

OPINION OF ADVOCATE GENERAL
MEDINA
delivered on 8 October 2026 (1)

Case C-222/25

X
v
Rahapesu Andmehüroo,
interested party:
Andmekaitse Inspektsioon

(Request for a preliminary ruling from the Riigikohus (Supreme Court, Estonia))

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 2(2)(d) – Directive (EU) 2016/680 – Article 1(1) – Scope – Concept of ‘competent authority’ – Directive (EU) 2015/849 – Prevention of the use of the financial system for the purposes of money laundering or terrorist financing – Financial Intelligence Units (FIUs) – Processing of personal data exchanged in connection with suspected money laundering – Data subject’s right of access – Restrictions provided for by a legislative measure – Indirect access through a supervisory authority)

I. Introduction

1. Crime, the proceeds of crime and illicit financial flows have no borders. Over the past few decades, the European Union has developed a robust anti-money laundering (AML) framework which aims also to counter the financing of terrorism (CFT). That framework is constantly evolving in line with efforts undertaken at international level in the field and, in particular, the Financial Action Task Force (FATF) (2) recommendations and instruments of other international bodies active in the area of AML/CFT. (3) Financial intelligence and the sharing of financial information constitute the cornerstone of those efforts. The national authorities with competence for financial intelligence matters, the Financial Intelligence Units (FIUs), are an essential component of the international and EU AML/CFT framework. (4)

2. In the context of the main task of the FIUs to collect, analyse and disseminate financial intelligence information, the FIUs process a large amount of personal data. Despite their significant powers and the amount of data they process, the data protection regime applicable to them is not yet entirely clear. The present case gives the Court the opportunity, for the first time, to delve into the legal status of the FIUs, the

data protection regime applicable to them and the conditions for the limitation of the right of access by the data subjects to the personal data held by the FIUs.

II. The facts, the national proceedings and the questions referred for a preliminary ruling

3. X submitted two separate requests for information, on 16 December 2019 and on 27 December 2019, to the Rahapesu Andmebüroo (Financial Intelligence Unit, Estonia; ‘the RAB’), seeking to ascertain whether information concerning him had been transmitted to, or whether enquiries had been made by, Estonian or foreign credit institutions or foreign authorities.

4. On 20 December 2019 and on 6 January 2020, the RAB rejected those two requests respectively on the ground that, in accordance with Paragraph 60(1) of the Rahapesu ja terrorismi rahastamise tõkestamise seadus (Law on the prevention of money laundering and terrorist financing) of 26 October 2017 (RT I, 17.11.2017, 2; ‘the RahaPTS’) (5) and Paragraph 23(1)(1) of the Avaliku teabe seadus (Law on Public Information) of 15 November 2000 (RT I 2000, 92, 597; ‘the AvTS’), (6) it could not disclose any data collected in the course of its duties or any information regarding the existence or any exchange of such data. In reply to X’s subsequent request to specify the ground for the restriction of access, the RAB reiterated that, on the basis of Paragraph 60(1) of the RahaPTS, it could neither confirm the existence of the requested information nor disclose it.

5. The Tallinna Halduskohus (Administrative Court, Tallinn, Estonia) and subsequently the Tallina Ringkonnakohus (Court of Appeal, Tallinn, Estonia) dismissed the action brought by X against the rejection of his requests. Both judgments were set aside by the Riigikohus (Supreme Court, Estonia), which, by a judgment of 24 March 2022, ordered the RAB to issue a new decision on X’s requests.

6. In that judgment, the Riigikohus (Supreme Court) held that, pursuant to Article 41 of Directive (EU) 2015/849 (7) and in the absence of criminal proceedings, Regulation (EU) 2016/679 (8) is applicable to the right of access of X to his data.

7. It also ruled that Paragraph 60(1) of the RahaPTS does not provide as such for a restriction of the data subject’s rights, but confers on the head of the RAB the power to restrict access to information by classifying such information as being intended for internal use. However, in the present case no such decision was adopted.

8. In the meantime, X submitted a third request for information to the RAB, seeking to determine whether the latter had opened an investigation file concerning him and whether it had made enquiries to the United States of America, which was again rejected by the RAB.

9. X lodged an administrative complaint with the Andmekaitse Inspektsioon (Data Protection Authority, Estonia; ‘the AKI’). The AKI upheld the administrative complaint and ordered the RAB to re-examine the request for information. On 17 February 2022, the RAB once again rejected the request for information, following which X submitted a new administrative complaint to the AKI.

10. By decision of 18 April 2022, the AKI issued an interim order requiring the RAB to provide the requested information, stating that the rights of the data subject could not be restricted under Paragraph 60(1) of the RahaPTS.

11. The head of the RAB, relying on the second sentence of Paragraph 60(1) of the RahaPTS, adopted a decision on 22 April 2022 restricting X’s access, explaining its obligation to preserve the confidentiality of the information contained in the RAB database in order to protect the Estonian financial system.

12. On 13 May 2022, the head of the RAB issued an order restricting, with retroactive effect, access to the data recorded in the RAB database and declaring the data referred to in Articles 8 to 17 of Decree No 56 of the Minister of Finance of 16 December 2020 on Rahapesu Andmebüroo andmekogu põhimäärus

(Statute of the RAB Database) (9) to be information for the exclusive use of the authority ('the order of the head of the RAB').

13. On 19 May 2022, the head of the RAB adopted a decision in which he reiterated the refusal to grant X's request for information, referring to point 1 of Paragraph 23(1) of the AvTS and the access restrictions set out in the decision of 22 April 2022 and in the order of the head of the RAB.

14. X challenged the decisions of 22 April 2022 and of 19 May 2022 as well as the order of the head of the RAB before the Tallinna Halduskohus (Administrative Court, Tallinn). That court upheld the action by judgment of 19 December 2022. It found that Paragraph 60(1) of the RahaPTS was incompatible with Article 23 of the GDPR. In that regard, it pointed out that Paragraph 60(1) of the RahaPTS did not specify which activities of the RAB involved the processing of personal data, the grounds on which information regarding the processing of personal data is refused or the duration of the restriction. It therefore ordered the RAB to rule again on X's requests for information.

15. The RAB lodged an appeal before the Tallinna Ringkonnakohus (Court of Appeal, Tallinn), which was dismissed by judgment of 10 April 2024. That court confirmed the reasoning of the judgment under appeal, noting that Paragraph 60(1) of the RahaPTS is not clear and precise and that it does not allow the data subjects to ascertain the duration of the restriction. It also considered that the decisions at issue and the order of the head of the RAB at issue lay down an absolute and unlimited restriction of the right of access which is not proportionate.

16. The RAB lodged an appeal on a point of law against the judgment of the Tallinna Ringkonnakohus (Court of Appeal, Tallinn) before the Riigikohus (Supreme Court), which is the referring court.

17. First, the referring court seeks clarification from the Court as to which data protection regime applies to the data processed by the RAB having regard, on the one hand, to Article 41 of Directive 2015/849, which provides that data processing carried out under that directive is subject to the GDPR, and, on the other hand, to recital 40 of Directive (EU) 2018/843, (10) which states that it applies without prejudice to the protection of personal data processed by the competent authorities in accordance with Directive (EU) 2016/680. (11)

18. The referring court states that the fact that the RAB is not an investigative body and does not conduct criminal proceedings should not necessarily be decisive for the delimitation of the scope of the GDPR and Directive 2016/680, in the light of the Court's judgment in [La Quadrature du Net and Others \(Personal data and action to combat counterfeiting\)](#). (12)

19. Second, the referring court asks whether, on the basis of Article 23(2)(h) of the GDPR or Article 15(3) of Directive 2016/680, the RAB may refrain from stating the legal basis justifying a refusal of access. In that regard, it notes the absence, in the GDPR, of any mechanism for the indirect exercise of the rights of the data subject through the competent supervisory authority equivalent to the one provided for in Article 17(1) of Directive 2016/680.

20. Third, the referring court emphasises that, while a limitation of the rights of the data subject by a legislative measure is permitted regardless of whether the GDPR or Directive 2016/680 applies in the specific case, the relevant legislative measure must satisfy the requirements of clarity and precision and its application must be foreseeable.

21. The referring court notes that Paragraph 60(1) of the RahaPTS does not expressly set out the conditions under which the head of the RAB can take the decision to restrict access to information, or the temporal or material scope of the restriction of access. The restriction of the data subject's rights may last until the expiry of the retention periods set out in Paragraph 26 of the Statute of the RAB Database (usually 15 years). After that period of time, data subjects are no longer able to obtain information on the data concerning them, since the data are deleted.

22. Moreover, the purpose of the restriction of access under the second sentence of Paragraph 60(1) of the RahaPTS can only be determined by interpreting the provision in conjunction with other provisions of the same law and the legal acts on the prevention of money laundering and terrorist financing.

23. Lastly, the referring court asks whether Article 23 of the GDPR and Article 15 of Directive 2016/680 preclude national legislation which restricts completely the exercise of the right of access to personal data until such data are destroyed.

24. In those circumstances, the Riigikohus (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

- ‘(1) Must Article 2(2)(d) of [the GDPR] and Article 2(1) in conjunction with Article 1 of [Directive 2016/680], be interpreted as meaning that the possible processing of personal data by [an FIU] constitutes processing of personal data by the competent authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, even if the [FIU] is not an investigative body as referred to in the Code of Criminal Procedure?
- (2) Must Article 23(2)(h) [of the] GDPR and Article 15(3) of Directive 2016/680 be interpreted as meaning that in administrative or judicial proceedings it is possible to refuse to disclose to the data subject the legal act on the basis of which a refusal to provide information regarding personal data of that data subject has been made, in order to prevent confirming or denying the fact that personal data related to that data subject [have] been processed, where that data subject has no knowledge of any such processing, and, in such a situation, may data subjects also be refused information as to whether it is possible for them to exercise the right referred to in Article 17(1) of Directive 2016/680?
- (3) Must Article 15 of Directive 2016/680 and Article 23 of the GDPR be interpreted as meaning that national legislation which confers on the head of [an FIU] the power to restrict the rights of data subjects and which specifies the purpose, conditions, and temporal and geographical scope of the restriction of data subjects’ rights in conjunction with other legal [provisions], including subordinate legal provisions, is compatible with those articles?
- (4) Must Article 15 of Directive 2016/680 and Article 23 of the GDPR be interpreted as meaning that a national provision which restricts completely the exercise of the right provided for in Article 14 of Directive 2016/680 and Article 15 of the GDPR until the data [are] destroyed, such that the data subject can never obtain information regarding [those] data[,] is compatible with those articles?’

25. Written observations have been submitted by the applicant in the main proceedings, the Republic of Estonia, the Kingdom of Spain, the Republic of Finland and the European Commission. The Republic of Estonia, the Kingdom of Spain, the French Republic, the Republic of Latvia, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Finland and the Commission participated in the hearing held on 3 June 2026 and responded to the questions for oral response put by the Court.

III. Assessment

A. First question (EU data protection framework applicable to FIUs)

26. By its first question, the referring court asks, in essence, whether Article 2(2)(d) of the GDPR and Article 2(1) of Directive 2016/680, read in conjunction with Article 1(1) of the latter, must be interpreted as meaning that the processing of personal data by an FIU, such as the RAB, can be considered as being carried out by a competent authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, even if the relevant FIU is not an investigative body within the meaning of the national code of criminal procedure.

27. That question seeks to determine which EU data protection legal framework is applicable to an FIU when it exercises the missions conferred on it in the context of AML/CFT. Such determination is particularly important in the light of the differences between the GDPR and Directive 2016/680. For the purposes of the present case, it is important to note the difference in the scope of the restrictions of the rights of the data subject, (13) the role of the supervisory authority under Article 17 of Directive 2016/680 to exercise indirectly the rights of the data subject, and the differences in the regime applicable for the transfers of data to third countries or organisations. (14)

28. The central issue for determining which data protection applies is whether the data processing by an FIU such as the RAB is to be considered to be processing by a ‘competent authority’, within the meaning of Directive 2016/680. If that were the case, the data processing by the RAB would fall within the material scope of Directive 2016/680, in accordance with Article 2(1) and Article 1(1) thereof. To analyse that issue, I will first give a brief overview of the criteria for the delimitation of the scope of the GDPR and Directive 2016/680. I will then examine the status, missions and functions of the FIUs, before reaching a conclusion on which data protection framework applies to the FIUs in the exercise of their core missions in the field of AML/CFT.

1. *Delimitation of the scope of the GDPR and Directive 2016/680*

29. The fundamental right of personal data protection is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (‘the Charter’) and Article 16(1) TFEU. The EU data protection framework relies on three pillars: the GDPR, Directive 2016/680 and Regulation (EU) 2018/1725, (15) which is applicable to the EU institutions.

30. As its name suggests, the GDPR lays down a general and horizontal regime for data protection. (16) Article 2(2) of the GDPR lays down four exceptions to the scope of that regulation, as defined in Article 2(1) thereof, which must be interpreted strictly. (17)

31. In particular, Article 2(2)(d) of the GDPR excludes from its scope 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, including the safeguarding against and the prevention of threats to public security.

32. The reason for that law enforcement exception, as is apparent from recital 19 of the GDPR, is that the processing of personal data for such purposes by the competent authorities is governed by a specific EU legal act, namely Directive 2016/680, which was adopted on the same day as the GDPR. (18)

33. The scope of Directive 2016/680, laid down in Article 2(1) in conjunction with Article 1(1) thereof, is determined on the basis of the person or the actor carrying out the processing and the purposes of the processing. (19) The person carrying out the operation must be a ‘competent authority’ within the meaning of point 7 of Article 3 of Directive 2016/680. The purposes of the processing operation cover the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

34. It follows from recital 10 of Directive 2016/680 that the concept of ‘competent authority’ is to be understood in relation to the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, in view of the arrangements which may prove necessary, in that regard, because of the specific nature of those fields. (20)

35. The definition of ‘competent authority’ is laid down in point 7 of Article 3 of Directive 2016/680.

36. Point 7 of Article 3 of Directive 2016/680 provides for two categories of competent authorities. In point 7(a) of that provision, the ‘competent authority’ is defined as ‘any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’. That

definition covers public authorities, such as the judicial authorities, the police or other law enforcement authorities. (21)

37. Point 7(b) of Article 3 extends the definition of competent authority to ‘any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’.

38. The definition of competent authority must be applied, by analogy, to Article 2(2)(d) of the GDPR and the law enforcement exception provided for by that provision. (22) It is clearly apparent from the wording of that provision that for the relevant exception to apply, the two conditions in relation to the purposes of the processing operation and the person carrying out the operation must be satisfied simultaneously. (23)

39. Thus, the fact that the processing of data is carried out for the objective of law enforcement is not sufficient alone to exclude the application of the GDPR. (24) Conversely, the fact that a competent authority processes data is not enough to bring it within the scope of Directive 2016/680 if such processing is unrelated to the objective of law enforcement. (25)

40. The Court’s case-law offers instructive examples on the delineation of the scope of the two legal instruments. The Court has considered that in carrying out an activity consisting in disclosing to the public, for a road safety purpose, personal data relating to penalty points imposed on drivers of vehicles for road traffic offences, the Latvian entity responsible (26) may not be regarded as a ‘competent authority’ within the meaning of point 7 of Article 3 of Directive 2016/680. Such activity falls, therefore, within the material scope of the GDPR. (27) The Court has also ruled that when tax authorities collect data from an economic operator for the purposes of the collection of tax and combating tax fraud, they may not be regarded as ‘competent authorities’ within the meaning of point 7 of Article 3 of Directive 2016/680. (28)

41. By contrast, the Court considered that the processing of passenger name record (PNR) data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime by a passenger information unit (PIU), an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime, established by Directive (EU) 2016/681, (29) is covered by the scope of Directive 2016/680. (30)

42. The Court has also ruled that Directive 2016/680 applies to the processing of data by the Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (French public authority responsible for the dissemination of works and the protection of rights on the internet; ‘Hadopi’), when that authority adopts measures in the context of the so-called ‘graduated response’ procedure, to the extent that those measures are of a pre-criminal nature directly linked to the judicial proceedings. (31)

43. It follows from that case-law that, with regard to crime prevention, the applicability of Directive 2016/680 does not depend on whether the relevant public authority is an investigative body according to national criminal law. It depends on the specific missions and functions of the relevant public authority in the chain of crime prevention under the legal act that governs the processing of the data by that authority for the purposes of crime prevention.

44. In the light of the above general considerations, I will now examine the status, missions and functions of FIUs in the AML/CFT legal landscape and then assess whether they meet the criteria for the application of Directive 2016/680.

2. *The status, missions and functions of FIUs in the EU AML/CFT legal landscape*

45. The obligation of Member States to establish FIUs is set out in Article 32(1) of Directive 2015/849 (also known as the fourth AML Directive).

46. However, FIUs existed for a long time before they were formally recognised in that directive. (32) Council Decision 2000/642/JHA, (33) adopted under the former ‘third pillar’ on police and judicial cooperation in criminal matters, (34) provided, in Article 1(1) thereof, for the obligation of Member States to ensure that ‘FIUs, set up or designated to receive disclosures of financial information for the purpose of combating money laundering shall cooperate to assemble, analyse and investigate relevant information within the FIU on any fact which might be an indication of money laundering in accordance with their national powers’. According to Article 3 thereof, Member States were to ensure that the performance of the functions of the FIUs was not affected ‘by their internal status, regardless of whether they are administrative, law enforcement or judicial authorities’.

47. The status of FIUs varies between Member States.(35) The FIU model has not been harmonised, with Member States remaining ‘entirely responsible for setting up and deciding on the organisational nature of FIUs’. (36)

48. Directive 2015/849 does, however, lay down one essential requirement which applies irrespective of the FIU status chosen by each Member State. The FIUs, according to Article 32(3) of Directive 2015/849, must be ‘operationally independent and autonomous’, it being understood that an FIU should have ‘the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information’.

49. Moreover, the variety in the legal status of the FIUs should not hamper their cooperation (37) and the effectiveness of the exchange of information between law enforcement or prosecution services and FIUs. (38)

50. The core mission of an FIU, (39) set out in Article 32(1) of Directive 2015/849, is to ‘prevent, detect and effectively combat money laundering and terrorist financing’. To that end, pursuant to Article 32(3) of Directive 2015/849 the FIU is the central national unit responsible for receiving (40) and analysing suspicious transaction reports and other information relevant to money laundering, associate predicate offences or terrorist financing. It is also responsible for disseminating the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing.

51. In the fulfilment of their mission and functions, it follows from Article 32(4) of Directive 2015/849 that FIUs have significant powers of access to the law enforcement information that they require to fulfil their tasks properly. (41)

52. FIUs are also empowered, according to Article 32(7) of Directive 2015/849, to take ‘urgent action ...where there is a suspicion that a transaction is related to money laundering or terrorist financing, to suspend or withhold consent to a transaction that is proceeding, in order to analyse the transaction, confirm the suspicion and disseminate the results of the analysis to the competent authorities’.

53. The missions, functions and powers of FIUs demonstrate their importance in crime detection and crime prevention in the AML/CFT field. The FIUs are both entrusted with the mission to prevent and combat money laundering and terrorist financing, which is a law enforcement mission, and are in close cooperation with competent law enforcement authorities. (42)

54. The FIUs have a *sui generis* status. Although they operate within the ‘broader policing sphere’, (43) they are not necessarily integrated into the police structure. Without denying their importance in ensuring the proper functioning of the EU financial market (which justifies reliance for the adoption of Directive 2015/849 on Article 114 TFEU), it has to be emphasised that specifically their role in the exchange of financial information, with law enforcement authorities and Europol, is laid down in a police cooperation instrument based on Article 87(2) TFEU, namely Directive 2019/1153 (which replaced Decision 2000/642, a former ‘third pillar’ instrument).

55. The core mission, tasks and powers of FIUs indicate that the applicable EU data regime for the processing of data by an FIU must be the one which is most appropriate for law enforcement purposes. I will elaborate on this below.

3. *Data protection framework applicable to FIUs*

56. All of the governments that adopted a position on the issue of the applicable EU data protection regime to the FIUs, (44) in their written submissions or at the hearing, considered that FIUs, in the exercise of their core mission, are ‘competent authorities’ within the meaning of Directive 2016/680. In that regard, they adopt, essentially, a functional approach for the interpretation of that directive, which focuses on the missions and functions exercised by the FIUs.

57. I agree that the processing of personal data by FIUs, in the exercise of their core missions and functions, falls within the scope of Directive 2016/680.

58. As I have already explained, the core mission of FIUs relates to crime detection and prevention in the field of AML/CFT. Article 83(1) TFEU includes terrorism and money laundering among the areas of particularly serious crime, with a cross-border dimension, for which the EU legislature may establish minimum rules concerning the definition of criminal offences and sanctions. (45) In the exercise of that mission, FIUs participate in the prevention and detection of the relevant criminal offences.

59. As I have already observed above, in the context of their missions, FIUs have close links with law enforcement authorities and Europol. They disseminate the results of their analysis to the law enforcement authorities, they respond to requests for information by such authorities and they themselves also have access to the law enforcement information that they require.

60. FIUs are positioned between the private sector entities that are subject to AML reporting obligations, namely, on the one hand, the obliged entities and, on the other hand, the law enforcement authorities. However, their role is not reduced to simply receiving and forwarding information. The added value of FIUs lies in their analysis of information, (46) which is essential in the chain of crime prevention. Taking into account their role in that analysis and the exchange and communication channels at their disposal, FIUs are, as aptly described in legal literature, the European Union’s ‘financial intelligence hubs’ (47) and, as such, they play a pivotal role in the AML/CFT structure.

61. They are at the crossroads (48) between prevention, on the one hand, and investigation and prosecution by law enforcement authorities, on the other hand within the system of AML/CFT. The core mission of an FIU, as the Latvian Government submitted at the hearing, is at the initial stage of criminal proceedings. In the same vein, the Luxembourg Government rightly observed that FIUs have a ‘pre-criminal’ function which forms part of a ‘functional continuum’ leading up to law enforcement.

62. In the light of their role in criminal detection and prevention, certain governments that participated in the written procedure and at the hearing drew the analogy with the findings of the Court in the judgment in [La Quadrature du Net and Others \(Personal data and action to combat counterfeiting\)](#), (49) in relation to the French authority Hadopi. In that case, as I have already noted above, (50) the Court considered that Hadopi, an administrative authority, which has the power to adopt measures of a ‘pre-criminal’ nature, should be classified as a ‘competent authority’, within the meaning of Article 3 of Directive 2016/680, involved in the prevention, investigation, detection or prosecution of criminal offences, namely the minor offence of gross negligence or the offence of counterfeiting, and therefore falls within the scope of that directive in accordance with Article 1 thereof. (51) That was the case even though the Court found that, under the applicable national law, Hadopi did ‘not have decision-making powers of its own’. (52)

63. If the processing of data by an administrative authority such as Hadopi falls within the scope of Directive 2016/680, the same conclusion should apply a fortiori to an FIU, a public authority, which, irrespective of its status under national law, is competent to take autonomous decisions to analyse, request

and disseminate financial intelligence information and has significant powers conferred by EU law necessary for crime detection and prevention in the field of AML/CFT.

64. Most of the governments emphasised, correctly in my view, the similar nature of the missions of FIUs to the missions of PIUs, (53) which the Court, in the judgment in [Ligue des droits humains](#), (54) classified as ‘competent authorities’ falling within the scope of Directive 2016/680. PIUs were classified as such on account of their competence, following from Articles 4 and 7 of the PNR Directive, for the prevention, detection, investigation or prosecution of terrorist offences and of serious crime. Those PIUs collect data from air carriers, process them and transfer the data or the result of the processing to the competent authorities. They are also responsible for exchanging PNR data and the result of that processing with the PIUs of other Member States and Europol. PIUs clearly belong to the criminal sphere and are embedded in the chain of crime prevention and detection.

65. The function of FIUs in the chain of crime prevention is similar to the one of PIUs, as they also receive information, analyse it and disseminate it to the law enforcement authorities.

66. The Court’s case-law supports, therefore, the conclusion that data processing by FIUs for the purposes of crime prevention in the field of AML/CFT falls within the scope of Directive 2016/680.

67. FIUs also satisfy the conditions of a ‘competent authority’ within the meaning of point 7(a) of Article 3 of Directive 2016/680. As noted above, (55) that definition does not cover only the ‘traditional’ judicial or law enforcement authorities, but it extends to ‘*any* public authority’ (emphasis added) which has competence in the field of law enforcement.

68. The classification of an FIU as a ‘competent authority’ under point 7 of Article 3 of Directive 2016/680 should not depend on the organisational structure chosen (law enforcement, judicial, administrative or hybrid) but on the mission and functions with which it is entrusted and the powers exercised. The fact that an FIU, such as the RAB, is not an investigative body within the meaning of the national code of criminal procedure is not decisive either. (56)

69. Even if it were considered that an FIU does not fall under point 7(a) of Article 3 of Directive 2016/680, as the Luxembourg Government stated, it should be considered to fall, in any event, under point 7(b) of that provision, which applies to ‘any other body or entity’ with law enforcement missions. To the extent that, under point 7(b) of Article 3 of that directive, a private entity may be classified as a ‘competent authority’ when it is entrusted by Member State law to exercise law enforcement powers, it should be all the more so for an FIU, which is a public authority with significant powers in the field of AML/CFT.

70. It follows that an FIU must be classified as a ‘competent authority’ within the meaning of point 7 of Article 3 of Directive 2016/680 when it carries out its core missions in the field of AML/CFT.

71. That is without prejudice to the application of the GDPR when FIUs process data, within the scope of other missions entrusted to them by Member State law, which do not relate to one of the activities laid down under Article 1(1) of Directive 2016/680. It follows from Article 9(2) thereof that the GDPR should apply to processing for such other purposes. The Estonian Government submitted that the RAB has supervisory competence vis-à-vis the non-financial sector and it also controls the execution of certain financial penalties. Thus, when an FIU processes data for purposes which are unrelated to its core mission in the field of AML/CFT, such processing falls within the scope of the GDPR. (57)

72. Nevertheless, the Commission considers that FIUs are not ‘competent authorities’ within the meaning of Directive 2016/680, so that the processing of data by those authorities falls under the GDPR.

73. In that regard, it takes the view that the activity of FIUs is limited to the ‘administrative pre-handling’ of any information they obtain. It is only the competent authorities to which they disseminate information that may draw conclusions as to whether the activities involved are of a criminal nature.

74. In the light of the missions, functions and powers of FIUs, which have already been extensively explained, that approach does not sit well, in my view, with the pivotal role of FIUs in the chain of crime prevention. FIUs, as their name indicates, are genuine intelligence hubs with the ability to take autonomous decisions when analysing relevant information. The power of FIUs to access the law enforcement information that they require to fulfil their tasks properly (under Article 32(4) of Directive 2015/849), to exchange information between them, with the law enforcement authorities and with Europol, and the power to suspend or withhold consent to a transaction strongly indicate that their role is not reduced merely to administrative pre-handling.

75. The fact that FIUs are positioned in the middle of the chain of crime detection and prevention and that they disseminate information to the competent authorities does not preclude them from being classified as ‘competent authorities’. Indeed, such classification does not depend on the exact positioning of the authority in the criminal structure but on its mission and functions. (58)

76. The strongest argument put forward by the Commission concerns the wording of Article 41(1) of Directive 2015/849 which states that the processing of personal data under that directive is subject to the GDPR. The Commission observes that that provision is broadly worded so as to cover all processing operations under Directive 2015/849, including processing by FIUs.

77. However, as argued by almost all the governments that submitted written observations and were present at the hearing, (59) Article 41(1) of Directive 2015/849 should be understood without prejudice to the application of Directive 2016/680.

78. The EU legislature has laid down a comprehensive set of data protection rules which have to be applied consistently across all areas of EU law. The GDPR and Directive 2016/680 are each applicable in their respective scope. In other words, as the Spanish Government stated at the hearing, Article 41(1) of Directive 2015/849 does not modify the conditions for the respective scope of the GDPR and Directive 2016/680.

79. That is confirmed by recital 42 of Directive 2015/849, in accordance with which that directive is without prejudice to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, including Council Framework Decision 2008/977/JHA, (60) predecessor to Directive 2016/680. It is important to recall that that framework decision, repealed by Directive 2016/680, had a limited scope in the area of justice and police cooperation as it covered only cross-border processing.

80. As the French Government submitted at the hearing, it is also apparent from recital 22 of Directive 2016/680 that the EU legislature did not attempt to modify the delimitation rule between the GDPR and Directive 2016/680 in the field of AML/CFT. That recital refers to a number of public authorities to which personal data are disclosed in accordance with a legal obligation of their official mission and states that the processing of personal data by those public authorities should comply with the applicable data protection rules according to the purposes of the processing.

81. The need to ensure consistency between Directive 2015/849 and the existing EU data protection legal framework is lastly confirmed by Directive 2024/1640 (the sixth AML Directive), which repeals Directive 2015/849. Directive 2024/1640 no longer contains any explicit provision on the applicable data protection regime. Although recital 122 states that the GDPR applies to the processing of personal data for the purposes of that directive, the same recital also refers to the application of Directive 2016/680.

82. The Commission expressed the concern that if FIUs were considered ‘competent authorities’, that could jeopardise their independence vis-à-vis the competent authorities to which they disseminate information.

83. I find it difficult to share the Commission’s concerns. FIUs are to be considered ‘competent authorities’ for the purpose of determining the applicable EU data protection regime. That determination

does not affect their operational independence and autonomy, which has to be ensured irrespective of their organisational status, even when the FIU is located within the existing structure of another authority. (61)

84. One last argument in favour of the application of Directive 2016/680 to FIUs, in the exercise of their AML/CFT missions and functions, is the need to safeguard the possibility of an indirect exercise of the right of access of data subjects through the supervisory authority under Article 17 of that directive. As I will further explain in my analysis of the fourth question for a preliminary ruling, indirect control through the supervisory authority is an important safeguard to offset the possibility of a total restriction of the right of access under Article 15(1) of Directive 2016/680.

85. In the light of all of the above, Article 2(2)(d) of the GDPR and Article 2(1) of Directive 2016/680, read in conjunction with Article 1(1) of that directive, must be interpreted as meaning that the processing of personal data by an FIU, such as the RAB, in the exercise of its mission to prevent, detect and combat money laundering and terrorist financing and in the light of its functions and powers in that field, must be considered as being carried out by a competent authority, within the meaning of point 7 of Article 3 of Directive 2016/680, even if the relevant FIU is not an investigative body within the meaning of the national code of criminal procedure. The processing of such data thus falls within the scope of Directive 2016/680.

86. In view of the answer that I propose that the Court give to the first question referred, I will analyse the remaining questions concerning the limitations to the right of access of the data subject on the basis of the relevant provisions of Directive 2016/680 without taking the GDPR into consideration.

B. Fourth question

87. By its fourth question, which it is appropriate to consider in the second place, the referring court asks, in essence, whether Article 15 of Directive 2016/680 must be interpreted as precluding a national provision which restricts completely the exercise of the data subject's right of access to his or her personal data held by an FIU, until the destruction of those data, such that the data subject can never obtain information regarding those data.

88. Article 15(1) of Directive 2016/680 authorises the national legislature, having regard to the specific nature of the purposes for which the data processing covered by that directive is carried out (to which attention is drawn, in particular, in recital 10 thereof), to adopt legislative measures limiting the data subject's right of access under certain conditions. The right of access may be limited 'wholly or partly ... to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person', in order to safeguard a number of objectives of general interest, listed exhaustively in points (a) to (e) of that provision. Those objectives include the need to 'avoid obstructing official or legal inquiries, investigations or procedures' and to 'avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences ...'.

89. Member States, in accordance with Article 15(2) of Directive 2016/680, are entitled to adopt legislative measures in order to determine categories of processing which may wholly or partly fall under those purposes.

90. Article 41(4) of Directive 2015/849 sets out a specific obligation for the Member States to restrict the right of access of data subjects 'in applying the prohibition of disclosure laid down in Article 39(1)'. In accordance with that provision, in applying that prohibition, Member States must adopt legislative measures restricting 'in whole or in part' the data subject's right of access, under the conditions laid down in that provision. Those conditions are essentially the same as those laid down in Article 15(1) of Directive 2016/680. They refer to the necessity and proportionality of the partial or the complete restriction and the need to ensure the objectives laid down in Article 41(4) of Directive 2015/849. (62)

91. The prohibition on disclosure to which the introductory sentence of Article 41(4) of Directive 2015/849 refers concerns the obliged entities which are prohibited from disclosing (or ‘tipping-off’, in the language of FATF Recommendation 21), the fact that information on suspicious transactions is being, will be or has been transmitted to an FIU in accordance with Article 33 of that directive. (63)

92. The reference to the prohibition on disclosure appears to indicate that Article 41(4) of Directive 2015/849 governs specifically the limitations of the right of access of data subjects in relation to the information held by the obliged entities and the fact that such information is being, will be or has been transmitted to an FIU (or a self-regulatory body). However, concerning the right of access to the data held by an FIU, it must be recalled that those authorities receive information not only from the obliged entities, but also from other sources (domestic and foreign competent authorities, FIUs of different Member States and Europol), with which they also exchange information. The FIUs also produce financial intelligence. (64) Following the adoption of Directive 2016/680 and taking into account the broad formulation of the requests for access of the data subject in the main proceedings, it appears more appropriate to examine the limitations of the right of access in the light of Article 15 thereof. That provision has a broad scope and is liable to apply to all the data and information held by FIUs. (65)

93. It is apparent from Article 15(1) of Directive 2016/680 that the restriction of the right of access that Member States are entitled to lay down can be ‘complete’. However, such complete (or partial) restriction must respect the principle of proportionality. According to that provision, the legislative measure restricting wholly or partly the data subject’s right of access may be adopted ‘to the extent that, and for as long as such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests of the natural person concerned’. Any restriction must therefore be limited in scope and in time to what is necessary and proportionate. (66)

94. In that regard, it must be recalled that the right of access to one’s personal data is enshrined in Article 8(2) of the Charter. That right is not absolute but must be considered in relation to its function in society.

95. Indeed, as can be seen from Article 52(1) of the Charter, that provision allows limitations to be placed on the exercise of those rights, provided that those limitations are provided for by law, that they respect the essence of those rights and that, in compliance with the principle of proportionality, they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. (67)

96. In the context of Directive 2015/849, full confidentiality of information is an essential prerequisite for the effectiveness of the AML/CFT system established by that directive. (68) It also follows from recital 46 of that directive that access by the data subject to any information related to a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. The information is and must remain confidential throughout the entire chain of the main actors of that system: the obliged entities, which are subject to a prohibition on disclosure; the FIUs, which gather and analyse confidential information; and the law enforcement authorities.

97. All the governments that submitted written observations maintained at the hearing that the requirement of confidentiality is an intrinsic feature of the AML/CFT system and is central to the cooperation of FIUs. Those governments emphasised the sensitivity of the information held by FIUs, whereby the simple knowledge that data are processed could be liable to jeopardise the ongoing analysis and investigations and allow the suspected persons to dissimulate the origins of the funds.

98. A total restriction of the right of access to the information held by FIUs in the context of their core mission appears, therefore, necessary and appropriate to achieve the AML/CFT objectives.

99. That being said, it must be recalled that according to settled case-law, the proportionality of the measures which result in interference with the rights guaranteed in Article 8 of the Charter requires

compliance not only with the requirements of appropriateness and of necessity but also with the requirement that the nature of those measures be proportionate to the objective pursued. (69) More specifically, derogations from and limitations to the protection of personal data should apply only in so far as is strictly necessary. (70)

100. More specifically, according to the Court's case-law, any legislation giving rise to interference with the right to the protection of personal data must, in accordance with the principle of proportionality, lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum requirements, so that the persons whose personal data are being processed have sufficient guarantees that those data will be effectively protected against the risk of abuse, as well as against any unlawful access to or use of those data. (71) That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary so as not to jeopardise a purpose of public interest. (72)

101. It follows from that case-law that an absolute and unconditional restriction of the right of access to the information held by the FIU, under which no circumstances, conditions or safeguards are permitted for that restriction, constitutes unjustified interference with the right of data protection which is not compatible with Article 15(1) of Directive 2016/680. In the absence of any conditions or criteria established by law, it is not possible either for the supervisory authority or for the competent jurisdiction exercising the judicial review of the decision of the controller to examine the legality of the restriction imposed.

102. It must also be observed that under Article 15(4) of Directive 2016/680, the controller must document the factual or legal reasons on which the decision to refuse access is based and make that information available to the supervisory authorities. The obligation of the controller to document the refusal ensures the accountability of the controller vis-à-vis the supervisory authority and allows for an effective judicial review. (73) In other words, the possibility for the controller to refuse access to the data subject does not give the controller (in the present case, the FIU) *carte blanche*.

103. The requirements of necessity and proportionality, which derive from Article 52(1) of the Charter, must also be met when Member States determine, in accordance with Article 15(2) of Directive 2016/680, categories of processing for which limitations apply under Article 15(1) of that directive.

104. With regard to the national legislation in the main proceedings, the referring court stated that it provides for an absolute limitation of the right of access of all individuals under all circumstances and until the destruction of the data. The order of the head of the RAB, which restricts access to all data in the RAB database, does not appear to set out any precise rules governing the scope and application of the restriction of access, nor does it impose any minimum requirements to safeguard against the risk of abuse and ensure that the FIU applies the relevant limitations in so far as is strictly necessary. As the Commission essentially noted in its written observations, the necessity and proportionality of the limitation of the right must be guaranteed on the basis of general criteria which allow for an assessment of each individual access request.

105. The Estonian Government stated at the hearing that the national legal framework does not establish an absolute or categorical limitation. It submitted that the head of the RAB has a discretionary power to assess and decide on each request for access. It confirmed that such power is exercised, for instance, when a person already knows that there is an ongoing inquiry or when the RAB decides to freeze the funds of that person.

106. It is for the referring court, which is competent to interpret its national law, to verify whether there are elements in the national legal framework which ensure that the limitation of the right of access applies only to the extent that it is strictly necessary so as not to jeopardise the purpose of public interest for which the restriction of access is laid down and that it is not arbitrary.

107. That being said, as the Commission rightly observed at the hearing, even if it were considered that the head of the RAB has a margin of discretion, the elements or criteria setting out the frame of such discretion

must be provided for in the respective national measure. However, those elements are not apparent from the presentation of the relevant national legislation.

108. Therefore, while national law may establish a total restriction of access to the data held by the FIU, it must lay down clear and precise rules governing the scope and the conditions of application of the legislative measure in question and imposing minimum requirements, so that the persons whose personal data are being processed have sufficient guarantees that those data will be effectively protected against the risk of abuse, as well as against any unlawful access to or use of those data by FIUs or any other competent authority within the AML/CFT system. (74)

109. Moreover, any total restriction of access imposed on the data subject must be counterbalanced by the mechanism laid down in Article 17 of Directive 2016/680. That provision provides for the indirect exercise of the rights of the data subject by the supervisory authority. That indirect exercise applies, inter alia, in the situation referred to in Article 15(3) of that directive, which provides the controller with the option of not informing the data subject of the refusal or restriction of access and of the reasons for the refusal or restriction of information, where the provision of such information would undermine one of the purposes of public interest laid down in Article 15(1) of that directive. According to paragraph 3 of Article 17, where the supervisory authority exercises the right of access on behalf of the data subject, that authority must inform the data subject at least that all necessary verifications or a review by that authority has taken place.

110. The case-law of the Court highlights the importance of the indirect exercise of the rights of the data subject in order to ensure that there is an appropriate balance between the public interest justifying the limitation of the right of access and the fundamental rights of the data subject to data protection and to an effective judicial review under Article 47 of the Charter. In the judgment in [Ligue des droits humains \(Verification by the supervisory authority of data processing\)](#), the Court ruled that, as is apparent from recital 48 of Directive 2016/680, the indirect exercise of the rights of the data subject through the competent supervisory authority must be regarded as necessary for the protection of those rights, their direct exercise before the controller being difficult or even impossible. (75)

111. With regard to the precise role of the supervisory authority in the indirect exercise of those rights, the Court has ruled that such an authority must engage in a confidential dialogue with the controller and, at the end of that dialogue, decide on which information is necessary for the data subject to exercise his or her right to an effective judicial remedy. (76)

112. Moreover, it follows from the Court's case-law that in the context of the judicial review of the correct application of Article 17 of Directive 2016/680, it is incumbent upon the Member States to lay down rules enabling the court with jurisdiction to examine all the grounds and the related evidence on which the supervisory authority based, within that framework, the verification of the lawfulness of the processing of the data at issue, as well as the conclusions which it drew from that verification. (77) The information that was made available by the controller to the supervisory authority concerning the reasons on which it based its decision must also be made available to the court before which an action against the supervisory authority has been brought. (78)

113. At the hearing, the Estonian Government submitted that the national supervisory authority has the power to verify the lawfulness of the data processing by the RAB. It falls on the national court to verify that national law ensures the proper application of Article 17 of Directive 2016/680.

114. In view of all of the above, Article 15 of Directive 2016/680 must be interpreted as precluding a national provision which restricts completely the exercise of the data subject's right of access to his or her personal data held by an FIU, until the destruction of those data, such that the data subject can never obtain information regarding those data, to the extent that the relevant national measure does not appear to lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum requirements, so that the persons whose personal data are being processed have sufficient guarantees that those data will be effectively protected against the risk of abuse, as well as against any unlawful access to or use of those data by the relevant FIU.

C. Second question

115. According to settled case-law, in the procedure laid down by Article 267 TFEU providing for cooperation between national courts and the Court of Justice, it is for the latter to provide the national court with an answer which will be of use to it and enable it to decide the case before it. To that end, the Court should, where necessary, reformulate the questions referred to it. (79)

116. In the present case, in the first part of its second question, the referring court asks whether Article 15(3) of Directive 2016/680 allows an FIU to refuse to disclose to the data subject the legal act on the basis of which a refusal to give access to personal data of the data subject has been made, in order to prevent confirming or denying the fact that personal data related to him or her have been processed.

117. In its written submissions, the Commission argued that the second question is inadmissible. It stated that the decision of refusal of access of the RAB in the case in the main proceedings referred explicitly to the legal basis of the refusal, namely Paragraph 60(1) of the RahaPTS and Paragraph 23(1)(1) of the AvTS.

118. At the hearing, the Estonian Government submitted that the question is admissible, while the Dutch Government argued that it is inaccurate to suggest that the disclosure of a ground for restriction is liable to disclose the fact that personal data have been processed. In any event, the restriction of the right of access allows restriction of the information as to whether data are being processed or not.

119. In the light of the explanations contained in the order for reference which refers, in general terms, to the ‘legal basis’ of the restriction but also to the ‘factual and legal reasons’ for decisions affecting the data subjects, the first part of the second question can be understood as asking whether an FIU can refuse to communicate the reasons for the refusal.

120. Thus, in application of the case-law referred to in point 115 of the present Opinion, it should therefore be considered that, by its second question the referring court asks, in essence, whether Article 15(3) of Directive 2016/680 must be interpreted as meaning that it allows an FIU to refuse to provide the reasons for the refusal or the restriction, in order to avoid confirming or denying the fact that personal data related to the data subject have been processed, and, in such a situation, whether data subjects may be refused information as to whether it is possible for them to exercise their right of access through the supervisory authority pursuant to Article 17(1) of Directive 2016/680.

121. Under Article 15(3) of Directive 2016/680, when a restriction of the right of access of the data subject applies, (80) the controller must inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may, however, be omitted where that provision would undermine a purpose of public interest (as laid down in Article 15(1) of that directive). (81)

122. It follows from that provision that, subject to the conditions set out therein, an FIU is permitted to provide a response such as ‘neither confirm nor deny’, omitting information as to whether any processing has been carried out at all.

123. However, it follows from Article 15(3) of Directive 2016/680 that the controller is obliged in such a case to inform the data subject of the possibility of lodging a complaint with the supervisory authority or seeking a judicial remedy. The controller is also obliged, in accordance with Article 17(2) of Directive 2016/680, to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1 of that article. No exemption is allowed for the provision of such information.

124. That is due to the paramount importance of the right of indirect access through the supervisory authority. As has already been noted above in the context of the analysis of the fourth question, (82) the existence of that right offsets the refusal by the controller of any information as to the processing of data. When the direct exercise of the right of access is difficult or impossible, the data subject must always be

informed of the possibility of exercising his or her rights indirectly. Moreover, an FIU is not exempt from the obligation to document the reasons on which the decision to refuse access is based and make such information available to the supervisory authorities, in accordance with Article 15(4) of that directive. (83)

125. In the light of the above, Article 15(3) of Directive 2016/680 must be interpreted as meaning that it allows an FIU to refuse to provide the reasons for the refusal or the restriction, in order to avoid confirming or denying the fact that personal data related to the data subject have been processed. However, in such a situation, data subjects must always be provided with information as to the possibility of exercising their right of access through the supervisory authority pursuant to Article 17(1) of Directive 2016/680.

D. Third question

126. By its third question, the referring court asks, in essence, whether Article 15(1) of Directive 2016/680 must be interpreted as precluding national legislation which by a general provision confers on the head of an FIU the power to restrict the rights of data subjects, where the understanding of the purpose, the conditions and the scope of that restriction requires the combined reading of other legal provisions, including subordinate legal provisions.

127. It follows from Article 15(1) of Directive 2016/680 that any restriction of the right of access by data subjects requires the adoption by Member States of a legislative measure.

128. It is apparent from recital 33 of that directive that the reference to a legislative measure does not necessarily require a legislative act adopted by a parliament. However, such a legislative measure must be clear and precise and its application foreseeable for those subject to it, in accordance with the case-law of the Court of Justice and the European Court of Human Rights. That recital also states that Member State law regulating the processing of personal data should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

129. In its case-law, the Court inferred from Article 8(2) of the Charter, which itself only reflects, by giving specific expression to, the requirement of Article 52 of the Charter that any limitation on the exercise of the fundamental rights recognised by the Charter must, in particular, be provided for by law, that any legal basis which permits interference with the right to the protection of personal data must itself define the scope of the limitation on the exercise of that right which it is liable to bring about. (84)

130. In addition, the Court has held, as regards the requirement laid down in Article 52 of the Charter, that any interference with the right to the protection of personal data must occur while also observing the principle of proportionality, which requires that any legislation giving rise to such interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum requirements, so that the persons whose personal data are being processed have sufficient guarantees that those data will be effectively protected against the risk of abuse, as well as against any unlawful access to or use of those data. (85)

131. It follows from the Court's case-law, referring to the settled case-law of the European Court of Human Rights, that the expression 'laid down by law' used in Article 8(2) of the Charter must be understood in its substantive sense and not its formal sense. (86) Moreover, it follows from the case-law of the European Court of Human Rights, that the term 'law' in the expression 'in accordance with the law', referred to in Article 8(2) ECHR, refers not only to legislative acts but also to subordinate legal provisions. (87) It refers to the text in force, as interpreted by the competent courts. (88)

132. Therefore, the requirement set out in Article 15(1) of Directive 2016/680 that any restriction must be based on legislative measures should be understood broadly so as to be satisfied not only when there is one single legislative act governing all aspects of the restriction of access to a certain category of data, such as

the data held by the RAB. The term ‘legislative measures’ may cover a set of legislative provisions including subordinate legal provisions, as interpreted by the competent courts.

133. That is so, provided, however, that the relevant legislative measures allow for a clear and precise understanding of the scope of the restriction they impose and that the application of such measures is foreseeable by the persons subject to it. The application of a measure adopted under Directive 2016/680 is foreseeable to the persons subject to it when they can identify the circumstances and conditions under which the scope of the rights conferred on them by that directive may be the subject of a restriction. (89)

134. In the case in the main proceedings, a number of legislative measures lay down provisions relevant for the exercise of the right of access. Paragraph 60(1) of the RahaPTS authorises the head of the RAB to restrict access to the data contained in the RAB’s database and to classify it as information for internal use. The order of the RAB of 13 May 2022 lays down restriction of access to the data of the RAB database, declaring that those data are intended for internal use. Paragraph 23(1)(1) of the AvTS allows restriction of access to data when the person making the request is not entitled to access those data.

135. Such provisions appear to be formulated in very general terms, without allowing data subjects to identify under what conditions and circumstances a restriction is allowed and the guarantees ensuring that the data processed will be effectively protected against the risk of abuse, as well as against any unlawful access to or use of those data. (90)

136. It is true that the internal regulation of the RAB contains certain information relevant for the processing of data, namely specifying the controller of the data (the RAB), the type of data entered in the database, (91) the classification of the security of the data(92) and the period of time for which data concerning a person in the database are stored. (93)

137. However, those elements concern, more generally, the processing of the data by the RAB without specific reference to the conditions and circumstances of the restriction of the right of access and to the safeguards against the risk of abuse.

138. At the hearing, the Estonian Government stated that the head of the RAB has a discretionary power to decide whether or not to provide access to the data contained in the RAB database, and there are circumstances in which access may be given. However, as already noted above, (94) the relevant legislative framework does not appear to frame that discretion or to provide for clear and precise conditions for restriction of the right of access. That corroborates the conclusion that the relevant national legislative measures do not appear to meet the standards of a clear and precise rule the application of which is foreseeable for the data subject seeking to exercise the right of access, which is however for the national court to assess.

139. In view of the above, Article 15(1) of Directive 2016/680 must be interpreted as meaning that it does not preclude national legislation which, by a general provision, confers on the head of an FIU the power to restrict the rights of data subjects, for the sole reason that the understanding of the purpose, the conditions and the scope of that restriction requires the combined reading of other legal provisions, including subordinate legal provisions. However, the same provision precludes such national legislation to the extent that the relevant national legislation does not appear to lay down clear and precise rules governing the scope and conditions of application of the restriction of the right of access so that the persons whose personal data are being processed have sufficient guarantees that the data processed will be effectively protected against the risk of abuse, as well as against any unlawful access to or use of those data.

IV. Conclusion

140. In the light of the foregoing, I propose that the Court should answer the questions referred by the Riigikohus (Supreme Court, Estonia) for a preliminary ruling as follows:

(1) Article 2(2)(d) 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) and Article 2(1) of 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, read in conjunction with Article 1(1) of that directive,

must be interpreted as meaning that the processing of personal data by a Financial Intelligence Unit (FIU), such as the RAB, in the exercise of its mission to prevent, detect and combat money laundering and terrorist financing and in the light of its functions and powers in that field, must be considered as being carried out by a competent authority, within the meaning of point 7 of Article 3 of Directive 2016/680, even if the relevant FIU is not an investigative body within the meaning of the national code of criminal procedure. The processing of such data thus falls within the scope of Directive 2016/680.

(2) Article 15 of Directive 2016/680

must be interpreted as precluding a national provision which restricts completely the exercise of the data subject's right of access to his or her personal data held by an FIU, until the destruction of those data, such that the data subject can never obtain information regarding those data, to the extent that the relevant national measure does not appear to lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum requirements, so that the persons whose personal data are being processed have sufficient guarantees that those data will be effectively protected against the risk of abuse, as well as against any unlawful access to or use of those data by the relevant FIU.

(3) Article 15(3) of Directive 2016/680

must be interpreted as meaning that it allows an FIU to refuse to provide the reasons for the refusal or the restriction, in order to avoid confirming or denying the fact that personal data related to the data subject have been processed. However, in such a situation, data subjects must always be provided with information as to the possibility of exercising their right of access through the supervisory authority pursuant to Article 17(1) of Directive 2016/680.

(4) Article 15(1) of Directive 2016/680

must be interpreted as meaning that it does not preclude national legislation which, by a general provision, confers on the head of an FIU the power to restrict the rights of data subjects, for the sole reason that the understanding of the purpose, the conditions and the scope of that restriction requires the combined reading of other legal provisions, including subordinate legal provisions. However, the same provision precludes such national legislation to the extent that the relevant national legislation does not appear to lay down clear and precise rules governing the scope and conditions of application of the restriction of the right of access so that the persons whose personal data are being processed have sufficient guarantees that the data processed will be effectively protected against the risk of abuse, as well as against any unlawful access to or use of those data.

¹ Original language: English.

² The FATF is an intergovernmental body which sets standards and develops and promotes policies to combat money laundering and terrorist financing.

³ See recital 4 of Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L, 2024/1624); Mitsilegas, V. and Vavoula, N., 'The evolving EU anti-money laundering regime: Challenges for fundamental rights and the rule of law', *Maastricht Journal of European and Comparative Law*, Vol. 23, Issue 2, 2016, pp. 261 to 293.

-
- [4](#) See the preamble to the Egmont Group of Financial Intelligence Units Charter, approved in July 2013 by the Egmont Group Heads of Financial Intelligence Units.
-
- [5](#) According to that provision: ‘Only an official or an employee of the Financial Intelligence Unit has access to and a right to process the information in the Financial Intelligence Unit database. On the basis of that law, the head of the Financial Intelligence Unit may establish restrictions on access to information, classifying information as intended for internal use. ...’
-
- [6](#) According to that provision: ‘A holder of information shall refuse to comply with a request for information if: 1) restrictions on access apply to the information requested and the person making the request for information is not entitled to access the information requested’.
-
- [7](#) Directive of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ 2015 L 141, p. 73).
-
- [8](#) 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’).
-
- [9](#) RT I, 18.12.2020, 38.
-
- [10](#) Directive of the European Parliament and of the Council of 30 May 2018 amending Directive 2015/849, and amending Directives 2009/138/EC and 2013/36/EU (OJ 2018 L 156, p. 43).
-
- [11](#) Directive 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).
-
- [12](#) Judgment of 30 April 2024 (C-470/21, EU:C:2024:370, paragraph 158).
-
- [13](#) The GDPR has a horizontal clause in Article 23, while under Directive 2016/680 each right can be limited on an individual basis. In particular with regard to the right of access of the data subject, Article 15 of Directive 2016/680 expressly allows Member States to adopt legislative measures restricting that right ‘wholly or partly’ and to adopt legislative measures in order to determine ‘categories of processing’ which may ‘wholly or partly’ fall under the different categories of the grounds for the restrictions. Legal literature rightly observes that even if subject rights, including the right of access, can also be limited under the GDPR, there is more room for limitations under Directive 2016/680, making it more likely that a person requesting access to data from a law enforcement authority will receive a ‘neither confirm nor deny’ type of response; see Mouzakiti, F., ‘Cooperation between financial intelligence units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive’, 2020, Vol. 11, Issue 3, *New Journal of European Criminal Law*, pp. 351 to 374, at p. 366.
-
- [14](#) The Commission adequacy decisions under Article 45 of the GDPR determining whether a third country offers an adequate level of protection do not apply to data exchanges under Directive 2016/680, for which there must be a separate adequacy decision under Article 36 of the latter. In the absence of such a decision, transfers may take place subject to appropriate safeguards, in accordance with Article 37 of Directive 2016/680.
-
- [15](#) Regulation of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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).
-
- [16](#) See recital 10 of the GDPR.
-

- [17](#) Judgment of 24 February 2022, [Valsts ieņēmumu dienests \(Processing of personal data for tax purposes\)](#) (C-175/20, EU:C:2022:124, paragraph 40).
-
- [18](#) Judgment of 24 February 2022, [Valsts ieņēmumu dienests \(Processing of personal data for tax purposes\)](#) (C-175/20, EU:C:2022:124, paragraph 42 and the case-law cited).
-
- [19](#) See, Vogiatzoglou, P., ‘Scope’ in Kosta, E. and Boehm, F. (eds), *The EU Law Enforcement Directive (LED)*, Oxford University Press, Oxford, 2024, pp. 67 to 77, at p. 74.
-
- [20](#) Judgment of 24 February 2022, [Valsts ieņēmumu dienests \(Processing of personal data for tax purposes\)](#) (C-175/20, EU:C:2022:124, paragraph 43 and the case-law cited).
-
- [21](#) See recital 11 of Directive 2016/680.
-
- [22](#) Judgment of 24 February 2022, [Valsts ieņēmumu dienests \(Processing of personal data for tax purposes\)](#) (C-175/20, EU:C:2022:124, paragraph 42 and the case-law cited).
-
- [23](#) See, to that effect, judgment of 21 June 2022, [Ligue des droits humains](#) (C-817/19, EU:C:2022:491, paragraph 67). See Brewczyńska, M., ‘A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation’ in Kosta, E. et al. (eds) *Research handbook on EU data protection law*, Edward Elgar, Cheltenham, 2022, pp. 91 to 114, at p. 104.
-
- [24](#) It is apparent from Article 23(1)(d) and (h) of the GDPR that the processing of personal data carried out by private individuals for the law enforcement purposes set out in Article 2(2)(d) of that regulation falls within the scope thereof; see judgment of 21 June 2022, [Ligue des droits humains](#) (C-817/19, EU:C:2022:491, paragraph 68 and the case-law cited).
-
- [25](#) As follows from recitals 11 and 12 of Directive 2016/680, the GDPR applies to processing of personal data that is carried out by a ‘competent authority’, within the meaning of point 7 of Article 3 of that directive, but for other non-law-enforcement purposes; judgment of 24 February 2022, [Valsts ieņēmumu dienests \(Processing of personal data for tax purposes\)](#) (C-175/20, EU:C:2022:124, paragraph 43 and the case-law cited).
-
- [26](#) The Ceļu satiksmes drošības direkcija (Road Traffic Safety Directorate, Latvia).
-
- [27](#) Judgment of 22 June 2021, [Latvijas Republikas Saeima \(Penalty points\)](#) (C-439/19, EU:C:2021:504, paragraph 72).
-
- [28](#) Judgment of 24 February 2022, [Valsts ieņēmumu dienests \(Processing of personal data for tax purposes\)](#) (C-175/20, EU:C:2022:124, paragraph 44).
-
- [29](#) Directive of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132; ‘the PNR Directive’).
-
- [30](#) Judgment of 21 June 2022, *Ligue des droits humains* (C-817/19, EU:C:2022:491, paragraph 80).
-
- [31](#) Judgment of 30 April 2024, [La Quadrature du Net and Others \(Personal data and action to combat counterfeiting\)](#) (C-470/21, EU:C:2024:370, paragraphs 158 and 159).
-
- [32](#) For an overview of the history of FIUs in the AML landscape, see European Parliament: European Parliamentary Research Service and Scherrer, A., *Fighting tax crimes – Cooperation between Financial Intelligence Units, Ex-post impact assessment – Study*, March 2017, p. 8 (‘the 2017 EP Study’); Mitsilegas, V., ‘New forms of transnational policing: The emergence of financial intelligence units in the European Union and the challenges for human rights: Part 1’, *Journal of Money Laundering Control*, Vol. 3, Issue 2, 1999, p. 147. The cooperation of the units specialised in financial intelligence materialised in the first ‘Egmont group’ gathering in 1995. In 2003, the FATF adopted a revised set of 40

recommendations which formally included a recommendation for the establishment and functioning of FIUs. The 2012 FATF Recommendations, updated in June 2026, contain a recommendation on the FIUs (Recommendation No 29).

-
- [33](#) Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (OJ 2000 L 271, p. 4).
-
- [34](#) Former Article 34(2)(c) TEU.
-
- [35](#) See International Monetary Fund, *Financial Intelligence Units: An Overview*, 2004 (available at: <https://www.elibrary.imf.org/display/book/9781589063624/9781589063624.xml>), p. 9. The 2017 EP Study refers, on pages 13 and 14, to a 2016 report prepared by the EU FIU platform where reference is made to three models of FIU: administrative, law enforcement (or judicial) and hybrid. The FIU models to which that report referred are distributed as follows: 12 EU FIUs are of an administrative nature, located for instance in the Ministry of Finance, the Ministry of Justice or the Ministry of the Interior, or embedded in the Central Bank or a supervisory authority, citing Belgium, Bulgaria, the Czech Republic, Spain, France, Croatia, Italy, Latvia, Malta, Poland, Romania and Slovenia; 11 EU FIUs are organised under a law enforcement (police and/or justice) model, citing Austria, Estonia, Finland, Germany, Ireland, Lithuania, Portugal, Slovakia, Sweden, Luxembourg and the United Kingdom; 5 FIUs have described themselves as having a ‘hybrid’ nature due to the combined presence of police and administrative elements, citing Denmark, Greece, Cyprus, Hungary and the Netherlands. On the reasons behind the choice of the FIU design, see Masciandaro, D. and Volpicella, A., ‘Designing financial supervision: The puzzling case of the FIUs against money laundering’, *Journal of Financial Regulation*, Vol. 2, Issue 1, 2016, pp. 79 to 113.
-
- [36](#) See recital 14 of Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ 2019 L 186, p. 122).
-
- [37](#) See Article 52 of Directive 2015/849, in accordance with which the FIUs should cooperate with each other to the greatest extent possible ‘regardless of their organisational status’.
-
- [38](#) See recital 14 of Directive 2019/1153. That directive, adopted under Article 87(2) TFEU on police cooperation (and which repealed Decision 2000/642), sought to strengthen the exchange of financial information with the designated competent authorities, and enhance legal certainty and operational effectiveness. Article 1(2)(a) thereof makes it clear that it is without prejudice to Directive 2015/849 and the related provisions of national law, ‘including the organisational status conferred on FIUs under national law as well as their operational independence and autonomy’.
-
- [39](#) FIUs, depending on the Member States, can be entrusted with other missions and functions to the extent that those do not interfere with their core mission. The Estonian Government submitted that the RAB also has a supervisory role. However, the case in the main proceedings concerns the right of access to data held by an FIUs in the exercise of its core mission and functions.
-
- [40](#) They receive information from obliged entities to which Directive 2015/849 applies, in accordance with Article 2(1) thereof. Obligated entities are obliged to inform FIUs, including by filing a report, of suspicious transactions, pursuant to Article 33 of that directive.
-
- [41](#) To that end Member States must ensure, in accordance with Article 8 of Directive 2019/1153, that their designated competent authorities are required to reply in a timely manner to requests for law enforcement information made by a national FIU on a case-by-case basis, where the information is necessary for the prevention, detection and combating of money laundering, associate predicate offences and terrorist financing.
-
- [42](#) That being said, even when the FIUs are located within the structure of the police or the judiciary, they must remain independent and operationally separate. See Article 19(4) of Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive 2015/849 [with effect from 10 July 2027] (OJ L, 2024/1640) (the sixth AML Directive).
-

[43](#) Mouzakiti, F., footnote 13, op. cit., p. 373, who describes FIUs as ‘new policing institutions’.

[44](#) The Kingdom of the Netherlands, in its oral pleadings, refrained from adopting a position on the issue of the data protection legal framework applicable to the FIUs.

[45](#) On that basis, Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (OJ 2018 L 284, p. 22) lays down requirements on the criminalisation of money laundering.

[46](#) That is also emphasised by the Council of Europe: Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval) in the presentation of the FIU functions (available at: <https://www.coe.int/en/web/moneyval/implementation/fiu>). According to the association Transparency International, when they analyse information the FIUs ‘connect fragments that no single bank or authority can see alone’ (see <https://www.transparency.org/en/news/financial-intelligence-units-powerful-tools-against-corruption>).

[47](#) Mouzakiti, F., footnote 13, op. cit., p. 353.

[48](#) See French Senate, ‘Rapport fait au nom de la commission d’enquête aux fins d’évaluer les outils de la lutte contre la délinquance financière, la criminalité organisée et le contournement des sanctions internationales, en France et en Europe, et de proposer des mesures face aux nouveaux défis’, Vol. I, 18 June 2005, p. 197, pointing out that the French FIU (Tracfin) is located on the border between prevention and prosecution (*‘à la frontière entre les volets préventif et répressif’*).

[49](#) Judgment of 30 April 2024 (C-470/21, EU:C:2024:370).

[50](#) Point 42 of the present Opinion.

[51](#) Judgment of 30 April 2024, [La Quadrature du Net and Others \(Personal data and action to combat counterfeiting\)](#) (C-470/21, EU:C:2024:370, paragraph 158).

[52](#) Ibid.

[53](#) See point 41 of the present Opinion.

[54](#) Judgment of 21 June 2022 (C-817/19, EU:C:2022:491, paragraphs 79 and 80).

[55](#) See point 36 of the present Opinion.

[56](#) See point 43 of the present Opinion.

[57](#) For the sake of comprehensiveness, I note that, as follows from recital 14 of Directive 2016/680, that directive does not apply to the processing of data in the course of an activity which falls outside the scope of EU law, particularly activities concerning national security.

[58](#) That is supported by the judgment of 21 June 2022, [Ligue des droits humains](#) (C-817/19, EU:C:2022:491), in which the Court ruled that the PIUs are to be classified as ‘competent authorities’ under Directive 2016/680. Such classification was not excluded by the fact that PIUs transfer PNR data or the result of processing to the competent authorities.

[59](#) Excluding the Netherlands Government, which did not adopt a position on that matter.

[60](#) Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350, p. 60).

- [61](#) See the second subparagraph of Article 19(4) of Directive 2024/1640.
-
- [62](#) Namely to enable the obliged entity or the competent national authority to fulfil its tasks properly and to avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of that directive, and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised. The existence of such a specific sectoral restriction of the right of access of the data subject in relation to the prohibition on disclosure can perhaps be explained by the fact that Directive 2015/849 predates the adoption of the EU data protection instrument for law enforcement, namely Directive 2016/680. Directive 2024/1640, which, as mentioned above (in point 81 of the present Opinion), repeals Directive 2015/849, no longer contains that provision on the restriction of the right of access.
-
- [63](#) Or to a self-regulatory body of the profession in accordance with the conditions set out in Article 34 of Directive 2015/849.
-
- [64](#) See point 60 of the present Opinion.
-
- [65](#) In the event that the Court adopts the position that Article 41(4) of Directive 2015/849 is applicable in relation to all the data held by FIUs, my analysis in relation to the fourth question remains relevant to the extent that that provision reflects, essentially, the main conditions for the restriction of the right of access laid down in Article 15(1) of Directive 2016/680.
-
- [66](#) See Dimitrova, D., ‘Limitations to the right of access’ in Kosta, E. and Boehm, F. (eds), footnote 19, *op.cit.*, p. 288.
-
- [67](#) Judgment of 6 October 2020, [Privacy International](#) (C-623/17, EU:C:2020:790, paragraph 64).
-
- [68](#) See Article 38(2) and Article 42 of Directive 2015/849, and the third subparagraph of Article 61(3) thereof.
-
- [69](#) Judgment of 22 November 2022, [Luxembourg Business Registers](#) (C-37/20 and C-601/20, EU:C:2022:912, paragraph 63).
-
- [70](#) Judgment of 22 November 2022, [Luxembourg Business Registers](#) (C-37/20 and C-601/20, EU:C:2022:912, paragraph 64).
-
- [71](#) Judgment of 18 June 2026, [NTH Haustechnik](#) (C-484/24, EU:C:2026:496, paragraph 72 and the case-law cited).
-
- [72](#) Judgment of 6 October 2020, [Privacy International](#) (C-623/17, EU:C:2020:790, paragraph 68 and the case-law cited).
-
- [73](#) See Dimitrova, D., footnote 66, *op. cit.*, p. 292, who points out that the documentation obligation seeks to ensure that restrictions will not be imposed randomly.
-
- [74](#) Such guarantees should be without prejudice to the safeguards laid down under national criminal law in the event that the data subject is formally accused of a crime.
-
- [75](#) Judgment of 16 November 2023 (C-333/22, EU:C:2023:874, paragraph 44).
-
- [76](#) *Ibid.*, paragraph 66.
-
- [77](#) *Ibid.*, paragraph 69 and the case-law cited.
-
- [78](#) *Ibid.*, paragraph 70.
-
- [79](#) Judgment of 16 July 2026, *AEDT and État du Grand-Duché de Luxembourg* (C-158/25, EU:C:2026:591, paragraph 21).
-
- [80](#) See point 88 et seq. of the present Opinion.
-

- [81](#) Judgment of 16 November 2023, [Ligue des droits humains \(Verification by the supervisory authority of data processing\)](#) (C-333/22, EU:C:2023:874, paragraph 42).
-
- [82](#) See point 109 of the present Opinion.
-
- [83](#) See point 102 of the present Opinion.
-
- [84](#) Judgment of 18 June 2026, [NTH Haustechnik](#) (C-484/24, EU:C:2026:496, paragraph 71 and the case-law cited).
-
- [85](#) Ibid., paragraph 72 and the case-law cited.
-
- [86](#) Ibid., paragraph 74 and the case-law cited.
-
- [87](#) ECtHR, 23 January 2025, *H.W. v. France*, CE:ECHR:2025:0123JUD001380521, § 65 and the case-law cited.
-
- [88](#) See, to that effect, judgment of 18 June 2026, [NTH Haustechnik](#) (C-484/24, EU:C:2026:496, paragraph 75 citing, to that effect, ECtHR, 23 January 2025, *H.W. v. France*, CE:ECHR:2025:0123JUD001380521, § 65 and the case-law cited).
-
- [89](#) See, to that effect, judgment of 24 February 2022, [Valsts ieņēmumu dienests \(Processing of personal data for tax purposes\)](#) (C-175/20, EU:C:2022:124, paragraph 56).
-
- [90](#) See point 100 et seq. of the present Opinion.
-
- [91](#) Articles 8 to 17 of the Statute of the RAB Database.
-
- [92](#) The security level of the data processed is designated as ‘high’ in Article 5(2) of the Statute of the RAB Database.
-
- [93](#) Article 26(1) of the Statute of the RAB Database specifies that the data in the database and the documents entered in the database concerning a person are retained therein for 15 years after the closure of the respective report or file. The data on a person, the person’s links with other data and the documents related to the person are deleted from the database in such a manner as to ensure the integrity of the data on persons, reports and files.
-
- [94](#) See point 107 of the present Opinion.