Case C-60/22

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:

1 February 2022

Referring court:

Verwaltungsgericht Wiesbaden (Germany)

Date of the decision to refer:

27 January 2022

Applicant:

UZ

Defendant:

Bundesrepublik Deutschland

Subject matter of the main proceedings

Data protection law – Regulation 2016/679 (General Data Protection Regulation) – Article 5(2) – Accountability – Articles 17(1)(d) and 18(1)(b) – Lawfulness of processing – Right to erasure or restriction – Use of processed data

Subject matter and legal basis of the request

Interpretation of EU law, Article 267 TFEU

Questions referred for a preliminary ruling

1. Does the failure of a controller to discharge or fully to discharge its obligation of accountability under Article 5 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, GDPR), for example due to the lack of

a record – or a complete record – of processing activities in accordance with Article 30 of the GDPR or the lack of an arrangement for a joint procedure in accordance with Article 26 of the GDPR, result in the data processing in question being unlawful within the meaning of Article 17(1)(d) of the GDPR and Article 18(1)(b) of the GDPR, so that the data subject has a right to erasure or restriction?

2. If Question 1 is answered in the affirmative, does the existence of a right to erasure or restriction have the consequence that the data processed must not be taken into account in judicial proceedings? Is that the case in any event where the data subject objects to the use of the data in the judicial proceedings?

3. If Question 1 is answered in the negative, does an infringement by a controller of Article 5, 30 or 26 of the GDPR have the consequence that, with regard to the question as to the use of the processed data in judicial proceedings, a national court may take the data into account only if the data subject expressly consents to that use?

Provisions of European Union law relied on

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) (OJ 2016 L 119, p. 1), recital 82 and Articles 5, 9, 17, 18, 26, 30 and 94

Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ 2013 L 180, p. 60), recital 52

Charter of Fundamental Rights of the European Union, Articles 7 and 8

Provisions of national law relied on

Bundesdatenschutzgesetz (Federal Law on data protection; 'the BDSG') (BGBl. I, p. 2 097), Paragraph 43(3)

Succinct presentation of the facts and procedure in the main proceedings

1 The applicant challenges a refusal decision by the Bundesamt für Migration und Flüchtlinge (Federal Office for Migration and Refugees) and seeks the grant of refugee status under Paragraph 3 of the Asylgesetz (Law on asylum; 'the AsylG'). The defendant's decision is based on the electronic 'MARiS' file (administrative file of the Federal Office), which is transmitted to the court via the Elektronisches Gerichts- und Verwaltungspostfach (Electronic Court and Administration

Mailbox; ‘EGVP’), including in the case of a joint procedure pursuant to Article 26. As regards the questions concerning the transmission of files in their entirety, reference is made to the questions already referred to the Court in that regard (Case C-564/21).

2 There are doubts as to whether the electronic ‘MARiS’ file kept by the defendant constitutes a record of processing activities within the meaning of Article 30 of Regulation 2016/679 (General Data Protection Regulation; ‘the GDPR’) at all, or at least a complete such record. Nor is there an arrangement or statutory regime within the meaning of Article 26 of the GDPR with regard to the procedure for the electronic transmission of files and the determination of responsibilities in that procedure. Those documents were requested by the referring court in the course of the proceedings. However, the defendant refused to submit them, on the ground, inter alia, that an arrangement pursuant to Article 26 of the GDPR does not exist with regard to the EGVP.

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

3 The question arises as to how the court should handle the applicant’s personal data, at least in the case where those data had been processed in a (formally) unlawful manner by the defendant, since, in accordance with Directive 2013/32, the GDPR applies to asylum proceedings under national law. Neither the Law on asylum nor the Verwaltungsgerichtsordnung (Rules of Procedure of the Administrative Courts) contains any statements on this.

4 According to recital 52 of Directive 2013/32, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data governs the processing of personal data carried out in asylum procedures in the Member States pursuant to this Directive. Directive 95/46 was repealed with effect from 25 May 2018, in accordance with Article 94(1) of the GDPR. However, according to Article 94(2) of the GDPR, references to the repealed Directive 95/46 are to be construed as references to this Regulation. The GDPR therefore applies in full to procedures for granting international protection.

5 Directive 95/46 already provided for the documentation of automatic processing operations, referred to as notification under Article 18 of that directive. The content of the notification under Article 19 of Directive 95/46 corresponded, in essence, to the current Article 30 of the GDPR, whereby the new standard applies to all forms of processing, that is to say, including filing systems.

6 During the period of application of Directive 95/46, as far as the electronic MARiS file was concerned, the defendant kept only a very rudimentary record of processing for the purposes of notification within the meaning of Directive 95/46 (Paragraph 4e of the BDSG, old). The record of processing (the notification) at that time was not subject to any special rules on the handling of special categories of personal data in accordance with Article 9 of the GDPR (Article 8 of Directive

95/46). Even today, such special rules on the handling of data in accordance with Article 9 and Article 10 of the GDPR do not appear to exist. This is because data concerning health and religion, as well as criminal convictions, are included in the electronic MARiS file in a general manner, as 'normal documents'. There does not appear to be any special protection with regard to data security, aside from the fact that there is probably access logging. However, an asylum seeker's file can be accessed from any of the defendant's branch offices throughout Germany, just as it can be accessed from the central office itself.

7 It is with regard, in particular, to the keeping of files and the submission of files to courts that the referring court has considerable doubts as to whether the defendant complies with the requirements of Article 5(1) of the GDPR, in conjunction with, for example, Articles 26 and 30 of the GDPR. Contrary to the order of the referring court, a record of processing activities was not submitted. The intention in that respect is to give the head of the authority of the responsible entity, that is to say, the defendant, the opportunity to be heard with regard to its accountability under Article 5(2) of the GDPR, following the decision of the Court of Justice.

8 Before it is heard, however, clarification is required as to whether a failure to comply with obligations under the GDPR and the resulting unlawfulness of the data processing leads to a penalty, such as the erasure of the data under Article 17(1)(d) of the GDPR or a restriction of processing under Article 18(1)(b) of the GDPR. That is the case in any event where the data subject – *in casu*, the applicant – so requests. This is because, otherwise, the court would be forced to participate in unlawful data processing in the judicial proceedings. The authority could constantly infringe the GDPR with impunity.

9 In such a case, only the supervisory authority pursuant to Article 58 of the GDPR would be able to act. However, the imposition of a fine on the Federal Office for Migration and Refugees would not be possible under national law. According to Paragraph 43(3) of the BDSG, which is based on Article 83(7) of the GDPR, administrative fines are not imposed on public authorities and other public bodies. There would be no incentive for the authority to act lawfully. This would have the consequence that neither the requirements of Directive 2013/32 nor the GDPR itself would be complied with.

10 The Court of Justice has already held that the 'notification' (now: records of processing activities) must be complete at the time of processing, but not earlier (Joined Cases C-92/09 and C-93/09, judgment of 9 November 2011, EU:C:2010:662, paragraph 95 et seq.). In the present case, the defendant had already processed the applicant's personal data by the time he filed his asylum application (on 7 May 2019). Therefore, at least in accordance with the case-law of the Court of Justice, there should have been a complete record of processing activities relating to the MARiS file (and thus in respect of the applicant's asylum file) at that time. That was not the case, however.

11 To date, the Court of Justice has not ruled on what applies in such a case, either under Directive 95/46 or under the GDPR. If it is taken into account that, in order to demonstrate compliance with the GDPR, the controller or processor should maintain records of processing activities under its responsibility (recital 82 of the GDPR), the question arises as to what consequence results from a controller's failure to do so. This is because the obligation of accountability under Article 5 of the GDPR cannot be discharged in such a case.

12 It is true that Article 83(5)(a) of the GDPR provides that an infringement of the obligation of accountability under Article 5 of the GDPR is punishable by administrative fines of up to EUR 20 000 000. However, as already stated, that does not apply to Federal authorities, in accordance with Paragraph 43(3) of the BDSG. Nevertheless, Article 17(1)(d) of the GDPR provides that unlawfully processed data must be erased, at least where the data subject so requests.

13 The absence of a record – or a complete record – of processing activities, leads the referring court to take the view that the data processing is 'formally' unlawful, at least in the light of Article 5 of the GDPR. The question therefore arises as to whether, in such a case, the data must be erased or at least blocked as a penalty for an omission under Article 5 of the GDPR, in conjunction with Article 30 thereof. This is because, otherwise, in the absence of the possibility of a penalty, effective enforcement of the GDPR could not take place.

14 In any event – as far as the referring court is aware – during the period of application of Article 18 et seq. of Directive 95/46, the French Republic, for example, laid down in national law a strict statutory prohibition on the use, in judicial proceedings, of personal data that had not been recorded by way of a notification from the responsible body to the supervisory authority (CNIL), as the use of the data was unlawful due to the lack of documentation. Thus, at least one penalty already existed there in so far as the data was not allowed to be processed and used by the court. During the period of application of the GDPR, provision has also been made in Portugal and other Member States for a prohibition of use as a result of a failure to maintain a record of processing activities. In the Federal Republic of Germany, such a mechanism does not exist within the framework of the transposition of Directive 95/46 or, moreover, during the period of application of the GDPR. Rather, in that country, the foundation was laid for 'acquiescence' to the lack of notification.

15 The electronic transmission of the defendant's file and pleadings also constitutes data processing within the meaning of point 2 of Article 4 of the GDPR, which must comply with the principles of data processing laid down Article 5 of the GDPR. Therefore, doubts also arise here as to the formal lawfulness of the data processing due to the transmission of the electronic 'MARiS' file and the pleadings of the defendant via the respective routes of transmission. In that respect, too, there is no record of processing activities or an arrangement on joint responsibility. It is true that there is a Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere

elektronische Behördenpostfach (Regulation on the technical framework conditions of electronic legal transactions and on the Special Electronic Mailbox for Authorities) of 24 November 2017 (BGBl. I, p. 3 803, amended by Article 6 of the Law of 5 October 2021, BGBl. I, p. 4 607). It regulates the transmission of electronic documents to the courts of the *Länder* and the Federal Republic. Within that framework, the supreme authorities of the Federal Government or the governments of the *Länder* can check, for their area, the identity of the authorities or legal entities governed by public law in order to grant them access to the Special Electronic Mailbox for Authorities (referred to as the 'BeBPo'). The supreme authorities of the Federal Government or several governments of the *Länder* can also jointly designate a public-law body for their areas. Precisely which body that actually is has not been regulated. Ultimately, it is most likely the 'Bund-Länder-Arbeitsgruppe der Justizministerien' (Government-*Länder* Working Group of the Ministries of Justice) (Bund-Länder-Kommission für Informationstechnik in der Justiz [BLK] Arbeitsgruppe IT-Standards in der Justiz (Government-*Länder* Commission for Information Technology in the Judiciary [BLK], Working Group on IT Standards in the Judiciary)). Which authority or authorities is or are responsible for the directory service of the EGVP or the BeBPo or even for the required server structure is not known or documented.

16 Nor are there any statutory or other written arrangements between the courts and authorities regulating their respective responsibilities in that regard, as would be required under Article 26 of the GDPR. Even in Federal *Länder* which, in accordance with their legislative regulations, have opted for the joint procedure model, there is no such implementation in conformity with data protection standards. In Hesse, its regulation even provides that the electronic mailbox is to be kept exclusively on the servers of the 'data centre' of the judiciary, that is to say, at the Hessische Zentrale für Datenverarbeitung (Hesse Data Processing Centre; 'the HZD'). In that context, the HZD is not part of the judiciary and, as an intermediary, is at most a processor pursuant to Article 28 of the GDPR.

17 It is only known that the Landesamt für Datensicherheit (Regional Office for Data Security) in North Rhine-Westphalia is in fact supposed to be responsible, as an 'intermediary', for the administration and operation of the central, transnational register server S.A.F.E. The SAFE ID should be unchangeable and allocated only once (see, in that regard, SAFE – http://www.egvp.de/Drittprodukte/SAFE_Abbildungsvorschrift _SAFE_ID_Stand_Dez_2014.pdf). In addition, mailboxes in the EGVP are designated by a unique identification number (referred to as the Govello ID). As far as the referring court is aware, those IDs are supposed to be registered in a directory service maintained by North Rhine-Westphalia (IT-NRW). Who is actually responsible for the allocation of the Govello ID in the network made up of the Federal Government and the *Länder* is not regulated.

18 It is not known on which legal basis under data protection law the EGVP operates. With regard to the inquiry regarding an arrangement pursuant to Article 26 of the GDPR, the defendant refused to state its position on the matter and to submit such

an arrangement. In that respect, it is also questionable whether lawful transmission can take place via the 'Special Electronic Mailbox for Authorities' in the case where responsibilities have not been determined in accordance with Article 26 of the GDPR. This also applies with regard to data security, as none of the documents are encrypted during transmission.

19 The referring court takes the view that, under current positive law, the circumstance of whether end-to-end encryption must be used for the Special Electronic Mailbox for Lawyers is not a decisive factor. At least in Hesse, there is no encryption of the messages to be transmitted between the intermediary, the HZD and the court concerned – including, therefore, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden).

20 This is not relevant to the present case, however, because the procedure corresponds to a mail procedure. With regard to the web-based Gmail service, the Court of Justice held that it is not a communications service, as the service does not itself provide internet access, does not consist wholly or mainly in the conveyance of signals on electronic communications networks and therefore does not constitute an 'electronic communications service' (judgment of 13 June 2019, C-193/18, EU:C:2019:498). The EGVP is therefore not a service covered by Directive 2002/58/EC (Article 2(4) of the GDPR). Consequently, the GDPR applies, with the consequence that the EGVP and the associated procedures must be recorded in a register of processing activities, and, given that the procedure has a plurality of controllers, the respective responsibilities must be agreed upon by arrangement in accordance with Article 26 of the GDPR. Neither has taken place in the present case. This raises doubts about the lawfulness of the data transmission.

21 The EGVP is a procedure of the judicial administrations, which are attributable to the second power, the executive, and of the defendant, which is also part of the executive branch. Thus, the referring court takes the view that the defendant is required to ensure that the electronic procedure for data transmission in respect of pleadings and files is in compliance with the GDPR.

22 Therefore, in the context of judicial activities, the question that arises for the referring court is how the data supplied via the EGVP system via the 'Mailbox for Authorities' are to be handled if the EGVP procedure and the associated data processing as such do not comply with the GDPR.

23 The referring court must observe and comply with the GDPR in the context of judicial activities.

24 It has no influence on the lawfulness of data processing by the judicial administration, as this is outside the 'judicial activity' of the second power, the executive. However, the referring court must observe and comply with EU law. If parties to proceedings infringe that law, the use of data by the courts would most likely not be permissible, as otherwise the court would be participating in

unlawful data processing. In the present case, the situation is exacerbated by the fact that, having regard to the correspondence to date, the defendant is (deliberately) infringing EU law.

25 There is also no case that would justify use by the courts on the basis of Article 17(3)(e) of the GDPR, for the establishment, exercise or defence of legal claims by the defendant. It is true that the defendant's data serve to ensure compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or to ensure the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 17(3)(b) of the GDPR). At the same time, however, this would permanently legalise an activity that infringes data protection law.

26 It follows that the questions referred are of particular importance as regards the implementation of the GDPR in judicial proceedings. The objective of protecting fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, as laid down in Article 1(2) of the GDPR, would be thwarted.

27 In that respect, at least in the event that Question 1 is answered in the negative, it would be necessary that the data subject – *in casu*, the applicant – agrees to, or, better, expressly consents to, the use of his or her data in the judicial proceedings despite the fact that they had been processed in a formally unlawful manner.

28 However, this would also have the consequence that, in the event that the data subject refuses to give such consent, the court would not be permitted to process (use) the data processed by the defendant, which it submits in the form of the electronic 'MARiS' authority file. This would further have the consequence that a decision-making basis would not exist until the breach of the documentation obligations is remedied. The defendant's initial decision would always have to be annulled. A decision on the asylum status claimed would not be possible until the breach of the documentation obligations is remedied.