Case C-563/23

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

Date lodged:

12 September 2023

Referring court:

Sofiyski rayonen sad (Bulgaria)

Date of the decision to refer:

11 September 2023

Applicant in the main proceedings:

Teritorialna direktsia na Natsionalnata agentsia za prihodite – Sofia

---

Subject matter of the main proceedings

The main proceedings were initiated upon an application by the Natsionalna agentsia za prihodite (National Revenue Agency, ‘the NAP’) for permission to access data covered by banking secrecy in connection with the inspection of a taxable person with regard to income tax evasion and in particular to access data on that person’s account balances.

Subject matter and legal basis of the request

The present request for a preliminary ruling is made under Article 267 TFEU and concerns the interpretation of Articles 4(7), 32(1)(b), 51, 57(1)(a) and 79(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (‘the GDPR’), and Article 47 of the Charter of Fundamental Rights of the European Union. The request raises questions about the scope of the control exercised by a court as a body which can allow the disclosure of personal data within the framework of verifying the existence of tax obligations.

Questions referred

1. Must Article 4(7) of Regulation (EU) 2016/679 ('the General Data Protection Regulation' or 'the GDPR') be interpreted as meaning that

   a judicial authority which allows another State authority to access data concerning the account balances of taxable persons determines the purposes or means of the processing of personal data and is therefore a 'controller' for the purposes of the processing of personal data?

2. If the first question is answered in the negative, must Article 51 of the General Data Protection Regulation be interpreted as meaning that a judicial authority which allows another State authority to access data concerning the account balances of taxable persons is responsible for monitoring [the application of] that regulation and must therefore be classified as a 'supervisory authority' in relation to those data?

3. If either of the above questions is answered in the affirmative, must Article 32(1)(b) of the General Data Protection Regulation and Article 57(1)(a) of that regulation be interpreted as meaning that a judicial authority which allows another State authority to access data concerning the account balances of taxable persons is obliged, in the presence of data concerning a personal data breach committed in the past by the body to which such access is to be granted, to obtain information on the data protection measures taken and to assess the appropriateness of those measures in its decision to permit access?

4. Irrespective of the answers to the [second] and [third] questions, must Article 79(1) of the General Data Protection Regulation, read in conjunction with Article 47 of the Charter of Fundamental Rights of the European Union, be interpreted as meaning that, where the national law of a Member State provides that certain categories of data may be disclosed only after permission to do so has been granted by a court, the court so competent must of its own motion grant legal protection to the persons whose data are to be disclosed, by requiring the authority which has applied for access to the data in question, and which is known to have received binding instructions from the authority under Article 51(1) of the GDPR following a personal data breach, to provide information on the implementation of the measures imposed on it by administrative decision pursuant to Article 58(2)(d) of the GDPR?

Provisions of EU law

Regulation (EU) 2016/679 (GDPR): Articles 4(7), 32(1)(b), 51(1), 57(1)(a), 58(2)(d) and 79(1)

Charter of Fundamental Rights of the European Union: Article 47

Provisions of national law:

Zakon za zashtita na lichnite danni (Law on data protection; 'the ZZLD'): Articles 6, 12a, 17, 17a and 20

Danachno-osiguritelen protsesualen kodeks (Code of Tax and Social Security Procedure, 'the DOPK'): Articles 34, 37 and 110

Zakon za kreditnite institutsii (Law on credit institutions, 'the ZKI'): Article 62

Succinct presentation of the facts and procedure

1 On 13 June 2023, the NAP began an inspection of a Bulgarian national with regard to income tax evasion. The NAP found that the taxable person had seven bank accounts with various Bulgarian financial institutions. It requested that the person in question provide it with data on his bank account balances for 1 January 2020 and 31 December 2021 or to supply it with a declaration stating that he consented to the disclosure of his data covered by banking secrecy. As the person in question neither provided the specified data nor supplied the requested declaration, the NAP applied to the requesting court to allow the disclosure of data covered by banking secrecy in respect of those account balances.

2 The referring court notes that on 15 July 2019 it was reported in several Bulgarian media outlets that the personal data, including tax and social security information, of more than five million persons had been made public from the NAP's database. Subsequently, the NAP provided for access to a special database for the benefit of the persons affected by the data leak.

3 For that infringement, the Komisia za zashtita na lichnite danni (Commission for personal data protection, 'the KZLD'), which is the main supervisory authority in Bulgaria under Article 51 of the GDPR, imposed an administrative fine on the NAP. Twenty binding instructions were issued with the aim of ensuring that the NAP would undertake technical and organisational measures to prevent future data leaks.

4 By its judgment of 2 February 2023, the Administrativen sad – Sofia-Grad (Sofia City Administrative Court) confirmed 18 of the binding orders challenged before it and set aside the remaining two. An appeal against that judgment was brought before the Varhoven administrativen sad (Supreme Administrative Court). In the administrative case pending before that court, the hearing is scheduled for 14 December 2023.

5 The referring court has also noted that, in the context of an established leak of personal data to NAP staff, the KZLD issued further binding instructions for the protection of such data on the part of the NAP and recommended measures to monitor electronic access.

6 No information is available as to whether the factors that led to the unlawful disclosure of personal data have been remedied and what measures the NAP has undertaken to prevent further risks of that kind.

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

7 The referring court raises the question of the role of the court as a body which, on the basis of Article 62(6)(3) of the ZKI, can at the request of the Director of the Regional Directorate of the NAP allow access to the personal data of the person being inspected. Under Article 62(7) of the ZKI, the court decides on the application by way of a reasoned decision given in closed session no more than 24 hours after the application is received, also determining the period of time to which the information relates. The decision of the court in those proceedings is not subject to appeal.

8 The consensus of opinion is that, in proceedings under Article 62(7) of the ZKI, the courts exercise a purely formal review that is confined to determining whether individuals affected by the disclosure of data covered by banking secrecy have the status of taxable persons and whether there is information in each case indicating that the relevant data for a tax inspection have been requested from them and not provided. It would appear, on an uncritical application of the Bulgarian national rules, that the courts must always permit the disclosure of the data covered by banking secrecy in those cases. The position would be otherwise, however, if the court were to be classified as controller in respect of the personal data to which it grants access, since Articles 32 to 34 of the GDPR impose on the controller a number of obligations aimed at ensuring the security of data, including a minimum level of checks as to the presence of security measures.

9 According to the definition contained in Article 4(7) of the GDPR, a ‘controller’, ‘alone or jointly with others, determines the purposes and means of the processing of personal data’. The following special rule applies: ‘where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law’.

10 Bulgarian law does not determine who the controller is in the procedure under Article 62(7) of the ZKI. In that regard, although the courts do not have direct access to personal data forming the subject of an application for disclosure (this is not necessary in order for a person to be capable of being regarded as a ‘controller’; see the judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 3 [of the operative part]), they do in a sense determine the purposes of the processing by permitting or prohibiting access to personal data covered by banking secrecy. It therefore seems possible, by interpreting the legislation in a certain way, to regard the court as a body which determines the purposes of the data processing.

11 The Bulgarian legislature has not made use of its power to determine which body has the rights and the obligations of controller in this particular situation, in which the purposes of the processing of personal data are listed in law. In those circumstances, the provision must be interpreted to establish a criterion by which to clarify whether the court which permits access may be regarded as acting jointly with the NAP as controller in respect of personal data (first question referred for a preliminary ruling).

12 Given that the national legislation is unclear, an answer is also needed to the question whether the judicial authority which lays down the conditions governing access by another State authority to personal data covered by banking secrecy may also be regarded as a supervisory authority exercising some of the powers provided for in the GDPR in the confined area of supervision of access to data (second question referred for a preliminary ruling).

13 The referring court notes that it is generally known that the NAP breached the protection of personal data by permitting information about more than five million persons to be passed on. The KZLD imposed an administrative fine on the NAP for that infringement. Technical and organisational deficiencies in respect of the NAP's provision of access to personal data are also known. At least 21 binding instructions have been issued to the NAP for it to undertake concrete measures. No information is available as to whether those measures have been implemented.

14 It is the view of the referring court that, in those circumstances, the court, if it held the role of controller or supervisory authority, should permit access to data covered by banking secrecy only after having obtained information on the security measures applied and after having satisfied itself that those measures, at least at first sight, provide protection against a further breach of the security of personal data (third question referred for a preliminary ruling).

15 In addition, an answer is also required to the question whether it is permissible for a court empowered under national law to allow access to personal data covered by banking secrecy, even if it cannot be classified as a controller in respect of personal data or as a supervisory authority, to carry out such reviews on the basis of the obligation under Article 79 of the GDPR to ensure effective judicial protection (fourth question referred for a preliminary ruling). In actual fact, that provision is intended for cases in which the data subject explicitly seeks the court's protection. Where, however, the procedure for the disclosure of data takes place without the participation of the data subject and national law has expressly introduced prior judicial review, it would seem that the court must also intervene of its own motion. That might also be inferred from the right of persons to an effective remedy under Article 47 of the Charter. In the absence of that duty, the court's task would always be confined to conducting a formal examination and confirming the conduct of the administration, which would seem to be contrary to the objectives of Article 79 of the GDPR.