Case C-509/23

Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice

Date lodged:

8 August 2023

Referring court:

Administratīvā rajona tiesa (Latvia)

Date of the decision to refer:

7 August 2023

Applicant:

SIA Laimz

Defendant:

Izložu un azartspēļu uzraudzības inspekcija

Subject matter of the main proceedings

Action for the annulment of the decision of the Izložu un azartspēļu uzraudzības inspekcija (Lotteries and Gambling Inspection and Supervision Service, 'the Inspection Service') imposing on the applicant a fine for failing to fulfil the requirements laid down in the Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums (Law on the prevention of money laundering and terrorist financing and nuclear proliferation) with respect to the screening of customers and the verification of their status.

Subject matter and legal basis of the request

On the basis of Article 267 TFEU, the referring court seeks an interpretation of the provisions of Directive 2015/849 in order to identify the criteria in accordance with which a person may be regarded as being a close associate of a politically exposed person and whether obliged entities belonging to the same group may share customer screening information and use the information so obtained, and the situations requiring customer due diligence measures.

Questions referred for a preliminary ruling

1. Must point 11(a) of Article 3 of Directive 2015/849 be interpreted as meaning that an individual may be regarded as being a close associate of a politically exposed person solely on the ground that those persons form part of the same public body, without regard to any other circumstances?

2. Must [point 9 of Article 3] of Directive 2015/849 be interpreted as meaning that, in order to determine whether a person is a politically exposed person, it is necessary to determine whether that person holds one of the positions referred to in that article and, in addition, to carry out an investigation and verify that this is a high-ranking position rather than a middle-ranking or more junior position?

3. Must Article 45(1) of Directive 2015/849, read in conjunction with paragraph 8 of that same article, be interpreted as meaning that Member States must allow the obliged entities referred to in Article 2(1) of Directive 2015/849, which are regarded as companies in the same group, to share information with each other, including by concluding information sharing agreements and ensuring the reciprocal flow and mutual enforceability of information, in order to attain the objectives of Directive 2015/849?

4. Does Article 45(1) and (8) of Directive 2015/849, read in conjunction with points 12 and 15 of Article 3 of that directive, allow such information, or decisions, to be used and enforced in several undertakings belonging to the same group, those being decisions adopted, within that group, by the senior management of an undertaking belonging to that group?

5. Must Article 14(5) of Directive 2015/849, read in conjunction with Article 8(2) thereof, be interpreted as meaning that an obliged entity is not under an obligation to apply customer due diligence measures to existing customers if neither the time limit laid down in national law nor the time limit imposed by the internal control procedures for the application of new due diligence measures has expired, and the obliged entity is unaware of any new circumstances that might affect the risk assessment carried out in relation to the customer concerned?

6. Must the obligation which Article 11(d) of Directive 2015/849 imposes on obliged entities to apply customer due diligence measures where, upon the collection of winnings, the wagering of a stake, or both, the transaction amounts in total to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked, be interpreted as meaning that such measures must be applied every time the total amount of the transaction reaches EUR 2 000, irrespective of how long it is before the sum of EUR 2 000 laid down in that provision is reached again?

Provisions of European Union law relied on

Treaty on the European Union, first subparagraph of Article 5(4).

Directive (EU) 2015/849 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: recitals 30, 31, 32 and 34 and Articles 3, points 9, 11(a), 12 and 15, 5, 8(1) and (2), 11(a), (d) and (f), 13(1)(a) to (d) and (2), 14(5), 26(2) and 45(1) and (8).

Case-law

Judgment of the Court of Justice of the European Union of 17 November 2022, C-562/20, *Rodl & Partner*, EU:C:2022:883, paragraph 91.

Provisions of national law relied on

Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likums (Law on the prevention of money laundering and terrorist financing and nuclear proliferation): [1] Articles 1, points 2^1(a), 8^1, 18 and 18^2, 3(1), point 7, (2) and (2^1), 10(1), 11(1), points 1 and 4, 11^1(1), points 1 and 5, (2), (6) and (7), 25(2) and 29(1).

Succinct presentation of the facts and procedure in the main proceedings

1 The applicant is a commercial company, registered in the Commercial Register in the Republic of Latvia, whose business activity consists in the provision of services in the field of gambling and betting. The applicant's share capital is wholly owned by SIA Optibet, whose business activity also consists in gambling and betting. Both companies form part of the Enlabs AB group, a company registered in Sweden.

2 On 2 March 2020, the applicant and SIA Optibet concluded a contract to facilitate access to technical solutions under which SIA Optibet developed a technical solution for collecting and processing information in accordance with the requirements of the Law on the prevention of money laundering and terrorist financing and nuclear proliferation ('the Law on Prevention'). SIA Optibet obtains from third parties information, for the purposes of risk assessment and risk management in connection with the requirements of the Law on Prevention,

[1] All Latvian legislation of general application, in its current and historical versions, is available at: *https://likumi.lv/*.

relating to the status of individuals as politically exposed persons, their situation as regards penalties and their situation as regards negative information in the media. For its part, SIA Optibet, as the parent company of the applicant, provides the latter with access to the technical solutions and information services provided by third parties so as to make the most efficient use of resources and ensure uniform compliance with the requirements of the Law on Prevention within the group of undertakings.

3 Between 10 February 2022 and 4 March 2022, the Inspection Service carried out an inspection on the applicant in connection with the prevention of money laundering and stated that a customer of the applicant to whom the latter had been providing interactive gambling services since 23 August 2021 ('the customer') was to be regarded as a politically exposed person.

4 On 14 March 2022, the Inspection Service carried out a further inspection on the applicant in the course of which it looked at the deposits paid by the customer on 27 and 28 January 2022, when the customer had been registered as a player, how the customer's identity had been determined, how the internal control system had been applied to the customer and what customer screening procedures had been followed. On 14 March 2022, the Inspection Service drew up an inspection report in relation to the foregoing. That report states the following.

5 If it is established that the customer is a politically exposed person, the business relationship with that customer must be terminated, but, if the customer is a relative or a close associate of the politically exposed person, the business relationship may continue with the consent of the applicant's management.

6 In 2020, 2021 and 2022, the applicant did not establish the existence of any business relationships with close associates of politically exposed persons. In addition, the applicant did not screen the customer after the screening threshold (EUR 2 000) had been reached on 26 August 2021, which would have required it to ask the customer for information on his sources of income, the size of his income, his gambling budget, and whether he is a politically exposed person, or a family member or close associate of such a person, and to check information contained in publicly available databases in order to identify additional risk factors.

7 In the light of the customer's gambling habits and the amount of the bets, the applicant, on 31 January 2022, began a detailed screening in relation to the customer, asking him for additional information. The applicant took into account the deposits made by the customer in the amount of EUR 15 000, as a result of which the customer had been rated a medium-high risk on 14 September 2021, and the customer's historical data from his customer profile with SIA Optibet. In addition, on the basis of the data sharing agreement it had concluded with SIA Optibet, the applicant abided by the decision of SIA Optibet's board of management of 27 March 2020 to maintain the relationship with the high-risk customer in question. It is not customary for the applicant to review or compare its

customers against information obtained by SIA Optibet in the course of customer screenings.

8 Consequently, the Inspection Service concluded, on the basis of the results of the inspection it had carried out, that the applicant had not screened the customer, notwithstanding that the threshold for such a screening had been reached, had not determined the customer's status as a close associate of a politically exposed person and had not subjected the customer to a detailed screening in this regard.

9 In the light of the foregoing, the Inspection Service, by decision of 15 June 2022, imposed on the applicant a fine for failure to comply with the requirements laid down in the relevant legislation.

10 In its decision, the Inspection Service considered that, when entering into, and subsequently developing, its business relationship with the customer, the applicant could not use and rely on the screening of that customer carried out by another undertaking (SIA Optibet), even if the latter was linked to the applicant; the applicant should have conducted that screening autonomously and independently. In its view, since the applicant used and relied on information obtained from another undertaking, without itself asking the customer for information, it must be concluded that the applicant failed over a long period of time to take steps to ascertain whether the customer was a close associate of a politically exposed person and, consequently, did not comply with the enhanced monitoring requirements. Accordingly, it formed the view that the applicant had not correctly applied the internal customer control system or carried out any customer screening.

11 The Inspection Service considered the applicant's customer to be a close associate of a politically exposed person, since, at the same time as having a role in politics, that customer performed tasks as an official within the executive body of an association.

12 On 18 July 2022, the applicant brought before the Administratīvā rajona tiesa (District Administrative Court, Latvia) an action for the annulment of the Inspection Service's decision.

The essential arguments of the parties in the main proceedings

13 The applicant claims that it concluded with SIA Optibet an information sharing agreement under which the latter provided it with the information necessary to comply with the requirements of the Law on Prevention in respect of any player who is a customer of SIA Optibet and has subsequently become a customer of the applicant. It is therefore of the view that there was no need to request and re-examine the information obtained by SIA Optibet in connection with a particular customer who had previously been one of SIA Optibet's customers, and that that information *could* also be used in the context of the business relationship between the applicant and that customer. In the applicant's opinion, the same can be said of

management decisions in respect of common customers, since SIA Optibet and the applicant are linked.

14 The applicant submits that the Inspection Service misinterprets the concept of 'any other close relationship' contained in Article 1, point 18[2], of the Law on Prevention, in taking the view that the fact that a customer belongs to a public body in which a politically exposed person also works is in itself a reason to regard the customer as being associated with a politically exposed person. It argues that establishing whether such a relationship exists calls for an individual and complex assessment in which that circumstance is not the only factor determining the status of the person in question.

15 The Inspection Service notes that the Law on Prevention does not provide for the conclusion of a contract for information sharing between gambling and lottery operators. It states that, at the time when the customer entered into a business relationship with the applicant, the customer had terminated his business relationship with SIA Optibet, which is all the more reason why the applicant could not use the information obtained by Optibet. It therefore considers that the applicant and the customer entered into a new business relationship without due diligence. According to the Inspection Service, the applicant and SIA Optibet, as economic operators each holding a licence for the organisation of gambling in Latvia, are not linked by the legal status of a single group. It submits that SIA Optibet, a partner of the applicant, is itself a licensed gambling operator subject to the Law on Prevention, and to the same requirements as the applicant, and operating in accordance with its internal control system in order to ensure compliance with that Law. In its view, the relevant legal framework does not allow customer data to be shared with another undertaking, the effect of which would be to exempt the recipient of the information from the duty to comply with its legal obligations. Only credit and financial institutions may receive the results of a customer screening. In the opinion of the Inspection Service, the fact of having held a long-term position as an official within an executive body along with someone who has been classified as a politically exposed person may enable the politically exposed person, with the assistance of the other person, to conceal a misuse of power for private ends.

Succinct presentation of the reasoning in the request for a preliminary ruling

16 [1.] The concept of 'close associate of a politically exposed person' was introduced into the Law on Prevention in accordance with point 11 of Article 3 of Directive 2015/849, which defines 'persons known to be close associates'. Point 11 of Article 3 of Directive 2015/849 clarifies the meaning of 'close associates' in the context of that directive, namely natural persons who are known to have any other close business relations with a politically exposed person. Thus, close business relations alone are relevant to whether a person is to be regarded as a close associate in the context of that directive. Article 1, point 18[2], of the Law on Prevention, however, provides that a person generally maintaining business

relations or any other close relationship with a politically exposed person is to be regarded as a close associate of that person.

17 According to the clarifications provided in the Politiski nozīmīgu personu, to ģimenes locekļu un ar tām cieši saistītu personu noziedzīgi iegūtu līdzekļu legalizācijas, terorisma un proliferācijas finansēšanas risku vadības vadlīnijas (Guidelines for managing the risk of money laundering, terrorist financing and nuclear proliferation posed by politically exposed persons, their relatives and close associates), drawn up by the Latvijas Republikas Finanšu izlūkošanas dienests (Financial Information Service of the Republic of Latvia), the concept of 'any other close relationship' means a relationship that enables the politically exposed person, with the assistance of the other person, to conceal a misuse of public power for private ends. In particular, persons regarded as close associates of a politically exposed person are persons outside the latter's family circle (friends, for example) who are prominent members of the same political party, public body or trade union as the politically exposed person, for example, or well-known figures in society. In that context, the most important criterion is the existence of a 'close relationship' that may enable the politically exposed person, with the assistance of that other person, to conceal a misuse of power for private ends. It follows from the Guidelines that the fact of belonging to the same public body may be regarded as constituting the existence of a close relationship.

18 On the one hand, the very fact that persons are part of the same public body is a higher risk factor for money laundering or terrorist financing, especially if any of those persons holds or has held a politically significant position or is a widely known or prominent member of society, since, as is noted in recital 30 of Directive 2015/849, risk itself is variable in nature, and the variables, on their own or in combination, may increase or decrease the potential risk posed. It is important to bear in mind, however, that such a circumstance is not always obvious, since public registers only list officials and, in organisations in which there are many members, such information is not usually available to the public. What is more, there is no public register in Latvia in which all public associations or bodies have to register and make public the identity of their members.

19 On the other hand, the purpose, structure and size of public bodies are very different factors that may influence the likelihood of a risk occurring. It would be essential to determine the status of the persons in question and their mutual interaction within the body concerned (as official or member, and whether or not they are able to influence processes and so on, for example), the scope of the public body's activities (whether or not, for example, that body is involved in matters affecting political or financial processes) and other circumstances. At the same time, however, it is important to bear in mind that such an assessment might require additional resources on the part of the obliged entity, since the only way to determine whether persons forming part of the same public body have a close relationship with each other would be to collect and analyse additional information.

20 Likewise, in the context of close associates, it is essential to determine whether one of them holds one of the positions referred to in point 9 of Article 3 of Directive 2015/849, which, as that article makes clear, does not include middle-ranking or more junior positions. Furthermore, that article establishes that a politically exposed person is not any person known and prominent in the public sphere, but someone who meets the criteria laid down in that article and has the status of a high-ranking official. It follows from this that, in order to be able to say that someone is an associate of the politically exposed person, it is not sufficient to establish that one of those persons is publicly known or holds or has held a position that might be among those listed in point 9 of Article 3 of Directive 2015/849. It must also be ascertained whether the position in question is high-ranking. This calls for an individual assessment.

21 It would therefore be necessary to clarify whether point 11(a) of Article 3 of Directive 2015/849 must be interpreted as meaning that an individual may be regarded as a close associate of a politically exposed person on the sole ground that those persons form part of the same public body, without regard to any other circumstance, in particular whether the person in question holds or has held a position that might be among those referred to in point 9 of Article 3 of Directive 2015/849, and without determining whether that position is high-ranking.

22 [2.] In accordance with recital 35 of Directive 2015/849, in order to avoid repeated customer identification procedures, it is appropriate to allow customers whose identification has been carried out elsewhere to be introduced to the obliged entities.

23 Article 45(1) of the aforementioned directive provides that Member States are to require obliged entities that are part of a group to implement group-wide policies and procedures, including data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes. Those policies and procedures are to be implemented effectively at the level of branches and majority-owned subsidiaries in Member States and third countries. For its part, Article 45(8) of Directive 2015/849 provides that Member States must ensure that the sharing of information within the group is allowed.

24 It must therefore be concluded that undertakings in the same group, such as the applicant and SIA Optibet, are not entitled but obliged to share information, in particular by concluding information sharing agreements and ensuring the reciprocal flow and mutual enforceability of information. In addition, Member States have an obligation to ensure that such information sharing within the group is permitted and is sufficient to support the conclusion that the obliged entity in question has screened its customer. Conferring that right on any of the obliged entities referred to in point 1 of Article 2 of Directive 2015/849 (not only credit and financial institutions), first, enables the repetition (within a group of undertakings) of substantive customer identification procedures to be avoided, and, second, ensures an efficient use of funds for the undertakings in the group.

25 Article 13(1) of Directive 2015/849 lays down the customer due diligence measures which must be applied by obliged entities, in accordance with paragraph 2 of that article. At the same time, however, paragraph 2 of that article provides that obliged entities may determine the extent of such measures on a risk-sensitive basis. The referring court therefore takes the view that the foregoing allows information obtained as a result of information sharing within the group of undertakings to be enforced for the purposes of common customers. According to that court, this is confirmed by Article 26(2) of Directive 2015/849, which provides that Member States are to prohibit obliged entities from relying on third parties established in high-risk third countries. Member States may exempt branches and majority-owned subsidiaries of obliged entities established in the Union from that prohibition where those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 45. That directive thus permits the reciprocal flow and mutual enforceability of information where that information is obtained and used within a group of undertakings, in particular where it is obtained from an undertaking in the group that is not established in a high-risk third country.

26 For its part, Article 5 of Directive 2015/849 provides that Member States may lay down stricter rules to prevent money laundering and terrorist financing, which in turn means that a Member State may actually restrict the range of obliged entities on which it confers the rights provided for in Article 45(8) of Directive 2015/849.

27 [3.] In the light of the foregoing considerations, it is also important to clarify whether Article 45(1) and (8) of Directive 2015/849, read in conjunction with points 12 and 15 of Article 3 of that directive, also allows such information, or decisions, to be used and enforced in several undertakings belonging to the same group, these being decisions adopted, within that group, by the management of an undertaking belonging to that group.

28 [4.] In accordance with Article 8(1) and (2) of Directive 2015/849, Member States are to ensure that obliged entities take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors. Those steps must be proportionate to the nature and size of the obliged entities. The risk assessment referred to in paragraph 1 must be documented, kept up-to-date and made available to the relevant competent authorities and self-regulatory bodies concerned.

29 Article 11 of Directive 2015/849 provides that the obliged entity must apply customer due diligence measures, in particular, when establishing a business relationship, when there are doubts about the veracity or accuracy of previously obtained customer information, and, in the case of providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked. Furthermore, Article 14(5) of the aforementioned directive provides that Member States must require that obliged entities apply the customer due diligence

measures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, including at times when the relevant circumstances of a customer change.

30 It follows from Article 11[1](1), (2) and (7) of the Law on Prevention that, under that Law, the obliged entity has an obligation to update customer data in accordance with the customer risk assessment at least once every five years.

31 Consequently, the aforementioned legislative framework provides that customer due diligence measures must be carried out if any risk is identified, but no less frequently than laid down in the national framework.

32 The applicant submits that the application of due diligence to existing customers (including those on which information is available within the group of undertakings) prior to the deadline laid down in the aforementioned legislation is based on a risk assessment. It is of the view that, if, when assessing a customer, the obliged entity found no risks to be present, but such risks do arise later, before the deadline for updating customer data is reached, and the obliged entity cannot be informed about those risks, that entity is not obliged to apply customer due diligence measures to existing customers ahead of time.

33 The Court of Justice has provided the clarification that Article 14(5) of Directive 2015/849, read together with Article 8(2) thereof, must be interpreted as meaning that obliged entities are required, on the basis of an updated risk assessment, to apply due diligence measures or, where necessary, enhanced due diligence measures to an existing customer where appropriate, including where the relevant circumstances of the customer change, irrespective of the fact that the time limit laid down by national law for carrying out a new risk assessment on that customer has not yet expired (judgment of 17 November 2022, *Rodl & Partner*, C-562/20, EU:C:2022:883, paragraph 91).

34 In that clarification, however, the Court of Justice does not answer the question of how to proceed if the obliged entity was unaware of other new circumstances concerning the customer in question that might affect the risk assessment of that customer.

35 It is therefore appropriate to raise the fifth question referred for a preliminary ruling.

36 [5.] Likewise, given that the obligations imposed on obliged entities must be proportionate, it is appropriate to raise the sixth question referred for a preliminary ruling.