СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

CVRIA
LUXEMBOURG

EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

OPINION OF ADVOCATE GENERAL
BOT
delivered on 24 October 2017 [1]

**Case C-210/16**

**Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein**
**v**
**Wirtschaftsakademie Schleswig-Holstein GmbH,**
**in the presence of**
**Facebook Ireland Ltd,**
**Vertreter des Bundesinteresses beim Bundesverwaltungsgericht**

(Request for a preliminary ruling from the Bundesverwaltungsgericht (Federal Administrative Court, Germany))

(Reference for a preliminary ruling — Directive 95/46/EC — Articles 2, 4 and 28 — Protection of individuals with regard to the processing of personal data and on the free movement of such data — Order to deactivate a fan page on the social network Facebook — Concept of 'controller' — Liability of the administrator of the fan page — Joint liability — Applicable national law — Extent of supervisory authorities' powers to intervene)

[1] Original language: French.

1. This request for a preliminary ruling concerns the interpretation of Articles 2(d), 4(1), 17(2) and 28(3) and (6) of 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, [2] as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003. [3]

2. The request has been made in proceedings between the Wirtschaftsakademie Schleswig-Holstein GmbH, a company governed by private law and specialising in the field of education ('the Wirtschaftsakademie'), and the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, a regional data-protection authority in Schleswig-Holstein ('ULD') concerning the lawfulness of an order issued by the latter against the Wirtschaftsakademie requiring it to deactivate a 'fan page' hosted on the website of Facebook Ireland Ltd.

3. The reason for that order was the alleged infringement of the provisions of German law transposing Directive 95/46. Specifically, visitors to the fan page were not warned that their personal data are collected by the social network Facebook ('Facebook') by means of cookies that are placed on the visitor's hard disk, the purpose of that data collection being to compile viewing statistics for the administrator of the fan page and to enable Facebook to publish targeted advertisements.

4. The background to the present case is the phenomenon known as 'web tracking', which consists in the observation and analysis of the behaviour of Internet users for commercial and marketing purposes. Web tracking helps identify the centres of interest of Internet users, through observation of their browsing habits. This is referred to as behavioural web tracking and it is usually carried out with the aid of cookies.

5. Cookies are text files that are downloaded onto an Internet user's computer whenever he or she visits a website.

6. Web tracking is used, amongst other things, in order to optimise websites and configure them more effectively. It also enables advertisers to target various segments of the public.

7. According to the definition given to it by the Article 29 data protection working party [4] in Opinion 2/2010 of 22 June 2010 on online behavioural advertising, [5] 'behavioural advertising is advertising that is based on the

2 OJ 1995 L 281, p. 31.

3 OJ 2003 L 284, p. 1, 'Directive 95/46'.

4 'The Article 29 working party'.

5 'Opinion 2/2010'.

observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests.' [6] To achieve that, information from the user's browser and terminal equipment is collected and used. The main tracking technique used to monitor users on the Internet is based on 'tracking cookies'. [7] Thus, 'behavioural advertising uses information collected on an individual's web-browsing behaviour, such as the pages visited or the searches made, to select which advertisements to display to that individual'. [8]

8. The tracking of browsing behaviour also makes it possible to provide website operators with user statistics concerning the people who visit their websites.

9. The collection and use of personal data for the purposes of compiling user statistics and publishing targeted advertising must meet certain conditions in order to comply with the personal data protection rules arising from Directive 95/46. In particular, such operations may not be carried out without first informing and obtaining the agreement of the person concerned.

10. Determining such compliance necessitates the resolution of a number of preliminary issues. These concern the definition of 'controller', the identification of the applicable national law and the determination of which authority has jurisdiction to exercise its powers of intervention.

11. The issue of identifying the controller becomes a particularly thorny one in the situation where an economic operator decides not to install on its own website the tools needed to compile user statistics and to publish targeted advertising, but instead to make use of a social network such as Facebook and to create a fan page so as to have the use of similar tools.

12. The issues of identifying which national law applies and of determining which authority has jurisdiction to exercise its powers of intervention also become

6 Opinion 2/2010, p. 5.

7 Opinion 2/2010, p. 7. According to the Article 29 working party's explanations, 'it usually works as follows: typically, the ad network provider places a tracking cookie on the data subject's terminal equipment, when he/she first accesses a website serving an ad of its network. The cookie is a short alphanumeric text which is stored (and later retrieved) on the data subject's terminal equipment by a network provider. In the context of behavioural advertising, the cookie will enable the ad network provider to recognise a former visitor who returns to that website or visits any other website that is a partner of the advertising network. Such repeated visits will enable the ad network provider to build a profile of the visitor which will be used to deliver personalised advertising.'

8 Opinion 1/2010 of the Article 29 working party of 16 February 2010 on the concept of 'controller' and 'processor', 'Opinion 1/2010', p. 25.

more complex where the processing of personal data in question implicates several entities located both outside the European Union and within it.

13. In recent months, the supervisory authorities of several Member States have decided to impose fines on Facebook, because of breaches of the rules on the protection of the personal data of its users. [9] The present case will enable the Court to clarify the extent of the powers of intervention of supervisory authorities such as ULD with regard to the processing of personal data which involves the participation of several parties.

14. For a proper understanding of the legal issues raised by this case, it is necessary to begin with a description of the factual background of the dispute in the main proceedings.

## I. The facts of the dispute in the main proceedings and the questions referred for a preliminary ruling

15. The Wirtschaftsakademie provides education and training services via a fan page hosted on the website of the social network Facebook.

16. Fan pages are special user accounts that individuals and businesses can set up on Facebook. To do that, the fan page administrator must first register with Facebook and can then use the platform created by Facebook to present itself to users of the social network and to post information of any kind, in particular with a view to developing a business.

17. Fan page administrators can obtain viewing statistics thanks to a tool called 'Facebook Insights', which is available free of charge under the standard terms and conditions of use. The statistics are compiled by Facebook and are then personalised by the fan page administrator using various selection criteria, such as sex or age. The statistics thus provide anonymous information on the characteristics and habits of the people who have visited the fan page, and so help the administrator better to target its communications.

18. For the purpose of compiling these viewing statistics, at least one cookie containing a unique ID number, active for two years, is stored by Facebook on the hard disk of every person that visits the fan page. The ID number, which can be matched with the connection data of users registered on Facebook, is collected and processed when Facebook pages are opened.

9 The Agencia española de protección de datos (Spanish data protection agency) announced, on 11 September 2017, that it had fined Facebook Inc. EUR 1.2 million. Earlier, the Commission nationale de l'informatique et des libertés (CNIL) (Committee for Information Technology and Freedoms, France) had decided, by resolution of 27 April 2017, to impose on Facebook Inc. and Facebook Ireland, jointly and severally, a fine of approximately EUR 150 000.

19. By decision of 3 November 2011, ULD ordered the Wirtschaftsakademie, in accordance with the first sentence of section 38(5) of the Bundesdatenschutzgesetz (Federal Data Protection Law, 'the BDSG'), [10] to deactivate the fan page which it had created on Facebook at the following Internet address: https://www.facebook.com/wirtschaftsakademie, failing which it would receive a penalty for failing to comply within the prescribed period, on the ground that neither the Wirtschaftsakademie nor Facebook had informed visitors to the fan page that Facebook was collecting their personal data with the aid of cookies and was then processing that data. The Wirtschaftsakademie challenged that decision, arguing in substance that, as regards the right to data protection, it was not responsible for the data processing carried out by Facebook or for the cookies which Facebook installed.

20. By decision of 16 December 2011, ULD dismissed that objection, holding that the Wirtschaftsakademie's responsibility as service provider had been established pursuant to section 3(3)(4) and section 12(1) of the Telemediengesetz (Telemedia Law). [11] By creating the fan page, the Wirtschaftsakademie had also made an active, voluntary contribution to the collection by Facebook of personal data, from which it also derived a benefit, through the user statistics made available by the social network.

21. The Wirtschaftsakademie then challenged that decision before the Verwaltungsgericht (Administrative Court, Germany), arguing that Facebook's data processing operations could not be attributed to it and that it had not instructed Facebook, under section 11 of the BDSG, [12] to process data that it

10 Section 38(5) of the BDSG provides:

'To guarantee compliance with this act and other data protection provisions, the supervisory authority may order measures to rectify infringements during the collection, processing or use of personal data or technical or organisational irregularities detected. In the event of serious infringements or irregularities, especially those connected with a special threat to privacy, the supervisory authority may prohibit collection, processing or use, or the use of particular procedures if the infringements or irregularities are not rectified within a reasonable period contrary to the order pursuant to the first sentence above and despite the imposition of fines. The supervisory authority may demand the dismissal of the data protection official if he/she does not possess the specialised knowledge and demonstrate the reliability necessary for the performance of his/her duties.'

11 Section 12 of the Telemedia Law is worded as follows:

'1. A service provider may collect and use personal data to make telemedia available only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.

…

3. Except as otherwise provided for, the relevant provisions concerning the protection of personal data shall apply even if the data are not processed automatically.'

12 That provision relates to the processing of personal data under a sub-contracting arrangement.

controlled or that it could influence. The Wirtschaftsakademie submitted that ULD was mistaken to take action against it, rather than directly against Facebook.

22. By judgment of 9 October 2013, the Verwaltungsgericht (Administrative Court) set aside the contested decision, essentially for the reason that the administrator of a Facebook fan page is not a 'controller' within the meaning of section 3(7) of the BDSG [13] and that the Wirtschaftsakademie could not therefore be made the addressee of a measure adopted under section 38(5) of the BDSG.

23. The Oberverwaltungsgericht (Higher Administrative Court, Germany) then dismissed as unfounded the appeal which ULD brought against that judgment, holding, in substance, that the prohibition on data processing set out in the contested decision was unlawful, since the second sentence of section 38(5) of the BDSG provides for a progressive procedure, the first stage of which merely allows for the adoption of measures to rectify infringements found in the processing of data. An immediate prohibition of data processing is only possible if a data processing procedure is unlawful in its totality and if suspending that procedure alone can remedy that. According to the Oberverwaltungsgericht (Higher Administrative Court), that was not the case in this instance, because Facebook is in a position to bring the infringements alleged by ULD to an end.

24. The order to deactivate the fan page was also unlawful because the applicant was not a controller within the meaning of section 3(7) of the BDSG, in so far as concerned the data collected by Facebook, and that an order under section 38(5) of the BDSG could be issued only against such a body. In the present case, Facebook alone decided on the purposes and means of the collection and processing of the personal data used for the 'Facebook Insight' function. As for its part, the applicant had received only statistical information that had been rendered anonymous.

25. Section 38(5) of the BDSG did not permit orders to be issued against third parties. So-called disturber liability ('*Störerhaftung*') on the Internet, a concept developed in civil case-law, was not applicable to the prerogatives of public authorities. Even though section 38(5) of the BDSG did not expressly name the addressee of an injunctive order, it was clear from the general structure, the object and the spirit of the BDSG, and from its origins, that such an addressee must be a controller.

26. In the appeal on a point of law which it has brought before the Bundesverwaltungsgericht (Federal Administrative Court, Germany), ULD argues, amongst other things, infringement of section 38(5) of the BDSG and claims that the appeal court made a number of procedural errors. It considers that the infringement committed by the Wirtschaftsakademie is that it gave instructions to an inappropriate supplier — inappropriate in that did not comply with

[13] According to that provision, a 'controller' is 'any person or body collecting, processing or using personal data on his or its own behalf or commissioning others to do the same'.

applicable data protection laws — namely Facebook Ireland, to create, host and maintain a website. The order to deactivate the fan page was thus intended to rectify the infringement committed by the Wirtschaftsakademie inasmuch as it would prohibit it from continuing to use Facebook's infrastructure as the technical basis for its website.

27. The referring court considers that, as regards the collection and processing of the personal data of people visiting the fan page by the intervener in the main proceedings, namely Facebook Ireland, the Wirtschaftsakademie is not a 'body collecting, processing or using personal data on his or its own behalf or commissioning others to do the same', within the meaning of section 3(7) of the BDSG, or the 'body which alone or jointly with others determines the purposes and means of the processing of personal data', within the meaning of Article 2(d) of Directive 95/46. Admittedly, by its decision to create a fan page on the platform provided by the intervener in the main proceedings, or by its parent company (Facebook Inc., USA), the Wirtschaftsakademie objectively gave the intervener in the main proceedings the opportunity to install cookies whenever its fan page is accessed and to collect data using those cookies. However, that decision did not put the Wirtschaftsakademie in a position to influence, guide, model or control the nature and extent of the processing of the data of users of its fan page by the intervener in the main proceedings. Nor did the terms of use of the fan page confer on the Wirtschaftsakademie any rights to intervene or control. The terms of use were laid down unilaterally by the intervener in the main proceedings. They are not the outcome of any negotiation and they give the Wirtschaftsakademie no right to prohibit the intervener in the main proceedings from collecting and processing the data of users of its fan page.

28. The referring court acknowledges that the legal definition of 'controller' given in Article 2(d) of Directive 95/46 must, in principle, be interpreted broadly, in the interests of the effective protection of the right to privacy. Nevertheless, the Wirtschaftsakademie does not satisfy that definition, since it has no influence, in law or in fact, over the manner in which the personal data is processed by the intervener in the main proceedings under its own responsibility and in complete independence. It is not sufficient, in this regard, that the Wirtschaftsakademie may objectively derive a benefit from the 'Facebook Insights' function provided by the intervener in the main proceedings in that it is sent data that has been rendered anonymous concerning use of its fan page.

29. According to the referring court, the Wirtschaftsakademie also cannot be regarded as a controller relying on a 'processor' under a sub-contracting arrangement, within the meaning of section 11 of the BDSG and Articles 2(e) and 17(2) and (3) of Directive 95/46.

30. The referring court considers that clarification is needed of whether, and if so under what circumstances, the supervisory powers and powers of intervention of the supervisory authorities in the field of data protection may be exercised solely with regard to a 'controller', within the meaning of Article 2(d) of Directive

95/46, or if liability may be incurred by a body that is not the data controller, according to the definition given in that provision, as a result of its decision to have recourse to Facebook for its information offering.

31. In the latter hypothesis, the referring court wonders whether such liability might be founded on the application by analogy of the obligations concerning the choice of controller which arise from Article 17(2) of Directive 95/46 in the context of the processing of data under a sub-contracting arrangement.

32. In order to be able to rule on the lawfulness of the injunctive order issued in the present case, the referring court also considers it necessary to clarify certain points concerning the competence of the supervisory authorities and the extent of their powers of intervention.

33. In particular, the referring court asks about the distribution of powers among the supervisory authorities in the situation where a parent company, such as Facebook Inc., has several establishments throughout the territory of the European Union and the tasks assigned to each of the establishments within the group are different.

34. The referring court points out, in this connection, that the Court held, in its judgment of 13 May 2014, *Google Spain and Google*, [14] that 'Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State. [15] The referring court wonders whether such a connection with an establishment such as Facebook Germany GmbH, which, according to the information in the order for reference, is responsible for the promotion and sale of advertising space and other marketing activities directed toward residents in the Federal Republic of Germany, is relevant in determining whether Directive 95/46 applies and which supervisory authority has jurisdiction in the situation where a subsidiary established in another Member State (in this case, Ireland) acts as 'controller' throughout the territory of the European Union.

35. In so far as concerns the addressees of a measure taken under Article 28(3) of Directive 95/46, the referring court states that the order issued against the Wirtschaftsakademie could be the result of an error of assessment, and consequently unlawful, if the infringement of the applicable right to the protection of data could be remedied by means of a measure addressed directly to the subsidiary, Facebook Germany, established in Germany.

14 C-131/12, EU:C:2014:317.

15 Paragraph 60 of the judgment.

36. The referring court also notes that the ULD considers that it is not bound by the findings and determinations of the Irish supervisory authority (the Data Protection Commissioner), which, according to the Wirtschaftsakademie and the intervener in the main proceedings, has not taken issue with the processing of personal data in question in the main proceedings. The referring court therefore wishes to know, first, whether such an independent assessment by ULD is permitted and, secondly, whether the second sentence of Article 28(6) of Directive 95/46 required ULD, in view of the diverging assessments of the two supervisory authorities as to whether the data processing at issue in the main proceedings is consistent with the rules arising from Directive 95/46, to request the Data Protection Commissioner to exercise her powers against Facebook Ireland.

37. In those circumstances, the Bundesverwaltungsgericht (Federal Administrative Court) decided to stay the proceedings and to refer the following questions to the Court for a preliminary ruling:

‘1. Is Article 2(d) of Directive 95/46 to be interpreted as definitively and exhaustively defining the liability and responsibility for data protection violations, or does scope remain, under the ‘suitable measures’ pursuant to Article 24 of Directive 95/46 and the ‘effective powers of intervention’ pursuant to the second indent of Article 28(3) of Directive 95/46, in multi-tiered information provider relationships for responsibility of a body that does not control the data processing within the meaning of Article 2(d) of Directive 95/46 when it chooses the operator of its information offering?

2. Does it follow *a contrario* from the obligation of Member States under Article 17(2) of Directive 95/46 to stipulate, in cases where data processing is carried out on the controller’s behalf, that the controller ‘must ... choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out’, that, where there are other user relationships not linked to data processing on the controller’s behalf within the meaning of Article 2(e) of Directive 95/46, there is no obligation to make a careful choice and no such an obligation can be derived from national law?

3. In cases in which a parent company based outside the European Union has legally independent establishments (subsidiaries) in various Member States, is the supervisory authority of a Member State (in this case, Germany) entitled under Article 4 and Article 28(6) of Directive 95/46 to exercise the powers conferred under Article 28(3) of Directive 95/46 against the establishment located in its territory even when this establishment is solely responsible for promoting the sale of advertising and other marketing measures aimed at the inhabitants of this Member State, whereas the independent establishment (subsidiary) located in another Member State (in this case, Ireland) is exclusively responsible within the group’s internal division of tasks for collecting and processing personal data throughout the entire territory of the European Union and hence in the other Member State

as well (in this case, Germany), if decisions about data processing are in fact taken by the parent company?

4. Are Article 4(1)(a) and Article 28(3) of Directive 95/46 to be interpreted as meaning that, in cases in which the controller has an establishment in the territory of one Member State (in this case, Ireland) and there is another, legally independent establishment in the territory of another Member State (in this case, Germany), whose responsibilities include the sale of advertising space and whose activity is aimed at the inhabitants of that State, the competent supervisory authority in this other Member State (in this case, Germany) may direct measures and orders implementing data protection legislation also against the other establishment (in this case, in Germany) not responsible for data processing under the group's internal division of tasks and responsibilities, or are measures and orders only possible by the supervisory body of the Member State (in this case, Ireland) in whose territory the entity with internal responsibility within the group has its registered office?

5. Are Article 4(1)(a) and Article 28(3) and (6) of Directive 95/46 to be interpreted as meaning that, in cases in which the supervisory authority in one Member State (in this case, Germany) takes action against a person or entity in its territory pursuant to Article 28(3) of Directive 95/46 on the grounds of failing to exercise due care in choosing a third party involved in the data processing process (in this case, Facebook), because this third party is in violation of data protection legislation, the active supervisory authority (in this case, Germany) is bound by the appraisal of data protection legislation by the supervisory authority of the Member State in which the third party responsible for the data processing has its establishment (in this case, Ireland) meaning that it may not arrive at a different legal appraisal, or may the active supervisory authority (in this case, Germany) conduct its own examination of the lawfulness of the data processing by the third party established in another Member State (in this case, Ireland) as a preliminary question prior to its own action?

6. Where the possibility of conducting an independent examination is available to the active supervisory authority (in this case, Germany), is the second sentence of Article 28(6) of Directive 95/46 to be interpreted as meaning that this supervisory authority may exercise the effective powers of intervention conferred on it under Article 28(3) of Directive 95/46 against a person or entity established in its territory on the grounds of their joint responsibility for data protection violations by a third party established in another Member State only and not until it has first requested the supervisory authority in this other Member State (in this case, Ireland) to exercise its powers?'

## II. My assessment

38. It must be observed that the questions which the national court has referred for a preliminary ruling do not touch upon the matter of whether the processing of personal data of which ULD complains, that is to say, the collection and use of the data of people visiting fan pages without their first being informed thereof, is contrary to the rules arising from Directive 95/46.

39. According to the explanations provided by the referring court, the lawfulness of the order submitted to it for review depends on a number of points. From its viewpoint, it is necessary to begin by determining whether ULD had grounds to exercise its powers of intervention against a person who is not a controller within the meaning of Article 2(d) of Directive 95/46. Next, the referring court considers that the lawfulness of the order also depends on whether ULD had jurisdiction to take action with regard to the processing of personal data at issue in the main proceedings, and also on whether ULD's addressing its order to the Wirtschaftsakademie rather than to Facebook Germany was an error of assessment, and lastly on whether ULD made some other error of assessment by ordering the Wirtschaftsakademie to close down its fan page without first requesting the Data Protection Commissioner to exercise her powers against Facebook Ireland.

### A. The first and second questions

40. By its first and second questions, which it is appropriate to examine together, the referring court is essentially asking the Court to rule whether Articles 17(2) and 24 and the second indent of Article 28(3) of Directive 95/46 must be interpreted as permitting supervisory authorities to exercise their powers of intervention against a body that cannot be regarded as a 'controller' within the meaning of Article 2(d) of that directive, but which might nevertheless be held liable in the event of infringement of the rules on the protection of personal data on account of its decision to have recourse to a social network such as Facebook for the publication of its information offering.

41. These questions rest on the premiss that the Wirtschaftsakademie is not a data processing 'controller' within the meaning of Article 2(d) of Directive 95/46. That is why the referring court wishes to know whether an injunctive order such as that at issue in the main proceedings may be addressed to a person that does not meet the criteria laid down in that provision.

42. However, I consider that premiss to be incorrect. Indeed, the Wirtschaftsakademie must, in my opinion, be regarded as jointly responsible for the phase of the data processing which consists in the collection by Facebook of personal data.

43. According to Article 2(d) of Directive 95/46, a 'controller' is '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'. [16]

44. The controller plays a fundamental role within the system established by Directive 95/46, and therefore identifying the controller is essential. Indeed, the directive provides that controllers are under a certain number of obligations which are intended to ensure the protection of personal data. [17] That fundamental role was highlighted by the Court in its judgment of 13 May 2014, *Google Spain*, [18] in which it held that controllers must ensure, within the framework of their responsibilities, powers and capabilities, that the data processing in question meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved. [19]

45. It is also clear from the case-law of the Court that the concept of 'controller' must be given a broad definition, so as ensure effective and complete protection of data subjects. [20]

46. The personal data processing controller is the person that decides why and how data will be processed. As the Article 29 working party has stated, 'the concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and [it is] thus based on a factual rather than a formal analysis'. [21]

16 According to the definitions offered in Opinion 1/2010, the word 'purpose' means 'an anticipated outcome that is intended or that guides your planned action' and 'means' signifies 'how a result is obtained or an end achieved' (p. 13).

17 By way of example, in accordance with Article 6(2) of the directive, controllers must ensure compliance with the principles relating to data quality listed in Article 6(1). In accordance with Articles 10 and 11 of Directive 95/46, controllers are under a duty to provide information to data subjects. Under Article 12 of the directive, data subjects have a right of access to data, which controllers must provide. The same is true of the right to object, provided for in Article 14 of the directive. Under Article 23(1) of Directive 95/46, the Member States must provide that 'any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to [the directive] is entitled to receive compensation from the controller for the damage suffered'. Lastly, supervisory authorities' effective powers of intervention, as stipulated in Article 28(3) of the directive, are exercised against controllers.

18 C-131/12, EU:C:2014:317.

19 See the judgment of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraphs 38 and 83).

20 See, in particular, the judgment of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 34).

21 Opinion 1/2010, p. 10.

47. As the designers of the data processing in question, it is, in my view, Facebook Inc. and, in so far as the European Union is concerned, Facebook Ireland that principally decided on the purposes and means of that data processing.

48. More specifically, Facebook Inc. developed the general economic model in accordance with which the collection of personal data during visits to fan pages and then the processing of that data enables the publication of personalised advertisements and the compilation of viewing statistics for fan page administrators.

49. In addition, it is apparent from the documents before the Court that Facebook Ireland has been designated by Facebook Inc. as being responsible for the processing of personal data within the European Union. According to the explanations provided by Facebook Ireland, the way in which the social network operates is slightly different in the European Union. [22]

50. Moreover, while it is common ground that any person residing in the European Union who wishes to use Facebook is required to conclude, at the time of his registration, a contract with Facebook Ireland, it must also be pointed out that some or all of the personal data of Facebook's users who reside in the European Union is transferred to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing. [23]

51. Given the involvement of Facebook Inc. and, with particular regard to the European Union, of Facebook Ireland in deciding on the purposes and means of the personal data processing at issue in the main proceedings, those two entities should, in light of the information before the Court, be regarded as jointly responsible for that data processing. In this connection, it should be pointed out that Article 2(d) of Directive 95/46 expressly provides for the possibility of such shared responsibility. As the referring court itself has stated, it will ultimately be for that court to clarify the internal decision-making structures and the internal arrangements for data processing within the Facebook group so that it may determine which establishment or establishments are controllers within the meaning of Article 2(d) of Directive 95/46. [24]

52. In so far as concerns the phase of the data processing which consists in the collection by Facebook of personal data, [25] I believe it necessary to add to the joint

22 Facebook Ireland explains that it regularly introduces new functions which are available solely to users in the European Union and are adapted to such users. In other cases, Facebook Ireland may decide not to make available in the European Union products which are made available by Facebook Inc. in the United States.

23 See the judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650, paragraph 27).

24 Paragraph 39 of the order for reference, [paragraph 21 of the English summary of the order for reference].

25 What is important in the present case is not the determination of the purposes and means of the data processing which occurs after the transmission to Facebook of the data of people who have

responsibility of Facebook Inc. and Facebook Ireland the responsibility of a fan page administrator, such as the Wirtschaftsakademie.

53. Admittedly, a fan page administrator is first and foremost a user of Facebook, one that makes use of Facebook's tools so as to gain better visibility. Nevertheless, that fact does not mean that the fan page administrator cannot also be regarded as responsible for the phase of the data processing which is the subject of the dispute in the main proceedings, that is to say, the collection of personal data by Facebook.

54. As regards the question of whether a fan page administrator 'determines' the purposes and means of data processing, it is necessary to check whether that administrator has any influence, in law or in fact, over those purposes and means. This element of the definition indicates that the controller is not the person that carries out the personal data processing, but the person that determines the means and purposes of that data processing.

55. By having recourse to Facebook for the publication of its information offering, a fan page administrator is subscribing to the principle that the personal data of visitors to his page will be processed for the purpose of compiling viewing statistics. [26] Even though a fan page administrator is not, of course, the designer of the 'Facebook Insights' tool, he will, by having recourse to that tool, be participating in the determination of the purposes and means of the processing of the personal data of visitors to his page.

56. For one thing, that data processing could not occur without the prior decision of the fan page administrator to create and operate a fan page on the Facebook social network. By making the processing of the personal data of users of the fan page possible, the administrator is adhering to the system put in place by Facebook. The administrator acquires a better insight into the profiles of the users of his fan page and, at the same time, enables Facebook better to target the advertising that is publishes over the social network. Inasmuch as he agrees to the means and purposes of the processing of personal data, as predefined by Facebook, a fan page administrator must be regarded as having participated in the determination of those means and purposes. Moreover, just as a fan page administrator has a decisive influence over the commencement of the processing

visited a fan page. The focus must be on the phase of the processing that is in issue here, that is to say, the collection of the data of people who visit a fan page, without their first being informed thereof or giving their consent thereto.

26 It is apparent from Facebook's terms and conditions of use that viewing statistics provide the fan page administrator with information about his target audience, so that he can create content that is more relevant to it. Viewing statistics provide the fan page administrator with demographic data concerning the target audience, including trends in terms of age, sex, personal and professional status, information on the life styles and centres of interest of the target audience and information on the purchasing habits of the target audience, including on-line purchasing, the categories of goods and services that appeal the most and geographic data which tell the administrator where to make special offers and where to organise events.

of the personal data of people who visit his fan page, he also has power to bring that data processing to an end, by closing the page down.

57. For another thing, while the purposes and means of the 'Facebook Insights' tool, as such, are generally defined by Facebook Inc., together with Facebook Ireland, a fan page administrator is able to influence the specific way in which that tool is put to use by defining the criteria for the compilation of the viewing statistics. When Facebook invites a fan page administrator to create or modify the audience for his page it indicates that it will do its best to show the page to the people who matter the most to the administrator. Using filters, a fan page administrator can define a personalised audience, which enables him not only to narrow down the group of people to whom information relating to his commercial offer will be published, but also, and most importantly, to designate the categories of people whose personal data will be collected by Facebook. Thus, by defining the audience he wishes to reach, a fan page administrator will also at the same time be identifying which target public is likely to become the subject of Facebook's collection and subsequent use of personal data. In addition to triggering the processing of personal data when he creates a fan page, the administrator of that page consequently plays a predominant role in how that data is processed by Facebook. In this way he participates in the determination of the means and purposes of the data processing, by himself exerting a de facto influence over it.

58. I conclude from the foregoing that, in circumstances such as those of the dispute in the main proceedings, the administrator of a fan page on a social network such as Facebook must be regarded as being responsible for the phase of personal data processing consisting in the collection by that social network of data relating to people who visit the fan page.

59. That conclusion is corroborated by the fact that a fan page administrator such as the Wirtschaftsakademie, on the one hand, and service providers such as Facebook Inc. and Facebook Ireland, on the other, pursue closely related objectives. The Wirtschaftsakademie wishes to obtain viewing statistics for the purpose of managing the promotion of its activities, and to obtain those statistics the processing of personal data is necessary. That same data processing will also enable Facebook better to target the advertising which it publishes on its network.

60. Any interpretation that is based solely on the terms and conditions of the contract concluded by the Wirtschaftsakademie and Facebook Ireland should, therefore, be rejected. Indeed, the division of tasks indicated in the contract can only suggest the actual roles of the parties to the contract in the processing of personal data. If it were otherwise, the parties would be able artificially to assign responsibility for the data processing to one or other of themselves. That is especially true when the general terms and conditions are drawn up in advance by the social network and are not negotiable. The view cannot, therefore, be taken that a person who may do no more than accept or refuse the contract cannot be a controller. Once such a party has concluded the contract of his own volition he

may always be regarded as a controller, given his actual influence over the means and purposes of the data processing.

61. Thus, the fact that the contract and its general terms and conditions are drawn up by a service provider and that operators that have recourse to the services which the former provides do not have access to the data does not preclude the latter from being regarded as controllers once they have accepted the contractual terms, thus accepting full responsibility for them. [27] It should also be acknowledged, as does the Article 29 working party, that any imbalance in the relationship of strength between service provider and service user does not preclude the latter from being classified as a 'controller'. [28]

62. Moreover, in order for a person to be regarded as a controller within the meaning of Article 2(d) of Directive 95/46 it is not necessary for him to have complete control over all aspects of data processing. As the Belgian Government rightly observed at the hearing, complete control is becoming less and less common in practice. Ever more frequently data processing is complex, comprising several distinct processes which involve numerous parties which themselves have differing degrees of control. Consequently, any interpretation which focusses on the existence of complete control over all aspects of data processing is likely to result in serious lacunae in the protection of personal data.

63. The facts which gave rise to the judgment of 13 Mary 2014, *Google Spain and Google* [29] illustrate this point. That case concerned a situation involving multi-tiered information providers in which various parties each had a distinct influence over the data processing. The Court refused to interpret the concept of 'controller' narrowly. It considered that the operator of the search engine must, 'as the person determining the purposes and means of [its] activity [,] ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46'. [30] The Court also mentioned the possibility of responsibility being shared between the operator of the search engine and publishers of websites. [31]

64. Like the Belgian Government, I believe that a broad interpretation of the concept of 'controller', for the purposes of Article 2(d) of Directive 95/46, which

27 See, to that effect, Opinion 1/2010, p. 26.

28 Ibid., p. 28: 'the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection laws'.

29 C-131/12, EU:C:2014:317.

30 Judgment of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 38 and, to the same effect, paragraph 83).

31 Judgment of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 40).

must, in my view, prevail in the present case, is likely to prevent abuse. Absent such an interpretation, it would be sufficient for an undertaking to have recourse to the services of a third party in order to escape its obligations in the field of personal data protection. In other words, no distinction should be made, in my opinion, between an undertaking which equips its website with tools similar to those offered by Facebook and an undertaking which joins the Facebook social network so as to benefit from the tools which Facebook offers. It is therefore necessary to ensure that economic operators that have recourse to a hosting service for their website are not able to evade liability by agreeing to the general terms and conditions of a service provider. Moreover, as the Belgian Government stated at the hearing, it is not unreasonable to expect undertakings to be diligent in their choice of service provider.

65. I therefore take the view that the fact that a fan page administrator uses the platform offered by Facebook and benefits from the services associated with that platform does not absolve it from its obligations in the field of personal data protection. I would observe in this connection that, had the Wirtschaftsakademie created a website elsewhere than on Facebook and implemented a tool similar to 'Facebook Insights' in order to compile viewing statistics, it would be regarded as the controller of the processing needed to compile those statistics. In my opinion, such an economic operator should not be relieved of the obligation to observe the rules on the protection of personal data arising from Directive 95/46 for the sole reason that it uses Facebook's social networking platform to promote its activities. As the referring court itself rightly observes, an information provider is not meant to be able to absolve itself, by choosing a particular infrastructure provider, of the legal data protection obligations toward the users of its information offering that it would have had to meet if it had acted as a mere content provider. [32] Any contrary interpretation would create a risk that the rules on the protection of personal data will be circumvented.

66. In my opinion, there is also no need to draw an artificial distinction between the situation in question in the present case and that in Case C-40/17, *Fashion ID*. [33]

67. That case concerns the situation in which the manager of a website embeds in its website a programming code (in this instance, Facebook's 'Like' button) of an external provider (Facebook) which, when activated, transmits personal data from the computer of the website user to the external provider.

68. In the dispute which has given rise to that case, a consumer protection association has made a complaint against the company Fashion ID for having enabled Facebook, by embedding in its website the 'Like' function provided by

[32] Paragraph 35 of the order for reference, [paragraph 18 of the English summary of the order for reference].

[33] Pending before the Court.

the Facebook social network, to access the personal data of users of that website without their consent and in breach of the obligations to provide information laid down in the provisions on the protection of personal data. Thus, the issue arises of whether the fact that Fashion ID enables Facebook to access the personal data of users of its website means that that company may be classified as a 'controller' within the meaning of Article 2(d) of Directive 95/46.

69. I fail to see any fundamental difference between the position of a fan page administrator and that of the operator of a website that embeds in its website a programming code of a provider of web tracking services, thus enabling the transmission of data, the downloading of cookies and the collection of data for the benefit of the provider of the web tracking services all without the knowledge of the Internet user.

70. Social plugins enable website operators to use certain social networking services on their own websites in order to increase their website's visibility, for example by embedding in their websites Facebook's 'Like' button. Like fan page administrators, operators of websites with embedded social plugins can benefit from the 'Facebook Insights' service and obtain precise statistical information about the users of their website.

71. As happens when a fan page is visited, visiting a website that contains a social plugin will trigger the transmission of personal data to the provider in question.

72. In my opinion, in such circumstances, like the administrator of a fan page, the manager of a website that contains a social plugin should, to the extent that it has a de facto influence over the phase of data processing which involves the transmission of personal data to Facebook, be classified as a 'controller' within the meaning of Article 2(d) of Directive 95/46. [34]

73. I would add that, as the Belgian Government rightly observes, the fact that the Wirtschaftsakademie acts as joint controller in so far as it decides to have recourse to Facebook's services for its information offering in no way relieves Facebook Inc. or Facebook Ireland of their obligations as controllers. Indeed, it is clear that those two entities have a decisive influence over the purposes and means of the processing of personal data which occurs when a fan page is visited and that they also use that data for their own purposes and interests.

[34] As the Swiss data protection authority notes, 'although the recording and analysis, in the strict sense, of data are in most cases carried out discretely by providers of web tracking services, website operators have equal responsibility. They embed the code of the web tracking services provider in their websites and thus enable the transmission of data, the downloading of cookies and the collection of data for the benefit of the provider of the web tracking services all without the knowledge of the Internet user' see 'Explications concernant le webtracking' of the Préposé fédéral à la protection des données et à la transparence (PFPDT) (Federal Data Protection and Transparency Commissioner, Switzerland) at the following Internet address: https://www.edoeb.admin.ch/datenschutz/00683/01103/01104/index.html?lang=fr.

74. However, recognising that fan page administrators share responsibility for the phase of the data processing which consists in the collection by Facebook of personal data will help ensure greater protection of the rights of those who visit that type of page. Moreover, actively involving fan page administrators in the observance of the rules on the protection of personal data by designating them as controllers is likely to have the ripple effect of encouraging the social networking platform itself to comply with those rules.

75. I should also clarify that the existence of shared responsibility does not imply equal responsibility. On the contrary, the various controllers may be involved in the processing of personal data at different stages and to differing degrees. [35]

76. According to the Article 29 working party, 'the possibility of *pluralistic control* caters for the increasing number of situations where different parties act as controllers. The assessment of this joint control should mirror the assessment of "single" control, by taking a substantive and functional approach and focussing on whether the purposes and the essential elements of the means are determined by more than one party. The participation of parties in the determination of purposes and means of processing in the context of joint control may take different forms and does not need to be equally shared'. [36] Indeed, 'in [the] case of plurality of actors, they may have a very close relationship (sharing, for example, all purposes and means of a processing) or a more loose relationship (for example, sharing only purposes or means, or a part thereof). Therefore, a broad variety of typologies for joint control should be considered and their legal consequences assessed, allowing some flexibility in order to cater for the increasing complexity of current data processing reality'. [37]

77. It follows from the foregoing, in my opinion, that the administrator of a fan page on the Facebook social network must be regarded as being, along with Facebook Inc. and Facebook Ireland, a controller of the processing of personal data that is carried out for the purpose of compiling viewing statistics for that fan page.

## B. The third and fourth questions

78. By its third and fourth questions, which it is appropriate, in my opinion, to examine together, the referring court seeks clarification from the Court on the interpretation of Articles 4(1)(a) and 28(1), (3) and (6) of Directive 95/46 in the situation where a parent company established outside the European Union, such as Facebook Inc., provides social network services in the territory of the European

35 See, to that effect, Opinion 1/2010, p. 24.

36 Opinion 1/2010, pp. 32 and 33.

37 Opinion 1/2010, p. 19.

Union through the intermediary of several establishments. One of those establishments, (Facebook Ireland) has been designated by the parent company as the controller of personal data processing in the European Union and the other is responsible for the promotion and sale of advertising space and other marketing measures directed toward residents in Germany (Facebook Germany). The referring court wishes to know, first, whether the German supervisory authority is entitled in such circumstances to exercise its powers of intervention with a view to stopping the personal data processing at issue and, secondly, against which establishment such powers may be exercised.

79. I would point out, in response to the doubts expressed by ULD and the Italian Government regarding the admissibility of the third and fourth questions, that the Bundesverwaltungsgericht (Federal Administrative Court) explains in its order for reference that it needs clarification on these points so that it may rule on the lawfulness of the order at issue in the main proceedings. In particular, the referring court points out that the order issued against the Wirtschaftsakademie might be the result of an error of assessment, and consequently unlawful, if the infringement of the applicable right to the protection of data which ULD alleges could be remedied by means of a measure addressed directly to the subsidiary, Facebook Germany, established in Germany. [38] That observation of the referring court clearly indicates, in my opinion, the reasons for which it has referred the third and fourth questions to the Court. Given the presumption of relevance which applies to requests for a preliminary ruling, [39] I propose that the Court answer these questions.

80. Article 4 of the directive, entitled ‘National law applicable’, is worded as follows:

‘1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

… ’

38 See paragraph 40 of the order for reference, [paragraph 22 of the English summary of the order for reference].

39 See, inter alia, the judgment of 31 January 2017, *Lounani* (C-573/14, EU:C:2017:71, paragraph 56 and the case-law cited).

81. In Opinion 8/2010 of 16 December 2010 on applicable law, [40] the Article 29 working party discussed the application of Article 4(1)(a) of Directive 95/46 in the following situation: 'A social network platform has its headquarters in a third country and an establishment in a Member State. The establishment defines and implements the policies relating to the processing of personal data of EU residents. The social network actively targets residents of all EU Member States, which constitute a significant portion of its customers and revenues. It also installs cookies on EU users' computers. In this case, the applicable law will be, pursuant to Article 4(1)(a) [of Directive 95/46], the data protection law of the Member State where the company is established within the [Union]. The issue of whether the social network makes use of equipment located in other Member States' territory is irrelevant, since all processing takes place in the context of the activities of the single establishment and the directive excludes the cumulative application of Articles 4(1)(a) and 4(1)(c).' [41] The Article 29 working party went on to state that 'the supervisory authority of the Member State where the social network is established in the EU will — pursuant to Article 28(6) [of Directive 95/46] — have a duty to cooperate with other supervisory authorities, in order for example to deal with requests or complaints coming from residents of other EU countries'. [42]

82. The example set out in point 81 above poses no difficulty for the determination of the applicable national law. Indeed, in such a case, since the parent company has only one establishment within the European Union, it is the law of the Member State in which that establishment is located that applies to the processing of personal data in question.

83. The situation becomes more complex where, as in the present case, a company established in a third country, such as Facebook Inc., conducts its business in the Union through the intermediary of an establishment designated by the parent company as having sole responsibility within the group for the collection and processing of personal data throughout the territory of the Union (Facebook Ireland) as well as through the intermediary of other establishments, one of which is located in Germany (Facebook Germany) and, according to the information in the order for reference, is responsible for the promotion and sale of advertising space and other marketing measures directed toward residents in that Member State. [43]

40 'Opinion 8/2010'.

41 Opinion 8/2010, p. 31.

42 Opinion 8/2010, p. 32.

43 The structures which groups like Google and Facebook adopt for conducting their business throughout the world makes it difficult to determine which national law applies and to identify the establishment against which individuals that have suffered harm and supervisory authorities may take action. See, on these point, Svantesson D., 'Enforcing Privacy Across Different Jurisdictions', in *Enforcing Privacy – Regulatory, Legal and Technological Approaches*, Springer, Berlin, 2016, pp. 195 to 222, especially pp. 216 to 218.

84. In such a situation, is the German supervisory authority entitled to exercise its powers of intervention, with a view to bringing to an end the processing of personal data for which Facebook Inc. and Facebook Ireland are jointly responsible?

85. In order to answer that question, it is necessary to determine whether the German supervisory authority has the right to apply its own national law to the data processing in question.

86. It follows from Article 4(1)(a) of Directive 95/46 that data processing carried out in the context of the activities of an establishment is governed by the law of the Member State on whose territory that establishment is located.

87. The Court has already held that, in light of the objective pursued by the directive, which consists in ensuring 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, the words 'in the context of the activities of an establishment' set out in Article 4(1)(a) of the directive cannot be interpreted restrictively. [44]

88. The applicability of a transposition law of a Member State to the processing of personal data requires two conditions to be met. First, the controller must have an 'establishment' in that Member State. Secondly, the processing must be carried out 'in the context of the activities' of that establishment.

89. As regards, first of all, the concept of 'establishment' within the meaning of Article 4(1)(a) of Directive 95/46, the Court has already given that concept a broad, flexible interpretation, holding that it extends to any real and effective activity, even a minimal one, exercised through stable arrangements, [45] thus excluding any formalistic approach. [46]

90. With this in view, both the degree of stability of the arrangements and the effective exercise of activities in the Member State in question must be assessed, [47] with account being taken of the specific nature of the economic activities and the provision of services concerned. [48] In this connection, it is not disputed that Facebook Germany, whose registered office is in Hamburg (Germany), effectively and really carries on an activity through stable

44 See, in particular, the judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 25 and the case-law cited).

45 See, in particular, the judgment of 28 July 2016, *Verein für Konsumenteninformation* (C-191/15, EU:C:2016:612, paragraph 75 and the case-law cited).

46 See the judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 29).

47 See, in particular, the judgment of 28 July 2016, *Verein für Konsumenteninformation* (C-191/15, EU:C:2016:612, paragraph 77 and the case-law cited).

48 See the judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 29).

arrangements in Germany. It is, therefore, an establishment within the meaning of Article 4(1)(a) of Directive 95/46.

91. Secondly, as regards the question whether the processing of personal data in question is carried out 'in the context of the activities' of that establishment, within the meaning of Article 4(1)(a) of Directive 95/46, the Court has already pointed out that that provision requires the processing of personal data in question to be carried out not 'by' the establishment concerned itself but only 'in the context of the activities' of the establishment. [49]

92. As is clear from Opinion 8/2010, 'the notion of "context of activities" — and not the location of the data — is a determining factor in identifying the … applicable law. The notion of "context of activities" implies that the applicable law is … the law of the Member State [not] where the controller is established, but where an establishment of the controller is involved in activities implying the processing of personal data. In this context, the degree of involvement of the establishment(s) in the activities in the context of which personal data is processed is crucial. In addition, the nature of the activities of the establishments and the need to guarantee effective protection of individuals' rights should be considered. A functional approach should be taken in the analysis of these criteria: more than the theoretical indication by the parties of the law applicable, it is their practical behaviour and interaction which should be decisive.' [50]

93. In its judgment of 13 May 2014, *Google Spain and Google*, [51] it was necessary for the Court to check compliance with this condition. It adopted a broad interpretation, holding that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if it is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that search engine profitable. [52] The Court pointed out that, 'in such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed'. [53] The Court added, in support of its solution, that since the display of personal data on a search results page 'is accompanied, on

49 See, in particular, the judgment of 28 July 2016, *Verein für Konsumenteninformation* (C-191/15, EU:C:2016:612, paragraph 78 and the case-law cited).

50 Opinion 8/2010, p. 33. See also, to that effect, p. 15 of the Opinion.

51 C-131/12, EU:C:2014:317.

52 Paragraph 55 of the judgment.

53 Paragraph 56 of the judgment.

the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory'. [54]

94. According to the information contained in the order for reference, Facebook Germany is responsible for the promotion and sale of advertising space and other marketing activities directed toward residents in the Federal Republic of Germany. Given that the processing of personal data at issue in the main proceedings, which consists in the collection of personal data by means of cookies installed on the computers of visitors to fan pages, is specifically intended to enable Facebook better to target the advertisements which it publishes, that data processing must be regarded as taking place in the context of the activities in which Facebook Germany engages in Germany. Given that social networks such as Facebook generate much of their revenue from advertisements posted on the web pages set up and accessed by users, [55] it must be concluded that the activities of the joint controllers Facebook Inc. and Facebook Ireland are indissolubly linked to those of an establishment such as Facebook Germany. Moreover, following the processing of personal data which is made possible by the installation of cookies on the computers of people visiting pages belonging to the domain name Facebook.com, visiting a Facebook page will cause to be displayed on that page advertisements relating to the visitor's centres of interest. It must be inferred from that that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance German territory.

95. The fact that, by contrast with the situation in the case which gave rise to the judgment of 13 May 2014, *Google Spain and Google*, [56] the Facebook group has a European head office, in Ireland, does not mean that the interpretation of Article 4(1)(a) of Directive 95/46 which the Court adopted in that judgment cannot be applied in the present case. In that judgment, the Court voiced the intention that the processing of personal data should not escape the obligations and guarantees laid down by Directive 95/46. It has been suggested in the present proceedings that the problem of such circumvention does not arise here, because the controller is established in a Member State, namely Ireland. According to that logic, Article 4(1)(a) of Directive 95/46 should be interpreted as requiring that controller to have regard to the legislation of only one Member State and to answer to only one supervisory authority, that is to say, Irish legislation and the Irish authority.

54 Paragraph 57 of the judgment.

55 See, to that effect, Opinion 5/2009 of 12 June 2009 on on-line social networks of the Article 29 working group, p. 5.

56 C-131/12, EU:C:2014:317.

96. Such an interpretation, however, is contrary to the wording of Article 4(1)(a) of Directive 95/46 as well as to the origins of that provision. Indeed, as the Belgian Government rightly observed at the hearing, the directive does not introduce a one-stop-shop mechanism or a country-of-origin principle. [57] Care should be taken not to confuse aspects of the policy objectives pursued by the European Commission in its proposal for the directive and the solution ultimately adopted by the Council of the European Union. In Directive 95/46, the legislature made a choice not to give priority to the application of the national law of the Member State in which the controller's principal establishment is located. The result, arrived at in Directive 95/46, reflects the wishes of the Member States to preserve their national powers of enforcement. By not adopting the country-of-origin principle, the EU legislature enabled each Member State to apply its own national legislation and thus made the application of multiple national legislations possible. [58]

97. With Article 4(1)(a) of that directive, the EU legislature deliberately chose the allow, in cases where a controller has several establishments within the European Union, the application of multiple national legislative systems for the protection of personal data to the processing of the personal data of residents in the Member States concerned, so as to ensure effective protection of their rights in those Member States.

98. That is confirmed by recital 19 of Directive 95/46, which states that, 'when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities'.

99. I therefore infer from Article 4(1)(a) of Directive 95/46 — the second clause of which provides, in accordance with what is stated in recital 19 of the directive, that, when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of those establishments complies with the obligations laid down by the national law applicable — that group structures which are characterised by the presence of establishments of the controller in several Member States must not have the effect of enabling the controller to circumvent the laws of the Member States within whose jurisdiction each of those establishments is established.

57 See, in particular, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in *Google Spain*' by the Article 29 working party, 16 December 2015, pp. 6 and 7.

58 As regards the possible application of the laws of several Member States, see Opinion 8/2010: 'the reference to "an" establishment means that the applicability of a Member State's law will be triggered by the location of an establishment of the controller in that Member State, and other Member States' laws could be triggered by the location of other establishments of that controller in those Member States' (p. 29).

100. I would add that any interpretation which favours the exclusive application of the law of the Member State in which the European head office of an international group is located can no longer be supported, in my opinion, following the judgment of 28 July 2016, *Verein für Konsumenteninformation*. [59] In that judgment, the Court decided that the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment located in that Member State. The Court came to that decision despite the fact that Amazon, like Facebook, is an undertaking that has not only a European head office in a Member State, but also a physical presence in a number of Member States. In such a situation, it is again necessary to consider whether the data processing is carried out within the framework of the activities of an establishment located in a Member State other than that in which the controller's European head office is located.

101. As the Belgian Government points out, it is therefore perfectly possible for an establishment other than an undertaking's European head office to be relevant to the application of Article 4(1)(a) of Directive 95/46.

102. Under the system established by the directive, where a controller has several establishments within the European Union, neither the place where the data processing is carried out nor the place where the controller has established its head office in the European Union is decisive in identifying the national law which applies to data processing or in entitling a supervisory authority to exercise its powers of intervention.

103. In this connection, the Court should not, in my opinion, pre-empt the scheme established by the general regulation on data protection [60] which will apply from 25 May 2018 onwards. As part of that scheme a one-stop-shop mechanism is instituted. This means that a controller that carries out cross-border data processing, such as Facebook, will have only one supervisory authority as interlocutor, namely the lead supervisory authority, which will be the authority for the place where the controller's main establishment is located. Nevertheless, that scheme, and the sophisticated cooperation mechanism which it introduces, are not yet applicable.

104. Admittedly, in that Facebook has chosen to set up its main establishment in the European Union in Ireland, the supervisory authority of that Member State will have an important role to play in checking whether Facebook is observing the rules arising from Directive 95/46. Be that as it may, as that authority itself has acknowledged, this does not mean that, under the present system based on that

[59] C-191/15, EU:C:2016:612.

[60] 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 (OJ 2016 L 119, p. 1).

directive, it has sole competence with regard to Facebook's activities within the European Union. [61]

105. All of the foregoing matters lead me to consider, as do the Belgian Government, the Netherlands Government and ULD, that the interpretation of Article 4(1)(a) of Directive 95/46 which the Court adopted in its judgment of 13 May 2014, *Google Spain and Google* [62] is equally applicable in a situation, like that in the main proceedings, where a controller is established in one Member State and has several establishments within the European Union.

106. Therefore, on the basis of the information provided by the referring court regarding the nature of the activities carried out by Facebook Germany, it must be concluded that the processing of personal data at issue is carried out in the context of the activities of that establishment and that Article 4(1)(a) of Directive 95/46 permits the application of German law on the protection of personal data in a situation such as that in the main proceedings. [63]

107. The German supervisory authority does, therefore, have power to apply its own national law to the processing of personal data at issue in the main proceedings.

108. It follows from Article 28(1) of the directive that each supervisory authority established by a Member State is to ensure compliance, within the

61 See, on this point, Hawkes B., 'The Irish DPA and Its Approach to Data Protection', in *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Springer, Berlin, 2016, pp. 441 to 454, especially p. 450, footnote 11. The author states that 'the degree to which, under existing EU law, other European DPAs can assert jurisdiction over entities such as Facebook Ireland is not entirely clear, linked as it is to interpretations of Article 4 of Directive 95/46/EC, notably the phrase "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State". The DPC, in its audit report, stated that "it ha(d) jurisdiction over the personal data processing activities of [Facebook Ireland] based on it being established in Ireland" but that this "should not however be interpreted as asserted sole jurisdiction over the activities of Facebook in the EU."'

62 C-131/12, EU:C:2014:317.

63 See, following similar logic, Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands, France, Spain, Hamburg and Belgium, 16 May 2017, in which those authorities stated the following: '... the DPAs united in the Contact Group conclude that their respective national data protection law applies to the processing of personal data of users and non-users by the Facebook Group in their respective countries and that each DPA has competence. Following case-law from the European Court of Justice ..., the DPAs note that the Facebook Group has offices in multiple countries in the EU. These offices aim to promote and increase the sales of targeted advertising aimed at national users and non-users of the service. For its revenues, the Facebook Group almost completely depends on the sale of advertising space, and personal data must necessarily be processed for the type of targeted advertising services offered by the Facebook Group. Therefore, the activities of these offices are "inextricably linked" to the data processing by the Facebook Group, and all the investigated national offices are relevant establishments under Article 4(1)(a) of the European Data Protection Directive 95/46/EC.'

territory of that Member State, with the provisions adopted by the Member States pursuant to Directive 95/46.

109. Pursuant to Article 28(3) of Directive 95/46, those supervisory authorities are in particular to be endowed with investigative powers, such as powers to collect all the information necessary for the performance of their supervisory duties, and effective powers of intervention, such as powers of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, or of warning or admonishing the data controller. Those powers of intervention may include the power to penalise the data controller by imposing a fine. [64]

110. Furthermore, Article 28(6) of Directive 95/46 is drafted as follows:

'Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.'

111. Given that the law of the Member State to which the German supervisory authority belongs is applicable to the processing of personal data at issue in the main proceedings, that authority is in a position to exercise all its powers of intervention in order to ensure that German law is applied and observed by Facebook on German territory. That conclusion follows from the judgment of 1 October 2015, *Weltimmo*, [65] which clarified the scope of Article 28(1), (3) and (6) of Directive 95/46.

112. The principal issue in that case was determining whether the Hungarian supervisory authority had power to impose a fine on a service provider established in another Member State, namely Slovakia. In order to determine that, it was necessary first to examine the question of whether, by applying the criterion laid down in Article 4(1)(a) of Directive 95/46, Hungarian law was applicable.

113. In the first part of its answer, the Court of Justice provided the referring court with information enabling the latter to establish the existence of an establishment of the controller in Hungary. It also considered that the processing of personal data at issue was carried out 'in the context of the activities' of that establishment and that, in accordance with Article 4(1)(a) of Directive 95/46, Hungarian law on the protection of personal data could, in a situation such as that at issue in the main proceedings, be applied.

64 See the judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 49).

65 C-230/14, EU:C:2015:639.

114. The first part of the Court's answer therefore tended to confirm the competence of the Hungarian supervisory authority to impose, pursuant to Hungarian law, a fine on a service provider established in another Member State, in that instance Weltimmo.

115. In other words, if Hungarian law could be recognised as the applicable national law, by application of the criterion set out in Article 4(1)(a) of Directive 95/46, the Hungarian supervisory authority would have power to ensure compliance with Hungarian law in the event of its infringement by a controller, even one established in Slovakia. As a result of the effect of that provision of the directive, it could be concluded that, even though registered in Slovakia, Weltimmo was also established in Hungary. The presence in Hungary of an establishment of the controller which performed activities in the context of which the data processing was carried out constituted the trigger for recognising the applicability of Hungarian law and, as a corollary, the competence of the Hungarian supervisory authority to ensure compliance with that law on Hungarian territory.

116. The second part of the Court's answer, in which it highlighted the principle of the territorial application of the powers of each supervisory authority, was given only in the alternative, that is to say, 'in the event that the Hungarian data protection authority should consider that Weltimmo [had], not in Hungary but in another Member State, an establishment, within the meaning of Article 4(1)(a) of Directive 95/46, performing activities in the context of which the processing of the personal data concerned [was] carried out'. [66] This was therefore the answer to the question whether, 'should the Hungarian data protection authority reach the conclusion that the law applicable to the processing of the personal data is not Hungarian law, but the law of another Member State, Article 28(1), (3) and (6) of Directive 95/46 should be interpreted as meaning that that authority would be able to exercise only the powers provided for by Article 28(3) of that directive, in accordance with the law of that other Member State, and would not be able to impose penalties'. [67]

117. Consequently, in this second part of its answer, the Court clarified both the scope *ratione materiae* and the territorial scope of the powers which a supervisory authority may exercise in a particular situation, one in which the law of the Member State to which the supervisory authority belongs is not applicable.

118. The Court considered that, in such a situation, 'the powers of that authority do not necessarily include all of the powers conferred on it in accordance with the law of its own Member State'. [68] Accordingly, 'that authority may exercise its investigative powers irrespective of the applicable law and before even knowing

66 See the judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 42).

67 See the judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 43).

68 See the judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 55).

which national law is applicable to the processing in question. However, if it reaches the conclusion that the law of another Member State is applicable, it cannot impose penalties outside the territory of its own Member State. In such a situation, it must, in fulfilment of the duty of cooperation laid down in Article 28(6) of [Directive 95/46], request the supervisory authority of that other Member State to establish an infringement of that law and to impose penalties if that law permits, based, where necessary, on the information which the authority of the first Member State has transmitted to the authority of that other Member State.' [69]

119. I draw from the judgment of 1 October 2015, *Weltimmo* [70] the following guidance for the present case.

120. By contrast with the hypothesis on the basis of which the Court set out its reasoning regarding the powers of the supervisory authorities in the second part of its judgment of 1 October 2015, *Weltimmo*, [71] the present case concerns the situation, similar to that addressed in the first part of that judgment, where, as I have already mentioned, the applicable national law is indeed that of the Member State of the supervisory authority which exercises its powers of intervention, as a result of the presence in the territory of that Member State of an establishment of the controller whose activities are indissolubly linked to that data processing. The presence in Germany of that establishment constitutes the trigger for the applicability of German law to the processing of personal data at issue.

121. Once that condition is fulfilled, the Germany supervisory authority must be recognised as having power to ensure compliance, on German territory, with the rules on the protection of personal data, exercising all of the powers conferred on it by the provisions of German law transposing Article 28(3) of Directive 95/46. Those powers may include orders prohibiting data processing temporarily or definitively.

122. As regards the question of which entity should be the addressee of such a measure, two solutions seem possible.

123. The first solution is to construe the territorial scope of the powers of intervention of the supervisory authorities narrowly and to take the view that the latter may exercise those powers only against an establishment of the controller that is located on the territory of the Member State to which they belong. If, as in the present case, that establishment (Facebook Germany in this instance) is not the controller, and is therefore not able itself to comply with a request from a supervisory authority to bring data processing to an end, it must relay that request to the controller, so that it may execute it.

69 See the judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 57).

70 C-230/14, EU:C:2015:639.

71 C-230/14, EU:C:2015:639.

124. The second solution, on the other hand, is to take the view that, since the controller is the only entity that exerts a decisive influence on the data processing at issue, it is to the controller that any measure requiring data processing to be stopped should be addressed.

125. In my opinion, the second solution should prevail, since it is consistent with the fundamental role which controllers occupy within the system put in place by Directive 95/46. [72] Since it averts the necessity of going through the intermediary that is the establishment which carries out activities in the context of which the data processing in question is performed, this solution is likely to ensure the immediate and effective application of national rules on the protection of personal data. Moreover, a supervisory authority which addresses a measure requiring data processing to be stopped directly to a controller that is not established on the territory of the Member State to which it belongs, such as Facebook Inc. or Facebook Ireland, is not overstepping its powers, which are to ensure that data processing complies with the law of that Member State on the territory of that Member State. It is irrelevant, in this regard, whether the controller or controllers are established in another Member State or in a third country.

126. I would also state, with reference to the answer which I suggest for the first and second questions referred for a preliminary ruling, that, given the objective of ensuring the fullest possible protection of the rights of people who visit fan pages, the fact that ULD may exercise its powers of intervention against Facebook Inc. and Facebook Ireland in no way prevents it, in my view, from taking measures against the Wirtschaftsakademie and cannot therefore, as such, affect the legality of such measures. [73]

127. It follows from the foregoing that Article 4(1)(a) of Directive 95/46 should be interpreted as meaning that processing of personal data such as that at issue in the main proceedings is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when an undertaking operating a social network sets up in that Member State a subsidiary which is intended to promote and sell advertising space offered by that undertaking and which directs its activities toward residents in that Member State.

128. In addition, in a situation such as that at issue in the main proceedings, in which the national law which applies to the processing of personal data in question is that of the Member State to which a supervisory authority belongs, Article 28(1), (3) and (6) of Directive 95/46 should be interpreted as meaning that that supervisory authority may exercise of all the effective powers of intervention conferred on it in accordance with Article 28(3) of the directive against the

72 See, in this regard, point 44 of this Opinion.

73 See also points 73 to 77 of this Opinion.

controller, including where that controller is established in another Member State or even in a third country.

## C. The fifth and sixth questions

129. By its fifth and questions, which it is appropriate, in my opinion, to examine together, the referring court is essentially asking the Court to rule whether Article 28(1), (3) and (6) of Directive 95/46 must be interpreted as meaning that, in circumstances such as those in the main proceedings, the supervisory authority of the Member State in which the establishment of the controller (Facebook Germany) is located is entitled to exercise its powers of intervention autonomously and without being required first to call on the supervisory authority of the Member State in which the controller (Facebook Ireland) is located to exercise its powers.

130. In its order for reference, the Bundesverwaltungsgericht (Federal Administrative Court) explains the connection between these two questions and the review of the lawfulness of the injunctive order which it must conduct in the main proceedings. It states, in substance, that issuing an injunctive order against the Wirtschaftsakademie could be regarded as an error of assessment on ULD's part if Article 28(6) of Directive 95/46 is to be interpreted as laying down an obligation for a supervisory authority such as ULD, in circumstances such as those in the main proceedings, to request the supervisory authority of another Member State, in this instance the Data Protection Commissioner, to exercise its powers in the event that the assessments of the two supervisory authorities diverge as to whether the data processing carried out by Facebook Ireland is consistent with the rules derived from Directive 95/46.

131. As the Court held in its judgment of 1 October 2015, *Weltimmo*, [74] if the law applicable to the processing of personal data in question is not the law of the Member State of the supervisory authority that wishes to exercise its powers of intervention, but the law of another Member State, Article 28(1), (3) and (6) must be interpreted as meaning that that authority cannot impose penalties on the basis of the law of its own Member State on a controller that is not established on the territory of that Member State, but should, in accordance with Article 28(6) of the directive, request the supervisory authority of the Member State whose law is applicable to act. [75]

132. In such a situation, the supervisory authority of the first Member State loses its entitlement to exercise its power to impose penalties on a controller established in another Member State. It must then, in fulfilment of the duty of cooperation laid down in Article 28(6) of Directive 95/46, request the supervisory authority of the other Member State to establish an infringement of the law of that Member State

74 C-230/14, EU:C:2015:639.

75 Judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 60).

and to impose penalties if that law permits, based, where necessary, on the information which the authority of the first Member State has transmitted to the authority of that other Member State. [76]

133. As I have already indicated, the situation in the present case is quite different, inasmuch as the applicable law is that of the Member State of the supervisory authority that wishes to exercise its powers of intervention. In this situation, Article 28(6) of Directive 95/46 should be interpreted as not requiring the supervisory authority to request the supervisory authority of the Member State in which the controller is established to exercise its powers of intervention against that controller.

134. I would add that, in accordance with the second [subparagraph] of Article 28(1) of Directive 95/46, a supervisory authority that is entitled to exercise its powers of intervention against a controller established in a Member State other than its own must act with complete independence in exercising the functions entrusted to it.

135. As I have already made clear, Directive 95/46 does not provide for a country-of-origin principle or for a one-stop-shop mechanism of the kind that appears in Regulation No 2016/679. A controller which has establishments in several Member States is, consequently, fully subject to the supervision of several supervisory authorities if the laws of the Member States to which those authorities belong are applicable. While consultation and cooperation among those supervisory authorities is obviously desirable, there is nothing to oblige one supervisory authority whose competence is recognised to align its position with the position adopted by another supervisory authority.

136. I conclude from the foregoing that Article 28(1), (3) and (6) of Directive 95/46 should be interpreted as meaning that, in circumstances such as those in the main proceedings, the supervisory authority of the Member State in which the establishment of the controller is located is entitled to exercise its powers of intervention against that controller autonomously and without being required first to call on the supervisory authority of the Member State in which the controller is located to exercise its powers.

## III. Conclusion

137. Having regard to the foregoing considerations, I propose that the Court answer the questions referred by the Bundesverwaltungsgericht (Federal Administrative Court, Germany) as follows:

(1) Article 2(d) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to

[76] Judgment of 1 October 2015, *Weltimmo* (C-230/14, EU:C:2015:639, paragraph 57).

the processing of personal data and on the free movement of such data, as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 is to be interpreted as meaning that the administrator of a fan page on a social network such as Facebook must be regarded as being a controller, within the meaning of that provision, in so far as concerns the phase of personal data processing consisting in the collection by that social network of data relating to people who visit the fan page for the purpose of compiling viewing statistics for that fan page.

(2) Article 4(1)(a) of Directive 95/46, as amended by Regulation No 1882/2003, is to be interpreted as meaning that processing of personal data such as that at issue in the main proceedings is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when an undertaking operating a social network sets up in that Member State a subsidiary which is intended to promote and sell advertising space offered by that undertaking and which directs its activities toward residents in that Member State.

(3) In a situation such as that at issue in the main proceedings, in which the national law which applies to the processing of personal data in question is that of the Member State to which a supervisory authority belongs, Article 28(1), (3) and (6) of Directive 95/46, as amended by Regulation No 1882/2003, is to be interpreted as meaning that that supervisory authority may exercise of all the effective powers of intervention conferred on it in accordance with Article 28(3) of the directive against the controller, including where that controller is established in another Member State or even in a third country.

(4) Article 28(1), (3) and (6) of Directive 95/46, as amended by Regulation No 1882/2003, is to be interpreted as meaning that, in circumstances such as those in the main proceedings, the supervisory authority of the Member State in which the establishment of the controller is located is entitled to exercise its powers of intervention against that controller autonomously and without being required first to call on the supervisory authority of the Member State in which the controller is located to exercise its powers.