EBU

OPERATING EUROVISION AND EURORADIO

9.7.2018

Case note on case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein* (Interveners: Facebook Ireland, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht)

CASE FACTS

On 5 June 2018, the Court of Justice of the European Union (CJEU) handed down a preliminary ruling in a case opposing the Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein (the regional data protection supervisory authority, DPA) to the Wirtschaftsakademie (WA) Schleswig-Holstein, a privately run company for higher education.

In a November 2011 decision, the ULD had ordered WA to deactivate its Facebook fan page through which it offered educational services, because WA (and Facebook) had failed to inform visitors to the page that Facebook used cookies to collect and process personal data.

WA in turn brought a complaint before the ULD, rejecting any liability under German data protection law, which transposes the 1995 EU Data Protection Directive (DPD).[1] WA argued that Facebook was solely responsible for the collection and processing of the personal data of WA's fan page visitors. However the ULD maintained that, by setting up its fan page on Facebook and receiving from Facebook statistics about the visitors to its fan page, WA had contributed to the collection and processing of users' personal data.

WA then initiated legal proceedings and the case moved up the German administrative courts, until it reached the Bundesverwaltungsgericht (Federal Administrative Court) which referred the case to the CJEU. The Federal Administrative Court entertained doubts as to the interpretation of the concept of "controller" as defined in the DPD, but also as to the scope of the ULD's competence to take a decision against Facebook, which has its European seat in Ireland.

Although the DPD is no longer in force as the General Data Protection Regulation (GDPR)[2] became applicable on 25 May 2018, the Court's judgment remains pertinent for the interpretation of similar provisions set out in the GDPR. It is also interesting in the context of the numerous actions lodged at the national level against current data processing and data sharing practices of Facebook and other US-based platform operators.[3]

---

[1] Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

[2] (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, OJ L 119, 4.5.2016, p. 1).

[3] See for example proceedings initiated in Belgium concerning Facebook's tracking of non-Members, in Germany regarding Facebook's default privacy settings, and in France as regards Facebook's sharing of personal data with WhatsApp. See https://www.theguardian.com/technology/2015/nov/10/belgian-court-orders-facebook-to-

EUROPEAN BROADCASTING UNION
L'Ancienne-Route 17A
PO Box 45
1218 Le Grand-Saconnex
Geneva, Switzerland

Tel. +41(0)22 717 21 11
www.ebu.ch

Legal & Policy/Jenny Weinand,
Anne-Catherine Berg

This judgment may have an important impact on media organisations' relationships with social platforms as it raises a number of critical issues. The Court only briefly touches upon some of these crucial questions, such as the interpretation of the concepts of "data controller"/"joint-controllers" and the related obligations and responsibilities, or the imbalance of negotiation powers between fan page administrators and Facebook and access to (personal) data.

RULING

The notion of "controller" according to Directive 1995/46/EC

The first part of the CJEU's ruling concerns the question of which entity(ies) was(were) to be considered as data controller(s) of a fan page run on a social networking site and therefore responsible for compliance with data protection law.

Art. 2(d) DPD defines "controller" as the person or entity which "alone or jointly with others determines the purposes and means of the processing of personal data". The CJEU underscored that this definition was to be interpreted broadly in order to ensure "effective and complete protection" of the persons whose personal data was being collected and processed.[4] In practice, this means that more than one entity may be considered a controller.[5]

According to the CJEU, it was indisputable that Facebook bore responsibility as a controller, as it "primarily determin[es] the purposes and means of processing" of Facebook fan page users' personal data, by placing cookies on users' terminal equipment.[6]

The significant question in the case in hand was whether WA could also be qualified as a controller, and thus be jointly responsible with Facebook.

To that end, the CJEU found that fan page administrators conclude a specific contract with Facebook, accepting the latter's terms and conditions. This includes Facebook's use of cookies and other identifiers to process personal data. The purpose of such processing is to improve Facebook's own advertising system (offering users more relevant advertisements) and to make user statistics available to the fan page administrator. This data, albeit in anonymous form, allows the administrator to improve its services and offer more relevant content or functionalities based on the profiles of the fan page's visitors.[7]

---

stop-tracking-non-members; https://www.theguardian.com/technology/2018/feb/12/facebook-personal-data-privacy-settings-ruled-illegal-german-court; https://www.theguardian.com/technology/2017/dec/19/france-orders-whatsapp-stop-sharing-user-data-facebook-without-consent. See also pending case C-40/17 *Fashion ID* dealing with the Facebook "Like" button.

[4] Paras. 27 and 28 of the judgment.

[5] Para. 29 of the judgment.

[6] Para. 30 of the judgment.

[7] Paras. 33-34 of the judgment.

The CJEU then examined the fan page administrator's involvement in the processing activity and found that the administrator "contributes to the processing" by determining the "parameters" used by Facebook to produce user statistics.[8] The "parameters" or "filters" which may be selected include, for example, demographic data (e.g. age, sex, occupation), geographical data (e.g. location), information on users' lifestyles and centres of interest or their purchasing habits.[9] The Court thus concluded that a fan page administrator is "taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing" of fan page users' personal data within the meaning of Art. 2(d) DPD.[10]

Interestingly, the CJEU determined that fan page administrators' responsibility is even greater in relation to users who do not have a Facebook account because the data collection and processing is triggered simply by visiting that specific fan page.[11]

Having confirmed that a Facebook fan page administrator is a controller, the CJEU underscored that "the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data".[12] The level of responsibility will thus be determined on a case-by-case basis.

Importance of the case and implications for media organisations

The CJEU's decision in *ULD v WA* fits into its recent line of case law, in which it has continuously strengthened the fundamental right to protection of personal data, which stems from Art. 8 of the EU's Charter of Fundamental Rights.[13]

- *Facebook and its fan page administrators are joint controllers*

The Court also looks through the lens of fundamental rights when interpreting the concept of "controller" broadly, highlighting the fact that control may be exercised by more than one party. In this respect, Advocate General (AG) Bot, in his opinion, quoted the concept of "pluralistic control",[14] as developed by Article 29 Working Party[15] in an opinion published in 2010, which captures the increasing complexities of data processing activities.[16]

[8] Para. 36 of the judgment.
[9] Para. 37 of the judgment.
[10] Para. 39 of the judgment. It is interesting to note that Advocate General Bot, in his opinion, applies the same reasoning and draws the same conclusions in relation to pending case C-40/17 Fashion ID, which deals with the Facebook "Like" button embedded by a website provider. See points 66-72 of the opinion, delivered on 24.10.2017, EU:C:2017:796.
[11] Paras. 35 and 41 of the judgment.
[12] Para. 43 of the judgment.
[13] See for example cases C-293/12 *Digital Rights Ireland*, Judgment of 8.4.2014, EU:C:2014:238 read in conjunction with joined cases C-203/15 *Tele2 Sverige AB* and C-698/15 *Tom Watson*, Judgment of 21.12.2016, EU:C:2016:970, C-131/12 *Google Spain*, Judgment of 13.5.2014, EU:C:2014:317, C-362/14 *Schrems*, Judgment of 6.10.2014, EU:C:2015:650, C-498/16 *Schrems*, Judgment of 25.1.2018, EU:C:2018:37.
[14] The concept of "pluralistic control" was originally developed by the Article 29 Working Party in Opinion 1/2010 on the concepts of "controller" and "processor", adopted 16.2.2010, p. 32-33.
[15] Since May 2018, the European Data Protection Board, which gathers all national DPAs of the EU, has replaced the Article 29 Working Party in accordance with Art. 68 GDPR.
[16] See point 62 of the opinion.

Both the CJEU and AG Bot pointed out that the exercise of joint control does not imply equal levels of responsibility of the parties involved,[17] but neither the Court, nor the AG specified what this means in practice. One might reflect upon a graduated system of responsibility with different legal consequences attached to different grades. This is a crucial point which would merit more in-depth analysis than can be provided here.

- *Imbalance of negotiation powers between Facebook and fan page operators*

The CJEU rightly observes that Facebook fan page administrators are not in a position to negotiate the social network's terms and conditions, but are in practice confronted with a "take it or leave it choice" if they want to make use of this platform.[18] However this element is disregarded, both by the Court and by the AG, in determining which entities should be regarded as "controllers".

AG Bot even went as far to say that a fan page administrator concludes a contract with Facebook "of his own volition".[19] In addition, he emphasized, again quoting Art. 29 WP that "any imbalance in the relationship of strength between service provider and service user" could not preclude a fan page administrator from being regarded as a (joint) controller.[20]

- *Access to data*

Another interesting question arising from the judgment relates to access to data. While Facebook collects and processes users' personal data for its own commercial purposes, it only provides anonymous statistical data to fan page administrators. For the CJEU, a classification as "controller" does not require actual access to personal data.[21] In other words, an entity may be regarded as "joint controller" even if that entity does not have access, or only has access in an aggregated and anonymous form, to the data collected.

The question of whether access to data is granted, but also what kind of data is provided to the "weaker" entity of joint controllers is, however, crucial for media organisations seeking to improve their services on the basis of accurate statistics and to offer tailored content and services.

In short, while a functional interpretation of the concept of "controller" seems appropriate (i.e. determining responsibility according to the functions carried out by the entities involved), this approach may overlook the blatant realities of a market that is dominated by a few big platforms. It begs the question of whether certain criteria, such as the balance of power in negotiations (reflected in the non-negotiable terms and conditions) and access to data should be considered when assessing the concept of "controller". The *Fashion ID* case[22] concerning the Facebook "Like" button may offer the Court the opportunity to re-examine this aspect.

[17] Para. 43 of the judgment and point 75 of the opinion.
[18] Para. 32 of the judgment. See also point 60 of the opinion.
[19] Point 60 of the opinion.
[20] Point 61 of the opinion.
[21] Para. 38 of the judgment.
[22] Pending case C-40/17 *Fashion ID*.

- *Exercise of users' rights*

In cases of joint controllership, it is also unclear which party carries primary responsibility towards the user. According to Art. 26(3) GDPR, data subjects may exercise their rights "in respect of and against each of the controllers".

In practice, users may find it easier to lodge a complaint against the "smaller" party, i.e. a fan page administrator, rather than against a giant US social network. This may raise questions of fairness in law enforcement.[23]

Preliminary observations regarding the practical implications for media organisations with a fan page

This case will remain relevant in the future despite the fact that the provisions interpreted by the Court are from a Directive which is no longer in force. Indeed, the wording in Art. 4(7) GDPR is identical to the definition of "controller" pursuant to Art. 2(d) DPD.

When considering the Court's judgment in light of the GDPR, operators of Facebook fan pages will have to put in place certain measures to ensure adequate protection of their sites' visitors' personal data.

This would first require fan page administrators to conclude a joint controller agreement with Facebook as prescribed by Art. 26 GDPR. In this agreement, joint controllers should "determine their respective responsibilities", particularly in view of data subjects' rights and information obligations. This agreement may serve to clarify the questions relating to data access, i.e. which party has a right to data and what kind of data.

It will also be necessary to update relevant privacy policies and notices to adequately inform users of any data processing activities and ensure that users can exercise their rights (e.g. access, rectification, erasure). In accordance with Art. 12, 13 and 14 GDPR, joint controllers are required to provide adequate information to users, inter alia, on the identity of the joint controllers, the purpose of the processing, data retention periods and data subjects' rights.

Importantly, fan page operators will have to clearly communicate the purpose of the processing as well as the legal basis for such processing as stipulated in Art. 6 GDPR. Any data collected and processed for the purpose of providing targeted advertising will require end-users' consent in accordance with Art. 7 GDPR.

These are preliminary observations which may require a more in-depth analysis, taking into account national case law and practice by DPAs.

[23] Similar questions raised by Jörg Ukrow, Wehrhafter transatlantischer Datenschutz, Institute of European Media Law, para. 4, available at https://emr-sb.de/wp-content/uploads/2018/06/EMR-Aktuelles-Stichwort-Datenschutz-1806-01.pdf.

The powers of national data protection authorities

In the judgment's second part, the CJEU examined the scope of a national DPA's powers in relation to companies whose European seat is located in another Member State. While Facebook Inc. is established in the United States, Facebook's European headquarters are based in Ireland and it maintains subsidiaries in many Member States, including in Germany.

While the entity established in Germany is responsible for promoting and selling advertising space, Facebook Ireland is generally in charge of the collection and processing of personal data for Facebook users throughout the EU. The German court thus raised the question whether the ULD was entitled to exercise its powers in relation to Facebook Germany, even if, as a result of the division of tasks within the Facebook group, that entity's responsibilities solely encompassed the sale of advertising space and other marketing activities.

In accordance with Art. 4(1)(a) DPD, the CJEU examined first whether there was "an establishment of the controller" situated in Germany, and second whether the processing was carried out "in the context of the activities" of the establishment.

The Court readily confirmed that the Hamburg-based entity of Facebook Germany was an establishment within the meaning of the DPD read in light of the Treaties, because it effectively and genuinely exercised its activities on a permanent basis.[24]

Regarding the second condition of Art. 4(1) DPD, the Court affirmed that the expression "in the context of the activities of an establishment" must be broadly interpreted so as to ensure "effective and complete protection of the fundamental rights and freedoms of natural persons".[25] The CJEU also highlighted the fact that, pursuant to the DPD, the processing need not be carried out by the establishment concerned (i.e. Facebook Germany) but only that it be carried out "in the context of the activities of" the establishment. Since Facebook Germany sells and markets advertising space "that makes Facebook's services profitable" and helps improve Facebook's system of advertising to better target users, the activities of the German Facebook subsidiary "must be regarded as inextricably linked to the processing of personal data" for which Facebook Inc. and Facebook Ireland are jointly responsible.[26]

It follows that the ULD was competent to exercise its powers and ensure compliance, on German territory, with data protection laws in relation to both WA as well as Facebook Germany.[27]

As national supervisory authorities are required to act in complete independence pursuant to Art. 28(1) DPD, read in light of Art. 8(3) CFR and Art. 16(2) TFEU, the Court furthermore clarified that the ULD may exercise its powers of intervention without first referring to the Irish supervisory authority.[28] The ULD was thus competent to assess the lawfulness of the data

[24] Para. 55 of the judgment.
[25] Para. 56 of the judgment.
[26] Para. 60 of the judgment where the CJEU quotes point 94 of the opinion.
[27] Para. 62 of the judgment.
[28] Paras. 68-73 of the judgment.

processing and to exercise its powers vis-à-vis Facebook Germany without prior cooperation with the Irish authorities.

The Court's decision contributes to a more effective supervision by national DPAs as the Court sets limits to the extent undertakings established outside of the EU can split tasks among EU-based subsidiaries in order to benefit from the most liberal regime.[29] As long as there is a link between the processing activities carried out by an entity located in one Member State and the activities performed by another entity in a different Member State, national DPAs may intervene.

The effect of the Court's decision regarding collaboration of DPAs in different Member States may however be more limited in the future, given the concept of "lead supervisory authority", introduced in Art. 56 GDPR.

[29] See Ukrow, Wehrhafter transatlantischer Datenschutz, para. 11.