JUDGMENT OF THE COURT (Fifth Chamber)
4 May 2023 (*)

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 5 – Principles relating to processing – Controllership – Article 6 – Lawfulness of processing – Electronic file compiled by an administrative authority relating to an asylum application – Transmission to the competent national court via an electronic mailbox – Infringement of Articles 26 and 30 – No arrangement determining joint responsibility for processing and maintaining the record of processing activities – Consequences – Article 17(1) – Right to erasure ('right to be forgotten') – Article 18(1) – Right to restriction of processing – Concept of 'unlawful processing' – Taking into account of the electronic file by a national court – Absence of consent of the data subject)

In Case C-60/22,

REQUEST for a preliminary ruling under Article 267 TFEU from the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), made by decision of 27 January 2022, received at the Court on 1 February 2022, in the proceedings

UZ

v

Bundesrepublik Deutschland,

THE COURT (Fifth Chamber),

composed of E. Regan (Rapporteur), President of the Chamber, D. Gratsias, M. Ilešič, I. Jarukaitis and Z. Csehi, Judges,

Advocate General: T. Ćapeta,

Registrar: A. Calot Escobar,

having regard to the written procedure,

after considering the observations submitted on behalf of:

UZ, by J. Leuschner, Rechtsanwalt,

the German Government, by J. Möller and P.-L. Krüger, acting as Agents,

the Czech Government, by O. Serdula, M. Smolek and J. Vláčil, acting as Agents,

the French Government, by A.-L. Desjonquères and J. Illouz, acting as Agents,

the Austrian Government, by A. Posch, M.–T. Rappersberger and J. Schmoll, acting as Agents,

the Polish Government, by B. Majczyna, acting as Agent,

the European Commission, by A. Bouchagiar, F. Erlbacher and H. Kranenborg, acting as Agents,

having decided, after hearing the Advocate General, to proceed to judgment without an Opinion,

gives the following

Judgment

This request for a preliminary ruling concerns the interpretation of Article 5, Article 17(1)(d), Article 18(1)(b) and Articles 26 and 30 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) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2; 'the GDPR').

The request has been made in proceedings between UZ, a third-country national, and the Bundesrepublik Deutschland (Federal Republic of Germany), represented by the Bundesamt für Migration und Flüchtlinge (Federal Office for Migration and Refugees, Germany) ('the Federal Office'), concerning the processing of the application for international protection lodged by that national.

Legal context

European Union law

Directive 2013/32/EU

Recital 52 of 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 (recast) (OJ 2013 L 180, p. 60) is worded as follows:

'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 [(OJ 1995 L 281, p. 31)] governs the processing of personal data carried out in the Member States pursuant to this Directive.'

The GDPR

Recitals 1, 10, 40, 74, 79 and 82 of the GDPR are worded as follows:

The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union … and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.

In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the [European] Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. …

In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.'

Chapter I of the GDPR, entitled 'General provisions', contains Articles 1 to 4.

Article 1 of that regulation, entitled 'Subject matter and objectives', provides:

'1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

…'

Article 4 of that regulation, entitled 'Definitions', provides in points 2, 7 and 21 thereof:

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

…

"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; 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;

…

"supervisory authority" means an independent public authority which is established by a Member State pursuant to Article 51;

Chapter II of the GDPR, headed 'Principles', comprises Articles 5 to 11.

Article 5 of that regulation, headed 'Principles relating to processing of personal data', states:

'1. Personal data shall be:

processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation");

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data

minimisation”);

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”);

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”);

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“accountability”).’

Article 6 of that regulation, headed ‘Lawfulness of processing’, provides in paragraph 1:

‘Processing shall be lawful only if and to the extent that at least one of the following applies:

the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

processing is necessary for compliance with a legal obligation to which the controller is subject;

processing is necessary in order to protect the vital interests of the data subject or of another natural person;

processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.’

Article 7 of the GDPR concerns the conditions for consent, while Article 8 of that regulation determines the conditions applicable to child’s consent in relation to information society services.

Article 9 of that regulation, entitled ‘Processing of special categories of personal data’, prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

Article 10 of that regulation, entitled ‘Processing of personal data relating to criminal convictions and offences’, concerns the processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) of that regulation.

Chapter III of the GDPR, entitled ‘Rights of the data subject’, contains Articles 12 to 23.

Article 17 of that regulation, entitled ‘Right to erasure (“right to be forgotten”)’, is worded as follows:

‘1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

the personal data have been unlawfully processed;

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

…

(e) for the establishment, exercise or defence of legal claims.’

Under Article 18 of that regulation, entitled ‘Right to restriction of processing’:

‘1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

…

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject’s consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public

interest of the Union or of a Member State.
…'

Chapter IV of the GDPR, entitled 'Controller and processor', contains Articles 24 to 43.

In Section 1 of that chapter, entitled 'General obligations', Article 26 of that regulation, entitled 'Joint controllers", is worded as follows:

'1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.'

Article 30 of that regulation, entitled 'Records of processing activities', provides:

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

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

the purposes of the processing;

a description of the categories of data subjects and of the categories of personal data;

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

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

In Chapter VI of the GDPR, entitled 'Independent supervisory authorities', Article 58 thereof, entitled 'Powers', provides in paragraph 2:

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

to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

to order the controller to communicate a personal data breach to the data subject;

to impose a temporary or definitive limitation including a ban on processing;

to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

to order the suspension of data flows to a recipient in a third country or to an international organisation.'

Chapter VIII of the GDPR, entitled 'Remedies, liability and penalties', includes Articles 77 to 84.

Article 77 of the GDPR, headed 'Right to lodge a complaint with a supervisory authority', provides, in paragraph 1 thereof:

'Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.'

Article 82 of the GDPR, entitled 'Right to compensation and liability', states in paragraphs 1 and 2:

'1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.'

Article 83 of that regulation, entitled 'General conditions for imposing administrative fines', provides in paragraphs 4, 5 and 7:

'4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to [EUR 10 000 000] or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

…

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to [EUR 20 000 000] or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.'

In Chapter XI of that regulation, entitled 'Final provisions', Article 94 thereof, entitled 'Repeal of Directive 95/46/EC', provides:

'1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.'

German law

Paragraph 43 of the Bundesdatenschutzgesetz (Federal Law on data protection) of 20 December 1990 (BGBl. 1990 I, p. 2954), in the version applicable to the dispute in the main proceedings ('the BDSG'), entitled 'Provisions relating to administrative fines', provides in subparagraph 3 thereof:

'No administrative fine may be imposed on public authorities and other public bodies within the meaning of Paragraph 2(1) [of the BDSG].'

The dispute in the main proceedings and the questions referred for a preliminary ruling

On 7 May 2019, the applicant in the main proceedings lodged an application for international protection with the Federal Office, which rejected it.

In order to adopt its rejection decision ('the decision at issue'), the Federal Office relied on the electronic 'MARIS' file which it had compiled, which contains the personal data relating to the applicant in the main proceedings.

The latter brought an action against the decision at issue before the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), which is the referring court in the present case. The electronic 'MARIS' file was then sent to that court, in the context of a joint procedure under Article 26 of the GDPR, via the Electronic Court and Administration Mailbox ('*Elektronisches Gerichts- und Verwaltungspostfach*'), which is managed by a public body forming part of the executive.

The referring court notes that it is apparent from recital 52 of Directive 2013/32 that the processing of personal data carried out by the Member States in the context of the procedures for granting international protection is governed by the GDPR.

That court doubts, however, that the maintenance of the electronic file compiled by the Federal Office and the transmission of that file to it by the Electronic Court and Administration Mailbox comply with that regulation.

First, as regards the maintenance of the electronic file, it has not been demonstrated that the Federal Office complies with the combined provisions of Article 5(1) and Article 30 of the GDPR. Despite a request made to that end by the referring court, the Federal Office did not produce a complete record of the processing activities relating to that file. Such a record should have been compiled at the time of the processing of the personal data relating to the applicant in the main proceedings, namely the date on which he lodged his application for international protection. The Federal Office should be heard on the issue of its accountability, under Article 5(2) of the GDPR, after the Court has ruled on the present request for a preliminary ruling.

Second, as regards the transmission of the electronic file via the Electronic Court and Administration Mailbox, such transmission constitutes 'processing' of data, within the meaning of Article 4(2) of the GDPR, which must comply with the principles laid down in Article 5 of that regulation. However, in disregard of Article 26 of that regulation, no national legislation governs that procedure for transmission between the administrative authorities and the courts by defining the respective responsibilities of the joint controllers and no arrangement to that effect has been produced by the Federal Office, despite a request to that effect made by the referring court. The latter thus raises the question of the lawfulness of that transfer of data via the Electronic Court and Administration Mailbox.

In particular, according to the referring court, it is necessary to determine whether the disregard of the obligations laid down in Articles 5, 26 and 30 of the GDPR from which the unlawful processing of personal data allegedly stems must be penalised by the erasure of those data, in accordance with Article 17(1)(d) of that regulation, or by a restriction of processing, in accordance with Article 18(1)(b) of that regulation. Such penalties must at least be envisaged in the case of a request by the data subject. Otherwise, that court would be obliged to participate in unlawful processing of those data in the context of the judicial proceedings. In such a case, only the supervisory authority would be able to intervene, pursuant to Article 58 of the GDPR, by imposing an administrative fine on the public authorities concerned, pursuant to Article 83(5)(a) of that regulation. However, in accordance with

Article 43(3) of the BDSG, which transposes Article 83(7) of that regulation, no administrative fine may be imposed at national level on public authorities and other public bodies. It follows that neither Directive 2013/32 nor the GDPR has been complied with.

Furthermore, the referring court considers that the processing at issue in the main proceedings does not fall within the scope of Article 17(3)(e) of the GDPR, which allows the use of personal data for the purposes of the establishment, exercise or defence of legal claims by the defendant. It is true that, in the present case, the data are used by the Federal Office to comply, in accordance with Article 17(3)(b) of that regulation, with a legal obligation which requires processing by EU or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. However, if that provision were applied, this would permanently legalise an activity that infringes data protection law.

The referring court is therefore uncertain as to what extent it may, in the context of its judicial activity, take into account the personal data provided in the context of such a procedure which is attributable to the executive. If the maintenance of the electronic file or its transmission via the Electronic Court and Administration Mailbox were to be classified as unlawful processing under the GDPR, that court would, by taking such data into account, participate in the unlawful processing at issue, which would run counter to the objective pursued by that regulation, which is to protect the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.

In that regard, the referring court also wonders whether the fact that the data subject has given his or her express consent or objects to the use of his or her personal data in the context of judicial proceedings is capable of affecting the possibility of those data being taken into account. If that court were unable to take into account the data contained in the electronic 'MARIS' file on account of the illegalities vitiating the maintenance and transmission of that file, there would be no legal basis, pending any rectification of those illegalities, for the purpose of taking a decision on the application of the applicant in the main proceedings for the grant of refugee status. Consequently, that court would have to annul the decision at issue.

In those circumstances, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

Does the failure of a controller to discharge or fully to discharge its obligation of accountability under Article 5 of the [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?

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?

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?'

Consideration of the questions referred

Admissibility

Without formally raising a plea of inadmissibility, the German Government expresses doubts as to the relevance of the questions referred for a preliminary ruling to the outcome of the dispute in the main proceedings. First of all, it is apparent from the order for reference that the disregard, by the Federal Office, of Article 5(2) of the GDPR has not been definitively established, the referring court merely presuming this to be the case. Next, that court did not state that the files of the Federal Office, on the assumption that it is not authorised to use them, are alone decisive for the solution of this dispute It also has other sources of information, which, in accordance with the principle of ex officio investigation, should be fully exploited where an authority does not submit files or where those files are incomplete. Lastly, the third question is manifestly hypothetical, since it is not apparent from the order for reference that the applicant in the main proceedings consented to or consents to the use of the processing of his personal data by the referring court.

It should be recalled that, according to settled case-law, questions relating to EU law enjoy a presumption of relevance. The Court may refuse to rule on a question referred by a national court for a preliminary ruling only where it is quite obvious that the interpretation of EU law that is sought bears no relation to the actual facts of the main action or its purpose, where the Court does not have before it the legal or factual material necessary to give a useful answer to the questions submitted to it or where the problem is hypothetical. What is more, in proceedings under Article 267 TFEU, which are based on a clear separation of functions between the national courts and the Court, the national court alone has jurisdiction to find and assess the facts in the case before it (see, inter alia, judgment of 24 March 2022, *Autoriteit Persoonsgegevens*, C-245/20, EU:C:2022:216, paragraphs 20 and 21 and the case-law cited).

As is clear from the second paragraph of Article 267 TFEU, in the framework of the close cooperation between the national courts or tribunals and the Court of Justice based on the assignment to each of different functions, it is for the referring court to decide at what stage in the proceedings it is appropriate for that court to refer a question to the Court of Justice for a preliminary ruling (judgment of 17 July 2008, *Coleman*, C-303/06, EU:C:2008:415, paragraph 29 and the case-law cited).

In particular, the Court has already held, in that regard, that the fact that factual questions have not yet been dealt with in an evidential adversarial procedure does not, as such, render a question referred for a preliminary ruling

inadmissible (see, to that effect, judgment of 11 September 2014, *Österreichischer Gewerkschaftsbund*, C-328/13, EU:C:2014:2197, paragraph 19 and the case-law cited).

In the present case, even though it is apparent from the request for a preliminary ruling that the referring court has not definitively ruled on the existence of an infringement, by the Federal Office, of its obligations under Article 5(2) of the GDPR, read in conjunction with Articles 26 and 30 of that regulation, since that aspect of the dispute in the main proceedings must still, according to the information provided in that request, be the subject of an exchange of arguments, the fact remains that that court found that neither the arrangement on the joint processing of the data nor the records of processing activities, which are referred to in the latter two provisions, have been produced by the Federal Office as controller, despite the request that the referring court has made to it for this purpose.

Furthermore, it is apparent from the order for reference that, in the opinion of that court, which alone is responsible for establishing and assessing the facts, the decision at issue was adopted solely on the basis of the electronic file compiled by the Federal Office, the holding and transmission of which could infringe the rules laid down by that regulation, with the result that that decision might have to be annulled on that ground.

Lastly, as regards the consent of the applicant in the main proceedings to the use of his personal data in the context of the court proceedings, it is sufficient to note that the third question referred for a preliminary ruling seeks specifically to determine whether it is necessary, in the present case, for such consent to be expressed in order for the referring court to be authorised to take those data into consideration.

In those circumstances, where the Court receives a request for interpretation of EU law which is manifestly not unrelated to the reality or the subject matter of the main proceedings and it has the necessary information in order to give appropriate answers to the questions put to it in relation to the effect of the GDPR on the main proceedings, it must reply to that request and is not required to consider the facts as presumed by the referring court or tribunal, a presumption which it is for the referring court or tribunal to verify subsequently if that should prove to be necessary (see, by analogy, judgment of 17 July 2008, *Coleman*, C-303/06, EU:C:2008:415, paragraph 31 and the case-law cited).

Consequently, it must be held that the present request for a preliminary ruling is admissible and that it is necessary to answer the questions submitted by the referring court, it being understood that it is, however, for that court to ascertain whether the Federal Office has failed to comply with the obligations laid down in Articles 26 and 30 of the GDPR.

Substance

The first question

By its first question, the referring court asks, in essence, whether Article 17(1)(d) and Article 18(1)(b) of the GDPR must be interpreted as meaning that failure by the controller to comply with the obligations laid down in Articles 26 and 30 of that regulation, which relate, respectively, to the conclusion of an arrangement determining joint responsibility for processing and to the maintenance of a record of processing activities, constitutes unlawful processing conferring on the data subject a right to erasure or restriction of processing, where such a failure entails an infringement by the controller of the principle of 'accountability' as set out in Article 5(2) of that regulation.

According to the Court's settled case-law, in interpreting a provision of EU law it is necessary to consider not only its wording but also its context and the objectives pursued by the legislation of which it forms part (see to that effect, inter alia, judgment of 12 January 2023, *Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-132/21, EU:C:2023:2, paragraph 32 and the case-law cited).

As regards, in the first place, the wording of the relevant provisions of EU law, it should be recalled that, in accordance with Article 17(1)(d) of the GDPR, the data subject is to have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller is to have the obligation to erase that data without undue delay where those data have been 'unlawfully processed'.

Similarly, under Article 18(1)(b) of the GDPR, if the data subject opposes the erasure of such data and requests the restriction of their use instead, he or she is to have the right to obtain from the controller restriction of processing where the 'processing is unlawful'.

The provisions mentioned in the two preceding paragraphs must be read in conjunction with Article 5(1) of that regulation, according to which processing of personal data must comply with a number of principles which are set out in that provision, including that set out in Article 5(1)(a) of that regulation, which specifies that personal data is to be processed 'lawfully, fairly and in a transparent manner in relation to the data subject'.

Under Article 5(2) of the GDPR, the controller, in accordance with the principle of 'accountability' laid down in that provision, is responsible for compliance with paragraph 1 of that article and must be able to demonstrate its compliance with each of the principles set out in paragraph 1 of that article, the burden of such proof thus being placed on it (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, paragraphs 77, 78 and 81).

It follows that, pursuant to paragraph 2 of Article 5 of that regulation, read in conjunction with paragraph 1(a) of that article, the controller must ensure that the processing of the data which it carries out is 'lawful'.

It should be noted that the lawfulness of processing is precisely the subject, as is apparent from its actual title, of Article 6 of the GDPR, which provides that processing is to be lawful only if at least one of the conditions set out in points (a) to (f) of the first subparagraph of paragraph 1 of that article is met, namely, as is also apparent from recital 40 of that regulation, either that the data subject has given consent to the processing of his or her personal data for one or more specific purposes, or that processing is necessary for one of the purposes referred to, which relate, respectively, to the performance of a contract to which the data subject is party or to the taking of steps at

the request of the data subject prior to entering into a contract, compliance with a legal obligation to which the controller is subject, the protection of the vital interests of the data subject or of another natural person, the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

That list of cases in which the processing of personal data may be regarded as lawful is exhaustive and restrictive, so that, in order that it can be regarded as lawful, processing must fall within one of the cases provided for in the first subparagraph of Article 6(1) of the GDPR (see, to that effect, judgments of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 99 and the case-law cited, and of 8 December 2022, *Inspektor* v *Inspektorata kam Visshia sadeben savet (Purposes of the processing of personal data – Criminal investigation)*, C-180/21, EU:C:2022:967, paragraph 83).

Thus, according to the case-law of the Court, any processing of personal data must comply with the principles relating to the processing of data which are set out in Article 5(1) of that regulation and satisfy the conditions governing lawfulness of the processing which are listed in Article 6 of that regulation (see, inter alia, judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 208; of 22 June 2021, *Latvijas Republikas Saeima (Penalty points),* C-439/19, EU:C:2021:504, paragraph 96; and of 20 October 2022, *Digi*, C-77/21, EU:C:2022:805, paragraphs 49 and 56).

Furthermore, in so far as Articles 7 to 11 of the GDPR, which appear, like Articles 5 and 6 thereof, in Chapter II of that regulation, which chapter relates to principles, are intended to clarify the scope of the data controller's obligations under Article 5(1)(a) and Article 6(1) of that regulation, the processing of personal data, in order to be lawful, must also comply, as is apparent from the Court's case-law, with those other provisions of that chapter which concern, in essence, consent, processing of special categories of sensitive personal data and processing of personal data relating to criminal convictions and offences (see, to that effect, judgments of 24 September 2019, *GC and Others (De-referencing of sensitive data)*, C-136/17, EU:C:2019:773, paragraphs 72 to 75, and of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraphs 100, 102 and 106).

It should be noted, as all the governments that have lodged written observations and the European Commission have done, that compliance by the controller with the obligation laid down in Article 26 of the GDPR to conclude an arrangement determining joint responsibility for processing and the obligation to maintain a record of processing activities laid down in Article 30 of that regulation is not among the grounds for lawfulness of processing which are set out in the first subparagraph of Article 6(1) of that regulation.

In addition, unlike Articles 7 to 11 of the GDPR, Articles 26 and 30 of that regulation are not intended to clarify the scope of the requirements set out in Article 5(1)(a) and Article 6(1) of that regulation.

It follows, therefore, from the actual wording of Article 5(1)(a) and the first subparagraph of Article 6(1) of the GDPR that infringement by the controller of the obligations laid down in Articles 26 and 30 of that regulation does not constitute 'unlawful processing' within the meaning of Article 17(1)(d) and Article 18(1)(b) of that regulation, which would stem from the controller's infringement of the principle of 'accountability' as set out in Article 5(2) of that regulation.

That interpretation is supported, in the second place, by the context of which those various provisions form part. It is clear from the very structure of the GDPR and, therefore, from its scheme that it distinguishes between, on the one hand, the 'principles', which are the subject of Chapter II thereof, which contains, inter alia, Articles 5 and 6 of that regulation, and, on the other hand, the 'general obligations', which form part of Section 1 of Chapter IV of that regulation relating to controllers, which include the obligations referred to in Articles 26 and 30 of that regulation.

That distinction is, moreover, reflected in Chapter VIII of the GDPR relating to penalties, since infringements of Articles 26 and 30 of that regulation, on the one hand, and those of Articles 5 and 6 thereof, on the other hand, are subject, respectively, in paragraphs 4 and 5 of Article 83 of that regulation, to administrative fines up to a certain amount, which differs according to the paragraph concerned on account of the degree of gravity of those respective infringements which is recognised by the EU legislature.

In the third and last place, the literal interpretation of the GDPR set out in paragraph 61 of the present judgment is supported by the objective pursued by that regulation, as set out in Article 1 thereof and recitals 1 and 10 thereof, which consists, inter alia, in ensuring a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data, as enshrined in Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) TFEU. (see, to that effect, judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, EU:C:2022:601, paragraph 125 and the case-law cited).

The absence of an arrangement determining joint responsibility, pursuant to Article 26 of the GDPR, or of a record of processing activities, within the meaning of Article 30 of that regulation, is not sufficient in itself to establish the existence of an infringement of the fundamental right to the protection of personal data. In particular, while it is true that, as is apparent from recitals 79 and 82 of that regulation, the clear allocation of the responsibilities between joint controllers and the record of processing activities are means of ensuring that those controllers comply with the guarantees laid down by that regulation for the protection of the rights and freedoms of data subjects, the fact remains that the absence of such a record or of such an arrangement does not demonstrate, in itself, that those rights and freedoms have been infringed.

It follows that an infringement of Articles 26 and 30 of the GDPR by the controller does not constitute 'unlawful processing' within the meaning of Article 17(1)(d) or Article 18(1)(b) of that regulation, read in conjunction with Article 5(1)(a) and the first subparagraph of Article 6(1) thereof, conferring on the data subject a right to erasure

or restriction of processing.

As all the governments which have lodged written observations and the Commission have argued, such an infringement must therefore be remedied by recourse to other measures provided for by the GDPR, such as the adoption, by the supervisory authority, of 'corrective powers', within the meaning of Article 58(2) of that regulation, in particular, in accordance with point (d) of that provision, the bringing of processing operations into compliance, the lodging of a complaint with the supervisory authority, in accordance with Article 77(1) of that regulation, or compensation for any damage caused by the controller, pursuant to Article 82 thereof.

Lastly, in view of the concerns expressed by the referring court, it should also be stated that the fact that, in the present case, the imposition of an administrative fine, pursuant to Article 58(2)(i) and Article 83 of the GDPR, is said to be precluded since national law prohibits such a penalty against the Federal Office is not such as to prevent the effective enforcement of that regulation. It is sufficient to note, in that regard, that Article 83(7) of that regulation expressly confers on Member States the power to provide whether and to what extent such fines may be imposed on public authorities or bodies. Moreover, the various alternative measures provided for by the GDPR, recalled in the preceding paragraph, make it possible to ensure such effective enforcement.

Consequently, the answer to the first question is that Article 17(1)(d) and Article 18(1)(b) of the GDPR must be interpreted as meaning that failure by the controller to comply with the obligations laid down in Articles 26 and 30 of that regulation, which relate, respectively, to the conclusion of an arrangement determining joint responsibility for processing and to the maintenance of a record of processing activities, does not constitute unlawful processing conferring on the data subject a right to erasure or restriction of processing, where such a failure does not, as such, entail an infringement by the controller of the principle of 'accountability' as set out in Article 5(2) of that regulation, read in conjunction with Article 5(1)(a) and the first subparagraph of Article 6(1) thereof.

The second question

In the light of the answer given to the first question, there is no need to answer the second question.

The third question

By its third question, the referring court asks, in essence, whether EU law must be interpreted as meaning that, where the controller of personal data has failed to comply with its obligations under Articles 26 or 30 of the GDPR, the lawfulness of the taking into account of such data by a national court is subject to the consent of the data subject.

In that regard, it should be noted that it is clear from the actual wording of the first subparagraph of paragraph 1 of Article 6 of that regulation that the data subject's consent, referred to in point (a) of that subparagraph, is only one of the grounds for lawfulness of processing, such consent not however being required by the other grounds for lawfulness set out in points (b) to (f) of that subparagraph, which grounds are based, in essence, on the need for processing for the attainment of specified purposes (see, by analogy, judgment of 11 December 2019, *Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraph 41).

Where a court or tribunal exercises the judicial powers conferred on it by national law, the processing of personal data which that court or tribunal is called upon to carry out must be regarded as necessary for the purpose set out in point (e) of the first subparagraph of Article 6(1) of that regulation, relating to the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Since, first, it is sufficient that one of the conditions laid down in Article 6(1) of the GDPR is satisfied in order for the processing of personal data to be regarded as lawful and, second, as was concluded in paragraph 61 of the present judgment, infringement of Articles 26 and 30 of that regulation does not constitute unlawful processing, the taking into account, by the referring court, of personal data which have been processed by the Federal Office in breach of the obligations laid down in those articles is not subject to the data subject's consent.

Consequently, the answer to the third question is that EU law must be interpreted as meaning that, where the controller of personal data has failed to comply with its obligations under Articles 26 or 30 of the GDPR, the lawfulness of the taking into account of such data by a national court is not subject to the data subject's consent.

Costs

Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Fifth Chamber) hereby rules:

Article 17(1)(d) and Article 18(1)(b) 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)

must be interpreted as meaning that failure by the controller to comply with the obligations laid down in Articles 26 and 30 of that regulation, which relate, respectively, to the conclusion of an arrangement determining joint responsibility for processing and to the maintenance of a record of processing activities, does not constitute unlawful processing conferring on the data subject a right to erasure or restriction of processing, where such a failure does not, as such, entail an infringement by the controller of the principle of 'accountability' as set out in Article 5(2) of that regulation, read in conjunction with Article 5(1)(a) and the first subparagraph of Article 6(1) thereof.

EU law must be interpreted as meaning that, where the controller of personal data has failed to comply with its obligations under Articles 26 or 30 of Regulation 2016/679, the lawfulness of the taking into account of such data by a national court is not subject to the data subject's consent.

[Signatures]

* Language of the case: German.