BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 7 • N° 27 • JUNE 2021

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

FASHION ID AND DECISIVELY INFLUENCING FACEBOOK PLUGINS: A FAIR APPROACH TO SINGLE AND JOINT CONTROLLERSHIP

by Paul De Hert* and Georgios Bouchagiar**

Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV [2019] OJ C319/2

1. Consumer-protection associations can bring legal proceedings for alleged infringements of the right to the protection of personal data.

2. The website operator, who embeds a plugin that can enable the website-visitor's browser to request content from the provider of that plugin and, to that end, to transmit personal data to the provider of the plugin, can be seen as a controller; liability is limited to the particular processing operation(s) that she actually determines.

3. Where the website operator embeds a plugin that can enable the website-visitor's browser to request content from the provider of that plugin and, to that end, to transmit personal data to the provider of the plugin, each actor (the website operator and the provider) must pursue a legitimate interest via the particular processing operations that are codetermined.

4. Where the website operator embeds a plugin that can enable the website-visitor's browser to request content from the provider of that plugin and, to that end, to transmit personal data to the provider of the plugin, it is the website operator who is bound by the duties to obtain consent and to inform the data subject –regarding the processing operation(s) that that website operator actually determines.

Key Words: Fashion ID; Facebook; joint controllership; like button

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.
Please quote the final version Paul De Hert and Georgios Bouchagiar, 'Fashion ID and Decisively Influencing Facebook Plugins: A Fair Approach to Single and Joint Controllership' (June 2021) Brussels Privacy Hub (Working Paper N° 27).

Disclaimer

Introduction

1. *Consumer-protection associations can have a standing under Articles 22-24 of the Directive 95/46/EC and bring legal proceedings for alleged infringements of the right to the protection of personal data.*
2. *The website operator, who embeds a plugin that can enable the website-visitor's browser to request content from the provider of that plugin and, to that end, to transmit personal data to the provider of the plugin, can be seen as a controller within the meaning of the Directive 95/46/EC; liability of this controller is limited to the particular processing operation(s) that she actually determines.*
3. *Where the website operator embeds a plugin that can enable the website-visitor's browser to request content from the provider of that plugin and, to that end, to transmit personal data to the provider of the plugin, each actor (the website operator and the provider) must pursue a legitimate interest, within the meaning of Article 7(f) of the Directive 95/46/EC, via the particular processing operations that are codetermined.*
4. *Where the website operator embeds a plugin that can enable the website-visitor's browser to request content from the provider of that plugin and, to that end, to transmit personal data to the provider of the plugin, it is the website operator who is bound by the (Directive 95/46/EC's) duties to obtain consent and to inform the data subject –regarding the processing operation(s) that that website operator actually determines.*

Articles 2(d), 2(h), 7(a), 7(f) and 10 of the 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 [1995] OJ L281/31.

> *'(…) 77 With regard to the means used for the purposes of the collection and disclosure by transmission of certain personal data of visitors to its website, it is apparent (…) that Fashion ID appears to have embedded on its website the Facebook 'Like' button made available to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook.*
> *78 Moreover, by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin.*
> *79 In these circumstances, and subject to the investigations that it is for the referring court to carry out in this respect, it must be concluded that Facebook Ireland and Fashion ID determine jointly the means at the origin of the operations involving the collection and disclosure by transmission of the personal data of visitors to Fashion ID's website.*
> *80 As to the purposes of those operations involving the processing of personal data, it appears that Fashion ID's embedding of the Facebook 'Like' button on its website allows it to optimise the publicity of its goods by making them more visible on the social network Facebook when a visitor to its website clicks on that button. The reason why Fashion ID seems to have consented, at least implicitly, to the collection and disclosure by transmission of the personal data of visitors to its website by embedding such a plugin on that website is in order to benefit from the commercial advantage consisting in increased publicity for*

its goods; those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID.
81 In such circumstances, it can be concluded (…) that Fashion ID and Facebook Ireland determine jointly the purposes of the operations involving the collection and disclosure by transmission of the personal data at issue in the main proceedings (…)'

1. Facts: Use of Facebook like-buttons raises four key issues

Fashion ID GmbH & Co KG ('Fashion ID'), a German website operator selling goods online, embedded the Facebook like-button (= a third party provider's plugin) within its website.[1] Such an embedding allowed for the processing of personal data: visitors'/users' browsers could request content from Facebook and transmit information of technical nature relating to these users (like their IP address) to Facebook.[2] Fashion ID could exercise control neither over the data transmitted to Facebook nor over the types of uses (such as storing) that Facebook might engage in after transmission.[3]

Verbraucherzentrale NRW, a consumer-protection association ('the association'), brought its case before the Regional Court of Düsseldorf, arguing that Fashion ID transferred personal data without complying with its duties to obtain consent and to inform the data subjects.[4] The Regional Court accepted in part the association's request for an injunction.[5] On appeal before the Higher Regional Court of Düsseldorf (the 'referring court'), Facebook Ireland ('Facebook') intervened in favour of Fashion ID. No less than four key issues were raised by the parties and brought before the Court of Justice of the European Union (the 'CJEU' or the 'Court'):[6]

- First, there were doubts about a consumer-protection association having standing to bring legal proceedings for the alleged infringement.[7]

* Professor, Law Science Technology & Society, Vrije Universiteit Brussel, paul.de.hert@vub.be; Associate Professor, Tilburg Law School, Department of Law, Technology, Markets, and Society, paul.de.hert@tilburguniversity.edu.
** Doctoral Researcher in Criminal Law and Technology, Faculty of Law, Economics and Finance, University of Luxembourg, georgios.bouchagiar@uni.lu; Law, Science, Technology & Society, Free University of Brussels, georgios.bouchagiar@vub.be.
Supported by the Luxembourg National Research Fund (FNR) (PRIDE17/12251371).

1 Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (Second Chamber, 29 July 2019) (*Fashion ID*), para 25.

2 *Fashion ID*, para 26 ('(…) when a website is visited, the browser allows content from different sources to be displayed. Thus, for example, photos, videos, news and the Facebook 'Like' button at issue in the present case can be linked to a website and appear there. If a website operator intends to embed such third-party content, he places a link to the external content on that website. When the browser of a visitor to that website encounters such a link, it requests the content from the third-party provider and adds it to the appearance of the website at the desired place. For this to occur, the browser transmits to the server of the third-party provider the IP address of that visitor's computer, as well as the browser's technical data, so that the server can establish the format in which the content is to be delivered to that address. In addition, the browser transmits information relating to the desired content (…)').

3 *Fashion ID*, para 26 ('(…) (t)he operator of a website embedding third-party content onto that website cannot control what data the browser transmits or what the third-party provider does with those data, in particular whether it decides to save and use them (…)').

4 *Fashion ID*, paras 28-29; 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 [1995] OJ L281/31 (Directive 95/46/EC), arts 7(a), 2(h), 10.

5 *Fashion ID*, para 30.

6 *Fashion ID*, para 31.

7 Fashion ID claimed that only data subjects and supervisory authorities could seek for remedies under Articles 22-24 of the Directive 95/46/EC; albeit, to the referring court, the bringing of proceedings by the association could fall under the scope of 'suitable measures' of Article 24 of the Directive 95/46/EC. See: *Fashion ID*, paras 33, 35-36.

- **Second**, in the absence of control over data transmitted, as well as over uses of such data by Facebook, the qualification of Fashion ID as a controller was, to the referring court, unclear.[8]
- **Third**, there were uncertainties regarding the grounds of the data processing: whose legitimate interests (Fashion ID's or Facebook's) should be taken into consideration for assessing lawfulness of the processing at issue?[9]
- **Fourth**, the referring court was uncertain as to who was bound by the duties to obtain consent and to inform the data subjects[10] (this was strongly related to the question of 'who is the controller?'; processors are not bound by informing-related duties).[11]

2. The CJEU on standing of associations, controllership, legitimate interest and consent

All four issues –standing of associations, controllership, legitimate interest-ground and consent/information-related duties– were addressed by the CJEU. On the first issue of standing, the Court found that enabling a consumer-protection association to bring legal proceedings can guarantee effective, complete and high-level protection of the right to privacy and the protection of personal data and, hence, promote the objectives of the Directive 95/46/EC.[12] Importantly, as the referring court had pointed out, Article 80(2)

8 To the referring court, civil liability could alternatively be established via the treatment of Fashion ID as a 'disrupter' ('*Störer*'). See: *Fashion ID*, paras 34, 37, 38. The concept of 'Störer' has been used in German case law to bring flexibility (and hold a person liable), where the elements of control or knowledge are not clear. In this case, Fashion ID could be considered as 'Störer' regarding data protection-related infringements by Facebook (*Fashion ID*, para 39). For examples of the use of the 'Störer'-notion in German case law, see among others: Martin Senftleben, 'Intermediary Liability and Trade Mark Infringement: Proliferation of Filter Obligations in Civil Law Jurisdictions?' in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).

9 *Fashion ID*, para 40; Directive 95/46/EC, art 7(f).

10 *Fashion ID*, para 41; Directive 95/46/EC, arts 7(a), 2(h), 10.

11 For the duties binding the processor, see European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (Version 1.0, adopted on 2 September 2020, version for public consultation), para 91 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf> accessed 30 September 2020.

12 Rejecting Fashion ID's argument for narrow interpretation of Articles 22-24 of the Directive 95/46/EC, the CJEU noted that general provisions, like those of Articles 22 to 24, are addressed to various situations and, hence, demand flexibility in interpretation; this, contrary to more specific rules (such as those regulating lawfulness of processing) that have in the past been narrowly interpreted (*Fashion ID*, paras 55-57). In this regard, the CJEU highlighted the absence of specific rules concerning the exercise of remedies under the Directive 95/46/EC and the lack of any definition of the 'suitable measures' of Article 24 of the Directive 95/46/EC (*Fashion ID*, paras 58-59). See: *Fashion ID*, paras 50-61 ('(…) (50) (…) it must be noted that one of the underlying objectives of Directive 95/46 is to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data (…) Recital 10 of Directive 95/46 adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection which they afford but must, on the contrary, seek to ensure a high level of protection in the European Union (…) (51) The fact that a Member State provides in its national legislation that it is possible for a consumer-protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data in no way undermines the objectives of that protection and, in fact, contributes to the realisation of those objectives (…) (54) (…) Directive 95/46 does indeed amount to a harmonisation of national legislation on the protection of personal data that is generally complete (…) (55) (…) The Court has thus held that Article 7 of that directive sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful and that Member States cannot add new principles relating to the lawfulness of the processing of personal data to that article or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in that article (…) (56) (…) The Court has, however, also held that Directive 95/46 lays down rules that are relatively general since it has to be applied to a large number of very different situations. Those rules have a degree of flexibility and, in many instances, leave to the Member States the task of deciding the details or choosing between options, meaning that, in many respects, Member States have a margin of discretion in implementing that directive (…) (57) This is also the case for Articles 22 to 24 of Directive 95/46, which (…) are worded in general terms and do not amount to an exhaustive harmonisation of the national provisions stipulating the judicial remedies that can be brought against a person allegedly responsible for an infringement of the laws protecting personal data (…) (58) (…) In particular, although Article 22 of that directive requires Member States to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the personal data processing in question, that directive does not, however, contain any provisions specifically governing the conditions under which that remedy may be exercised (…) (59) (…) In addition, Article 24 of Directive 95/46 provides that Member States are to adopt 'suitable measures' to ensure the full implementation of the provisions of that directive, without defining such measures. It seems that a provision making it possible for a consumer-protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data may constitute a suitable measure, within the meaning of that provision, that contributes (…) to the realisation of the objectives of that directive (…) (60) (…) the fact that a Member State

GDPR[13] expressly allows for the bringing of such proceedings; to the Court, this new provision made the will of the legislator clear.[14]

On controllership –the second issue raised before the CJEU–, the Court emphasised the broadness that the controller-notion has enjoyed and that serves the goal of ensuring effective protection of the data subject.[15] Relying on *Tietosuojavaltuutettu*,[16] the Court stressed that (joint) controllership can be established, insofar as a person influences the processing, for its own goals, and, thus, contributes to the determination of particular processing operations –despite the fact that this person may not have access to the data processed.[17] Furthermore, given the many actors who may be involved in the processing, the various stages of the processing or the multiple processing operations, liability of the joint controller is (to the CJEU) to be assessed on a case-by-case basis.[18] What is decisive for such an assessment is the

can provide for such a possibility in its national legislation does not appear to be such as to undermine the independence with which the supervisory authorities must perform the functions entrusted to them under Article 28 of Directive 95/46, since that possibility affects neither those authorities' freedom to take decisions nor their freedom to act (…) (61) (…) although it is true that Directive 95/46 does not appear among the measures listed in Annex I to Directive 2009/22, the fact nonetheless remains that (…) that directive did not provide for an exhaustive harmonisation in that respect (…)').

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation or GDPR).

14 *Fashion ID*, paras 36, 62 ('(…) (62) (…) the fact that Regulation 2016/679 (…) expressly authorises (…) Member States to allow consumer-protection associations to bring or defend legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data does not mean that Member States could not grant them that right under Directive 95/46, but confirms, rather, that the interpretation of that directive in the present judgment reflects the will of the EU legislature (…)'). The CJEU therefore found that associations, like the one at issue, can have a standing under Articles 22 to 24 of the Directive 95/46/EC and bring legal proceedings for alleged infringements of the right to the protection of personal data: *Fashion ID*, para 63 ('(…) Articles 22 to 24 of Directive 95/46 must be interpreted as not precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data (…)'). Regarding this (applaudable) finding, particularly interesting is how the CJEU deals with standing, its method of interpretation, especially in the absence of relevant provisions in the Directive 95/46/EC.

15 *Fashion ID*, paras 65-66 ('(…) (65) (…) in accordance with the aim pursued by Directive 95/46, namely to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data, Article 2(d) of that directive defines the concept of 'controller' broadly as the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (…) (66) (…) the objective of that provision is to ensure, through a broad definition of the concept of 'controller', effective and complete protection of data subjects (…)').

16 Case C-25/17 *Tietosuojavaltuutettu intervening parties: Jehovan todistajat — uskonnollinen yhdyskunta* (Grand Chamber, 10 July 2018) (*Tietosuojavaltuutettu*). In *Tietosuojavaltuutettu*, a religious community, organising door-to-door preaching, was deemed a controller jointly with its members, even though it had no access to data processed by its members (ie, the door-to-door preachers) and although it did not give any precise (written) instructions to its members. See: *Tietosuojavaltuutettu*, para 75 ('(…) Article 2(d) of Directive 95/46, read in the light of Article 10(1) of the Charter, must be interpreted as meaning that it supports the finding that a religious community is a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, without it being necessary that the community has access to those data, or to establish that that community has given its members written guidelines or instructions in relation to the data processing (…)').

17 *Fashion ID*, paras 67-69 ('(…) (67) the concept of 'controller' relates to the entity which 'alone or jointly with others' determines the purposes and means of the processing of personal data, that concept does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data-protection provisions (…) (68) (…) a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46 (…) (69) (…) the joint responsibility of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned (…)').

18 *Fashion ID*, paras 70-73 ('(…) (70) (…) the existence of joint liability does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, with the result that the level of liability of each of them must be assessed with regard to all the relevant circumstances of the particular case (…) (72) (…) the processing of personal data may consist in one or a number of operations, each of which relates to one of the different stages that the processing of personal data may involve (…) (73) (…) where several operators determine jointly the purposes and means of the processing of personal data, they participate in that processing as controllers (…)').

particular processing operation(s) that is/are *actually*[19] determined by the (joint) controller in question.[20] In the case at hand, the CJEU stressed that Fashion ID embedded the like-button and that this embedding could in itself trigger the possibility of data processing. Facebook could obtain a given visitor's/user's data upon her own action: mere consulting of the website; the user need not create a Facebook account, click the 'Like-button' or know about the data processing.[21] To the Court, by embedding the button that it knew it entailed processing, Fashion ID codetermined, jointly with Facebook, the particular processing operations involving the collection and disclosure by transmission of personal data.[22] That Fashion ID had no access to data transmitted to Facebook was, in light of *Tietosuojavaltuutettu*, irrelevant for the establishment of joint controllership.[23] Thus, to the Court, the website operator (here, Fashion ID), who embeds a plugin (here, the like-button) that can enable the website-visitor's browser to request content from the provider of that plugin (here, Facebook) and, to that end, to transmit personal data to the provider of the plugin, can be seen as a controller; albeit, liability of this controller is, to the CJEU, limited to the particular processing operation(s) that she *actually* determines.[24]

19 It is noted that, for the liability-assessment, as well as for the bearing of the duties to obtain consent and to inform the data subjects, the Court demands 'actual' determination of the means and purpose of the processing. See: *Fashion ID*, paras 85, 99 (referring to liability), 100, 102, 105-106 (on the duties to obtain consent and inform the data subjects).

20 This means that operations following or preceding the codefined operation(s) are irrelevant. See: *Fashion ID*, para 74 ('(…) it appears that a natural or legal person may be a controller (…) jointly with others only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means. By contrast (…) that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means (…)').

21 *Fashion ID*, para 75 ('(…) by embedding on its website the Facebook 'Like' button, Fashion ID appears to have made it possible for Facebook Ireland to obtain personal data of visitors to its website (…) such a possibility is triggered as soon as the visitor consults that website, regardless of whether or not the visitor is a member of the social network Facebook, has clicked on the Facebook 'Like' button or is aware of such an operation (…)'); see also para 27: '(…) With regard, in particular, to the Facebook 'Like' button, it seems to be apparent from the order for reference that, when a visitor consults the website of Fashion ID, that visitor's personal data are transmitted to Facebook Ireland as a result of that website including that button. It seems that that transmission occurs without that visitor being aware of it regardless of whether or not he or she is a member of the social network Facebook or has clicked on the Facebook 'Like' button (…)'.

22 To the Court, Facebook provides and programs the plugin that is then embedded by Fashion ID, which (Fashion ID) moreover exerts influence over the processing; thus, they codetermine the means of the processing with regard to the particular operations involving collection and disclosure by transmission (*Fashion ID*, paras 77-79). Moreover, as the CJEU held, Fashion ID and Facebook codetermine the purposes of the processing operations (again, concerning collection and disclosure by transmission), since the embedding serves the economic interests of both actors (*Fashion ID*, paras 80-81). See: *Fashion ID*, paras 77-81 ('(…) (77) With regard to the means used for the purposes of the collection and disclosure by transmission of certain personal data of visitors to its website, it is apparent (…) that Fashion ID appears to have embedded on its website the Facebook 'Like' button made available to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook (…) (78) (…) by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin (…) (79) (…) it must be concluded that Facebook Ireland and Fashion ID determine jointly the means at the origin of the operations involving the collection and disclosure by transmission of the personal data of visitors to Fashion ID's website (…) (80) (…) As to the purposes of those operations involving the processing of personal data, it appears that Fashion ID's embedding of the Facebook 'Like' button on its website allows it to optimise the publicity of its goods by making them more visible on the social network Facebook when a visitor to its website clicks on that button. The reason why Fashion ID seems to have consented, at least implicitly, to the collection and disclosure by transmission (…) is in order to benefit from the commercial advantage consisting in increased publicity for its goods; those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID (…) (81) (…) it can be concluded (…) that Fashion ID and Facebook Ireland determine jointly the purposes of the operations involving the collection and disclosure by transmission of the personal data at issue (…)').

23 *Fashion ID*, para 82 ('(…) the fact that the operator of a website, such as Fashion ID, does not itself have access to the personal data collected and transmitted to the provider of the social plugin with which it determines jointly the means and purposes of the processing of personal data does not preclude it from being a controller within the meaning of Article 2(d) of Directive 95/46 (…)').

24 *Fashion ID*, para 85 ('(…) the operator of a website, such as Fashion ID, that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46. That liability is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue (…)').

It is noted that the Court, here, sets an important limitation: the one *deciding* upon implementation of the plugin is the controller; but controllership (and liability stemming from it) is limited to the degree of the *actual* decision-making. *Below*, we discuss in more detail this *decisional* controllership (and distinguish it from *abstract* controllership).

As regards the third issue of whose legitimate interests should be taken into account to determine lawfulness of the processing, the Court relied upon *Rīgas satiksme*[25] to find that each joint controller (Fashion ID and Facebook) must pursue such interests via the particular processing operations that are codetermined.[26] This finding complies with the demand that the legitimate interest-ground be applied for *every* decision that the determiner (of the processing-purpose/means) controls. This application is necessary to perform the balancing exercise (legitimate interests of the controller versus interests or fundamental rights/freedoms of the data subject)[27] before finding potential justifiability of *each* and *every* processing operation.[28]

Finally, on the duties to obtain consent and to inform the data subject, the duty-bearer was, to the CJEU, Fashion ID, ie the website operator who *actually* determines the purposes and the means of the processing. On one hand, consent need be obtained prior to processing; and, on the other hand, information must be given immediately when data are processed.[29] Hence, it is the website operator, embedding the plugin that triggers the processing, who must comply with these duties.[30] Here, one would logically

25 Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* (Second Chamber, 4 May 2017) (*Rīgas satiksme*). In this case, the Court specified that Article 7(f) of the Directive 95/46/EC required three cumulative conditions: the pursuit of legitimate interests, the need to process data for the purposes of these interests and the condition that the rights and freedoms of the data subjects do not prevail (*Rīgas satiksme*, para 28).

26 *Fashion ID*, paras 95-97 ('(…) (95) Article 7(f) of that directive thus lays down three cumulative conditions for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence (…) (96) (…) Given that (…) it seems that (…) the operator of a website that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor can be considered to be a controller responsible, jointly with that provider, for operations involving the processing of the personal data of visitors to its website in the form of collection and disclosure by transmission, it is necessary that each of those controllers should pursue a legitimate interest (…) through those processing operations in order for those operations to be justified in respect of each of them (…) (97) (…) in a situation (…) in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, it is necessary that that operator and that provider each pursue a legitimate interest, within the meaning of Article 7(f) of Directive 95/46, through those processing operations in order for those operations to be justified in respect of each of them (…)').

27 On the legitimate interests-ground and the balancing task, see: GDPR, recital 47, art 6(1)(f); European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018 edn, European Union Agency for Fundamental Rights and Council of Europe 2018) 155-158.

28 *Fashion ID*, paras 96-97.

29 *Fashion ID*, paras 102-104 ('(…) (102) consent must be given prior to the collection and disclosure by transmission of the data subject's data. In such circumstances, it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent, since it is the fact that the visitor consults that website that triggers the processing of the personal data (…) it would not be in line with efficient and timely protection of the data subject's rights if the consent were given only to the joint controller that is involved later, namely the provider of that plugin. However, the consent that must be given to the operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means (…) (103) (…) The same applies in regard to the duty to inform under Article 10 of Directive 95/46 (…) (104) (…) it follows from the wording of that provision that the controller or his representative must provide, as a minimum, the information referred to in that provision to the subject whose data are being collected. It thus appears that that information must be given by the controller immediately, that is to say, when the data are collected (…)').

30 *Fashion ID*, para 106 ('(…) in a situation (…) in which the operator of a website embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider personal data of the visitor, the consent referred to in those provisions must be obtained by that operator only with regard to the operation or set of operations involving the processing of personal data in respect of which that operator determines the purposes and means. In addition, Article 10 of that directive must be interpreted as meaning that, in such a situation, the duty to inform laid down in that provision is incumbent also on that operator, but the information that the latter must provide to the data subject need relate only to the operation or set of operations involving the processing of personal data in respect of which that operator actually determines the purposes and means (…)').

ask why there is a need to assess the obtaining of consent, in light of the above considerations on the legitimate interests-ground: if processing is lawfully relying upon the legitimate interests-basis, obtaining consent is not necessary. The answer seems to lie in the fact that, in marketing contexts that are (here) intertwined with social media contexts, the legitimate interests-basis might fail; in case of such a failure, the consent-basis would be the last resort; it would, therefore, be for the benefit of the data subjects that the controller be, in any event, bound by the duty to obtain consent.

3. (Joint) controllership before Fashion ID: from (co)determining to (co)influencing

It would be worthwhile to read and discuss the *Fashion ID*-judgment in the context of recent developments with regard to the concepts of controllership and joint controllership. In general, the controllership-concept was introduced to guarantee accountability: the person, exercising power over the data processing and reaping the benefits from such a processing, is to be held accountable.[31] The idea of 'joint' controllership helps make accountability possible in situations with more than one controller or to impose controllership on actors other than the official controller that play a significant role in determining aspects of a given processing activity. In this regard, the SWIFT-case is of great importance.[32] SWIFT was a processor with regard to a particular processing operation, meaning the transferring of personal data on behalf of the controller and on the basis of their agreement. Yet, SWIFT went beyond the agreement and disclosed personal data (disclosure being another processing operation). Such disclosure and acting beyond the agreement led to an Article 29 Data Protection Working Party-recommendation for treating SWIFT as 'a joint controller' (a term absent in the 1995 Data Protection Directive). Strictly speaking, SWIFT should have been labelled 'controller' for the actions that it allowed without consultation of its clients (the banks). Indeed, there had never been joint determination of the processing operation in question –SWIFT alone had decided to disclose the data. The logic behind the SWIFT-recommendation was, however, to guarantee a high-level protection for the people, whose data had been disclosed. Such protection could be ensured through the subjection of processors (like SWIFT), who were not expressly the ones to be held liable (under existing legal provisions) but who nevertheless held decision-making power over the processing, to the controller-regime;[33] this, directly or through the concept of joint controllership.

31 For an analysis of the element of 'mastery' (as decision-making power over the processing) and the position of the data controller as the key beneficiary of the processing, see: Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia 2019), paras 353ff, 682ff.

32 In this case, European banking institutions employed SWIFT to run data transfer regarding banking transactions. SWIFT disclosed transaction data to the United States Treasure Department, without being explicitly instructed. To the Article 29 Data Protection Working Party, the European banking institutions and SWIFT were joint controllers, responsible to European customers for the disclosure of their data to the United States authorities. Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (01935/06/EN WP128, adopted on 22 November 2006). For a discussion on the SWIFT-case, see also: Valsamis Mitsilegas, 'The Transformation of Privacy in an Era of Pre-Emptive Surveillance' (2015) 20 Tilburg Law Review 35, 43-47; Gloria González Fuster, Paul De Hert and Serge Gutwirth, 'SWIFT and the Vulnerability of Transatlantic Data Transfers' (2008) 22(1-2) International Review of Law, Computers & Technology 191; Yves Poullet and Elise Degrave, 'L' «Affaire SWIFT»' <https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/poullet_degrave_/poullet_degrave_fr.pdf> accessed 30 September 2020.

33 Applicable (then) law, namely Articles 22 to 24 of the Directive 95/46/EC on remedies, liability and sanctions, made no reference to the 'processor'. The aforementioned Opinion of the Article 29 Data Protection Working Party (n 32) was important in an era when the data protection framework did not explicitly provide for the liability-regime that was later set out in more detail by the GDPR. Compare, for example, Articles 22 to 24 of the Directive 95/46/EC to Articles 79 and 82 GDPR (for instance, a data subject may initiate proceedings against any joint controller, who may then bring its own case against the other joint controller(s)).

We will come back to joint controllership and SWIFT later on this article. Here it is enough to underline that the case reveals how easily the lines between controllers and processors may be blurred. Of course, there might be a justified need to hold processors, who may enjoy ever-growing decision-making powers, accountable. This need becomes even more apparent in contemporary processing realities; in the face of today's often long processing-chains, where several actors may be involved in various processing operations, we are looking at making responsible for their actions, for instance, service providers with a view to improving safety of processing activities and making them more accountable. This seems logical.[34] The problem seems to lie in the responsibilisation of non-decision-makers (more on this later).

Prior to 2018, there had been no case law of the CJEU on joint controllership. The notion of joint controllership was, as mentioned, absent in the 1995 Directive and introduced by the 2016 GDPR. More concretely, it was defined in Article 4(7) GDPR, referring to the 'controller' as the 'natural or legal person, public authority, agency or other body which, alone or *jointly* with others, *determines the purposes and means of the processing of personal data*' (own emphasis); and it was explained in recital 79 GDPR:

> '(…) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller (…)'.

Under this legal framework, joint controllership is about the 'determination' of the means and purposes of the processing. It is surprising that, in the CJEU's recent judgments, the Court went beyond 'determination' and used the term 'influence' –a term nowhere in the text of the GDPR. In its 2018 *Schleswig-Holstein*-judgment, the CJEU found that the administrator of a fan page hosted on a social network (in that case, Facebook) can 'influence' the processing and be treated as a controller.[35] The Court looked for contribution (understood as influence over) to the determination of the means and purposes of the processing; this was sufficient for the establishment of controllership.[36] To the CJEU, the administrator of the fan page 'influenced' the means and purposes of the processing together with Facebook:[37]

34 In this regard, see: Jeroen Terstegge, 'Do we need a new GDPR?' (*Netkwesties*, 4 February 2020): '(…) With the introduction of cloud computing, the artificial distinction between data controller and data processor was already questioned. However, the GDPR still makes that distinction for no specific reason. Professional service providers, who now technically qualify as processors, also in other areas than cloud services, are more often than not taking far-reaching decisions with respect to the personal data they process (…)' <https://www.netkwesties.nl/1421/do-we-need-a-new-gdpr.htm?u%E2%80%A69-feb-2020&utm_medium=e-mail&utm_term=do-we-need-a-new-gdpr> accessed 30 September 2020.

35 Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (Grand Chamber, 5 June 2018) (*Schleswig-Holstein*), paras 36, 44 ('(…) (36) (…) the creation of a fan page on Facebook involves the definition of parameters by the administrator, depending inter alia on the target audience and the objectives of managing and promoting its activities, which has an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page. The administrator may, with the help of filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook. Consequently, the administrator of a fan page hosted on Facebook contributes to the processing of the personal data of visitors to its page. (…) (44) (…) Article 2(d) of Directive 95/46 must be interpreted as meaning that the concept of 'controller' within the meaning of that provision encompasses the administrator of a fan page hosted on a social network (…)').

36 *Schleswig-Holstein*, para 36.

37 It is noted that, from paragraph 36 (*Schleswig-Holstein*, para 36), it can be obvious that there is influence on the means of the processing; albeit, it seems unclear whether there is influence on the purposes of the processing.

> '(…) the creation of a fan page on Facebook involves the definition of parameters by the administrator, depending inter alia on the target audience and the objectives of managing and promoting its activities, which has an influence on the processing of personal data for the purpose of producing statistics based on visits to the fan page. The administrator may, with the help of filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook. Consequently, the administrator of a fan page hosted on Facebook contributes to the processing of the personal data of visitors to its page (…)'.[38]

We recall that the legal definition of joint controllership in 4(7) GDPR is about *co-determining the purposes and means of the processing of personal data*. Neither this provision, nor recital 79 refers to 'influencing'. The conditions for applying this GDPR definition seem to be fulfilled in *Schleswig-Holstein* since the CJEU finds that the setting up of a fan *page can entail determination of the purposes and the means of the processing*. So why then does the Court in this judgment comes up with 'influence'? The term is clearly vaguer; 'influencing' appears to be broader than 'determining'.

One month after *Schleswig-Holstein*, came *Tietosuojavaltuutettu*. Again, the CJEU emphasises 'influence' over 'determination'. This time, the Court's agenda is clear: the use of 'influence' clearly allows the Court in this case to reach a broader application of the concept of joint controllership. More concretely, the CJEU regarded a religious community that organised door-to-door preaching (eg, by deciding upon the areas of preaching or supervising its members' conduct) as influencing the data processing and, on this basis, as participating in the determination of this processing.[39] To the Court, the community was a joint controller, despite the fact that it neither accessed data processed by its members nor gave particular (written) instructions to the members.[40] Borrowing *Schleswig-Holstein*'s 'influence', the CJEU found participation in the determination of the processing; this established controllership.[41]

4. (Joint) controllership in Fashion ID: from '(co)influencing' to 'decisive (co)influencing'

Against the background of these 2018 judgments, *Fashion ID*, -one year later-, offers particularly useful insights into single, as well as joint controllership in the context of Facebook technologies.

On single controllership, the Court does two things. First, it demonstrates verbal and conceptual loyalty to the term 'influence' to understand Article 4(7) GDPR in an effort to be coherent with its previous judgments. Second, beyond these loyalty statements, it applies and respects in practice the text of Article 4(7) GDPR and its term 'determination' by looking in the fact of the case at hand at decisions made by respective actors involved. More precisely, the CJEU focuses on the intentions of Fashion ID as a website operator and its decisions with regard to the incorporation of the Facebook plugin upon the purposes

38 *Schleswig-Holstein*, para 36 (own emphasis).
39 *Tietosuojavaltuutettu*, para 68 ('(…) a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46 (…)').
40 *Tietosuojavaltuutettu*, para 75 ('(…) a religious community is a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, without it being necessary that the community has access to those data, or to establish that that community has given its members written guidelines or instructions in relation to the data processing (…)').
41 *Tietosuojavaltuutettu*, para 68.

and means of the processing activity made possible by the plugin.[42] Apparently, there is no use to rely on 'influencing' since the operator is 'determining' the purpose and means of the plugin-processing activity. Hence, Article 4(7) GDPR applies.

However the referring German court had pointed out that Fashion ID did *not* control everything, only certain aspects of the processing.[43] Its question to the CJEU was 'whether a website operator, like the one at issue, can be seen as the controller, even though he exercises *no influence* over the processing'.[44] To deny the factual assessment implicit in this question the CJEU retorts in paragraphs 77 to 81 of the judgment by emphasising Fashion ID's important role in the decision making process around the Facebook plugin and speaks in this regard of the 'decisive influence' by Fashion ID,[45] a word game that has, in our view, only purpose, namely to convince us about the unquestionable applicability of Article 4(7) GDPR to both Facebook *and* Fashion ID:

> Fashion ID 'exerts a decisive influence over the collection and transmission of the personal data',[46] and can therefore be seen as a (joint) controller[47] –despite lack of access to data transmitted.[48] So Fashion ID has to render account for its decision to use the Facebook plugin, -as an operator it *influences* the processing,[49] and can be seen as a controller (and a joint controller together with Facebook)-, but its liability is nevertheless limited to the processing operations she *actually* determines.[50]

What can be learnt from these important paragraphs 77 to 81 of *Fashion ID*- (referring to decisions made by the relevant actors upon the purposes and means of the processing) is that the person embedding the plugin influences the processing. Still, it is reminded that the plugin is Facebook's product;[51] this can mean a genuine 'contract' between the embedder (Fashion ID) and the owner (Facebook), both benefiting from the like-button.

42 *Fashion ID*, paras 77-81 (cited in the beginning of this paper).

43 In the initial technical analysis of how the plugin works, it is clearly stated that Fashion ID has no control over data transmitted to Facebook (as well as over subsequent uses). See: *Fashion ID*, para 26 ('(…) (t)he operator of a website embedding third-party content onto that website cannot control what data the browser transmits or what the third-party provider does with those data, in particular whether it decides to save and use them (…)').

44 The referring court's wording: 'if that person is himself unable to influence this data-processing operation' (*Fashion ID*, para 42); the CJEU's rephrasing: 'despite that operator being unable to influence the processing of the data transmitted' (*Fashion ID*, para 64).

45 *Fashion ID*, para 78 ('(…) by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data (…)')

46 *Fashion ID*, para 78. It is added that the Court finds that 'Fashion ID exerts a decisive influence over the *collection and transmission* of the personal data' (*Fashion ID*, para 78; emphasis ours), but it concludes that there is controllership 'in respect of the operations involving the collection *and disclosure* by transmission of the personal data' (*Fashion ID*, para 84; emphasis ours). Whether Fashion ID influences 'disclosure' is not explicitly addressed.

47 *Fashion ID*, para 84: 'Fashion ID can be considered to be a controller (…) jointly with Facebook'

48 *Fashion ID*, para 82. Irrelevance of lack of access for the establishment of controllership could be related to the fact that access is not expressly treated as a processing operation. See indicative list of processing operations of Article 4(2) GDPR. Still, the list is not exhaustive; it could be argued that the definition of the processing as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means' could include accessing data. For a discussion on access as processing, see: Arye Schreiber, 'Mere Access to Personal Data: Is It Processing?' (2020) International Data Privacy Law, ipaa005 <https://doi.org/10.1093/idpl/ipaa005> accessed 30 September 2020.

49 *Fashion ID*, para 78 ('(…) by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data (…)')

50 *Fashion ID*, para 85. To the extent that 'influence' is involved in, related to or synonymous with 'control', it can fairly be argued that the Court here addresses issues relating to the very facts of the case, meaning the fact that the website operator in question had neither control nor influence over the data and their processing (*Fashion ID*, paras 26, 34, 37, 42).

51 Facebook for Developers, 'Like Button for the Web' (Facebook for Developers) <https://developers.facebook.com/docs/plugins/like-button/> accessed 30 September 2020.

While having gone loose in *Tietosuojavaltuutettu* and (to a certain extent in) *Schleswig-Holstein*, the CJEU now applies 'decisive influence'. It seems to return to, engage in the classical scheme of taking decisions (implying 'determination', rather than 'influence'). It can then be argued that *Fashion ID* is not revolutionary; it creates some coherency with the preceding case law (by toying with the concept of 'influencing') and, more importantly, it is in line with the concept of 'determination' as used in the legal definition of joint-controllership in 4(7) GDPR. The description in the judgment of the plugin-advantages for both website operators and Facebook and the contractual nature of this formula already strongly suggests the applicability of shared controllership. In our view, there is no need to speak about 'influencing' or 'decisively influencing': the nature of contractual relationship with regard to Facebook's plugin ('if you use it, we both win') already implies co-determination.

5. Making the innocent responsible by calling them joint controllers?

Fashion ID and Facebook are *jointly* controlling two particular processing activities with regard to the plugin in view of the Court. That is handy for the data subject that can now litigate against both corporations. But is it fair? Are we now calling everybody a controller of everything through generous use of the notion of *joint* controllership to make sure that whatever actors involved in the processing chain can be held accountable for the full harm to the data subject?

Legal certainty warrants against over-extension of the concepts. If any influencer, that is any person with the slightest contribution to the codetermination of the processing, were to be called a (joint) controller, there would be the risk of establishing a multilevel responsibility scheme; a jigsaw puzzle of tiny responsibilities complicating and prejudicing the effective establishment of accountability, as well as the efficiency of data protection laws.[52] Qualifying these 'marginal' influencers as *joint* controllers would make non-decision-makers joint controllers; and that this would strike at the heart the idea of accountability and individual responsibility.

In *Fashion ID* there is even more at stake and to see that one has to look also at the position of Facebook in this legal jigsaw. The CJEU only treats Fashion ID, -influencer contributing to the determination of the processing-, as a joint controller regarding two operations that it *actually* determines, namely collection and disclosure by transmission. The CJEU furthermore limits Fashion ID's liability to these two operations and clarifies that Fashion ID is the duty-bearer, concerning obtaining consent and informing the data subjects, because it *actually* determines these two operations. This line of reasoning implies that there can be another joint controller, who does *not actually* determine these particular processing operations, escapes liability (because liability rests with the person who *actually* determines these processing operations and

52 It is worth quoting the question posed and the response provided by Advocate General Bobek in his *Fashion ID*-opinion: '(…) Will effective protection be enhanced if everyone is made responsible for ensuring it? (…) Making everyone responsible means that no-one will in fact be responsible. Or rather, the one party that should have been held responsible for a certain course of action, the one actually exercising control, is likely to hide behind all those others nominally 'co-responsible', with effective protection likely to be significantly diluted.' (…)'. *Fashion ID*, Opinion of AG Bobek, paras 71, 92.

is limited to these operations) and bears no duties to obtain consent and inform the data subjects (again, because these duties bind the *actual* determiner).[53] This other is Facebook.

The qualification of Facebook as a joint controller can have further implications. Such implications have already been addressed by literature. As Alsenoy points out in his excellent work on controllers and processors,[54] the qualification of entities as controllers/processors may (among others) extend (alarmingly) the scope of application of the GDPR,[55] as well as introduce new formalities, such as compliance with the duty to inform the data subjects[56] or arrangements with relevant providers (joint controllers).[57] One could further add uncertainties relating to the determination of the main establishment (and, therefore, of the

53 It is reminded that the *Fashion ID*-judgment dealt with two actors. On one hand, there is Facebook, ie the person who provides and programs the technology (the like-button) and pursues for-profit goals. On the other hand, there is Fashion ID, ie the person who implements this technology (the like-button) and pursues similar goals. Fashion ID was considered as codetermining the 'means' of the processing (concerning the particular operations of collection and disclosure by transmission), because it embedded the technology that was provided for and programmed by Facebook. Moreover, Fashion ID was considered as codetermining the 'purposes' of the processing (regarding the above-mentioned operations of collection and disclosure by transmission), because the embedding served the for-profit goals pursued by the operator (*Fashion ID*, paras 77-81). Speaking of joint control, the Court finds that Facebook, from its part, contributes to the determination of the means (because it offers and programs the plugin) and the purposes (because it pursues similar economic goals) of the processing with regard to the particular operations of collection and disclosure by transmission (*Fashion ID*, paras 79, 81).

54 Brendan Van Alsenoy, *Data Protection Law in the EU* (n 31).

55 Brendan Van Alsenoy, *Data Protection Law in the EU* (n 31), paras 261-265. In the *Fashion ID*-context, it could be argued that all cases involving the popular like-button could render the European Union's data protection laws applicable. This could be the case, even if the relevant website operators ran their businesses elsewhere and even if the processing (for example, initial collection by the operators) occurred in non-EU territory, provided that Facebook engaged in real and effective exercise of activities through stable arrangements in the European Union (GDPR, recital 22, art 3(1)). This criterion can be met rather too easily; for instance, mere presence of a single representative may suffice (see: Case C–230/14 *Weltimmo sro v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] OJ C381/6, para 41). Importantly, even if Facebook were not considered as having an establishment in the Union (and even if it had no intention to target visitors of the relevant website with its services), European law could apply in respect of the monitoring of users' behaviour that would take place within the Union, to the extent that the clicking of the like-button would allow for, exempli gratia, tracking of the website's visitors who are in the Union (GDPR, recital 24, art 3(2)(b)). For a discussion on and the evaluation of the monitoring-criterion, see: EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)' (Version 2.1, 12 November 2019), 19-20; Brendan Van Alsenoy, 'Reconciling the (Extra) territorial Reach of the GDPR with Public International Law' in Gert Vermeulen and Eva Lievens (eds), *Data Protection and Privacy Under Pressure: Transatlantic Tensions, EU Surveillance, and Big Data* (Maklu 2017) 77, 87-90; Merlin Gömann, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) 54 Common Market Law Review 567, 586-588. It is added that the above considerations in relation to the territorial scope might also become relevant for the material scope of the GDPR; due diligence need be demonstrated, when reflecting on expansions of basic terms of the above Regulation. See, for example, the recent judgment in: Case C-272/19 *VQ v Land Hessen* [2020] (Judgment of the court (third chamber), 9 July 2020; not yet published in the OJ) (*VQ*). In this case, the CJEU found that the Petitions Committee of the Parliament of Land Hessen is a controller, because it satisfies the controller's functional requirements (determining the purposes and the means of the processing) and the relevant parliamentary activities are not expressly excluded from the scope of the GDPR. More concretely, to the Court, the notion of the controller may enjoy broad interpretation and can encompass any public body that determines the purposes and the means of the processing (*VQ*, paras 64-65); the processing conducted by the Petitions Committee was not to be considered as processing 'in the course of an activity which falls outside the scope of Union law', according to the exception of Article 2(2)(a) GDPR, which must, moreover, be interpreted restrictively (*VQ*, paras 66-71); and there was no concrete exception for the parliamentary activities at issue (*VQ*, para 72).

56 Brendan Van Alsenoy, *Data Protection Law in the EU* (n 31), paras 266-268. It is reminded that, in *Fashion ID*, the CJEU holds that the duty to inform the data subjects regarding the operations at issue binds (solely) Fashion ID. Fashion ID may now have a duty to inform the data subjects also about the identity of the new controller, meaning Facebook (GDPR, arts 13(1)(a), 14(1)(a)). It could, thus, be argued that the *Fashion ID*-Court introduces formalities that bind all website operators embedding the like-button, as well as similar plugins that are provided for by third parties and function in a similar way (for example, allow for collection and disclosure of data by transmission).

57 Brendan Van Alsenoy, *Data Protection Law in the EU* (n 31), para 270. It could be claimed that, after *Fashion ID*, website operators embedding like-buttons and similar plugins need proceed to arrangements with third party providers (like Facebook) and comply with formalities demanded by the establishment of joint controllership (GDPR, art 26).

lead supervisory in case of cross-border processing)[58] or the increase of litigation-workload.[59] Note that these observations bring us far beyond the question of responsibility,[60] that is at the heart of *Fashion ID*.

6. Comparing Fashion ID with Terstegge's single controllership concept

In the previous section we saw that *Fashion ID* 1) is good for data subjects that can sue in court both Facebook and the website operator using the Facebook plugin; 2) is fair for operators such as Fashion ID that use Facebook-plugins since their liability is limited to the operations they *actually* determine (namely, collection and disclosure by transmission); and 3) is bad and good for Facebook who is regarded as a joint controller with regard to the plugin, but escapes liability (because liability rests with the person who *actually* determines these processing operations and is limited to these operations) and bears no duties to obtain consent and inform the data subject.

Earlier this year, Terstegge highlighted several failures of the GDPR to address contemporary processing realities.[61] The author criticised the distinction between controllers and processors,[62] as well as the concept of joint controllership.[63]

58 Indeed, the consideration of Facebook as a controller in such like-button-scenarios, in an era when it is hard to find a commercial website without this popular plugin, makes the detection of the controller's lead supervisory authority peculiarly hard. Does the exercise of controllership by Facebook imply de facto decision-making powers? Or should we accept that, despite controllership, Facebook has no decision-making authority? (it is noted that the interpretation of controllership in such a way as to include non-decision-makers has no basis in contemporary EU data protection law that requires 'determination' of the purposes and means of the processing; what matters for the qualification of a person as a controller is the factual and/or legal impact on the processing resulting from the real exercise of decision-making power over this processing; for an analysis of the 'determination' of the processing as real exercise of decision-making power, see: Brendan Van Alsenoy, *Data Protection Law in the EU* (n 31), paras 76, 105ff, with further references). These questions on decision-making are important for determining the main establishment and, hence, the lead supervisory authority in case of cross-border processing (GDPR, arts 4(16), 56(1)). It is expressly added that such uncertainties are not resolved by the GDPR's joint controllership-scheme, which does not explicitly address designation of the lead authority, where many controllers determine the processing (Article 29 Data Protection Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority' (adopted 13 December 2016, 16/EN WP 244 rev.01), paras 1.2-2.1, 2.1.3).

59 If Facebook can be seen as a joint controller, data subjects can bring legal proceedings against it regarding infringements resulting from initial collection, even though Facebook never *actually* determined such collection; and Facebook may then bring its own case against website operators (GDPR, arts 79 and 82). This may increase litigation-workload that could be avoided, were controllership limited to one accountable actor.

60 Brendan Van Alsenoy, *Data Protection Law in the EU* (n 31), para 261 (referring to the scope of application, transparency of the data processing operations, rights of the data subjects, balance of interests, as well as legal binding between controllers and processors: '(…) (t)he qualification of an actor as either a controller or processor has implications beyond the allocation of responsibility and liability (…)').

61 Jeroen Terstegge, 'Do we need a new GDPR?' (n 34).

62 Jeroen Terstegge, 'Do we need a new GDPR?' (n 34) ('(…) With the introduction of cloud computing, the artificial distinction between data controller and data processor was already questioned. However, the GDPR still makes that distinction for no specific reason. Professional service providers, who now technically qualify as processors, also in other areas than cloud services, are more often than not taking far-reaching decisions with respect to the personal data they process. Not only how the data is processed, but also where and by whom the data is processed. And they increasingly also advise - or as part of their services even determine - which personal data are processed (…) Ergo, service providers often have a huge impact on the processing and protection of the personal data. Business models have become very complex, and often involve a number of parties that operate in data processing chains. It is only logical to make a service provider more accountable for the way he processes the data than only the 10 GDPR obligations that now apply to data processors (…) Since the introduction of the GDPR, especially its rules regarding engaging data processors (article 28) and its focus on data breaches (article 33/34), data protection has become a major obstacle for service providers to do business. The GDPR does not only create a lot of costs when doing business with a service provider, it even has - often unnecessary - acted as a deal breaker. In negotiations, pushing the risk of non-compliance with the GDPR to the other party is often more important than the actual data protection provisions. And because of the GDPR's high fines, clients don't trust the data protection practices of service providers, leading to endless negotiations and overly burdensome contracts (…)').

63 Jeroen Terstegge, 'Do we need a new GDPR?' (n 34).

Advocating that things can be better off with a single controller, the author challenges the GDPR's twofold approach –that of increasing the duties of processors, which might identify with those of controllers, and that of recognising the presence of joint controllers in the line of SWIFT:

> 'In practice, there is no such thing as joint controllers. There are only controllers controlling their own part of the GDPR's obligations in a chain of data processing operations. Which controller controls which part, is determined by the nature of their relationship, their tasks in the data processing chain and the circumstances of the case. If a website decides to use the Facebook Pixel, it is utterly nonsense to treat Facebook as a joint controller for the collection of the data resulting from it. There is only a website owner responsible for the decision to allow Facebook to collect data, and there is Facebook responsible for the fair, proportionate and secure processing of the data resulting from such decision (…)
> To accommodate a situation where there are only controllers, the GDPR should make clear that the principle of accountability does not exceed a contracting party's administrative sphere of influence. If the client, under the circumstances of the case, did a proper due diligence on the service provider, he should never be liable for the mistakes of the service provider, nor should he be risking a fine for violating the principle of accountability. If every party is only responsible and liable for its own actions and its own compliance, that would make doing business so much easier.[64]

The CJEU in *Fashion ID* operates closely to Terstegge's scenario: the website operator (Fashion ID), who embeds the plugin (the like-button), is the controller (*note*: to Terstegge, the decision to use the plugin results in control, not joint control); and its liability is, to the CJEU, limited to the particular processing operations that it actually determines.[65] Yet, the *Fashion ID*-judgment (relying upon and bound by the European Union's law) is at the same time (and must, of course, be) close to the conceptual choices made in the GDPR: the website operator is a controller *jointly* with Facebook.

In our view, the CJEU appears to be careful and convincing. Its approach is fair: the Court takes into due consideration the actual decision-making. Facebook offers a plugin and Fashion ID decides to make us of it.

Step 1 (there is a decision by Fashion ID): It is Fashion ID the one who decides to embed the like button (*note*: the embedding triggers the processing); therefore, it must be the controller. This is in line with Terstegge's call for (single) controllership, as well as Alsenoy's analysis of the 'determination' (of the processing's means and purpose) as real exercise of decision-making power.[66] This can be seen as real, contextual and specific controllership; it is *decisional controllership*, clearly distinguishable from *abstract controllership* (a type of controllership that could rely upon, for example, formalities, such as a contract-based attribution of responsibility).

64 Jeroen Terstegge, 'Do we need a new GDPR?' (n 34).
65 *Fashion ID*, para 85.
66 Brendan Van Alsenoy, *Data Protection Law in the EU* (n 31), paras 76, 105ff.

Step 2 (there is a kind of contractual arrangement around the plugins): The Court does not stop there; it resorts to joint controllership. Resorting to joint control, where it is clear that a single entity decides upon the processing, would be unnecessary and, probably, troublesome or even disappointing;[67] but resorting to such a (joint) control, because there is actually another actor involved in the means/purpose-determination, can be a 'necessary evil', satisfactorily compensated by the limitation (by the CJEU) of Fashion ID's liability to the processing operations that it actually determines.

Fashion ID 'exerts a decisive influence over the collection and transmission of the personal data', and can therefore be seen as a (joint) controller –despite lack of access to data transmitted. So Fashion ID has to render account for its decision to use the Facebook plugin, -as an operator it influences the processing, and can be seen as a controller (and a joint controller together with Facebook)-, but its liability is nevertheless limited to the processing operations she actually determines.

Therefore, despite the Court's former 'punky' reasoning (especially, in *Schleswig-Holstein* where 'influence' was introduced) and even though 'joint controllership' has been recognised in cases where there is only 'controllership' (in the SWIFT case, SWIFT had made decisions alone, behind the back of banking institutions), *Fashion ID* uses 'joint control' with care; legitimately and reasonably, in a way that makes sense.

7. Comparing Fashion ID with the EDPB 2020 Guidelines on controller and processor

Before concluding, it need be added that the European Data Protection Board seems to have relied upon the above-analysed background on controllership (that is, the Article 29 Data Protection Working Party's considerations on the SWIFT-case, as well as the CJEU's *Schleswig-Holstein-*, *Tietosuojavaltuutettu-* and *Fashion ID*-judgments), in its effort to provide for useful guidance regarding the ('functional' and 'autonomous')[68] concepts of the controller and the processor.[69] The guidance of the Board offers a considerable degree of certainty on the following issues:

- First, the Board confirms the approach adopted by the Article 29 Data Protection Working Party in the SWIFT-case: the processor, a separate actor who acts on behalf of the controller and under her instructions, becomes the controller, where he goes beyond these instructions.[70]

67 In this regard, it is reminded that, in the SWIFT-case, SWIFT alone had decided to disclose the data; yet, to the Article 29 Data Protection Working Party, control had been exercised jointly with the European banking institutions. Of course, as explained above, the intention of the Article 29 Data Protection Working Party was to enhance protection of the data subjects.

68 The 'functional'-element refers to the linkages that need be drawn between the attribution of responsibility and the actual role of the relevant entity (who can be either a controller or a processor). The 'autonomous'-feature is connected with the application of the European Union's law when interpreting these concepts. European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) paras 12-13.

69 Even though the above-analysed cases were concerned with the interpretation of the provisions of the Directive 95/46/EC, the coming into force of the GDPR did not affect the controller/processor-regime. In this regard, see: European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) paras 11 (referring to the concept of the controller and the processor), 44 (referring to joint controllership and citing the above-discussed case law of the CJEU in footnote 14).

70 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) pages 3-4.

- **Second**, the Board clarifies that, regarding controllership, the 'determination' of the processing's means and purposes refers to the *actual influence* exerted over the processing.[71] This influence may be established by the law or the facts of a given case.[72] On facts, there must be 'determinative influence' relating to particular activities.[73] In any event, the person actually exerting influence over the purposes and the means of the processing cannot mask her role as a controller via, for instance, contractual arrangements.[74] Therefore, the 'determination' of the purposes and the means of the processing refers to the 'determinative influence' that a person exerts over these purposes and means.[75] This is in line with the above-analysed case law of the CJEU (namely, *Schleswig-Holstein*, *Tietosuojavaltuutettu* and *Fashion ID*). And this can support our view on 'decisional' controllership (as opposed to abstract control, relying upon, for example, contract-based responsibility).
- **Third**, to the Board, the establishment of joint controllership depends upon whether two or more actors are involved in the above 'determination' of the purposes and the means of the processing.[76] This is, again, a factual assessment of the actual influence.[77] Importantly, the participation of a joint controller in the determination of the processing is the key factor to be taken into account when examining the, potentially differing, degrees of responsibility.[78] These considerations of the Board can be linked to the *Fashion ID*'s finding on the limitation of liability to the concrete processing operation(s) that the joint controller *actually* determines.[79]

8. 'Decisive influencing' as a wise limit to the 'influence'-idea (theoretical conclusion)

In this note, we discussed the four key issues addressed by Fashion ID: 1) the standing of consumer-protection associations to bring legal proceedings with regard to a personal data breach; 2) the qualification of a website operator, embedder of a social plugin, as a controller; 3) the legitimate interests-ground as a lawful basis for the processing triggered by the implementation of the like-button; and 4) the duties to obtain consent and inform the data subjects.

71 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) para 19.
72 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) para 20.
73 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) paras 23-24.
74 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) paras 26, 28.
75 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) para 42. It is added that the Board distinguishes between essential and non-essential means. The former can refer to the nature of the information processed, as well as the duration of the relevant operation and the actors involved (what categories of personal data are processed? how long does the processing last? who are the recipients involved? who are the data subjects affected?). The latter can refer to more practical issues, such as the selection of soft/hardware or technicalities referring to, for instance, security measures. To the Board, the essential means should be defined by the controller; whereas the non-essential means may be left at the discretion of the processor. European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) paras 38, 42.
76 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) para 48.
77 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) para 49. The Board differentiates between common and converging decisions. On one hand, common decision-making entails decisions taken together by the controllers, who share same intention. On the other hand, converging decisions 'complement' each other and are 'necessary' for the relevant processing operation to occur; they have a 'tangible impact' on the determination of the processing; they are then 'inextricably linked'; the processing would not take place, were one of the converging decisions absent. European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) paras 52-53.
78 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) para 56.
79 Interestingly, the Board analyses in more detail the codetermination of the purposes, on the one hand, and that of the means, on the other hand. Concerning the purposes, there need be a common benefit resulting from the processing (this was indeed the case with *Fashion ID*). On the means, the joint controller must 'exert influence' over the means; and this exertion can occur at different phases or degrees (as was the case with *Fashion ID*). Moreover, the Board clarifies that the above exertion can encompass the use of a technology (that another person produced) by the (joint) controller (this was the case with the like-button that was produced by Facebook and used by Fashion ID). European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) paras 58, 61, 65.

Fashion ID made clear that: 1) such associations do have a standing; 2) the website operator, embedding a social plugin that enables the website-visitor's browser to request content from the provider of that plugin and, to that end, to transmit personal data to the provider of the plugin, can be seen as a controller (liability of this controller is, nevertheless, limited to the particular processing operations that she actually determines); 3) for the processing to be lawful, each joint controller need pursue legitimate interests through the (co-determined) processing operations; and 4) the website operator that actually determines the purposes and the means of the processing is the duty-bearer regarding obtaining consent and informing the data subject.

Moreover, we analysed prior case law, as well as soft law, on joint controllership. First, we found that Schleswig-Holstein introduced the 'influence'-idea that, to the Court, entails (and, in our view, can be broader than the) determination of the purposes and the means of the processing. Second, we stressed the way Tietosuojavaltuutettu, borrowing the 'influence'-concept, allowed for an admittedly wider application of the notion of joint controllership.

We, then, discussed Fashion ID's 'decisive influencing' as a term coherent with both case law and the GDPR's concept of 'determination', albeit, perhaps, redundant, in light of the contractual relationship between the embedder and the owner of the plugin that implies co-determination. Thereafter, we focused on Fashion ID's added value. This case: allows data subjects to bring proceedings against both the social plugin-owner and -embedder; limits liability of the plugin-embedders (website operators) to the processing activities they actually determine; and allows plugin-owners to escape liability with regard to the concrete processing operations (that they do not actually determine), as well as to be absolved from the duties to obtain consent and inform the data subject. Here, it is important to highlight the two-step process for establishing liability. First, Fashion ID's findings on joint controllership enable data subjects to bring their case against all relevant actors involved; but this, as analysed above, might create 'fictitious' liability. Still, the CJEU has with precision identified the scope of Fashion ID's liability with regard to the plugins and every possible 'fictitiousness' liability can be cured by a final step: a joint controller, who has fully compensated the data subject, can (under Article 82(4-5) GDPR)[80] turn to another joint controller and claim from her the amount that corresponds to the her responsibility (regarding the particular processing operations).

This led us to the conclusion that the use of 'joint control' by Fashion ID was fair. Indeed, it seems that the Court makes its best efforts to reach a fair outcome; though bound by the European Union data protection laws, the CJEU avoids extremity and tries to help the consumer organisation. Respecting Ockham's razor-principle (demanding that 'entities are not to be multiplied without necessity'),[81] the CJEU does not

80 GDPR, art 82 ('(…) 4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject (…) 5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2 (…)').

81 Or '(e)ntities should not be multiplied beyond necessity'. See among many others: Stephen Chak Tornay, *Ockham: Studies and Selections* (Open Court Publishing Company 1938).

resort to joint controllership as a 'catch-all' solution making everyone or (according to the warning of Advocate General Bobek) no one responsible;[82] nor does the Court deploy joint controllership as an unjust, unfair means to 'punish', where there is neither 'crime' nor 'guilt',[83] in the sense of non-blameworthiness (it was not Facebook's decision to implement the like-button; it would be unfair, unethical to 'blame' Facebook for decisions taken by Fashion ID).[84] Rather, the CJEU entertains joint controllership as a necessary tool to protect the data subject and mechanisms like the plugins (offered by one actor, used by another actor and both benefit from it) only remind us of the relevance of the joint-liability scheme behind the concept.

9. Dutiful controllership beyond Fashion ID: too high a burden in the name of illusory user-control over personal data? (practical conclusion)

Despite the above theoretical conclusions, it can be questioned whether Fashion ID is, at a practical level, a data subject-centred judgement. On the one hand, it can be argued that, after Fashion ID, user-control is enhanced; for consent must be obtained and website visitors must be informed about the processing and prior to the processing. On the other hand, this processing can, to the CJEU, be triggered by the mere visiting/consulting of the website; no clicking of the 'like-button' or other identical plugin is demanded. This means that the website operator, using such a plugin, must undertake all necessary actions to inform the user about the processing and to obtain her consent; and this, prior to the processing. But, where we, users are presented with pop-ups and boxes that make the very visiting of the webpage conditional upon reading and ticking, the quality of the service is reduced, sacrificed in the name of (our) control over (our) data.

Two remarks need be made here. First, in light of thus far studies on website visitors' behaviour and their approach to box-ticking and policy-reading,[85] it can be fairly claimed that such a type of control is rather illusory. Second, website operators, who are the primary duty-bearers regarding the provision of information and the obtaining of consent (because of their position at the initial stage of visiting/consulting of their website), must now bear the financial burden of implementing appropriate measures to ensure that they will successfully fulfil their duties.[86] Such practical implications can have a major financial impact on small and medium enterprises, which, unlike Fashion ID, may not have sufficient resources to support

82 *Fashion ID*, Opinion of AG Bobek (n 52), paras 71, 92.

83 For a discussion on the principle of guilt in the European Union's context, see: Piet Hein van Kempen and Joeri Bemelmans, 'EU Protection of the Substantive Criminal Law Principles of Guilt and Ne Bis In Idem Under the Charter of Fundamental Rights: Underdevelopment and Overdevelopment in an Incomplete Criminal Justice Framework' (2018) 9(2) New Journal of European Criminal Law 247.

84 It could be argued that the European Data Protection Board touches upon the unfair nature of the attribution of responsibility to non-decision-makers, when mentioning that: '(…) The assessment of joint controllership should be carried out on a factual, rather than a formal, analysis of the actual influence on the purposes and means of the processing. All existing or envisaged arrangements should be checked against the factual circumstances regarding the relationship between the parties. A merely formal criterion would not be sufficient for at least two reasons: in some cases, the formal appointment of a joint controller - laid down for example by law or in a contract - would be absent; in other cases, it may be that the formal appointment does not reflect the reality of the arrangements, *by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing* (…)'. European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11) para 49 (own emphasis).

85 See among others: Asma Vranaki, 'Social Networking Site Regulation: Facebook, Online Behavioral Advertising, Power and Data Protection Laws' (2016) Queen Mary School of Law Legal Studies Research Paper No 221/2016, 29 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2731159> accessed 30 September 2020; Simon Chesterman, 'Privacy and Our Digital Selves' (*The Straits Times*, 2 September 2017) <https://ssrn.com/abstract=3033449> accessed 30 September 2020.

86 For an excellent analysis, see: Primož Gorkič, 'Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.: More Control, More Data Protection for Website Visitors? (C-40/17 Fashion ID)' (2019) 5(4) EDPL 579.

implementation of relevant measures; but also on providers of plugins, third parties that, unlike Facebook, develop less popular 'Like'-like plugins, unable to generate sufficient economic benefit; a benefit that did compensate for the establishment of dutiful (joint) controllership in the Fashion ID-case/context, in light of its particularities.

In addition, there could be side effects on advertising and targeting practices. In its recent guidelines on the targeting of social media users,[87] the European Data Protection Board distinguishes between and clarifies the roles of the 'social media providers'[88] (like Facebook) and the 'targeters' (like Fashion ID), who can target their communications at the users via their own websites and through the use of various tools (including plug-ins).[89] Extensively citing the Fashion ID-judgement, the Board explicates what duties (already known from the GDPR) can mean in targeting contexts. Important for our analysis are the following: first, consent-obtaining, binding primarily the joint controller who is first involved in the processing,[90] can imply a duty to mention any (joint) controller(s) that is/are involved in later stages of the processing chain;[91] second, (joint) controllers need be transparent by showing directly (for example, on screen and via 'layered

87 European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (Version 1.0, adopted on 2 September 2020) <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_en> accessed 30 September 2020. These guidelines do not prevail the above-analysed guidelines on the 'concepts of controller and processor in the GDPR'. See: European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) footnote 8, referring to: European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (n 11).

88 European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) paras 20-23 ('(…) Social media providers offer an online service that enables the development of networks and communities of users, among which information and content is shared (…) The social media provider determines the functionalities of the service. This in turn involves a determination of which data are processed, for which purpose, under which terms, as well as how personal data shall be processed (…) Social media providers increasingly gather data not only from activities on the platform itself, but also from activities undertaken 'off-platform', combining data from multiple sources, online and offline, in order to generate further insights (…)').

89 European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) paras 24-25 ('(…) These guidelines use the term "targeter" to designate natural or legal persons that use social media services in order to direct specific messages at a set of social media users on the basis of specific parameters or criteria (…) Targeting may also involve the creation of content hosted by the social media provider (…) or elsewhere (i.e. on third-party websites). Targeters may have their own websites and apps, where they can integrate specific social media business tools or features such as social plugins (…)'). As the Board stresses, targeting (effected by providers or targeters) can be conducted through data observed or inferred (in our case, by Facebook or Fashion ID through, for example, the processing after the embedding of the like-button). See: European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) para 36 (point b) ('(…) Observed data are data provided by the data subject by virtue of using a service or device (…) For example, a particular social media user might be targeted on the basis of (…) data collected through third-party websites that have incorporated social plugins (…)'); para 36 (point c) ('(…) "Inferred data" or "derived data" are created by the data controller on the basis of the data provided by the data subject or as observed by the controller (…) For example, a social media provider or a targeter might infer that an individual is likely to be interested in a certain activity or product on the basis of his or her web browsing behaviour and/or network connections (…)').

90 This does not negate the demand that consent, initially obtained, remain valid throughout the entire set of processing operations. European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) para 68 ('(…) Any (joint) controller seeking to rely on consent as a legal basis is responsible for ensuring valid consent is obtained. In Fashion ID, the CJEU emphasized the importance of ensuring the efficient and timely protection of the data subject rights, and that consent should not be given only to the joint controller that is involved later in the processing. Valid consent must be obtained prior to the processing, which implies that (joint) controllers need to assess when and how information should be provided and consent should be obtained. In other words, the question as to which of the joint controllers should be in charge of collecting the consent comes down to determining which of them is involved first with the data subject (…)').

91 If these controllers are unknown, there can be a duty to name them at a following phase. European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) para 69 ('(…) The EDPB also recalls that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named (…) Insofar as not all joint controllers are known at the moment when the social media provider seeks the consent, the latter will necessarily need to be complemented by further information and consent collected by the website operator embedding the social media plugin (…)').

notices') necessary information,[92] but also by making the 'essence' of their arrangement available to the data subjects;[93] third, they must implement appropriate (user-friendly) measures to enable data subjects to effectively exercise their rights;[94] and, fourth, they need conduct data protection impact assessments[95] (if applicable)[96] and take into due consideration the potential involvement of special categories of data.[97]

We conclude and sum up with questions that need be addressed in a beyond-Fashion ID-context: can the imposition/introduction of duties/costs (perhaps, in practice unfulfillable/unbearable by website operators and plugin providers who are economically weaker than big firms and tech-giants like Fashion ID and Facebook), in conjunction with the reduction of service-quality (in light of the addition of boxes that need reading and ticking), be considered as the right way to ensure effective protection of personal data? Or can one fairly argue for a potential financial and commercial suicide of small players or, at least, for a hardly bearable burden imposed on any influencer of the processing in the name of users' illusory control over their data?

92 This information refers to data mentioned in Articles 13 and 14 of the GDPR. European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) para 84.

93 Reference to the 'essence' entails a duty to make available all dimensions of the processing in a comprehensive way (in an appendix and online, for example). European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) paras 86-91. Moreover, this arrangement must refer to all processing operations and their purpose(s); and this presupposes that the joint controllers know these operations (European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) paras 123-126). Furthermore, this arrangement must mention the relevant legal basis/es (European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) para 126); and it must reflect the actual roles of the controllers involved –explicit reference can be made to how they can *in practice* influence the processing and, again *in practice*, comply with their duties (European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) paras 128ff, especially 132-133).

94 The Board pays special attention to the right of access that can, in light of processing complexities, demand remote access to data necessary. European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) paras 92-97.

95 European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) paras 98-105.

96 It is reminded that the nine criteria for the determination of whether a processing operation is 'likely to result in a high risk' are set out in: Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (Adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017, 17/EN WP 248 rev.01) 9-10 ('(…) 1. Evaluation or scoring (…) 2. Automated-decision making with legal or similar significant effect (…) 3. Systematic monitoring (…) 4. Sensitive data or data of a highly personal nature (…) 5. Data processed on a large scale (…) 6. Matching or combining datasets (…) 7. Data concerning vulnerable data subjects (..) 8. Innovative use or applying new technological or organisational solutions (…) 9. When the processing in itself "*prevents data subjects from exercising a right or using a service or a contract*" (…)') <ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236> accessed 30 September 2020.

97 European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' (n 87) paras 106-121.

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri and Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommunications operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou and Paul de Hert (13 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou and Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

N°18 Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (January 2020) by Dr Monique Mann and Professor Tobias Matzner (18 pages)

N°19 Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment? (February 2020) by Lina Jasmontaite and Paul de Hert (23 pages)

N°20 The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? (March 2020) by Elena Gil González, Paul De Hert & Vagelis Papakonstantinou (31 pages)

N°21 Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law (April 2020) by Paul De Hert & Gianclaudio Malgieri (42 pages)

N°22 The "Ethification" of Privacy and Data Protection Law in the European Union. The Case of Artificial Intelligence (May 2020) by Niels van Dijk and Simone Casiraghi (23 pages)

N°23 Logic and Key Points of China's Cybersecurity Review Measures (June 2020) by Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (9 pages)

N°24 Individuation: re-imagining data privacy laws to protect against digital harms (July 2020) by Anna Johnston (22 pages)

N°25 The Dark Side of the MOOC? The Rise of EdTech in Times of COVID-19: A Data Protection Challenge for Universities (August 2020) by Jonas Botta (16 pages)

N°26 European Law Enforcement and US Data Companies: A Decade of Cooperation Free from Law (September 2020) by Angela Aguinaldo and Paul De Hert (16 pages)

N°27 Fashion ID and Decisively Influencing Facebook Plugins: A Fair Approach to Single and Joint Controllership (June 2021) by Paul De Hert and Georgios Bouchagiar (24 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.eu