Reports of Cases

OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 15 December 2022[1]

Case C-579/21

J.M.
intervener:
Apulaistietosuojavaltuutettu,
Pankki S

(Request for a preliminary ruling from the Itä-Suomen hallinto-oikeus (Administrative Court of Eastern Finland, Finland))

(Reference for a preliminary ruling – Processing of personal data – Regulation (EU) 2016/679 – User log data – Right of access – Definition of personal data – Definition of recipient – Personnel in the department responsible for processing)

1. An employee who was also a customer of a financial institution requested the latter to tell him the identity of the persons who had consulted his personal data in the context of an internal investigation. Following the refusal of the institution to provide him with that information, the applicant used the appropriate means of appeal which ultimately led to him bringing an action before the Itä-Suomen hallinto-oikeus (Administrative Court of Eastern Finland, Finland).

2. That court has made a reference to the Court of Justice for a preliminary ruling on the interpretation of Regulation (EU) 2016/679.[2] In answering the questions referred, the Court of Justice will have to rule on the right of the data subject to access certain information relating to the processing of his or her personal data.

[1] Original language: Spanish.

[2] Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119 p. 1, 'the GDPR').

I. Legislative framework

A. European Union law. The GDPR

3. Recital 11 states:

'Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.'

4. Article 4, entitled 'Definitions', states:

'For the purpose of this Regulation, the following definitions shall apply:

(1) "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

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

…

(9) "recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. …'

5. Article 15, entitled 'Right of access of the data subject', provides in paragraph 1 thereof:

'The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.'

6. According to Article 24, entitled, 'Responsibility of the controller', paragraph 1 thereof states:

'Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.'

7. According to Article 25, headed 'Data protection by design and by default', paragraph 2 thereof provides:

'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.'

8. Article 29, entitled 'Processing under the authority of the controller and processor', states:

'The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law'.

9. Article 30, entitled 'Records of processing activities', provides:

'1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

…

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 30(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data … Or personal data relating to criminal convictions and offences …'

10. According to Article 58, entitled 'Powers', paragraph 1 thereof states:

'Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

…'

B. National law

1. Tietosuojalaki (1050/2018) [3]

11. According to Paragraph 30, the provisions concerning the processing of employees' personal data, the tests and checks to be carried out on employees, the requirements to be met for that purpose, as well as those concerning technical surveillance at the workplace and access to and opening of an employee's emails are laid down in the Laki yksityisyyden suojasta työelämässä (759/2004). [4]

12. Under Paragraph 34(1), the data subject does not have a right of access to the data collected concerning him or her within the meaning of Article 15 of the GDPR, in so far as:

(1) the provision of the data is likely to endanger national security, defence, public security and public policy or the prevention and investigation of criminal offences;

(2) the provision of the data could pose a serious risk to the health or care of the data subject or to the rights of the data subject or a third party; or

(3) the personal data are used in supervisory and control activities and the withholding of the data is necessary for the protection of an important economic or financial interest of Finland or the European Union.

13. Pursuant to Paragraph 34(2), where only part of the data referred to in subparagraph 1 is not covered by the right laid down in Article 15 of the GDPR, the data subject is to have the right of access to all other data relating to him or her.

14. According to Paragraph 34(3), the data subject must be informed of the reasons for the restriction, unless that would undermine the purpose thereof.

15. Pursuant to Paragraph 34(4), upon request of the data subject, the data referred to in Paragraph 15(1) of the GDPR must be made available to the Data Protection Supervisor, where the data subject has no right of access to the data collected in respect of him or her.

2. Laki yksityisyyden suojasta työelämässä (759/2004)

16. According to Section 2, Paragraph 4(2), the employer is obliged to inform the employee in advance of the collection of the data used to assess his or her reliability. When verifying the worker's creditworthiness, the employer must also inform him or her of the records from which the financial information was obtained. Where data relating to the employee have been obtained from a person other than the employee him or herself, the employer must communicate the data obtained to the employee before using them to take decisions affecting the employee. The obligations of the controller to make data available to the data subject, as well as the data subject's right of access to the data, are regulated in Chapter III of the GDPR.

[3] Law on data protection. According to Paragraph 1 thereof, that law extends and supplements the GDPR.

[4] Law on the protection of privacy in working life.

II. Facts, proceedings and the questions referred for a preliminary ruling

17. In 2014, J. M. discovered that his personal data as a customer of the financial institution Suur-Savon Osuuspankki ('the Bank') had been consulted between 1 November and 31 December 2013. During that period, in addition to being a customer, J. M. was an employee of the Bank.

18. On 29 May 2018, suspecting that the reasons for the consultation had not been entirely lawful, J. M. asked the Bank to provide information as to the identity of the employees who had accessed his data in the aforementioned period and the purposes of the processing.

19. In the meantime, the Bank had dismissed J. M., who justified his request, in particular, clarification of the reasons for his dismissal.

20. On 30 August 2018, the Bank, in its capacity as controller, refused to provide J. M. with the names of the employees who had processed his personal data. It argued that the right under Article 15 of the GDPR does not apply to log data of the Bank's data processing system recording which employees have had access to the computer system containing customer data and at what time. Moreover, the information requested would relate to personal data of those employees, not of J. M.

21. In order to avoid misunderstandings, the Bank provided the further explanations to J. M. set out below:

– In 2014, the Bank's internal audit department had investigated J. M.'s customer data for the period from 1 November to 31 December 2013.

– Those investigations were linked to the processing of the data of another of the Bank's clients, from which it would appear that the latter had a connection with J. M. that could give rise to a conflict of interest. The aim of the processing was therefore to clarify that situation [5].

22. J. M. referred the matter to the national supervisory authority (Office of the Data Protection Supervisor, Finland), requesting that the Bank be ordered to hand over the information concerned.

23. On 4 August 2020, the Assistant Data Protection Supervisor rejected J. M.'s complaint.

24. J. M. brought an action before the Itä-Suomen hallinto-oikeus (Administrative Court of Eastern Finland), arguing that, on the basis of the GDPR, he is entitled to access information on the identity and positions of the persons who consulted his data at the financial institution.

[5] The Bank wanted to clarify the existence of a potential conflict of interest between J. M and a client of the bank for whose account J. M. was responsible. It was ultimately concluded that J. M. was not suspected of any wrongdoing.

25. It is against that background that court referred the following questions to the Court of Justice:

'(1) Is the data subject's right of access under Article 15(1) of the [GDPR], considered in conjunction with the [concept of] "personal data" within the meaning of Article 4(1) thereof, to be interpreted as meaning that information collected by the controller, which indicates who processed the data subject's personal data and when and for what purpose they were processed, does not constitute information in respect of which the data subject has a right of access, in particular because it consists of data concerning the controller's employees?

(2) If Question 1 is answered in the affirmative and the data subject does not have a right of access to the information referred to in that question on the basis of Article 15(1) of the [GDPR], because it does not constitute 'personal data' of the data subject within the meaning of Article 4(1) of the [GDPR], it remains necessary in the present case to consider the information in respect of which the data subject does have a right of access in accordance with Article 15(1)[(a) to (h)]:

(a) How is the purpose of processing, within the meaning of Article 15(1)(a), to be interpreted in relation to the scope of the data subject's right of access, that is to say, can the purpose of the processing give rise to a right of access to the user log data collected by the controller, such as information concerning personal data of the processors and the time and the purpose of the processing of the personal data?

(b) In that context, can the persons who processed J. M.'s customer data be regarded, under certain criteria, as recipients of the personal data within the meaning of Article 15(1)(c) of the [GDPR], in respect of whom the data subject would be entitled to obtain information?

(3) Is the fact that the bank at issue performs a regulated activity or that J. M. was both an employee and a customer of the bank at the same time relevant to the present case?

(4) Is the fact that J. M.'s data were processed before the entry into force of the [GDPR] relevant to the examination of the questions set out above?'

III. Procedure before the Court

26. The request for a preliminary ruling was received by the Court on 22 September 2021.

27. J. M., the Bank, the Austrian, Czech and Finnish Governments and the European Commission submitted written observations.

28. At the hearing on 12 October 2022, J. M., the Office of the Data Protection Supervisor, the Bank, the Finnish Government and the Commission appeared before the Court.

IV. Analysis

29. In so far as the referring court asks about the interpretation of several provisions of the GDPR, it must first of all be determined whether that regulation is, *ratione temporis*, applicable to the original dispute. That is the subject of the fourth question referred for a preliminary ruling.

A. Applicability of the GDPR (fourth question referred)

30. Pursuant to Article 99(1) thereof, the GDPR entered into force on May 24 2016. However, its application was postponed until 25 May 2018 [6].

31. The consultation of J.M.'s personal data took place between 1 November and 31 December 2013, that is before the GDPR entered into force and became applicable.

32. However, the relevant date in this case is 29 May 2018, the date on which J. M., relying on Article 15(1) of the GDPR (applicable from 25 May 2018), requested the information at issue.

33. As the Austrian Government observed, Article 15(1) of the GDPR confers a procedural right (right of access) on data subjects to obtain information on the processing of their personal data. [7] As such a rule, it applies from the time of its entry into force. [8] J. M. was therefore entitled to rely on it when he requested the information from the Bank.

34. It is true that, the lawfulness of the processing of data collected before the entry into force of the GDPR must be determined in the light of the substantive rules in force at the time, namely Directive 95/46/EC [9] and, in so far as retroactively applicable, the GDPR. [10]

35. Since it is not disputed that the information requested was in the possession of the controller when J. M. requested access to it (which is the right guaranteed by Article 15(1) of the GDPR), the latter regulation applied. [11]

36. Whether the data at issue were processed before the entry into force of the GDPR is thus irrelevant for the purposes of granting or refusing access to the information requested by the data subject under Article 15(1) of the GDPR.

B. First and second questions referred

37. It is appropriate to examine Questions 2 and 3 together. The issue they raise is, in essence, whether J. M.'s personal data collected and processed by the Bank, corresponds to the *information* that the data subject is entitled to obtain under Article 15(1) of the GDPR.

6 Article 99(2) of the GDPR.

7 In the same vein, see Opinion of Advocate General Pitruzzella in *Österreichische Post (Information regarding the recipients of personal data)* (C-154/21, EU:C:2022:452, paragraph 33): ' … the right of access under Article 15(1)(c) of the GDPR plays a functional and instrumental role in the exercise of the other rights which the GDPR confers on data subjects.'

8 Or, as is in this case, from the moment the regulation itself is applicable, if that is not the same as the date of its entry into force.

9 Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

10 The Court's case-law on the effectiveness in time of regulatory amendments is summarised in the judgment of 15 June 2021, *Facebook Ireland and Others* (C-645/19, EU:C:2021:483).

11 With reference to Directive 95/46, the judgment of 7 May 2009, *Rijkeboer* (C-553/07, EU:C.2009:293), paragraph 70, stated that 'Article 12(a) of the Directive requires Member States to ensure a right of access to information … *not only in respect of the present but also in respect of the past*'. It is for Member States to set a time limit for storage of those data, and to provide for access to it which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his or her privacy, in particular by way of his or her rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store those data represents for the controller. Italics added.

1. Identity of the employee and personal data of the data subject

38. It should be remembered that the information requested by J. M. concerned the identity of the employees who had consulted his customer data in 2013, as well as the time at which the processing took place and the purpose of the processing.

39. It was confirmed at the hearing that J. M. has limited his request to disclosure of the identity of those employees. The dispute does not specifically challenge the lawfulness of the manner in which his data was processed by the Bank. [12]

40. Thus:

– As regards the *time* of processing, it is clear from the order for reference that J. M. was already aware of it when he made his application.

– As to the *purpose* of the processing, the Bank notified J. M. in the terms set out above. [13]

41. Therefore, argument solely concerns the information on the identity of the employees of the Bank who handled J. M.'s personal data.

42. Specifically, that information concerns a breakdown of the *processing operations* and not, strictly speaking, the *personal data* of the data subject within the meaning of Article 4(1) of the GDPR. [14]

43. It is clear that the person whose data were consulted was J. M. [15] Once he had obtained confirmation from the Bank that his data had been processed [16], the *information* to which he was entitled, pursuant to Article 15(1) of the GDPR, is that listed in points (a) to (h) thereof [17]. Providing that information, supports the exercise of the data subject's rights [18], within the framework of the mechanisms guaranteeing the lawfulness of the data processing.

44. It follows from Article 15(1) of the GDPR that the *information* to which it refers concerns the circumstances surrounding the processing of the data.

[12] Without prejudice to the fact that that issue would have to be decided, if necessary, by the referring court, it was argued at the hearing that the processing of the data was justified on the basis of, first, the obligations arising under Finnish law, according to which the Bank, as a financial institution, must ensure proper risk management and comply with the rules on the prevention and combating of money laundering, as regards the traceability of transactions, and, second, the Bank's contracts with its customers and employees, that authorise the consultation of their data in circumstances such as those in the present case.

[13] See point 21 of this Opinion.

[14] According to that provision, personal data are 'any information relating to an identified or identifiable natural person', that is to say, 'whose identity can be established, directly or indirectly'.

[15] His identity was not established as a consequence or as an effect of the processing, which was carried out after J. M. had been identified.

[16] As the Commission observed, it may well be that J. M. considers the information provided to be insufficient or inaccurate. In any event, and in accordance with Article 15(1) of the GDPR, J. M. is entitled to obtain confirmation as to whether his data have been or are being processed (which entails an indication of when) and the purposes for which they are being processed. It would be for the referring court to determine whether he received sufficient information.

[17] See point 9 of this Opinion.

[18] As the Court of Justice held in relation to Directive 95/46, in terms that may be applied to the GDPR, the principles of protection provided for by EU law in that field, 'are reflected, on the one hand, in the obligations imposed on those responsible for processing data, obligations which concern in particular data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the rights conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances' (judgment of 20 December 2017, *Nowak*, C-434/16, EU:C:2017:994, paragraph 48).

45. Article 15(1) of the GDPR gives the data subject the right to obtain the following from the controller:

– First, 'confirmation as to whether or not personal data relating to him or her are being processed'.

– Secondly, once the existence of a processing operation has been confirmed, the 'access to personal *data* and to the following *information*',[19] that is to say, to what is listed in letters (a) to (h) of that provision.

46. The provision distinguishes between 'personal data' on the one hand and the 'information' referred to in paragraph 1(c) and (e) on the other hand.

47. The information to be provided to the data subject pursuant to Article 15(1)(a) to (h) of the GDPR cannot therefore be confused with the data subject's personal data within the meaning of Article 4(1) thereof.

48. It is not *data*, of course, but *information*, concerning:

– 'the purposes of processing'(point (a));

– 'the categories of personal data concerned' (point (b));

– the 'expected retention period' (point (d));

– the rights of the data subject referred to in (e), (f) and (g)[20];

– the existence of automated decisions (point (h)).

49. In all those cases, the information concerns either certain rights of the data subject or, in particular, information relating to the processing carried out, such as its purpose (in other words the reason for it) and the subject matter (the categories of data processed).

50. The information on the recipients to whom the personal data of the data subject have been or will be disclosed (Article 15(1)(c) of the GDPR) presents further conceptual problems, to which I will immediately refer.

51. Article 15(1) of the GDPR establishes, in short, a right to i*nformation about the actual fact of processing and the circumstances surrounding it*. In addition to that information, there is also information on the rights of the data subject with regard to the data processed, such as the right to complain to a supervisory authority.

52. The mere fact of the processing and the circumstances in which it occurred do not in my view constitute 'personal data' within the meaning of Article 4(1) of the GDPR.

[19] Italics added.

[20] Rights to request rectification or erasure of data, or restriction of or objection to processing; to complain to a supervisory authority; and to be informed of the origin of data that have not been obtained from the data subject.

53. It is true that decisions affecting the data subject may result from the processing, as the referring court has pointed out.[21] However, the outcome does not depend on which specific natural person or persons examined the data on behalf of and under the responsibility of the Bank, which is the information at issue in the main proceedings.

54. Thus, J. M. has the right to be informed by the Bank, as the controller, as to the personal data in its possession, either obtained from J. M. himself (Article 13 of the GDPR) or by other means (Article 14 of the GDPR). He is also entitled (now under Article 15 of the GDPR) to information on the existence and circumstances of each processing operation to which those data have been subjected, not because the latter in itself constitutes 'personal data', but as expressly provided by Article 15 of the GDPR.[22]

55. To summarise what I will explain below in more detail: what is relevant to this case is that the identity of the employees who consulted J. M.'s data does not constitute his 'personal data'.

56. It is a different matter if the log data or records to which I will refer later contain, directly or indirectly, personal data of the data subject, other than the mention of which employees accessed them. Whether or not this is the case will largely depend on the content of the relevant log data or records. However, I repeat, as the original dispute is confined to the identity of the Bank's employees, that is not J. M.'s personal data but of those employees themselves.

2. Access to information on the recipients to whom the personal data were disclosed

57. The referring court wishes to know whether, even though it does not constitute J. M.'s personal data, he is entitled, in the light of Article 15(1)(a) and (c) of the GDPR, to be provided by the Bank with information about the employees who had processed his personal data.

58. In accordance with Article 15(1)(a), the data subject has the right to obtain confirmation from the *controller* as to the purposes of the processing. However, that provision (which, in the present case, was complied with, since the Bank informed J. M. of the purpose of the processing) does not lay down criteria to determine who the *recipients* of J. M.'s personal data are.

59. The question makes perfect sense when it requires the interpretation of Article 15(1)(c) of the GDPR. It must be recalled that, according to that provision, the data subject has the right to obtain information on the 'recipients or categories of recipients to whom the personal data have been or will be disclosed …'.

60. According to Article 4(9) of the GDPR 'recipient' 'means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not'.

61. That paragraph ('whether or not a third party is involved') could give rise to misunderstandings as to the scope *ratione personae* of the provision, as was noted at the hearing. A superficial and, in my view, incorrect reading might support the view that 'recipient' is not only

[21] Paragraph 38 of the order for reference.

[22] Articles 13, 14 and 15 of the GDPR, in Chapter III ('Rights of the data subject'), Section 2 ('Information and access to personal data'), constitute a system based on the recognition of the right to know: (a) the personal data held by the data controller, whatever the form in which they were obtained (Articles 13 and 14); and (b) the circumstances of each treatment of those data, in particular (Article 15).

any third party to whom the Bank communicated J. M.'s personal data, but also each of the employees who, specifically, consult those data on behalf of and by reference to the legal person which is the Bank.

62. Article 4(10) of the GDPR defines 'third party' as 'a natural or legal person, public authority, agency or body *other* than the data subject, controller, processor and *persons who, under the direct authority of the controller or processor, are authorised to process personal data*'. [23]

63. In the light of those considerations, I take the view that the concept of recipient does not include employees of a legal person who, when using the latter's computer system, consult the personal data of a client on behalf of its administrative bodies. Where such employees act under the direct authority of the controller, they do not, on that basis alone, acquire the status of 'data recipients'. [24]

64. However, there may be situations in which an employee does not comply with the procedures established by the controller and, on his or her own initiative, accesses the data of customers or other employees in an unlawful manner. In such a case, the dishonest employee would not have acted for and on behalf of the controller.

65. To that extent, the dishonest employee could be described as a 'recipient' to whom personal data of the data subject was 'communicated' (figuratively speaking). [25] either by his or her own hand and thus unlawfully, or even as a data controller in his or her own righ.t [26]

66. It is clear from the facts set out in the order for reference and from the arguments put forward at the hearing by the Bank, that the latter was responsible for authorising its employees to consult J. M.'s personal data. Those employees therefore followed the instructions of the controller and acted on its behalf. They cannot therefore be regarded as *recipients* within the meaning of Article 15(1)(c) of the GDPR. [27]

67. The identification of those employees and the time at which any of them had access to the customer's personal data (that is, the content of those mentions of the files or registers to which I will address straightaway) is a separate issue which must be submitted to the supervisory authorities in order to verify the lawfulness of their actions.

68. That is confirmed by Article 29 of the GDPR which refers to persons acting 'under the authority of the controller or processor and having access to personal data'. Such persons may only process such data on the instructions of their employer, who is the actual controller (or processor).

[23] Italics added.

[24] That is also the position of the European Data Protection Board in its Guidelines 07/2020, adopted on 2 September 2020, on the concepts of controller and processor in the GDPR, paragraphs 83 to 90.

[25] In that case Article 34(1) of the GDPR would apply

[26] This is the view of the European Data Protection Board in Guidelines 07/2020, cited above in paragraph 86: 'An employee … who obtains access to data that he or she is not authorised to access and for other purposes than that of the employer does not fall within this category. Instead, this employee should be considered as a third party vis-à-vis the processing undertaken by the employer. In so far as the employee processes personal data for his or her own purposes, distinct from those of his or her employer, he or she will then be considered a controller and take on all the resulting consequences and liabilities in terms of personal data processing'.

[27] The same result is reached by interpreting the references made in Articles 13 and 14 of the GDPR, as well as in recital 61 thereto, to the time at which information on the processing of personal data communicated to the recipients must be provided to the data subjects. It is clear from those provisions that the recipient is an external entity or person other than the controller or processor.

69. The purpose of Article 15(1) of the GDPR is to enable the data subject effectively to exercise (defend) the rights he or she has with regard to his or her personal data. It is therefore necessary to inform him or her of the identity of the controller and, where appropriate, to which recipients the data have been disclosed. With such information, the data subject may contact, in addition to the controller, the recipients who became aware of his or her data.

70. Certainly, the data subject may have doubts about the lawfulness of the involvement of certain persons in the management of the processing of his or her data on behalf of and under the control of the controller or processor.

71. In such a situation, as the Czech Government points out and as the Commission observed at the hearing, the data protection officer (Article 38(4) of the GDPR) or the supervisory authority can be approached to lodge a complaint (Article 15(1)(f) and Article 77 of the GDPR). What is not recognised is the right to directly collect personal data (the identity) of the employee who, as a subordinate of the controller or processor, acts in principle on the latter's instructions.

72. At the hearing, there was discussion as to whether the possibility of addressing the data protection officer or the supervisory authority constituted a sufficient guarantee, from the point of view of the protection of the rights of the data subject whose data have been processed.

73. In order to resolve the issue, a broad approach could be taken, so that any data subject would have the right to know the identity of the controller's employees who have accessed his or her data, even if that access was undertaken on behalf and under the direction of the controller.

74. In my view the GDPR does not provide support for such an argument, although a Member State may wish to adopt such an approach in its domestic legislation, with regard to one or more specific sectors. [28]

75. I consider that it would be unwise for the Court of Justice, acting in a quasi legislative manner, to *amend* the GDPR in order to introduce a new obligation to provide information, in addition to those provided for in Article 15(1) thereof. That would be the case if the data controller were required, in every case, to provide the data subject with the identity, not only of the r*ecipient* to whom the data was communicated, but of any *employee*, or person from the within the company, who had legitimate access to them. [29]

76. As the Bank pointed out at the hearing, the identity of individual employees who have handled the processing of customer data is particularly sensitive information from a security point of view, at least in certain economic sectors.

77. Those employees could be exposed to attempts to exert pressure and influence by those who, as customers of the banking institution, may have an interest in *personalising* their interlocutor, which would no longer be so much the financial institution itself, but one or more of its employees, as the weakest link in the business chain. That would be the case, for example, where the monitoring of transactions, through the consultation of customer data, were carried out in order to comply with the obligations to which banks are subject in terms of preventing and combating crime in the financial sector.

[28] The Finnish Government stated at the hearing that it has done so with regard to health data.

[29] The consequences of recognising such an obligation are hard to imagine for the day to day activity of companies, in particular those who are obliged to process (logically, through their employees) millions of items of personal data of their customers.

78. It is true that the customer may doubt the probity or impartiality of the natural person who has acted on behalf of the controller in the processing of his or her data. Such doubt, if it were reasonable, could justify his or her interest in knowing the identity of the employee, with a view to exercising his or her right to take action against that employee.

79. Considering the sensitivity of such information, the interest in knowing the identity of the employee conflicts with the equally undeniable interest of the data controllers in maintaining secrecy as to the identity of their employees, and the right of those employees to the protection of their own data. The right balance, in my view, is achieved by the intermediation of the supervisory authority acting as an arbitrator weighing these competing interests.

80. Thus, in a case such as that in the main proceedings, it will be the supervisory authority that, from its position of impartiality, will have to assess whether the doubts about the actions of the employees acting on behalf of the banking institution are sufficiently well founded and reliable to justify disclosing their identity.

3. Access to the information on the identity of the employees contained in the files or transaction records

81. In answering the first and second questions referred for a preliminary ruling there is no need to go further, having established that the employees of the entity acting on its behalf and on its instructions are not, as such, the recipients referred to in Article 15(1)(c) of the GDPR.

82. However, it is appropriate to supplement the answer with an analysis of the alleged right of the data subject to know the identity of employees, where it is recorded in the files or records of transactions of an entity. Although, as I have already argued, not all such files or records will necessarily have the same content, it is generally accepted that they reflect who (among the controller's employees), how and when he or she consulted the customer data.

83. Such records enable the controller to fulfil its obligation to comply with the principles set out in Article 5(1) of the GDPR and to implement appropriate technical and organisational measures to ensure and demonstrate the compliance of the processing with the requirements of that regulation (Article 24(1) and Article 25(2) of the GDPR).

84. Within the remit of Directive (EU) 2016/680,[30] mentioned by the Commission as an example[31] of a particular data protection scheme with regard to criminal offences:

– Article 24 requires each controller to keep a register of all categories of processing activities carried out under its responsibility (paragraph 1); and each processor to keep a register of all categories of processing activities carried out on behalf of a controller (paragraph 2).

– Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it

[30] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

[31] At the hearing it was made clear that the reference to Directive 2016/680 did not imply that it was applicable to the present case, which has no criminal connotations.

possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.' [32]

85. However, in accordance with Article 14 of Directive 2016/680, information relating, in particular, to the identity of the employee who processed the personal data is not among the information to which the data subject has a right of access.

86. Similarly, Article 30 of the GDPR provides for the existence of what is calls a 'record of processing activities', the content of which is the same, with a lesser degree of specificity as regards the definition of operations, as that in Article 25 of Directive 2016/680. [33] In neither case is the information recorded on the identity of the employee included in information available to the data subject under Article 15 of the GDPR.

87. The reason for the asymmetry between the information recorded, on the one hand, and the right of access to it, on the other, lies in the difference in the purposes served by the provisions governing the records of processing activities and the accessibility of their content.

88. The purpose of the records referred to in Article 30 of the GDPR is, I repeat, to ensure the lawfulness of the processing and to guarantee data integrity and security. The responsibility for that lies, as a general rule, with the supervisory authority, to whom the records of transactions must be made available by the controller and the processor (Article 30(4) of the GDPR).

89. In the GDPR, the right to complain to the supervisory authorities (Article 15(1)(f)), which are responsible for ensuring its proper implementation, aims to protect the rights of natural persons with regard to the processing of their data. That is provided for in Article 51(1) of the GDPR, and it follows from the list of functions conferred on them by Article 57 thereof.

90. The general function of monitoring the application of the GDPR and protecting the rights of natural persons justifies the supervisory authority's prerogatives. Those include the circumstances in which the processing operations were carried out by a processor or a controller. In particular, one of those situations is relevant to the present case: the identity of those persons who consult the personal data of the clients on behalf of the controller or processor.

91. However, no provision of the GDPR requires that those references to the identity of employees contained in the internal records of institutions, on the basis of which the institutions can find out (and, where appropriate, to make available to the supervisory authority) the identity of persons who have examined a customer's personal data and when those data were accessed, must be made available to the latter.

[32] Provisions which are reproduced in Article 88 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies, and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ 2018 L 295, p. 39), with the addition, in paragraph 3, that the records shall be deleted after three years, unless they are necessary for the purpose of continuous monitoring.

[33] Article 25(1) of Directive 2016/680 explicitly refers to 'the person who consulted or communicated personal data'. More generally, and without referring to each individual processing activity, but to 'categories of processing activities carried out on behalf of a controller', Article 30(2)(a) of the GDPR refers to the 'name and contact details of the processor', that is, according to Article 4(8) of the GDPR, 'the … Person … processing personal data on behalf of the controller'.

92. Quite the opposite, the person concerned by a specific processing operation must be provided with the information necessary to ascertain the relevant circumstances in order to assess the lawfulness of the processing and to challenge it, if necessary, before the supervisory authority or, ultimately, before the courts.

93. That is without prejudice to the fact that, if such transaction records do contain personal data of the data subject (that is other than the mere identity of the employees), the data subject naturally has a right to obtain confirmation from the controller that his or her personal data are being processed. For that purpose, it is irrelevant whether the latter are contained in a record of transactions or in any other internal file or database of the institution.

C. Third question

94. The referring court wishes to know whether 'it is relevant to the proceedings that the bank at issue performs a regulated activity or that J. M. was both an employee and a customer of the bank at the same time.'

95. In my view, it makes no difference to what has been said so far that the data controller exercises a regulated activity. The fact that the controller is a bank subject to the specific regulations applicable to banks [34] may, however, have a bearing on the lawfulness (the legal basis) of the processing, where the processing is carried out in compliance with the legal obligations to which it is subject. [35]

96. In principle, it is also irrelevant that the person whose data has been consulted was both an employee and a customer of that bank. Article 15(1) of the GDPR does not differentiate on the basis of the data subject's professional activity, in addition to his or her status as a customer of the financial institution. [36]

97. It is true, as the Commission has pointed out, that Article 23 of the GDPR allows Member States to limit legislatively the scope of the obligations and rights laid down, inter alia, in Article 15 thereof, by means of sectoral provisions for a specific category of persons concerned. However, the referring court does not mention any such national restrictions.

V. Conclusion

98. In the light of the foregoing, I propose that the Court of Justice reply as follows to the Itä-Suomen hallinto-oikeus (Administrative Court of Eastern Finland, Finland):

Article 15(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), read with Article 4(1) of that regulation,

[34] That specific regulation may require, for example for example, as set out in recital 11 to Directive 2016/680 '… for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law'.

[35] See footnote 12 to this Opinion.

[36] The referring court did not ask about the possible infringement of J. M.'s rights as an employee of the Bank.

must be interpreted as meaning that:

It is applicable when the request for access to information that the data subject has addressed to the data controller was submitted after 25 May 2018.

It does not give the data subject the right to know, from among the information available to the controller (where applicable, through records or log data), the identity of the employee or employees who, under the authority and on the instructions of the controller, have consulted his or her personal data.