)
e (. . .)
f. the data processing is necessary to satisfy 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) AVG reads, to the extent relevant, as follows.

Processing is lawful only if and to the extent that at least one of the following conditions is met:
(a)the data subject has consented to the processing of their personal data for one or more specific purposes;
b. the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take measures at the request of the data subject prior to the conclusion of a contract;

(f) the processing is necessary for the purposes of the legitimate interests of the controller or of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring 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.[2] 'The principles of proportionality and subsidiarity must be met in any data processing, both under the PDPA and under the AVG. 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."

12.4. Under both the Wbp and the AVG, it is up to the (processing) controller to prove that the data processing is lawful.[2] 'Thus, Facebook Ireland has the burden of proof 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, invokes Facebook Ireland relies on the following bases:
i) consent (Article 8 preamble and sub a Wbp),

" 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.
-' Supreme Court Sept. 9, 2011, **ECLI:NL:HR:2011:BQ8097, para. 3.3** and Supreme Court Dec. 3, 2021, **ECLI:NL:HR:2021:1814, r.o. 3.1.2.**
- See the MoT to **the Wbp**(Parliamentary Papers **11 1997/1998, 25892, No. 3, p. 66/67) and the** provisions of Article 15 Wbp.See further the provisions of Articles 5(2)(in conjunction with 5(1) and 6. 7 paragraph 2 read in conjunction with ovenveging 42 of the preamble and 24 paragraph 1 AVG.

ii) contractual necessity(Article 8 opening words and under b Wbp)and
iii) legitimate interest(article 8 opening words and under f Wbp).

12.6. For that part of the relevant period when the AVG applied, Facebook Ireland generally (exclusively) invokes the basis of contractual necessity(Article 6 under b AVG). For a number of specific situations, Facebook Ireland invokes consent under the AVG(Article 6 under a AVG). Whetherin those specific situations the requirements for consent are met is not for assessment 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 assess below first the basis of contractual necessity(Article 8 opening words and under a Wbp; Article 6 paragraph 1 under a AVG) invoked by Facebook lerland, as this basis was invoked for the entire relevant period.

Contractual necessity as verse basis?

12.8. Facebook Ireland takes the position that the processing of personal data by advertising purposes was necessary to give effect to the agreement. To this end, it argues the following. The Facebook service is at its core 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. Also at the time of the AVG, the terms and conditions made it clear to users 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 core of the service Facebook Ireland offered and provided. Therefore, in its view, this processing was necessary for Facebook lreland to fulfill its contractual obligations.

12.9. The Foundation disputes that the processing of personal data for advertising purposes was necessary for the implementation of the user agreement between Facebook Ireland and the constituency members. To this end, the Foundation argues that for a user, the personalization of ads is not the reason for signing up for the Facebook service. The core idea 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. The Foundation refers to guidance from the EDPB from 2019 on the application of the AVG. These state that the processing of personal data for'behavioral advertising' is not necessary for the performance of a contract. Incidentally, according to the Foundation, a social network, such as the Facebook service, can also be offered without processing personal data for commercial oradvertising purposes.

12.10. The court considered the following.

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

12.12. It follows from the case law of the CJEU that the concept of 'necessary' in the various parts of Article 7 of the Privacy Directive and Article 6 AVG is an autonomous concept of Union law.[2] 'On the interpretation of the criterion 'necessary for the performance of the contract' the CJEU has not yet ruled.

12.13. For the interpretation of the 'contractual necessity' basis, the Court also considers the advice and guidelines of the Article 29 Data Protection Working Party (hereinafter also: WP29) and of the European Data Protection Board (hereinafter: EDPB) to be important. 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 consultative character(Article 29(1) Privacy Directive)and its main task was to promote 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 AVG.

12.13.1. WP29's Opinion 06/20 14 on Article 7 of the Privacy Directive(of which Article 8 Wbp was the implementation)stated, inter alia, the following[2] ':

> The provision [Article 7(b) of the Privacy Directive, *court added]* 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.
>
> 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.

'[3] ECJ EU December 16, **2008**, **C-524/06**, **ECLI:EU:C:2008:724**, Huber, para. 52.

*' 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**, pp. 20-21.

12.13.2. The EDPB's Guidance 2/2019 on Article 6(b) of the AVG in the context of the provision of online services states, **among other things, the following**":

> 23.(...) it should be noted that the notion of 'necessary for the performance of a contract' is not simply an assessment of what is permitted or included in the terms of a contract. The concept of "necessity" has an independent meaning in Union law, which must reflect the objectives of data protection law.
>
> 27.(. .) When a controller wishes to demonstrate that the processing is based on the performance of a contract with the data subject, it is important to assess what is *objectively gen-ally* necessary to perform the contract. The concept of "necessary for performance" clearly requires more than a contractual provision.
>
> 30. When assessing whether Article 6(1)(b) is an appropriate legal basis for processing in the context of a contractual online service, the specific aim, purpose or objective of the service should be considered. Article 6(1)(b)is only applicable if the processing is *objectively necessary* for a purpose integral to the provision of that contractual service to the data subject. The processing of pay1ng data for payment for the service is not excluded. The controller must be able to demonstrate how the main subject matter of the *specific contract may* not actually be performed to *the data subject* if the specific processing of the *personal data in question* does not take place. The key issue here is the connection between the personal data and the relevant processing activities and whether or not the service provided under the agreement is performed.
>
> 32. The controller must be able to justify the necessity of the processing by reference to the main and mutually understood purpose of the agreement. This depends not only on the perspective of the controller, but also on the perspective of a reasonable data subject when entering into the agreement and whether the agreement can still be considered "performed" without the processing in question.(...)
>
> 33. In conducting the assessment of whetherarticle 6(1)(b)is applicable, the following questions may serve as guidelines:
> • What is the nature of the service provided to the individual? What are its distinguishing characteristics?
> • What is the exact rationale of the agreement (i.e., its essential content and fundamental objective)?
> • What are the essential elements of the agreement?
> • What are the perspectives and expectations of both parties to the agreement? Höe will the service be promoted to the individual or how will it be advertised? Should

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

> a normal user of the service would reasonably expect that, given the nature of the service, the intended processing would occur to perform the contract to which they are a party?
>
> 51. Advertising based on surfing behavior, and the associated tracking and profiling of data subjects, is often used to fund online services. (...)
>
> 52. As a general rule, the processing of personal data for advertisements based on surfing behavior is not necessary for the performance of a contract for online services. Normally, it is difficult to argue that the contract would not have been performed because there were no ads based on surfing behavior.(...)
>
> 53. In addition, Article 6(1)(b) cannot provide a lawful basis for advertisements based on surfing behavior because such advertisements indirectly finance the provision of the service. While such processing may support the provision of a service, this alone is not sufficient to establish that it is necessary for the performance of the relevant contract. The controller must consider the factors listed in paragraph 33.

12.14. It follows from the above that the processing ground 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 offering 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 offer 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 offering 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. It is therefore not established that it could not. Therefore, in order to offer 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 agreement between Facebook Ireland and a user of the Facebook service. Thus, Facebook Ireland cannot successfully rely on contractual necessity (as referred to in Article 8 opening words and under b of the Wbp and Article 6 (1) under b of the AVG, respectively) as a basis for processing, either under the Wbp or the AVG.

12.18. This means that during the part of the relevant period when the AVG 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 PDPA was applicable,the two other bases (consent and legitimate interest) invoked by Facebook Ireland will be further assessed below.

Toesteitinting as a basis for verification*?*

12.20. Facebook Ireland takes 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 Data Protection Act, 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. That Data Policy provided links to other pages where further information could be found. Incidentally, users were also subject to a certain duty of inquiry. Existing users were informed of changes to the Data Policy through notifications and e-mail messages, among other things.

l 2.21. The Foundation takes the position that Facebook Ireland did not obtain legally valid consent. To this end, it submits, in brief, the following. At no time during the relevant period did Facebook Ireland properly inform the Backers about the processing of personal data for advertising purposes.
Information about the purposes of data processing was fragmented and not in the first layer of information. Facebook Ireland's tiered 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. lnstead of placing all relevant information about data processing succinctly and clearly in the first layer of information

provide, 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 constituency could not know what it would consent to. Thus, the requested consent did not meet the requirements of free, specific, informed and unambiguous.

Review framework

12.22. In the meaning **and interpretation** of the term consent, the court considers the following.

12.23. Consent must be obtained prior to data processing.

12.24. In Article 1 opening words and under i Wbp (as implementation of Article 2 under 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. Article 8 opening words and under a Wbp stipulates that consent must be given unambiguously.

12.25. This means that an expression of will must meet the following requirements before it constitutes consent as referred to in Article 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. It must be clear which processing, of which data, for which purpose will take place, and if this involves disclosure to third parties, also to which third parties.[26]

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 information obligations of Articles 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*":

> (...) the data subject can only give his consent responsibly if he is informed to the best of his ability.(...) Seeking the data subject's consent implies that he must be informed of the course of events regarding the data processing. In principle, this (information) duty rests with the person responsible and/or the data controller.

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

-' Parliamentary Papers I l997/l998, 25 892, no. 3, pp. 65-66.

processor. The data subject must be adequately and intelligibly informed by the controller about the various aspects of data processing that are of interest to him. The information obligation of the controller is limited by the facts that the data subject already knows or should know. The information obligation of the responsible party does not imply that the individual bears no responsibility. The data subject has a certain duty to investigate before passing judgment. What is decisive for the extent to which the person responsible must inform the data subject or the data subject himself must investigate is what can reasonably be expected in society. This will have to be determined by weighing all the circumstances of the concrete case.
Factors that may play a role in 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 MoT to the Wbp states the following about this requirement, among other things":

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 behavior. For example, filling out a form for the purpose of requesting a certain service may, under circumstances, be regarded as granting 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 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 information obligations in the digital context.

12.27. In 201 l, WP29 issued a comprehensive opinion on the definition of consent in the Privacy Directive. Among other things, that opinion stated the following":

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

-‖ Parliamentary Papers II 1997/1998, 25 892, no. 3, p. 67.
" Opinion 15/201 l on the definition **of "consent" (WP 187), adopted July 13, 201 l, pp. 20, 23,** 40 and 41.

consent is required for each element. In particular, consent relates to the data being processed and the purposes for which it is being processed. 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 information - The manner in which the information has been provided (in clear and understandable language, without jargon, conspicuous) is crucial in assessing whether informed consent has been given. How the data subject should be informed depends on the context: a typical user should be able to understand it.

• Accessibility and visibility of information - Information must be provided directly to the data subject. It is not enough to make the information "available" somewhere. (...) The information must be clearly visible (type and size of letters), conspicuous and complete. Dialogue frames can be used to provide specific information at the time consent is sought. As noted above in connection with "specific consent," online information tools are especially useful in connection with social networking services, to ensure sufficient differentiation and clarity regarding privacy settings. The use of layered messages can also be useful, as it allows the necessary information to be provided in an easily accessible way.

• A consent must be *specific*. A general consent without specifying precisely the purpose of the processing to which the data subject consents does not meet this requirement. This means that information about the purpose of processing should not be included in the general terms and conditions, but in a separate consent clause.

• A consent must be based *on information.* (...) Two additional requirements flow from the requirement that a consent must be based on information. First, the information must be provided in language that is understandable to the individual so that he understands what he is consenting to. This is contextual. Providing information that uses overly complicated legal or technical jargon does not meet the legal requirements. Second, the information provided must be clear and sufficiently prominent so that it is not overlooked. The information must be provided directly to the data subject. It is not enough to make the information "available" somewhere.

(…)

• For data other than sensitive data, Article 7(a) requires consent to be *unambiguous*. "Unambiguous" calls for the use of mechanisms for obtaining consent that leave no doubt that the data subject is in fact

wanted to give his consent. In practice, this requirement for data controllers allows them to use different types of mechanisms for obtaining consent, ranging from statements of agreement(outdated consent) to mechanisms in which the data controller bases "consent" on an action by the data subject by which he or she indicates his or her consent.

• A "consent" deemed to result from the inaction or silence of the data subject is normally not legally valid, especially in an online environment. This is particularly true when "consent" is given via default configuration settings that the data subject must change if they do not want their data to be processed. This is the case, for example, with pre-ticked boxes or with browsers that are set to accept cookies by default.

12.28. Also relevant in this context are the Guidelines on Transparency under Regulation (EU)2016/679 of l April 2018 of the Article 29 Data Protection Working Party on Layered Privacy Statements in the Digital Context mentioned above under l 1.13.

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.Following the parties, the court will therefore distinguish between three time periods (periods A, B and C) in its assessment.

- PERIOD A(l April 2010 to June 8, 2012)

12.30. Facebook Ireland undisputedly explained that the account registration of a new user during this period consisted of two steps and proceeded as follows. After the new user entered his initial information, such as name, email address and password, he was redirected 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 then current versions of the(in English) Data Policy(titled: *Privacy Policy)* were always four or five pages in a relatively small font. The December 22, 2010 version of the Data Policy stated, among other things, the following:

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 Ri3hts 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 accorInt 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 favorite 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 mahe 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 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 without more, qualify as a declaration of agreement with its contents. From the way Facebook Ireland had structured the registration process, it could 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 with regard to 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.
Already in view of the foregoing, the reading confirmation does not constitute consent.

12.35. To the extent that Facebook Ireland 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 reachable 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. Furthermore, Facebook Ireland still 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 help 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 knowledge of such a communication cannot be considered 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 notification, and the mere reference therein to amended Terms of Use and/or Data Policy does not meet **the requirements to be required.**

12.39. It has not been alleged or shown 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 constituency for data processing for advertising purposes.

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

12.41. Facebook Ireland undisputedly explained that a new user seeking to register with the Facebook service during this period was shown the following:

Figure 43 (2012-2014)

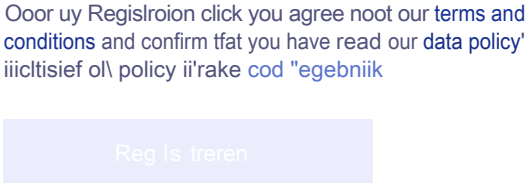
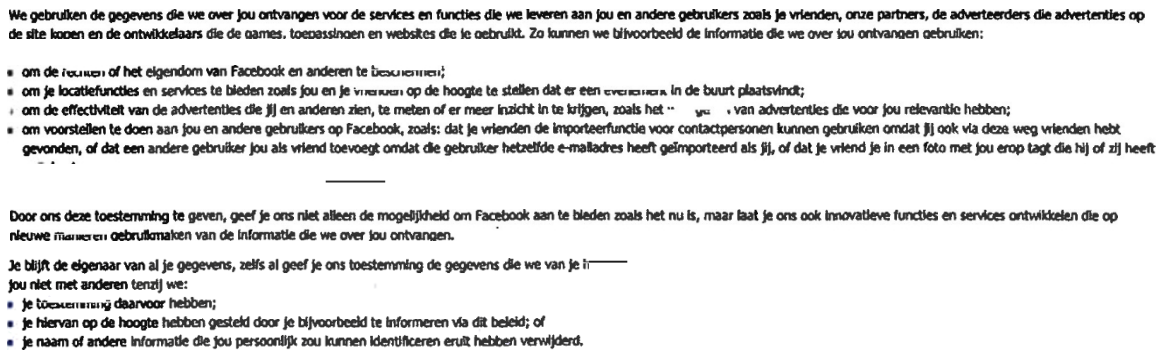


Figure 44 (2014-2018)

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

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



We gebruiken de gegevens die we over jou ontvangen voor de services en functies die we leveren aan jou en andere gebruikers zoals je vrienden, onze partners, de adverteerders die advertenties op de site kopen en de ontwikkelaars die de games, toepassingen en websites die je gebruikt. Zo kunnen we bijvoorbeeld de informatie die we over jou ontvangen gebruiken:

- om de rechten of het eigendom van Facebook en anderen te beschermen;
- om je locatiefuncties en services te bieden zoals jou en je vrienden op de hoogte te stellen dat er een evenement in de buurt plaatsvindt;
- om de effectiviteit van de advertenties die jij en anderen zien, te meten of er meer inzicht in te krijgen, zoals het aantal keren dat van advertenties die voor jou relevantie hebben;
- om voorstellen te doen aan jou en andere gebruikers op Facebook, zoals: dat je vrienden de importeerfunctie voor contactpersonen kunnen gebruiken omdat jij ook via deze weg vrienden hebt gevonden, of dat een andere gebruiker jou als vriend toevoegt omdat die gebruiker hetzelfde e-mailadres heeft geïmporteerd als jij, of dat je vriend je in een foto met jou erop tagt die hij of zij heeft

Door ons deze toestemming te geven, geef je ons niet alleen de mogelijkheid om Facebook aan te bieden zoals het nu is, maar laat je ons ook innovatieve functies en services ontwikkelen die op nieuwe manieren gebruikmaken van de informatie die we over jou ontvangen.

Je blijft de eigenaar van al je gegevens, zelfs al geef je ons toestemming de gegevens die we van je krijgen jou niet met anderen tenzij we:

- je toestemming daarvoor hebben;
- je hiervan op de hoogte hebben gesteld door je bijvoorbeeld te informeren via dit beleid; of
- je naam of andere informatie die jou persoonlijk zou kunnen identificeren eruit hebben verwijderd.

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 rulings 12.33-12.39 regarding period A also applies to period B. This means that the required consent for period B also cannot be based on the reading confirmation upon registration or on later agreement upon changes to the Data Policy.

12.45. Thus, even in period B, Facebook did not obtain legally valid consent from the constituency for data processing for advertising purposes.

- PERIOD C(January 30, 2015 to April 19, 2018)

12.46. Facebook Ireland undisputedly explained that a new user seeking to register with the Facebook service during this period was shown the following:

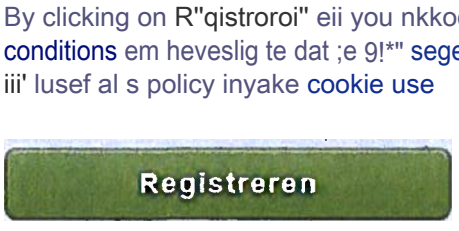


Figure 44 (2014-2018)

The text above the "Register" button contained hyperlinks to the Terms of Use, Data Policy and Cookie Policy.

12.47. The version(dated January 30, 2015) of the(in Dutch) Terms of Use(titled: *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**
> Gege''ens policy **that can be adjusted periodically.**

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

> I. **Welhe 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 post and communicate with others. This may include data in and about the content you provide, such as the location of a photo 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 photo of you, send you a message, or upload, sync or import your contact information.
> • 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, sync 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 consent to
> given. We may associate the data collected with 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.

• **Facebooh 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.

ll. 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 analyze 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. Learn more about advertising through our services and how you can opt out.

Control how personal information 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 Helpcenti ulu.

III. How will this data be shared?

Sharing with external partners and customers

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 ad litlijiii.
View your advel tentievoorketlreii 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 lreland 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.

12.5 1. 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 brought forward 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 stepped form of obtaining consent in this case does not meet the requirements for consent under Article 7 Privacy Directive. To this end, the following are reasons.

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 then 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 lerland 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. Thus, an average user has not been 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 above in
rulings 12.36, 12.38 and 12.39.

12.55. Thus, even in period C, Facebook did not obtain legally valid consent from the constituency for data processing for advertising purposes.

Chartered 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. The Foundation disputes that Facebook Ireland can use the "legitimate interest" basis to process personal data for advertising purposes. To this end, it submits the following. The commercialization of a supposedly freely offered service is not a legitimate interest. In addition, the processing is also 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. The necessity requirement also involves the fact that Facebook lerland 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 offundamental rights of users are not disproportionately affected is not met because Facebook Ireland has not made a concrete 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 court not only takes into account the case law of the
ECJ EU but also on the opinions of WP29.

12.59. According to established case law'[0] of the ECJ, three cumulative conditions must be met in order for personal data to be processed on the basis of legitimate interest:

3° See, for example, ECJ EU 29 July 2019, C-40/17, ECLI:EU:C:2019:629 (Fashion ID), para. 95.

1. there must be the protection of a legitimate interest of the controller (or of the third party to whom the data is disclosed);
2. the processing must be necessary for that legitimate interest, and
3. the interests or fundamental rights and freedoms of the person whose personal data are processed do not prevail.

12.60. ECJ case law shows that a legitimate interest(the first condition) must be existing, actual and not hypothetical at the date of processing."

12.61. WP29 issued an opinion on the concept of legitimate interest in Article 7 of the Privacy Directive(whose implementation was Article 8 Wbp). Among other things, that opinion stated the following'[2] :

> 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 the

'' **ECJ EU Dec. 11, 20 19, C-708/18, ECL[:EU:C:2019:1064(TK /M5A-Scara), para. 44.**

'- **WP29 Opinion** 06/2014 on **the** notion of **legitimate** interest **of** the **data processor.** responsible" in Article 7 **of** Directive 95/46/EC **(WP217), adopted April** 9, **2014, pages 29-31.**

> data protection 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:
> - be lawful (i.e. in accordance with applicable EU and national law);
> - be articulated with sufficient clarity to allow for balancing with the interests and fundamental rights of the data subject (i.e., sufficiently specific);
> - represent a real and present interest (i.e., are not speculative).

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."

12.63. WP29's 2014 opinion" includes the following on the second condition:

> This condition complements the necessity requirement under Article 6 [of the Privacy Directive, *court added]* 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, under (b)-(f)[of the Privacy Directive, *court added],* 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 purpose to be served by the processing. Under the principle of subsidiarity, the purpose for which the personal data are processed should not reasonably be able to be achieved in another way which is less prejudicial to the data subject.

12.65. With respect to the third condition - the(further) consideration of the relevant rights and interests - according to established case law of the ECJ, that balancing and the outcome of that balancing depends in principle on the particular circumstances of a concrete case.[35]

" See, for example, ECJ EU May 4, **2017**, **C-13/16**, **ECLI:EU:C:2017:336**(Rigas), para. 30.
" 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.
" See, for example, **ECJ** 4 May 2017. **C-13/16**, **ECLI:EU:C:2017:336**(Rigas), **para. 31.**

12.66. WP29's 2014 opinion'[6] states the following about the third condition, among other things:

> 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.

*Sluielfactors to be taken into account in the **consideration** of interests*

Based on the foregoing, the useful factors to be considered in the interest assessment include:

• The nature and source of the legitimate interest, 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;

• The impact on those affected, including:

- 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"),

'[6] **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, pages 36 and 60- 62.

- 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 ver-et 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 that 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 ECJ 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 ECJ.'[7] For the assessment of the dispute between the Foundation 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.
Unlike the Foundation has argued, for the time being the Court sees no reason to assume that commercial interests could not be regarded as a legitimate interest within the meaning of Article 7 under f of the Privacy Directive and Article 8 opening words and under 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 by the ECJ and in the WP29 opinion, that the alleged legitimate interest must be existing, actual (present), not of hypothetical nature(actual) and legitimate, the legitimate interest alleged by Facebook Ireland meets in any case. The court therefore presumptively assumes that Facebook Ireland had a legitimate interest

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

when processing personal data for advertising purposes and that the first condition is thus met.

12.69. As a second condition, the necessity requirement must be met. This requires an assessment against 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 did not clearly address the requirements of proportionality and subsidiarity in its submission. It merely stated that its interests and those of its users run parallel because users also benefit from personalization. By doing so, Facebook lerland 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 (processing) controller must take into account the reasonable expectations of data subjects. It has not been shown that Facebook Ireland actually did so. It has only 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 (processing) controller should therefore be transparent about that processing and about its business model. This means that it must also be made clear to users that in return for offering the service as free, users' personal data will be processed for advertising purposes. Facebook Ireland has not been sufficiently transparent about this in its terms and data policy. Also 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 applies 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 has to be considered less intrusive. 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 the Foundation's position that Facebook Ireland can also suffice with the sale of advertisements that are not 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 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 Article 8 opening words and under 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 Article 8 opening words and under f Wbp cannot serve as a processing basis either.

Conclusion on the processing bases

12.73. In conclusion, Facebook Ireland cannot rely on any of the processing bases it has invoked for 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 Supporters for advertising purposes throughout the period from April 1, 2010 to January 1, 2020 was not permissible. By processing those personal data for advertising purposes,without having a legal basis for doing so, Facebook Ireland has infringed the right guaranteed by, inter alia, Article 8 ECHR protected fundamental right to protect the personal data of the constituency. Thereby, Facebook Ireland has acted (culpably) unlawfully towards the members of the Supporters. The declaratory judgment claimed by the Foundation as a.ii.l is therefore admissible for the entire period from l April 2010 to l January 2020.

13. Special personal data

13.1. Under Article 16 Wbp and Article 9 AVG, 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. After the AVG comes into force, genetic and biometric data will also fall under 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 AVG, the burden of proof that explicit consent has been given rests on the party processing the special personal data.

13.3. The Foundation claims that Facebook lreland violated the ban on processing special personal data by using such constituency data for advertising purposes without 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 are not special personal data, nor did Facebook Ireland intend to derive them. These interest categories only **reflect** interests, **do** not concern or reveal personal characteristics. Furthermore, Facebook Ireland uses an unambiguous "user consent module" that requires users to explicitly

consent is required before Facebook lreland processes special personal data of those users. The documents referred to by the Foundation in support of its contentions refer to the period before the introduction of the AVG 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 (without obligation) and (ii) data that Facebook Ireland obtains by monitoring users' surfing behavior and deriving certain interests from it.

(i) profile fields

13.6. The Foundation argues that Facebook Ireland uses the special data obtained from the profile fields for advertising purposes, basing its argument in particular on the AP report. Facebook Ireland disputes the Foundation's contention and argues that it does not process data entered in a user's profile fields to offer personalized ads.

13.7. The court does not follow Facebook lerland's position. The AP report shows that the AP conducted its own investigation using a fictitious user of the Facebook service and a fictitious website. Based on that investigation, the AP concludes that the Facebook group(to which Facebook lerland belongs) processes special data of sexual orientation for advertising purposes. According to the AP, the Facebook group enables advertisers to show targeted ads to people in the Netherlands based on their sexual orientation as they have indicated in their profiles. The AP conducted further investigation in response to the argument that Facebook lerland does not use data from the content of profiles. Using ten accounts created(with which no activities were subsequently performed), the AP found that information from the profile fields was we1 used, as some of these accounts received ads related to their profile. Facebook lerland has not disputed the findings and outcomes of the AP's investigation with sufficient specificity. It has not come up with a logical explanation for these findings. It suffices with 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 lerland did not have the opportunity to challenge the content of the report. However, given the results of the investigation in the AP report, Facebook lerland cannot be content with a bare dispute. 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 lerland has not concretely and substantiatedly contested the concrete results of the AP investigation itself.

13.8. The court therefore concludes 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 AP Report(February 21, 2017), the Foundation did not provide any concrete substantiation of its claim, so that, in view of Facebook Ireland's dispute, the Court cannot determine whether it also processed special personal data in that

period processed special personal data from profile fields for advertising purposes.

(ii) interests based on surfing behavior

13.9. The Foundation argues that the interests that Facebook Ireland derives from the personal data it obtains by tracking the surfing behavior of members of the constituency also fall under special data within the meaning of Article 16 of the Wbp and Article 9 of the AVG. The Foundation points out that, according to the AP's investigation, at least in the period from June 8, 2012 to January 30, 2015 and in the period from January 30, 2015 to April 19, 2018, Facebook Ireland offered advertisers the ability to select by interests divided into main categories and subcategories. It follows from the AP's report that advertisers could select by, for example, "health," "Islam" or "pregnancy" or by sexual preferences.

13.10. Facebook Ireland disputes this, arguing that the data obtained only show possible interest by a user in a particular topic. The interests are at most indirectly related to special personal data and are not processing thereof within the meaning of the law. To illustrate; 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 follow Facebook Ireland in this. Unlike Facebook Ireland argues, when processing special personal data, 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 AVG. What matters is whether the processing of data may reveal special personal data. That not all processing resulting from the tracking of the surfing behavior of users reveals special personal data - as in the example cited above by Facebook Ireland - is correct, but it can be assumed that the tracking of surfing behavior and the categorization of users into interest categories such as "interested in men" or "interested in winning" can lead to processing of special personal data. If this processing takes place for advertising purposes without the consent of the user, it is without legal basis and thus unlawful. Unlike Facebook Ireland argues, the processing of special personal data is 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 l August 2022(OT/Vtec)" which states under point 127:

> Therefore, the above provisions cannot be interpreted to mean that the processing of personal data that may indirectly reveal sensitive information about a natural person is not covered by the enhanced protection regime laid down in those provisions, otherwise the useful effect of
> • this regulation as well as to the protection of fundamental rights and freedoms of natural persons that it seeks to safeguard.

" ECJ EU l August **2022**, C- **184/20**, **ECLI:EU:C:2022:601**

13.12. The above also follows from EDPB Guideline 8/2020 on the Targeting of Social Media Users dated April 13, 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 Privacy Act.

13.14. Facebook Ireland has not (sufficiently) disputed that, as established in the AP Report, it offered main categories and subcategories of areas of interest in the field of, for example, health, religion and political or sexual preference 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. Thereby, it is sufficiently established that Facebook lreland also, by tracking users' surfing behavior and classifying the information thus obtained into interest categories, processed special personal data of the Backers for advertising purposes during the relevant period.

Has Facebook received lerland toestentniing for processing 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 falls within the statutory exception.

13.16. Over the period up to the introduction of the AVG, 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 behavior and use for determining interest categories.

13.17. As for the period after the implementation of the AVG, Facebook lerland has not claimed that it sought consent to derive categories of interest from users' surfing behavior for advertising purposes,so the court concludes that there is no express consent within the meaning of Article 9(2)(a) of the AVG.
Facebook Ireland, when using personal data from profile fields, in the period after the introduction of the AVG alternatively (so the court understands) relies on the "user consent module" or "the AVG 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 February 21, 2017, whether Facebook Ireland continued to process special

processed personal data from profile fields for advertising purposes(see above under 13.8).

13.18. This establishes a violation of Article 16 of the PDPA and Article 9 of the AVG.

Statement for right

13.19. Facebook Ireland argues that the declaratory judgment sought by the Foundation is not admissible because the infringement alleged by the Foundation did not occur to everyone. In doing so, Facebook Ireland also points to the judgment in incident.

13.20. This argument does not succeed. ln paragraph 7.13 of the judgment in incident, it states:

> "7.14 To the extent the Foundation seeks an opinion on one or more specific events, the claims related to them are also bundleable. Here, too, the first question is whether the event in question occurred and whether the conduct of Facebook et al. is (un)lawful. 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 of the constituency can determine whether he has been affected by a possible privacy violation. On the basis of the claims formulated by the Foundation, it will have to be possible to determine that, as the court's assessment may, if necessary, differentiate by, for example, statutory provision, time period and/or event."

13.21. In the judgment in incident, the court ruled that the similarity requirement of Section 3:305a of the Dutch Civil Code (old) has been met. In the court's opinion, the circumstance that not every Facebook user belongs to the Achterban because he did not fill in any profile fields does not stand in the way of granting the declaratory judgment (see also below under 19.6). The argument is rejected.

14. Cookie-trickiztg-, 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 behavior. 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 behavior, to create a

compile profiles that can be used to serve ads specifically targeted to that user.

Review framework

14.3. Parties using third-party cookies must thereby comply with Article l 1.7a (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 aims to protect users against interference in their private lives, regardless of whether such interference relates to personal data. This means that the protection given by the Directive applies to any information stored on terminal equipment regardless of whether it is personal data. In particular, the Directive aims to protect the user from the risk of hidden identifiers and other similar software entering his device, also called 'peripherals', without his knowledge[3] '.

14.4. Article 11.7a paragraph l Tw stipulates that storing or gaining access to information in a user's peripheral equipment is only permitted if l)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 permission. Information and consent must take place in accordance with the Wbp,and(after implementation) the AVG.

14.5. Article 11.7a Tw has been in force since June 5, 2012(and amended in 2013, 2015 and 2018). Before that, Article 4.1 of the Decree on Universal Service and End User Interests(Bude)(which was repealed as of June 5, 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.

Claim Foundation

14.6. In summary, the Foundation seeks a declaratory judgment that Facebook Ireland has not, or at least has insufficiently, complied with the duty to inform and the requirement of consent by not informing, or not clearly or to a sufficient extent and/or not in a timely manner, the Backers about the tracking of surfing behavior 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.

Disputing Facebook

14.7. Facebook Ireland argues that the Foundation'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 meant in Article 1.7a subsection 1 Tw rest on that operator and not on Facebook Ireland, so that already for that reason the claim fails. Facebook Ireland relies in this respect on the judgment of the CJEU of 29July 2019(Fashion ID[40] , mentioned earlier in this judgment, that Facebook Ireland is not obliged to comply with Article l 1.7a (l) Tw if it installs personal data through

[3]'ECJ EU 1 October **2019**, **C-673/17**, ECLI:EU:C:20 **19:801**, Planet49, puni 70
[40] ECJ EU 29July 2019, C-40/17, ECLI: **EU::C:2019:629**, Fashion ID

receives cookies on third-party websites also follows - as far as the period before the introduction of the AVG is concerned - from the explanatory memorandum to the Tw" and communications from the Authority Consumer and Market(ACM). In addition, Facebook lerland requires the website operator to agree to the terms of the Facebook Business Tools (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 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 Article 11.7a(1) Tw did not enter into force until June 5, 2012. There can be no violation before that period at all. The non-binding AP and KU Leuven reports cited by the Foundation cannot serve as evidence. Moreover, the AP report was finalized on February 21, 2017. For the period after that date, the report is irrelevant. Moreover, the Foundation's claim is unsubstantiated as it does not state anything about the period after the entry into force of the AVG.

The court's assessment

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

Applicable law/relevant period

14.11. As explained above under 14.5, the use of cookies before Article 11.7a (1) Tw had to comply with Article 4.1 Bude. Since the Foundation's claim concerns a violation of Article I 1.7a subsection 1 Tw,or at least corresponding provisions, the Court will ignore Facebook et al. lerland's argument that before Article 11.7a subsection 1 Tw came into effect there could be no violation. After all, prior to the introduction of the Tw, Article 4.1 Bude applied, which contains a similar obligation.

14.12. Furthermore, it has not been shown that 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 the Foundation's claims do not relate to the period after implementation of the AVG,that argument is incorrect. In addition, the Court is of the opinion that Facebook Ireland has not disputed sufficiently concretely that it used third-party cookies after the introduction of the AVG. To this end it is relevant that also its own policy in that period refers to the use of third-party cookies.

[4]'Parliamentary Papers Il 2010/11. 32 549, no. 3 and Parliamentary Papers 1 2011/12, 32 549, E

Does l l.7a para l Tw apply to information obtained through cookies via third-party websites?

14.13. Facebook Ireland's most far-reaching argument is that it is not bound by the obligations in Article 11.7a(l) Tw when it receives information about the Achterban 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 AP 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 information and consent obligation under the Tw: the operator of the website the user visits and/or the advertiser (in this case Facebook Ireland) from whom a cookie is placed on the user's device.

14.15. The obligations under Article 11.7a Tw rest with whoever is responsible for placing data in the peripherals and accessing the data stored in the peripherals. Facebook lerland is also responsible in the case of third-party cookies. After all, the cookies are placed on the third-party website at its request. However, the advertiser can agree with the relevant website eKploitant that the obligations under article 11.7a Tw
exercised by the website operator". Facebook lerland's contention that it enters into such agreements with website operators and that website operators must agree to Facebook lerland's BTT and Platform Policy which requires the website operator to provide the necessary information and obtain consent has not been sufficiently refuted by the Foundation. This means that if the website operator provides information about and obtains consent to the placement of cookies, Facebook lerland does not have to do so as well. In view of Facebook Ireland's dispute, it should have been up to the Foundation to make it concrete that Facebook Ireland does not enter into agreements with website operators, or does not supervise 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 Article 11.7a Tw. As the Foundation failed to do so, it cannot be determined that Facebook lerland violated Article l 1.7a Tw (or Article 4.1 Bude) and the claim a.ii.3 will be dismissed.

14.16. The foregoing is without prejudice to the fact that Facebook Ireland must comply with the requirements of the AVG 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 judged 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 judgment also applies insofar as those personal data were obtained and/or processed through cookies.

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

15. Friends of the constituency

15.1. Claim b relates to friends of Backers. The Foundation argues that the conduct alleged against Facebook c.s. 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 Achterban. If a Facebook friend lived abroad and does not himself belong to the Achterban, then the processing of personal data of friends without a processing basis is not only unlawful towards those friends, but is also unlawful towards the Facebook user with whom those friends are friends. Indeed, Facebook c.s. unlawfully appropriated the data that a Facebook user kept on his account about his friends, according to the Foundation.

15.2. 'Facebook et al. argued against this that the basis for this claim is unclear and lacking. The Wbp and AVG give no right to bring claims that concern the processing of personal data of others. The statutory purpose of the Foundation is limited to Facebook users and the claims revolve around alleged actions against the Supporters. As far as Facebook users are concerned, such claims are already covered by claim a.i.1.

15.3. The Court is of the opinion that claim b cannot be **allowed**. Insofar **as** the **allegation** relates to a Facebook friend who belongs to the Supporters, this action is covered by claim a. The Foundation has not sufficiently explained that there is a separate, distinct unlawful action against the Supporters. Insofar as the allegation concerns a Facebook friend who does not belong to the Supporters, contrary to the Foundation's contention, unlawful processing of a friend's personal data cannot be regarded as unlawful conduct ***towards the Supporters***. After all, the processing concerns that friend's personal data. To the extent that the Foundation means to argue that unlawful action was also taken against friends of the Achterban who do not belong to the Achterban, it has no right of action in view of the group of persons for whom the Foundation stands up in this collective action according to its statutory objective.

16. Location details

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

16.2. The court notes that the Foundation has not articulated a separate claim specifically addressing the processing of location data. Apparently, the Foundation'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 are classifiable as data on the processing of which Facebook Ireland has not adequately informed the constituency (see

the judgment on claim a.i.) and/or among the data that Facebook Ireland processed without a valid processing basis (see the judgment on claim a.ii.1), those judgments also apply to the location data. To that extent, therefore, the processing of location data does not require a separate discussion. For the rest, the Foundation has not made it clear in light of which other claim(s) a (separate) judgment on the location data is relevant.

17. Unfair trade practice?

17.1. The Foundation argues that Facebook et al. is also guilty of unfair and/or deceptive trade practices.It argues the following in summary.

- Facebook Inc., Facebook lreland and Facebook Netherlands are traders within the meaning of the Unfair Commercial Practices Directive(hereinafter also referred to as the OHP Directive)[4] '.
- Facebook et al. acted unlawfully as a merchant for the following reasons:
  1. Facebook c.s. processed (confidential) personal data with the purpose of generating turnover and did not inform Facebook users sufficiently clearly and/or timely about that purpose(Section 6:193b (1) and/or Section 6:193d (2) and (3) of the Dutch Civil Code)
  2. Facebook et al. did not inform Facebook users sufficiently clearly and/or timely 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 (Section 6:193b subsection 1 and/or Section 6:193d subsections 2 and 3 of the Dutch Civil Code). The data policy and cookie policy used by Facebook et al. do not show the unprecedented scale of the data processing and only 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(Section 6:193b subsection 1 and/or Section 6:193c subsection 1 under a and d in conjunction with Section 6:1939 under t of the Civil Code). The Facebook service is not free. Personal data may qualify as a prize within the meaning of the OHP Directive.Until August 2019, Facebook's home page stated under "Register": "It's free(and it will stay that way)". As of August 2019, this text was no longer used. Then the Terms of Use stated, "We do not charge for using Facebook(...)."

17.2. Facebook c.s. disagrees with the Foundation's contentions. It points out that claims a.iii.1 and a.iii.2(as also explained above in r.o. 17.1 under 1 and 2) are entirely duplicative with claim a.i. It also argues in this respect that the unfair trade practices claims are based entirely on a violation of the right to data protection while the right to data protection is a *lex specialis*, leaving no room for claims under the OHP Directive 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 Achterban that are relevant to the claims on this basis. Finally, Facebook c.s. disputes the existence of an unfair trade practice on the three alleged grounds. In that

" Directive 2005/29/EC of the European Parliament and of the Council of 1 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

link, among other things, that Facebook Ireland does not sell its users' data to generate revenue, but 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. argues that it has provided sufficient(and not misleading) information and that the free statement is also not misleading and unfair. There is no evidence that any member of the constituency was influenced in his transaction decision.

Assessment Framework

17.3. In assessing whether there is an unfair commercial practice, the following framework is important. The OHP Directive has been implemented in Sections 6:193a et seq. of the Dutch Civil Code.

17.4. A trader acts unlawfully towards a consumer under Section 6:193b (1) of the Civil Code if he engages in a commercial practice that is unfair. A commercial practice is unfair, according to article 6:193b paragraph 2 of the Dutch Civil Code, 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 would not otherwise have made. The consumer must therefore be given the opportunity to reach an informed decision when (at least) entering into the agreement. For a successful reliance on Section 6:193b(2) of the Dutch Civil Code, 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 decision about a contract that he 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 sections 6:193c to 1939 of the BW.

17.5. There is a misleading commercial practice within the meaning of Article 6:193c of the Dutch Civil Code 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 Section 6:1939 under t of the Civil Code, it is misleading under all circumstances to describe a product as free, for nothing or cost-free if the consumer has to pay something other than the unavoidable costs of accepting the offer and collecting the product or having it delivered. For the situation of article 6:1939 under t of the Civil Code, there is no causality requirement.

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 to make an informed decision about a transaction is omitted, as a result of which the average consumer takes or may take a decision about a contract that he

otherwise would not have been taken. 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 late, or fails to reveal the commercial intent, if not already clear from the context.

17.7. Pursuant to Article 6:193a of the Dutch Civil Code, 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, there is a reversed burden of proof(article 6:193j BW).

17.9. The European Commission's Guidelines for the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices of May 25, 2016 - which are intended only as guidance - explain the prohibition on falsely declaring 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:

> If a trader violates the Data Protection Directive or the ePrivacy Directive, this does not in itself always mean that the practice also violates the Unfair Commercial Practices Directive. However, such data protection violations should be taken into account when assessing the overall unfairness of commercial practices under the Unfair Commercial Practices Directive, especially when the trader processes consumer data in violation of data protection rules, i.e.for direct marketing or other commercial purposes such as profiling, personalized pricing or big data applications.
> From the perspective of the Unfair Commercial Practices Directive, the first thing to be assessed is the transparency of the commercial practice.
> According to Articles 6 and 7 of the Unfair Commercial Practices Directive, traders shall not mislead consumers on aspects which may influence their transactional decision. More specifically, Article 7(2) and point 22 of Annex I prevent traders from concealing the commercial intent of the commercial practice.
> The data protection information required from consumers about the processing of personal data, not only limited to information related to commercial communications, can be considered essential (Article 7.5).
> Personal data, consumer preferences and other user-generated content have de facto economic value and **are** sold to third parties.
> Consequently, pursuant to Article 7(2) and point 22 of Annex I of the Unfair Commercial Practices Directive, it may be considered a misleading omission of material information considered if the merchant fails to inform a consumer that the data that is

he must provide to the merchant to access the service will be used for commercial purposes. Depending on the circumstances, this could also be considered a breach of EU data protection obligations to provide the data subject with the required information regarding the purposes of processing personal data.

17.11. On December 29, 2021, the European Commission issued new Guidelines" in connection with the Modernization Directive[4] 'D he Modernization Directive amended the OHP Directive and some other directives in 2022 and thus does not cover the period to be assessed by the court in this case. These Guidelines include the following:

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.

Products presented as "free" are particularly common in the online sector. However, many such services collect personal data from users, such as their identity and e-mail address. It is important to note that the Unfair Commercial Practices Directive applies to all commercial practices involving "free" products and that payment with money is not a condition for its application. Data-driven practices involve an interaction between EU data protection law and the Unfair Commercial Practices Directive. There is a growing awareness of the economic value of information about consumer preferences, personal data and other user-generated content. Marketing such products as "free," without adequately explaining to consumers how their preferences, personal data and user-generated content will be used, potentially constitutes a violation of data protection law and may also be considered a misleading practice.

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 OHP Directive.

Collaboration

17.13. Articles 6:193a et seq. of the Civil Code implement the OHP Directive. 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 OHP Directive states that this Directive does not affect contract law and, in particular, the rules on the validity, formation and legal effect of contracts. 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

[4] 'Guidelines 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** 1, 2021/C 526/01
" **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 201** 1 **/83/EU** of the European **Parliament and of the Council** as regards beiere enforcement and modemization of consumer protection **rules** in the Union(OJ 2019, L 328)

In cases of concurrence, the principle is that both sets of rules may apply in parallel, unless the relevant rule provides otherwise. There is no evidence to suggest that the Union legislator intended for the Privacy Directive and the AVG, 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] The contrary position of Facebook et al, therefore, finds no support in law and is therefore not followed. This means that the court is left to assess the Foundation's unfair trade practice claims.

ÏPf'e *is 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 dispute, it has not been established that Facebook Inc. and Facebook Nederland provided information to the Achterban that is relevant in the context of unfair trade 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 Nederland 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 the Foundation 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 the Foundation in its (insufficiently substantiated) position that Facebook Inc. and Facebook Nederland can also be regarded as traders with respect to the Achterban.

Is there an unfair trade practice?

17.15. The court then turns to the core issue: is there an unfair trade practice by Facebook Ireland?

17.16. The court begins with the third allegation presented as independent by the Foundation: the gratuitous statement. The court must judge this by the regulations in the relevant period.
It was(and is) not permissible to describe a product as free if the consumer does not have to pay a fee to take up the offer and collect or have the product delivered, but does for something else. The issue at the relevant time, as explained in the 2016 Guidelines (and, for that matter, also in the 2021 Guidelines), was that when a consumer claims that something is "free," he or she expects exactly that, i.e. that he or she gets something without having to give money in return. The statement that the Facebook service is free can therefore be understood as indicating that the use of the service does not require monetary consideration.
Since it has been established that there is no need to pay money for the Facebook service, the

[6] CJEU 28 April 2022, C-319/20, ECU:EU:C:2022:322,paragraphs 78 and 66 Meta Platforms lreland Limited v. Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzenirale Bundesverband e.V.

free statement in the relevant period taken by itself is therefore not misleading to that extent. To the extent that a different approach could possibly also be inferred from the 2021 Guidelines, the 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 Section 6:1939(t) of the Dutch Civil Code and the claim directed to it must therefore be dismissed.
That said, that free statement may well play a role in assessing the first allegation, which will be assessed below.

17.17. In view of the testing 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 entering into the agreement to use the Facebook service, Facebook Ireland did not sufficiently inform Achterban about the purpose for which and how personal data were 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 hidden away in veiled language in an underlying layer of information. Failure to inform (clearly enough), at the time of entering into the agreement, of the circumstance that the (personal) data provided by the consumer to Facebook Ireland in order to access the Facebook service will also be used for advertising purposes in the way this is done must be considered a misleading omission of essential information that the average consumer - i.e. the
reasonably informed, circumspect and observant consumer - needsÏ to make a informed decision about participating in the Facebook service as meant in Section 6:193d of the Civil Code.This is essential information in this case, also because the processing of (personal) data of an individual user by Facebook Ireland for advertising purposes was comprehensive and in principle extended to all (personal) data of that user, including special personal data. This omission is sufficiently material to be capable of misleading the average consumer. A further judgment on causation need not be made in these proceedings - a class action. Only in the context of determining liability to an individual consumer does the issue arise as to whether and,if so, to what extent he was actually influenced in his decision by the misleading communication and harmed as a result.

17.18. The Foundation also accuses Facebook Ireland of failing to inform about the scope 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 the Foundation specifically means by "the size and scale" and "the unprecedented scale" in relation to the question of whether there is an unfair trade practice. Thus, the Foundation has also failed to meet its burden of proof on this point.

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 r.o. 17.17.

18. Unjust enrichment?

18.1. The Foundation argues that Facebook et al. enriched themselves unjustifiably by processing the personal data at the expense of Supporters. The processing (and further) use of personal data of Facebook users was unauthorized due to the lack of a basis. The personal data represent an economic value. With the personal data of the Backers, the assets of Facebook et al. increased, thus giving the enrichment. The revenue 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 use of personal data that can be valued in money. The enrichment of Facebook et al. is counterbalanced by the impoverishment of the constituency, because it has lost property that includes the loss of control over personal data and the fact that personal data has become accessible from inaccessible sources.

18.2. Facebook c.s. disputes that there is an impoverishment of the Backers, an enrichment of Facebook c.s., as well as that there is a causal connection between them and that the enrichment is unjustified. It argued, inter alia, that the loss of control over personal data alleged by the Foundation did not result in material damage and that this was not explained by the Foundation 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 6:212(1) of the Dutch Civil Code, he who has been unjustly enriched at the expense of another is obliged, in so far as this is reasonable, to compensate his loss up to the amount of his 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. The Foundation has the burden of establishing, and if necessary proving, the facts and circumstances necessary to conclude that there is unjust enrichment and thus the four aspects of it mentioned above. In paragraph 7.16 of the judgment in incidental proceedings it was ruled that the extent of any enrichment does not yet need to be answered in these collective proceedings, but that it should only be assessed whether there has been unjust enrichment.

18.4. The question of whether there is unjustified enrichment must be answered on the basis of Section 6:212 of the Dutch Civil Code. One of the requirements is that there is impoverishment/damage. This means, contrary to what the Foundation seems to argue, that the possibility of damage is not sufficient for granting the claimed declaratory judgment that Facebook et al. have been unjustly enriched. To that extent, therefore, a different standard applies than for claims seeking declarations of law on the ground that there has been a wrongful 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, the Foundation 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 deprivation of the Facebook user's assets, the Foundation has not made sufficiently clear.

l 8.6. The conclusion is that the claim based on unjust enrichment is not allowable. Whatever further submissions the parties have made on this issue therefore need no further discussion.

19. Concluding considerations and conclusion

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

19.2. In short, Facebook Ireland violated the privacy rights of Dutch Facebook users and engaged in an unfair trade practice.

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

a) violated the basis requirement from Articles 6 and 8 Wbp and Article 5(1)(a) and Article 6(1) AVG, respectively, by processing personal data of Dutch Facebook users for advertising purposes without such processing being able to be based on a legally valid processing basis;
b) violated the ban on processing special data in Article 16 of the PDPA and Article 9.1 of the AVG, respectively, by processing special personal data (e.g. on religion, ethnicity, sexual preference and political affiliation) for advertising purposes;
c) violated the information duties of Article 33 Wbp and Article 13 AVG respectively by:
    - o 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 l 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;
    - O allowing Kogan and GSR to access personal data of Dutch Facebook users,without Facebook having informed Ireland of the purposes of that

data processing and the circumstance that Graph API version 1 also allowed personal data of Facebook users to be shared with Kogan/GSR through Facebook friends;

- not to inform about the integration partnership' program and 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 violations occurred, please refer to the related chapters and recitals.

19.5. Facebook Ireland further argued that the claimed declarations of law are not admissible because the Foundation has not made clear which of its allegations relate to which group of users. According to Facebook Ireland, therefore, no declarations of law can be **made** that relate to the Foundation's entire constituency.

19.6. The court does not follow Facebook lerland in this. The term Achterban refers to the description given to it by the Foundation according to its statutes (see r.o. 5.2). A person belongs to the constituency if he 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 can be specified by various data processing operations and conduct. Partly on the basis of this judgment it can be determined who belongs to the constituency of the Foundation. This means that it can be ruled that unlawful conduct towards the constituency has occurred. There is no further need to differentiate. The exact size of the constituency 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 violation, (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 April 1, 2010 and January 1, 2020 were affected.

19.7. The claims against Facebook Ireland are allowable in the manner set forth below under the decision.

19.8. Insofar as the Foundation intended to argue that Facebook Inc. and Facebook Nederland, even though they do not qualify as (processing) responsible parties or traders (within the meaning of Section 6:193a of the Dutch Civil Code),are nevertheless (co-)liable for the alleged unlawful acts, the Court rejects that position. The Foundation has not substantiated on the basis of which entities other than the (processing) responsible party respectively trader would in this case be (co-)liable for the alleged non-compliance with the obligations resting on Facebook Ireland as (processing) responsible party and as trader.

19.9. Thus, the claims against Facebook Netherlands and Facebook Inc. are dismissed.

20. Litigation Costs

20.1. Facebook Ireland will be ordered to pay the Foundation's legal costs as the predominantly unsuccessful party. The court awards 4 points for the Foundation's procedural acts(with 2 points for the oral hearing in connection with the extensive handling time). Due to the complexity and scope of the case, as well as the interests involved, the court considers the maximum flat rate of £4,247.00 per point appropriate. The costs on the part of the Foundation, taking into account the foregoing, are assessed at:

- subpoena	£	99,01
- court fee	£	656,00
- salary lawyer	£16,988.00	(4 points - rate £4,247.00)
Total	£	17.743,01

20.2. In the dispute between the Foundation on the one hand and Facebook Nederland and Facebook Inc. on the other, the Foundation is to be regarded as the defeated party. Since Facebook et al. put up a joint defense, while that defense was the same for all three defendants with regard to the vast majority of the points in dispute, and to that extent it has not been shown that Facebook Nederland and Facebook Inc. have incurred costs separately, there is no reason to pronounce an order for costs of proceedings at the expense of the Foundation in favor of Facebook Nederland and Facebook Inc.

20.3. The statutory interest claimed on the legal costs to be paid by Facebook Ireland is allowable 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 court

21.1. declares that Facebook Ireland has acted (imputably) unlawfully toward the Foundation's constituency because Facebook Ireland has violated the privacy rights of the constituency in the manner adjudicated in Chapter 11,
main titl' 12 and chapter 13 of this judgment,

21.2. Declares that Facebook Ireland has acted (imputably) unlawfully towards the Foundation's constituency because Facebook Ireland has 'engaged in a commercial practice towards the Foundation's constituency which is unfair within the meaning of article
6:193b (3) under a BW in conjunction with article 6:193d BW as referred to in paragraph 17.17 of this judgment,

21.3. ordersFacebook Ireland to pay the costs of the proceedings, assessed on the part of the Foundation to date at €17,743.01, to be increased by the statutory reiite as referred to in Section 6:119 of the Dutch Civil Code on this amount with effect from the fourteenth day after the dattim of this judgment until the day of payment in full,

21.4. orders Facebook lerland to paythe costs incurred by the Foundation after this judgment, estimated at E 73.00 for attorney's fees, to be increased, subject to the condition that Facebook lerland has not complied with the judgment within fourteen days after notice has been given and service of the judgment has subsequently been served, with an amount of € 90.00 for attorney's fees and the costs of serving the judgment, to be increased with the statutory interest as referred to in Article 6:119 BW with effect from the fourteenth day after service until the day of payment in full,

21.5. declares this judgment to be provisionally enforceable as to costs orders,

21.6. Dismisses the more or otherwise claimed.

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